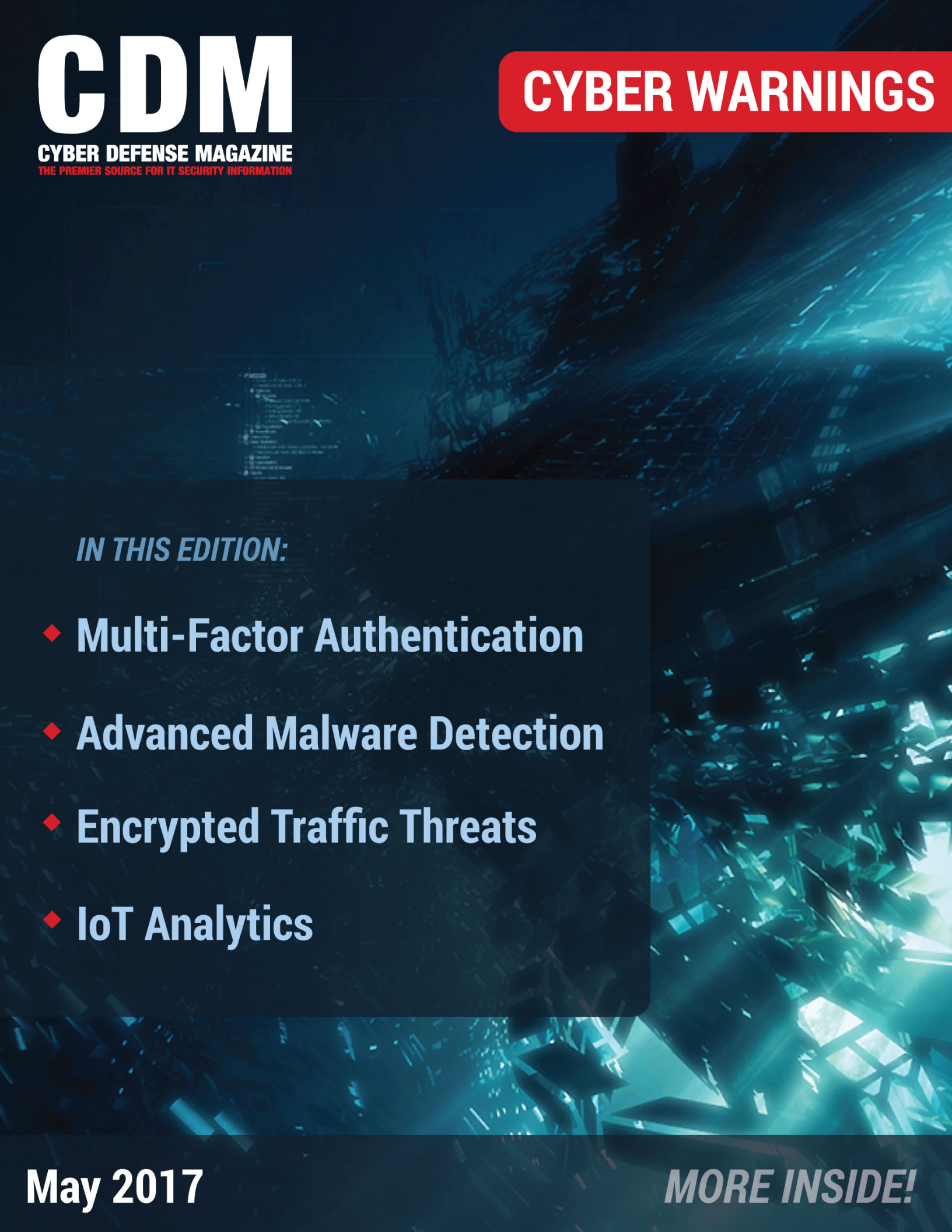


CDM

CYBER DEFENSE MAGAZINE

THE PREMIER SOURCE FOR IT SECURITY INFORMATION

CYBER WARNINGS

IN THIS EDITION:

- Multi-Factor Authentication
- Advanced Malware Detection
- Encrypted Traffic Threats
- IoT Analytics

May 2017

MORE INSIDE!

CONTENTS

CYBER WARNINGS

Published monthly by Cyber Defense Magazine and distributed electronically via opt-in Email, HTML, PDF and Online Flipbook formats.

PRESIDENT

Stevin Miliefsky
stevinv@cyberdefensemagazine.com

EDITOR

Pierluigi Paganini, CEH
Pierluigi.paganini@cyberdefensemagazine.com

ADVERTISING

Jessica Quinn
jessicaq@cyberdefensemagazine.com

KEY WRITERS AND CONTRIBUTORS

Charles Parker, II
George Brostoff
John Cloonan
Lisa Barrie
Tim Bedard
Asher de Metz
Marcelo Delima
Milica D. Djekic
Jonathan Stock
Daniel Jetton
Alex Blau
Simon Parker
Ryan Orsi
Nate Lesser
François Amigoren
Jason Matlock
Summer ParkerPerry
Leo Taddeo
Bob Heckman
Anna Jones
Andrew L. Rossow, Esq.
Jeff Steuart
Anas Baig

Interested in writing for us:
writers@cyberdefensemagazine.com

CONTACT US:
Cyber Defense Magazine
Toll Free: +1-800-518-5248
Fax: +1-702-703-5505
SKYPE: cyber.defense
Magazine: http://www.cyberdefensemagazine.com

Executive Producer:
Gary S. Miliefsky, CISSP®

From the Editor's Desk

Dear Readers,

Here at Cyber Defense Magazine, we are all about continuing to focus on best practices and solutions for you. Cyber Warnings monthly e-magazine covers hot INFOSEC topics with some of the best advice from industry experts.

In 2017, we should focus on best practices at logging, encryption of data at rest and in transit, and system hardening through vulnerability remediation.

Our future depends upon the cyber security skills of teens and college students entering our field.

Let's continue to share a wealth of information with each other to stay one step ahead of the next cyber threat.

To our faithful readers, Enjoy

Pierluigi Paganini

Pierluigi Paganini, Editor-in-Chief, Pierluigi.Paganini@cyberdefensemagazine.com

Veiled Vulnerability

AD

by Charles Parker, II

In this day, there are vulnerabilities throughout the environment. These are blatant with malicious websites and more camouflaged as with phishing and ransomware. With another unique view, these vulnerabilities may be external. There are attackers across the globe all with one singular mission to attack you and compromise your system. These persons are actively completing their reconnaissance and gauging the potential data to steal or analyzing the possibility of a success ransomware attack.

The data having value may be the client list, employee listing, banking information, healthcare records, and many other sources of data. The internal version of this is from the business employees. The employees may click inadvertently or negligently on malicious websites or links. This may create the opportunity for ransomware or scareware to infect the system. From this door being opened by the unsuspecting employee, the attackers could abscond with trade secrets, CAD schematics, or new technology.

To alleviate these issues to some extent, there are ample well-utilized remediation techniques, including scanning for vulnerabilities and malware, log management, third parties conducting pentests and vulnerability assessments, SIEM apps, log acquisition and analysis tools (e.g. Splunk), and many other options.

There is however one area that is also pertinent, however has not garnered the attention the other aspects and defensive measures have. This act of simply working with this is another tool to secure the enterprise.

Active Directory (AD)

AD is in use in one form or another is most medium- and larger-sized businesses. This application is exceptionally useful and functional.

This may be used with employees, in combination of employees and hardware, for tracing and a number of other uses. If this is not fully used, the administrators are not actively using all of the capabilities.

With AD, the normal usage includes setting up the new employee or making adjustments to the employee's record as needed. Each person's role in the organization is different. This directly impacts the person's responsibilities, as part of their job. As each person has a unique role in their group, the same set of rules should not be applied to everyone.

Granted applying a boilerplate set of rules to everyone, or all employees except the C-level, is quicker and easier, however this would be mostly ill-advised.

As much as reasonably possible, these rules should be narrowed per group in this instance. When this general rule is not applied, the administrator is allowing for the staff member to complete unauthorized tasks, escalation or privileges and a greater level of risk, by their own actions. There is not a need to make this more difficult than it already is.

People occasionally leave their position, either voluntarily or are provided the opportunity to seek other employment immediately. There are a number of high profile actions that tend to be effected directly thereafter, especially when the person is leaving of the business' choice. This may include securing the ID card, access card, the corporate credit card, corporate issued phone, and corporate email.

These may contain sensitive and confidential information that needs to be maintained as such. In a much more mundane scenario, the person may also just change their position. In this alternative use case, the employee may not need the same access. Adjusting these assists to the appropriate level assists with limiting data loss.

Often, regardless of the person's underlying rationale for the position change, the person's AD may not be thought of as a point to check and modify. There may not be a checklist or other template to remind the management and support staff to review all affected areas.

Leaving the prior employee's set of access per AD also has other issues. The prior employee may have rights to services they should not have. The future staff members may review the AD file entry and believe through no fault of their own, this person is still an active employee. The business may also be examined or audited.

This provides an issue when the current employee list from Human Resources is compared to the AD list, which shows the person's last login was two years in the past, when they were actually an employee. The auditor may view this being indicative of a systemic issue, requiring further reviews.

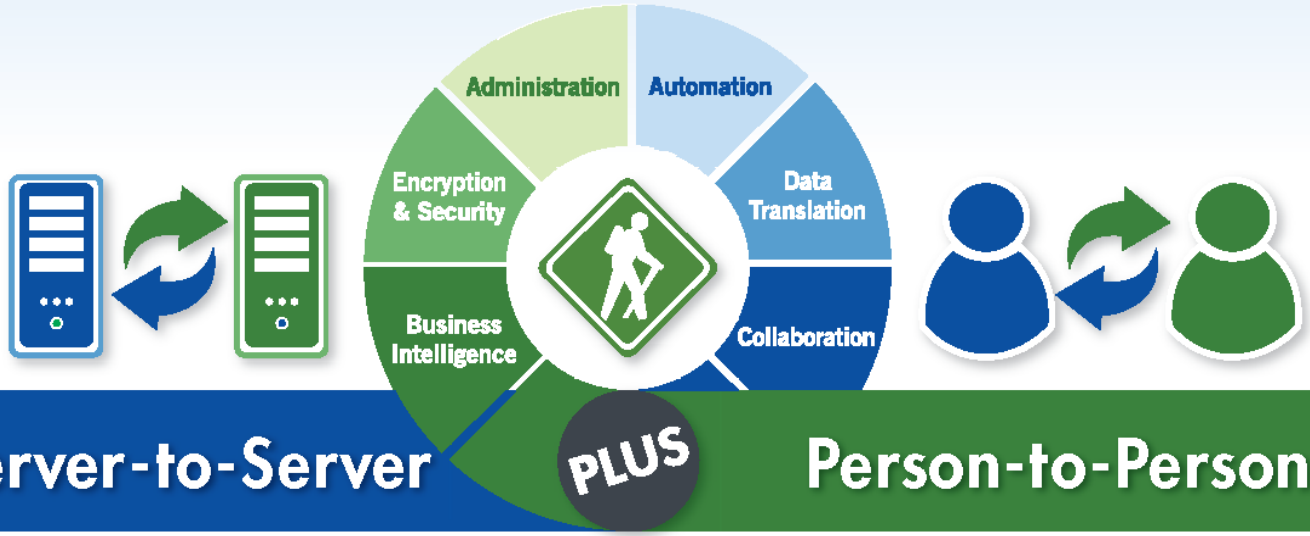
The IT world is amply busy and complex on its own rights without adding more issues requiring time and resources to remediate. Not adjusting AD as employee changes are effected is not a great choice to make. This is a quick area to be mitigated and also can save a significant amount of time when implemented as needed.

About The Author

Charles Parker, II began coding in the 1980's. Presently CP is an Information Security Architect at a Tier One supplier to the automobile industry. CP is presently completing the PhD (Information Assurance and Security) in the dissertation stage at Capella University. CP also is an adjunct faculty at Thomas Edison State University. CP's interests include cryptography, SCADA, and NFC.

He has presented at regional InfoSec conferences. Charles Parker, II may be reached at charlesparkerii@protonmail.com and InfoSecPirate (Twitter).

Secure File Transfer



Simplify File Transfers with GoAnywhere MFT™

GoAnywhere Managed File Transfer automates and secures file transfers with your customers, vendors and enterprise servers.

Through a browser interface, GoAnywhere MFT allows your organization to connect to almost any system (internal or external) and securely exchange data using a wide variety of standard protocols.

GoAnywhere MFT can parse XML, CSV and XLS files to/from databases, and includes the ability to encrypt file transfers using Open PGP, SFTP, FTPS, AS2, HTTPS and AES.

Visit GoAnywhere.com for a FREE trial.

"GoAnywhere MFT monitors queues and automates encrypted file transfers (SFTP, FTPS, HTTPS).

We currently have 45,000 scheduled and 'triggered' transfers running daily."

One of the Largest North American Railroads

GO ANYWHERE™ → a managed file transfer solution by LINOMA SOFTWARE

GoAnywhere.com 800.949.4696

"Best Overall Value" and "Leader" awards -- Info-Tech Research Group, Managed File Transfer Vendor Landscape Review 2015

Multi-Factor Authentication and Mobile Devices

Smart Security Makes Life Easier for Users...and Harder for Hackers

by George Brostoff, CEO, SensibleVision

Security is as much about deterrence as prevention. From the highest-clearance government servers to the halls of the Louvre, no security system is impenetrable to a sufficiently clever (and motivated) criminal.

The key to proper security is not to make a system uncrackable, but to make it so time-consuming and inconvenient to crack that the perpetrator will simply reassess and look elsewhere.

After all, a burglar alarm won't actually stop a criminal from invading your home, but knowing that one is installed (or even a decoy sticker on the front door) may cause a robber to skip your house in favor of one without the risk of the police getting a call.

And if you also have a guard dog or security camera, each additional layer or protection makes the invasion that much more of a hassle and gives robbers yet another reason to look elsewhere.

In the world of cybersecurity, this approach is called **multi-factor authentication**, and it relies on one of the basic principles of a good defense: making systems more challenging and thus less desirable to attack.

Why We Need to Change

Passwords and physical and virtual tokens provide multi-factor security, but traditional multi-factor security can be frustrating for authentication on mobile devices. Several issues are forcing security experts to seek new ways to protect users:

1. **Mobile is in**: Most people work on their personal devices at home and on the road more than at a desktop in an (often secure) office. This makes more secure authentication more critical than ever..

2. **Users prefer simplicity**: The more security steps users have to take, the more onerous they will find the process and the more likely they are to skip one or more steps - or opt out of the process entirely. And unlike desktops, users access mobile devices far more frequently each day, virtually mandating a simple secure solution.

3. **Traditional authentication solutions are geared for desktops and laptops:** Asking user to carry another token for their mobile device is just not practical. And as noted above, a phone can be its own second factor.

Out from Behind the Firewall and into the World

Remember when workplace cybersecurity was as easy as keeping everyone behind the same firewall and enforcing strict access control methods and policies? Of course breaches happened, but at least IT departments could maintain their control of most data.

Today, we live and work in an age of BYOD (bring your own device) where even employees who spend most of their workday at the office still perform plenty of tasks on their personal mobile devices.

On one hand, this makes employees more flexible and available to work from anywhere (a good thing). On the other hand, instead of having to break through a firewall, all a hacker needs to do is hack a PIN, password, or perhaps even a fingerprint on a single device. That old cliche about a chain being only as strong as its weakest link starts to feel painfully true when a company loses millions because one employee shared a password.

Better Unsafe than Inconvenienced?

If you're a security professional you might be thinking, "Who doesn't even put a password on his phone?" The truth is, many people would rather risk a security breach than perform even one security step, let alone several, because they are so intrusive.

While most of us are happy to type in a single password to access a device or service, each additional step raises users' frustration until they simply opt out, either by leaving the system entirely or ignoring basic security protocols.

For example, many companies require that all files be kept on a central server, but Google Docs is so easy to use that many documents are stored there even if that's prohibited by company policy. It's the classic tradeoff between ease of use and data protection.

In a customer-service setting, this might mean that a potential customer becomes discouraged and takes his or her business elsewhere. In a workplace, it may mean that an employee foregoes simple security steps in the name of easy access, such as when workers don't log out of their computers whenever they walk away from their computers or skip security procedures like authenticator codes or password recovery questions.

Facial Recognition Takes the Pressure Off

Some security solutions like firewalls are great because they require no effort from end users. But with mobile taking people outside the protection of a firewall, businesses require a new solution for security factors that don't require onerous extra steps.

So what's the solution to this seemingly intractable problem? To find the answer, we need look no further than the most common criticism of modern tech users: "Your face is always stuck in a phone!" Whether for work or play, we use our devices by looking right at them, and that means

that passive facial recognition can become an invisible, painless step in simultaneous multi-factor authentication.

The user simply takes a selfie using a security app, and then whenever they turn to look at their device, the app performs a scan to make sure the right person is in control. The user just does exactly they would have done anyway, plus one additional security step like a password, PIN, or fingerprint, and you've enacted multi-factor authentication without requiring multiple active steps to frustrate the device owner.

Of course this means the facial recognition software has to be smart enough to see through a photograph, but such innovations are already available on the market.

It's Not About Outrunning the Bear

You've probably heard the old joke about two friends being chased by a bear: "I don't have to outrun the bear. I just have to outrun you!" A similar principle applies in cybersecurity. If a hacker has his choice of which system to try and breach, he's likely to pick the easiest target.

Simultaneous multi-factor authentication is powerful deterrent because it means the hacker will have to do more work to get in and out unscathed, and a hacker who sees such a system in place may well decide to seek out softer prey.

And if the barrier to enacting multi-factor authentication is that each successive factor requiring active participation from the user is more likely to be ignored, at least one factor should require no participation from the user at all beyond doing what they were already going to do: looking at their device.

The key to strong security is not an impenetrable system, because impenetrable systems don't exist. Strong security should be easy on you and hard on the hackers. With smart facial recognition technology, at least one easy step for customers and employees becomes a serious hurdle for criminals.

About the Author

George Brostoff is the founder and CEO of SensibleVision, a technology firm specializing in Simultaneous Multi-Factor Authentication headquartered in Cape Coral, Florida. He has founded three successful tech companies, holds seven patents, and grew up working in a family business. George can be reached at george@sensiblevision.com, on Twitter at @SensibleVision, and at SensibleVision.com.

Advanced Malware Detection – Signatures vs. Behavior Analysis

By John Cloonan, Director of Products, Lastline, Inc.

Malware has threatened our computers, networks, and infrastructures since the eighties. It is constantly evolving, and deploying products that effectively detect it is crucial to preventing costly data breaches. There are two major technologies to accomplish this, but surprisingly, most organizations rely almost exclusively on just one approach, the decades old *signature-based* methodology. The more advanced method of detecting malware via *behavior analysis* is gaining rapid traction, but is still unfamiliar to many.

Signature-based malware detection is a proven method for identifying "known" malware. Unfortunately, new versions of malicious code appear daily that are not recognized by signature-based technologies. These newly released forms of malware can only be distinguished from benign files and activity by analyzing its behavior.

Signature-Based Technologies Track Known Threats

In computing, all objects (including operating system components, executable programs, documents, images and others) have attributes that can be used to create a unique digital fingerprint or *signature.* Algorithms can quickly and efficiently scan an object to determine its digital signature.

When an anti-malware solution provider identifies an object as malicious, its signature is added to a database of known malware. These repositories may contain hundreds of millions of signatures that identify malicious objects. This method has been the primary technique used by most malware detection products and remains the fundamental approach used by the latest firewalls, email and network gateways, and other intrusion detection systems.

Signature-based malware detection technology has a number of strengths, including:

- Signature-based malware detection is well known and well understood. The very first anti-virus programs used this approach.
- It's fast. Signature-based technologies can rapidly identify *known* malware.
- Signature-based malware detection is relatively simple and will run in minimal endpoint environments.
- It's readily available within a number of leading network security tools such as next-generation firewalls, email gateways, and IPS.
- It provides good protection from the many millions of older, but still active threats.

But there are over a million new versions of malware released daily[i]. Many of these have very specific targets—often just one. As a result, on top of the much greater number of overall

threats, fewer organizations are successfully discovering and then reporting these highly targeted attacks, making information about new attacks less available for informing signature-bases solutions.

Don't Wait for Signatures

Verifying that a new file is malicious, and adding its signature to a database of known malware usually takes several days and is complicated. And often the malware has already evolved by then. The Cisco 2017 Annual Cybersecurity Report found that up to 95% of malware files they analyzed were less than 24 hours old, indicating a very fast "time to evolve." The delay in identifying new forms of malware makes corporations vulnerable to serious damages.

Modern malware will often strike immediately, inflicting incredible damage in a short period of time. Jigsaw, a particular nasty form of ransomware, starts deleting files within 24 hours. HDDCryptor, another ransomware monster infected 2000 systems at the San Francisco Municipal Transport Agency before it was detected. Being vulnerable to infection while waiting for a signature is very risky.

Another major problem with signature-based malware detection is that today's advanced malware can alter its signature to avoid detection. Signatures are created by examining the internal components of an object. Malware authors simply modify these components while preserving the object's functionality and behavior. There are multiple transformation techniques, including code permutation, register renaming, expanding and shrinking code, and the insertion of garbage code or other constructs.

Another example that has seen a significant increase over the past few years is *Metamorphic* malware, which automatically changes itself with each new instance or infection.

Behavior-based Malware Detection

Behavior-based malware detection evaluates an object by its intended actions before it can actually execute that behavior. This is typically accomplished by activating it within an isolated environment such as a sandbox.

An object's behavior, or in some cases its *potential* behavior, is analyzed for suspicious activities. Any attempt to perform actions that are clearly abnormal or unauthorized would indicate the object is malicious, or at least suspicious.

There's a multitude of behaviors that point to potential danger. Here are some examples:

- Any attempt to discover a sandbox environment
- Disabling anti-virus or other security controls
- Modifying the boot record or other initialization files to alter boot-up

- Installing rootkits
- Registering for autostart
- Shutting down or disabling system services
- Downloading and installing unknown software
- Deleting, altering, or adding system files
- Modifying other executable programs
- Connecting with known malicious sites
- Encrypting files that are unrelated to the program
- Adding or modifying user accounts
- Dynamic code building to enhance evasion capabilities
- Executing a dropped file
- Spawning Powershells
- Performing any actions that are highly abnormal

Evaluating an object for malicious behavior as it executes is known as *dynamic analysis.* Threat potential, or malicious intent can also be assessed by *static analysis,* which looks for dangerous capabilities within the object's code and structure.

Static analysis is extremely efficient and is often performed prior to dynamic analysis. It's also useful for detecting malicious activities within code that may not execute during dynamic analysis. Dynamic analysis monitors actual behavior, and detects malicious actions that are missed by static analysis. Both approaches have their advantages and are important for behavior-based malware detection.

While no solution is one hundred percent foolproof, behavior-based detection is the leading technology today to uncover new and unknown threats in near real-time. Some examples of where behavior-based technology succeeds when signature-based systems fail are:

- Protecting against new and unimagined types of malware attacks
- Detecting an individual or one-time instance of malware targeted at one organization or one person
- Identifying what the malware will do in a specific environment when files are opened
- Obtaining comprehensive information about the malware, helping analysts classify the object and respond appropriately to potential threats

There are however, a few important limitations to be aware of.

- If malware determines it's running in a sandbox, it will attempt to avoid detection by curtailing malicious activities. It's critical that a sandbox remains undetectable—and most fail to do this.
- It takes time to analyze the behavior of an object. While static analysis can be performed in real-time, dynamic analysis may introduce latency while the object is exercised. The ability to detect internal stalling is an important feature to maintain high throughput.
- Some behavior-based malware detection requires more hardware resources than signature-based detection.

- Many behavior-based solutions are exclusively cloud-based. Transmitting sensitive files to an outside service may be an issue for some organizations.

Not All Behavior-based Technology Is Created Equal

Conventional sandbox technologies have limited visibility and can only evaluate the interaction between an object and the operating system. By observing 100 percent of the actions that a malicious object might take, even when it delegates those actions to the operating system or other programs, CSOs can evaluate not only the malware's *communication* with the operating system, but *each instruction* processed by the CPU.

How Behavior-based Solutions Work

Advanced malware detection solutions observe and evaluates in context every line of code executed by the malware in context. Furthermore, they analyze all requests to access specific files, processes, connections, or services. This includes each instruction executed at the operating system level or other programs that have been invoked, including low-level code hidden by rootkits.

The technology identifies all malicious, or at least suspicious activity, which, when taken together, makes it very clear that a file is malicious before it is released onto the network to actually execute any potentially damaging behavior.

Both signature and behavior based malware detection are important and have distinct advantages. The best security will come from utilizing both technologies simultaneously. Too many security officers are misled by vendors promoting "next-generation" firewalls and other "state-of-the-art" security tools.

They don't realize that these "latest" products are relying exclusively on the decades old signature-based approach to malware detection that will miss evasive malware and zero-day attacks. No organization with sensitive data or critical operations to protect should be without behavior-based malware detection to augment the capabilities of existing security tools.

About the Author

John Cloonan is Director of Products for Lastline with a passion for creating innovative information security solutions. Of his nearly 25 years of professional experience, he has spent more than 15 years in Information Security software development and service delivery. John Cloonan is Director of Products for Lastline with a passion for creating innovative information security solutions. Of his nearly 25 years of professional experience, he has spent more than 15 years in Information Security software development and service delivery.

C-SUITE & SR. LEVEL EXECUTIVES ONLY

2017 | CYBERSUMMITUSA.COM

CYBER SECURITY SUMMIT 2017






The **Cyber Security Summit** connects C-Suite & Senior Executives responsible for protecting their companies' critical infrastructures with **innovative solution providers** and **renowned information security experts.**

CyberSummitUSA.com >

REGISTER AT **CYBERSUMMITUSA.COM** | **50% OFF ADMISSION** WITH PROMO CODE: **CDM2017** | STANDARD TICKET PRICE $350

The Cyber Security Summit Expands into Key Markets in 2017

Seattle, WA
Thursday, June 1, 2017
The Westin Seattle

DC Metro
Thursday, June 29, 2017
Ritz-Carlton Tysons Corner

Chicago, IL
August 8

New York, NY
September 15

Boston, MA
November 1

Los Angeles, CA
November 29

Engage in Interactive Discussions & Roundtables Including:

- The Compliance Nightmare: Using Your Solution Provider as a GPS For Navigating The Perilous Road To Compliance -
- Hacking Back & Its Legal Repercussions. What's Your Strategic Incident Response Plan? -
- Emerging Risks Likely To Become Major Threats Facing IoT and Big Data? -
- Protecting Your Enterprise from Corporate Espionage: Keeping Insider Threats Outside -

The Growing List of 2017 Solution Providers Includes: (Partial List)

910Telecom, ALERTLOGIC, APCON, ARBOR NETWORKS, AVANAN, BAE SYSTEMS INSPIRED WORK, BeyondTrust, BLACKDUCK, BLUE COAT, CENSORNET, Centrify, CenturyLink, cipher, CISCO, CLOUDFLARE, ConsoleWorks, CYBERARK, CYBRICS, DARKTRACE, EC-Council, ENSILO TARGETED DEFENSE, GSA FEDSIM, IBM Security, iboss CYBERSECURITY, Infoblox, IOvations, ivanti, LogRhythm, MILITUS, nccgroup, OPSWAT, plixer, proofpoint, protegrity, rackspace, red canary, REDSEAL, root9B, SailPoint, SECURONIX, SentinelOne, Symantec, SYNOPSYS, TERRANOVA, THALES, veeam, VENAFI, VIRTUALFORGE

To Exhibit Contact Bradford Rand at 212.655.4505 ext 223 or BRand@CyberSummitUSA.com

Best Practices to keep your Home WiFi Secured

by Lisa Barrie, Sub-editor at List Enthusiast

Wi-Fi internet or traditional wired internet?

Ask any person and he/she'll go for the former. The ease-of-use, easier installation, and maintenance means Wi-Fi network has fewer problems than a wired network.

But if there's one area where wired networks are way ahead, it's security. Wi-Fi networks are far easier to break-in than wired networks. Because of their wireless nature, any person in your signal range can attempt to connect to your Wi-Fi network.

An intruder can create many problems for you. Apart from increasing your internet bills, an unknown person can try to access your personal information. That's why it's important to secure your Wi-Fi network. Here are some of the **best practices regarding Wi-Fi security**.

Change your Router's Admin Username

Although changing your default router's admin username won't make it stronger, not changing it may land you in trouble. If you don't change it, a person can try to access your router's admin panel.

Activate Encryption and Create a strong Password

A weak or predictive password will only make it easier for others to connect to your network. This is the reason you need a hard-to-guess and long password. But according to this report, "123456" is still one the most commonly used passwords in our world. You need a much better password than this.

For this purpose, you can use many online password generators to make sure your password is full of capital and small case letters, and special characters.

A password alone is not sufficient. You must set an encryption standard for your network. It's because all Wi-Fi encryption standards are not equal. First, there was WEP (Wired Equivalent Privacy), it's used on older routers, but very easy to crack and no one uses it nowadays.

WPA2-AES is widely used and most recommended encryption method nowadays but it's not available on older routers. That's why you may need to upgrade your router.

Turn off Guest Networks:

Guest networks are a convenient and easier way to give Wi-Fi access to you guests. What makes these guest networks vulnerable is that most people set a very easy password for these networks or worse, no password at all.

Many times, Wi-Fi signals range is more than your house' boundaries and this way your neighbours and even strangers can connect to your guest network.

Although you can disable important tasks such as file sharing on guest networks, those unwanted users can still make you pay more for your internet bills by consuming more internet bandwidth.

Turn off WPS

WPS, also known as Wi-Fi Protected Setup, is a feature using which a device can connect to your router without any password authentication, even if you have encryption turned on.

All you need to do is pressing a WPS button on your router and connect your device with that router. That's it.

There are many disadvantages of WPS, however, that easily outweighs its utility.

- If your router is placed in an unsecured area, anyone can press that WPS button and connect to your router.
- WPS-feature only has 8-digit PIN and a hacker can easily run different techniques (like Brute force attack) to unlock it.
- WPS pins cannot be changed.

Considering these above points, it's better to turn WPS off.

Reduce your router bandwidth

Sometimes we have a small house and a very long range router like Asus AC88U. In this scenario, Wi-Fi signals can be broadcasted far more than your house' boundaries.

One simple solution to deal with this problem is to turn on "Power-saving mode" on your router.

Have latest router firmware

A firmware works as the OS of a router and can have a security vulnerability unintentionally unfixed, just like any other software. These vulnerabilities are often dealt-with in newer updates

of that firmware. That's why it's good to check if you have an updated firmware version available.

Activate firewall

A firewall is a defence mechanism, in both software and hardware form, that keeps your internal network secured from malicious data coming from the internet or any other source. In simple terms, a firewall has one objective: Inspect network traffic and keep network safe from any potential threat.

What many people don't know is that their router has an internal firewall. Since all the internet data transfer between your devices and the web goes through your router, this firewall can make your whole network safe. If you don't know how to activate your router's internal firewall, go and read this article on how to do it.

Activate VPN

VPN, also called Virtual Private Network, acts as a medium between your home network and the web. After turning on a VPN, all the data transaction between your device and the web will be done via a VPN server.

A VPN gives you many advantages like staying anonymous over a public Wi-Fi or accessing a website/app with geographical restrictions.

Some other not-so-important Methods:

There are some other things you can do like Mac filtering, Disable DHCP or Hiding your SSID. But many experts criticize them that they are not going to give you as much security relief as you hope. That's why I haven't discussed them here. But you can try them out if you want.

About the Author

Lisa is a Tech Blogger who specializes in writing networking related blog posts at List Enthusiast

Venafi Survey: Many Organizations Overlook Threats Hiding in Encrypted Traffic

By Tim Bedard, director of threat intelligence and analytics for Venafi

Encryption plays a critical role in the safety and security of our digital economy. Whether it's protecting data from malicious actors or government intrusion, encryption provides organizations with strength, integrity and privacy.

Encryption usage is on the upswing, especially with unpredictable geopolitical situations driving data protection concerns. For example, almost three-fourths (72%) of security professionals say they are more concerned about data privacy. As a result, two-thirds of security professionals (66%) say their organizations are considering increasing their use of encryption.

But as we adopt these solutions, cyber criminals are finding ways to hide attacks inside the very encrypted traffic that is designed to protect your privacy. These tactics will only become worse as the drive for encryption continues to explode. After all, a recent study from A10 Networks found that 41% of cyber attacks used encryption to evade detection.

But, are organizations successfully responding to these growing cyber risks? During RSA Conference 2017, one of the largest information security events in the world, Venafi conducted a survey to see if security professionals are properly defending themselves against threats hiding in encrypted communications.

More than 1540 attendees participated in the survey, and unfortunately, the responses revealed major gaps in their protection.

Interesting highlights from the survey included the following:

- Nearly a quarter of the respondents (23%) had no idea how much of their encrypted traffic was decrypted and inspected.

- 41% of respondents thought they could detect and respond to a cyber attack hidden in encrypted traffic within one week. Additionally, 20% believed they could detect and respond to a cyber attack within 24 hours.

- A surprising number of respondents (41%) said they encrypted at least 70% of their *internal* network traffic. Additionally, 57% said they encrypted 70% or more of their *external* web traffic.

Ultimately, it's pretty alarming that nearly one out of four security professionals is unaware if their organization is actively looking for threats hiding in encrypted traffic.

Encryption offers a useful cover for cyber criminals. But, it's startling clear that most IT and security professionals don't realize how these blind spots can impact the security technologies they depend on. Organizations need proper visibility into their encryption program. Without this understanding, many of their security solutions are useless against the increasing number of attacks hiding in encrypted traffic.

In addition, it's clear that many security professionals are overconfident in their ability to quickly remediate a cyber attack hidden in their encrypted traffic, despite only inspecting and decrypting a small percentage of their internal traffic. According to the 2017 Mandiant M-Trends report, the average time it takes to detect a cyber attack is 99 days.

Unfortunately, the problem is that attackers lurking in encrypted traffic make quick responses even more difficult. This is especially true for organizations without mature inbound, cross-network, and outbound inspection programs. This bullishness makes it very clear that most security professionals don't have the right strategies necessary to protect against malicious encrypted traffic.

Security professionals must understand that encryption, like all security solutions, is not a silver bullet. Additional tools and protocols are needed to effectively utilize encryption and protect their organization's traffic, including solutions that offer consistent identification, remediation and protection. Security professionals must inspect and decrypt their traffic on a regular basis in order to catch malicious actors before they take advantage of encrypted systems.

Sadly, most security programs were developed before encrypted TLS/SSL contributed the majority of an organizations network traffic. However, integrating security with machine identity protection is a huge leap forward in the effective inspection of encrypted traffic. Combined with automation, organizations can streamline the entire process of encryption monitoring.

Encryption is a fundamental security tool, but it can carry unique risks. With proper machine identity protection, you can utilize encryption without exposing your organization sensitive corporate data and IP from malicious actors.

About the Author

Tim Bedard is responsible for digital trust analytics at Venafi. With more than twenty years of IT security and strategy experience, Tim successfully launched SailPoint Technologies cloud-based identity and access management offering with responsibilities for strategic planning to execution of all services. Previously, he has held leadership positions in product strategy, management and marketing at RSA Security and CA Technologies. Tim is active security evangelist at industry leading tradeshows and events.

(ISC)²

SECURITY CONGRESS | APAC 2017

03 - 04 July • Hong Kong

LEADERS OF TOMORROW

At (ISC)² Security Congress APAC 2017, you'll get to join thought leaders, (ISC)² Asia-Pacific Advisory Council members, (ISC)² Chapter leaders and over 350 InfoSec professionals for 2 days of knowledge sharing, strategic insights and networking with your peers.

50+ Speakers | **2** Days | **6** Tracks | **35+** Sessions

Why Attend?

Invest in yourself in 2017

Learn the latest strategies and techniques to address cyber security threats

Meet regional experts & influencers face-to-face

Enjoy a customized learning journey

Earn up to 16 CPEs

Register Today & Save!

10% Discount Code: US$ 324 (M17CDM)

Regular Price: US$ 360

5% additional discount for group purchase.

For Inquiries: (852) 2850 6953
securitycongressapac@isc2.org

Tracks Include:

- Cloud Security
- Critical National Information Infrastructure (CNII)
- Emerging Technologies & Security
- Governance, Regulation & Compliance
- Professional Development
- Security Operations

Visit **apaccongress.isc2.org**

#ISC2congressAPAC

In Partnership with: image engine

Supported by: GovCERT.HK 政府電腦保安事故協調中心 | CSA cloud security alliance

Platinum Sponsor: 阿里安全 ALIBABA SECURITY

Gold Sponsors: Hewlett Packard Enterprise | People 众人科技 | tenable

Silver Sponsors: SKYBOX SECURITY | SOLARED CYBER SECURITY | SYNOPSYS

10 cyber security measures growing companies should implement

Tips to keep your business safe as it expands

By Asher de Metz, Lead Senior Consultant (Information Security), Sungard Availability Services (Sungard AS)

This may surprise you, but growing companies are the perfect target for cyber attackers. That's because they're just becoming large enough to have data and financial resources worth going after, while often not yet having the infrastructure in place to implement sufficient security measures. This makes them an easy target compared to large multinationals, who usually have the budget and resources to protect themselves effectively.

If that's where your company is at now, this is probably the last thing you want to read. You're just starting to make enough to pay the bills, so you hardly want to be splashing any extra cash on cyber secuity. If you're wondering what can you do about this that won't take up too much time or cost more than you can afford, you'll be glad to know that we've rounded up some simple advice to help you make your company safer online.

Here are our top ten tips:

1: Make sure software is always up to date

The updates that software providers offer include improvements to security in response to the latest identified risks. You should keep all of the software you're using up to date – as well as anti-malware, this includes operating systems, applications, browser plug-ins, and firmware. Don't delay before implementing these updates – the longer you wait, the more chance you have of placing your systems at risk. Just double check that all your software is set to update automatically, which will save you the headache of constantly checking.

2: Keep your passwords secure

Sometimes the biggest security risks are the most obvious things. Using passwords that are easy to guess is a classic error that can land you in serious trouble. Avoid using the same passwords for multiple online locations, and then use a password manager to keep track of all your passwords for you.

3: Implement security measures for mobile devices

Many organizations fail to consider the potential for security breaches on the smartphones and tablets their employees use at work. Simple measures you can take include locking devices to prevent opportunistic thieves from gaining access to sensitive data, and encrypting the data so

that more advanced hackers are unable to get hold of information that may compromise your security. You should also make use of the built-in tracking software, which enables you to remotely lock or wipe devices that go missing – this software comes as standard with iOS and Android.

4: Take care when installing new software

When downloading and installing new software or plug-ins for your browser, it's always advisable to proceed with caution. Free software and applications from a provider whose name isn't recognized and trusted can often contain spyware or even install harmful programs on your computer. You can ask your system administrator to apply settings that only allow staff to install approved programs.

5: Don't get caught out by phishing

With so much awareness about phishing, it's surprising how many people still fall for it. Make sure your staff are vigilant about any emails asking them to click on links or open attachments, even if they seem to be from legitimate sources. Phishing scams are becoming increasingly elaborate, and sometimes it can be hard to tell the difference between a genuine email from a bank or other organization and a fake one. Once you click on a link or download a file from such an email, you could end up with unwanted software or scripts running on your computer.

6: Watch out for ransomware

Hackers are constantly finding new and clever ways to take advantage of businesses that fail to keep themselves secure, and ransomware is a method that is becoming increasingly common. Ransomware uses a virus to encrypt and hold your important files hostage, so to speak, refusing to release them back to you until you pay up.

You can protect yourself against this by using the 3-2-1 rule: store three copies of all important files in two separate devices, one of which is in a different physical location and not connected to other back-ups. Using cloud storage is a simple and increasingly secure way to do this.

7: Maintain privacy when out in the open

As well as in the office, you need to keep your data safe when your staff are working remotely. To offer them a secure, encrypted connection to your network with access to files, applications, printers, and other resources, you can set up a virtual private network (VPN).

This will also protect your staff from hackers when they're using public Wi-Fi hotspots, which can be particularly vulnerable to attack.

8: Don't over-use your privileges

Administrative privileges give you permission to change configuration settings and install software on your systems. If you have these privileges, you should only use them when you actually need them, rather than logging in to an account that has your privileges activated whenever you use your computer for every-day activities. If you're logged in to an account that doesn't have administrative privileges, you'll be notified when a program is trying to install software or change your settings, so you can give permission at this point in time if you're sure that it's safe. Setting up tiered administration throughout your organization allows you to make sure that your staff only have permission to carry out activities relevant to their rank and job description.

9: Share files where possible

Sharing files using secure cloud storage services or file-sharing apps is by far the safest way to send files to your staff. This is because you keep more control over the file than when you sent it by email, and you can track as it gets modified. It also allows you to send a link to a file and limit who can access it and how long it's available. Once you send a file by email, anything can happen to it – it could be forwarded to someone who shouldn't see it, or stored in an insecure location.

10: Use advanced authentication

These days, there are many emerging methods to keep your data safe that go beyond the use of a password – and measures like fingerprint readers and iris scanners are becoming increasingly affordable. If it's simply that important that your sensitive files and information don't fall into the wrong hands, these could be worth investing in, because not only are passwords hackable, they can often be easily guessed or given away by mistake by your staff.

Stay safe

If you want to find out where your main cyber security vulnerabilities lie, you may want to try penetration testing. It can be a scary or unsettling experience to find out how unsafe your systems are, but discovering where you can improve your security, and then implementing the required measures to do so, could save you from a fate much worse. In the meantime, following the tips above, along with a bit of common sense, is a good start.

About the Author

Asher de Metz has approximately 20 years of experience in the cyber security industry consulting to some of the world's largest companies in all of the top vertical markets. Starting in London he has worked across Europe, the Middle East, and has spent the last 8 years in America working for Sungard Availability Services where he runs the Technical Security Practice.

Addressing the government data security problem

By Marcelo Delima, Global Product Marketing Manager at HPE Security – Data Security

Throughout federal, state, and local governments, the digital revolution is driving an exponential growth of high-value data. Personally identifiable information (PII) is collected on government employees, taxpayers, students, retirees, military personnel, and anyone doing business with the government.

This data is a valuable resource that has the potential of transforming the government as we know it. Big data analytics could allow for better allocation of resources and more efficiency; transparency initiatives could allow better citizen services and more accountability, and data sharing could enable better coordination between agencies in key fields such as national security, healthcare or education.

But this same data is also highly prized by cyber-criminals, malicious insiders and nation-states. The challenge is how to protect the data, but in such a way that it can still be safely shared and analyzed by data scientists in its protected form.

Government under attack

Federal and state government agencies disclosed a total of 203 data breaches between 2010 and 2016, with 72 breaches in 2016 alone. In the majority of cases, government breaches involved personal information such as names, Social Security numbers, and birthdates.

The United States Office of Personnel Management (OPM) alone experienced the theft of PII and security clearance background investigation information for 22.1 million individuals in 2015.

The growth in data breaches is a proof that the most common cybersecurity measures—firewalls, intrusion prevention systems, antivirus software, and other security technology operating at the network and endpoint layers—are increasingly ineffective against advanced cyberattacks, leaving gaps where data is exposed.

The data security challenge

Government entities have some of the same challenges faced by private sector corporations, including:

- **Big data and data sharing:** Government agencies are challenged with providing better citizen services and being more transparent, but that requires increased data sharing between agencies and with contractors. It also requires big data analytics and adoption of new technologies to manage the "data lake" such as Hadoop.

- **New technologies and innovations:** As the public sector adopts new technologies and innovations, data security becomes more complex.

  Internet of Things (IoT), mobile and cloud create not only more data for hackers to target, but also increase the surface area for attacks, including more devices, connections, and networks.

- **Legacy systems:** A major challenge faced by government agencies is the dependency on legacy applications and platforms with limited native data security options.

  These sometimes decades-old systems may no longer have vendors that supply patches or otherwise maintain the code, making it vulnerable to hackers.

- **Limitations of traditional security:** Common cybersecurity measures only protect data indirectly. For example, firewalls and intrusion prevention systems operate predominately at the network level.

  Likewise, desktop antivirus software works to stop the spread of malware infections, but none protect data directly.

- **Gaps in data protection:** Most data-protection techniques shield only stored data. While helpful when equipment is lost or stolen, it doesn't protect data when it is in-use.

  Data is exposed to attack when it is decrypted and retrieved from an encrypted database and before it flows through an encrypted link.

- **Compliance:** Stringent data-privacy requirements make greater data protection. Agencies must comply with federal standards and regulations such as the Cybersecurity Act of 2015, DFARS CUI, and the National Institute of Standards and Technology (NIST).

Why data needs a new approach to protection

In an ideal world, sensitive data travels in well-defined paths from data repositories to a well-understood set of applications.

In this scenario, data can be protected by armoring the repository, the links, and the applications using point solutions such as database encryption and SSL network connections.

In real systems, data travels everywhere. Today's IT environment is a constantly shifting set of applications running on an evolving set of platforms.

The data lifecycle is complex and extends beyond the container and application, into offsite backup services, cloud analytic systems, and outsourced contractors.

Data-centric security – a proven approach

Recent advances in data-centric security techniques protect data no matter where it resides, how it is transported, and even how it is used—without increasing complexity and without requiring massive application changes, or impeding mission performance.

An essential part of a layered-defense security strategy, data-centric security includes encryption, tokenization, data masking, and enterprise key management techniques to help effectively protect data from the moment it is ingested, through analysis, to backend storage.

In the private sector, Format Preserving Encryption (FPE) is the main data-centric approach that helps reduce exposure of personal data to cyber thieves or internal threats.

Format preserving encryption (FPE) – Neutralizing data breaches

Format-preserving encryption (FPE) makes it far easier and cost effective for organizations to use encryption. It is critical in protecting sensitive data-at-rest, in-motion and in-use while preserving data format. Traditional encryption methods significantly alter the original format of data.

For example, a 16-digit credit card number encrypted with AES produces a long alphanumeric string. FPE maintains the format of the data being encrypted so that a social security number or birth date still look like a social security number or birth date when encrypted. That usually means no database changes and minimal application changes.

FPE enables government organizations to de-identify sensitive personal data without extensively revamping existing IT infrastructure. With FPE, even if a security system is breached, the data is worthless to attackers because it's encrypted.

However, because the encrypted data looks like the real thing, analysts can still use it to identify patterns, and run queries without decryption. It also allows data to be mobile so it can be moved between systems and shared.

NIST validation brings FPE to government

In 2016, the National Institute of Standards and Technology's (NIST) released the AES FF1 Format-Preserving Encryption (FPE) mode standard that makes encryption easier using an approved and proven data-centric encryption method for government agencies and contractors.

The NIST standard allows the use of FPE to protect sensitive data-at-rest, data-in-motion, and data-in-use while preserving data formats, enabling government agencies to use this breakthrough technology widely used in the private sector.

Format-Preserving Encryption, when properly implemented, enables the protection of all kinds of high value data, from personally identifiable information (PII) to protected health information (PHI) or Classified data types.

It also allows safe data sharing, between agencies or with contractors, and deep big data analytics, leveraging Hadoop and cloud. This technology allows security to be layered into decades old legacy systems and applications, and address specific privacy requirements in legislations.

Bottom line: De-identified data should be the natural state of data

Data can be leveraged to usher in an era of better, more efficient government services and programs at all levels. The challenge is how to protect this data when it is used. The solution lies in the fact that the natural state of data in systems should be de-identified data.

That would remove all identifiers that could be of value to attackers, while leaving enough data in the clear for analytics and business processes to continue.

Only a few select people should have the ability to decrypt the sensitive portions of the data, while a very large number of people should be able to work on projects and leverage the huge treasure trove of available “de-identified” data for the betterment of government.

About the Author

Marcelo Delima, Global Product Marketing Manager, HPE Security – Data Security

In his capacity as Global Product Marketing Manager at HPE Security – Data Security, Marcelo focuses the US Federal market sector among other responsibilities. Marcelo has over 16 years of experience marketing secure technology solutions for highly regulated enterprises and government agencies.

In his career Marcelo has held marketing leadership and management positions in technology organizations large and small in Silicon Valley.

The challenges of an Internet of Things analytics

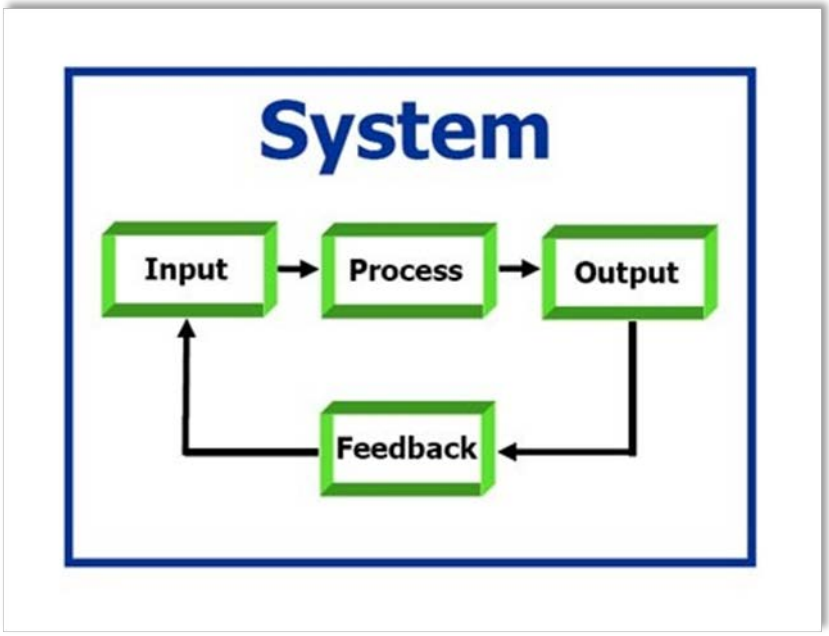
By Milica D. Djekic

Through a history – we would notice the importance of good analytics in many areas of human activities. For instance, many military strategists would deal with the intelligence before they decide to make any move on. Today's economy is also a place looking for the brilliant business strategists who would use an analytics in order to produce some sort of findings that would offer them a competitive advantage.

This new time would bring us many technological solutions that would deal with so many data. The good example of such a new technology is the Internet of Things (IoT) that would offer us a plenty of opportunities being in a correlation with our everyday's lives and businesses. Through this article – we intend to discuss some of the challenges coping with the IoT concept as well as its analytics being a key pillar in understanding such collected data.

What is the IoT analytics?

Have you ever wondered how many data could produce some IoT device? For instance, we would talk about the smart heating system being the part of much larger smart home solution or further – smart grid advancement. That smart heating solution would rely on temperature subsystem and humidity subsystem. These two subsystems would use the temperature and humidity sensors that would deal with the temperature and humidity in such an environment and send such an information to the control system that would adjust those two parameters to get as desired. In other words, we would talk about the control systems dealing with the feedback as illustrated in a Figure being down on the right.



Many experts would suggest that it's crucially important to collect data from the IoT solution being exactly where they are – at their edge. Once gathered data could serve in a better understanding of their role in the entire system and the next step in such a case would be to define your upcoming course of action.

Right here, we would use some effort to explain how the control systems with the feedback operate. For instance, it's possible that you would deal with the small regulating box that would seek from you to define your desired temperature and humidity in a room. You would do that – so, you would get those two data being the input parameters to your heating system. Those input data would cause your controller dealing with the process being the state of your temperature and humidity in that room.

Practically, at the end of this block diagram, you would get some output variables that would indicate those two heating parameters. As it's suggested before – the feedback branch would deal with the sensors that would measure the temperature and humidity at that place and send those data at the input trying to compare them with the desired values. If these two variables match the desired temperature and humidity values – the system would obtain a certain level of accuracy. On the other hand, if not – it would keep adjusting the output parameters to get as desired.

So, the question here would be how this could be correlated with the analytics. Well, you would agree with us that what we've just demonstrated to you – could get called some sort of analysis. That sort of stuff would support you in a better understanding of how things work as well as give you an opportunity to make some corrections or at least improvements to your solution. Everyone would agree that your sophisticated heating system being the part of a smart home solution would be capable to communicate with the rest of smart home subsystems using the web. Those subsystems could be media system, lighting system and so on – depending on how well your home got equipped. In order to analyze all these signals and data you would use some of the platforms being created to the IoT analytics. Right here, we would not deal with any of the IoT analytics platforms for a reason they are the matter of their vendors. In other words, we would try to be more explaining and less commercial which should be the point of any good insight.

The role of actionable-intelligence with an IoT

Some sources would recommend that the best way to deal with the IoT analytics is through the scheme – *Sense, Understand and Act*. In other words, you should use smart sensors or measuring devices in order to gather data from your surroundings. Further, you should deal with

some IoT analytics in order to understand your data and finally, you should take some actions on once you've realized how your system operates. In other words, that final step in such a concept should cope with the actionable-intelligence being something so useful for your strategy formulation. Sometimes it would be sufficient to rely on some free IoT search engines such as the Shodan and Censys in order to analyze or – in other words, better understand your IoT environment. The next chapter of this article would attempt to deeply explain the strategic perspectives of this concept relying on the previously mentioned concept of the actionable-intelligence.

The strategic perspectives of this concept

So, how the strategy being formulated to improve the entire IoT experience could get correlated with the IoT analytics and finally – the actionable-intelligence. The things here are quite simple. If you want to deal with some intelligence being a product of well-analyzed data and information – you would easily come to a level of the strategy formulation. Obviously – the IoT analytics would provide us the quite useful actionable-findings that would suggest such a sort of intelligence could serve in a deeper dealing with the entire system. In other words, the final step in a process being *Sense, Understand and Act* would offer us much more information which course of actions we should take in order to gain some sort of advantage. At the end, we believe that the strategy is smartly formulated course of actions that should get taken in order to obtain the certain goals.

The final thoughts

In conclusion, we would make an advice to the rest of a researcher's community to put some efforts on and deeply investigate this sort of a topic. Also, we believe that the similar efforts could get used in making a better strategic approach to this field of interest. Anyhow, the point is to make people think how to resolve a certain issue and once they gain that habit – we could count on a progress to all.

About The Author

Since Milica Djekic graduated at the Department of Control Engineering at University of Belgrade, Serbia, she's been an engineer with a passion for cryptography, cyber security, and wireless systems. Milica is a researcher from Subotica, Serbia. She also serves as a Reviewer at the Journal of Computer Sciences and Applications and.

She writes for American and Asia-Pacific security magazines. She is a volunteer with the American corner of Subotica as well as a lecturer with the local engineering society.

Look into my Crystal Ball; let's see what 2017 has in store.

by Jonathan Stock, Cyber Security Recruitment Consultant, IntaPeople.

The Christmas hangovers are starting to clear, every advert on TV seems to tell me that I need to begin the 2017 diet (maybe it's a sign!) and Meryl Streep turned into Tyson, firing punches at Mr Trump in her Golden Globe speech.

Who knows if he's going to respond, or if he's dazed and confused in 'La La Land', but one thing is for sure, 2017 is going to be a memorable year for many reasons.

2016 was the year of the high profile hack; LinkedIn, Yahoo, Oracle and DropBox were some of the major players to hit the headlines for all the wrong reasons.

So what does 2017 have in store for us? Are we going to see an increase in cyberattacks?

Are attacks going to change strategy and become more sophisticated? Are our defences going to get stronger?

Or are we going to go back to the dark ages and use pen and paper for all of our work so that we can reduce cybersecurity?

Experts within the industry have given predictions of what we can expect in 2017, I wonder if any of these will become true or if we're going to witness another Leicester City FC / Brexit / Trump shock to stun us all.

What will happen with the strategy of hackers? As mentioned above, 2016 was the year of the large organisations being targeted.

They were high profile, they had a massive gain for each hacking group and it took a long time for companies to recover both financially and with their reputation.

2017, might find hackers taking the easier route; targeting small and medium sized businesses.

Yes the reward financially might be less for them per organisation, but it's quicker and they can use their power to target several at once.

What will hackers do with the data they collect from breaches? Previously, it's been a case of theft, keeping it for themselves either to hack again, or using them as ransomware.

This year, we might see the rise of data manipulation.

Rather than theft, which is a quick and straightforward attack, hackers may start changing the data on internal systems, which in turn could lead to long term reputational damage for the company.

Like Ryan Gosling speeding along in Drive, IoT is on the horizon, it's going to be a bigger influence on our everyday lives than expected and it's going to cause massive ructions within the security world.

All of our devices are going to turn into the Von Traps, singing together in perfect harmony, but the majority of these are still on their default settings, open and internet ready; hackers thrive on this and will be able to integrate malware into home networks.

Finally, onto some positive outlooks rather than the doom and gloom. Cyber Insurance, 10 years ago, this wouldn't have been talked about, but now with the growing threat on all companies the IT budgets will start to include the insurance side of things.

Yes it's good news for Law Firms and Insurance brokers, but it's also great to see that Cyber Security is getting more recognition across all aspects of businesses.

There's going to be a greater commitment to Cyber Security and don't be surprised if roles like Chief Cybercrime Officer (COO) start coming to the forefront, tasking one person with the responsibility to ensure a company is 'cyber-ready'.

With GDPR starting to tootle along like the Hogwarts Express, companies are going to need to be on top of everything and make sure that they are in the best position to combat Cyber Security threats with both technology and processes.

About The Author

My Name is the Jonathan Stock and I am a cybersecurity recruitment consultant working for IntaPeople. In addition to sourcing candidates for various cybersecurity companies,

I am also a contributor to several cybersecurity online magazines, a member of the UK Cyber Security Cluster and an event coordinator.

Jonathan can be reached online at j.stock@intapeople.com, @JonathanStock86 and at our company website http://www.intapeople.com

Phishermen

How Insider Threats are Realized

by Daniel Jetton, VP Cyber Services, OBXtek, Inc.

While technical security problems can be dealt with through technical solutions, people must be approached in a different manner. The insider threat is one of the greatest liabilities in cybersecurity today due to the unpredictability of humans and their interactions with computers and networks. Humans account for over 90% of security incidents and the genesis of these incidents and breaches originate from computers, user mistakes, infections, resentment, fraud and carelessness.

A popular way of manipulating people from outside of an organization is to make them an insider threat using social engineering. Social engineering (SE), considered mostly an art but involving some science, demonstrates how people can be manipulated using a minimal amount of information. A confidence game based on human nature, social engineering pits human nature against security. Social engineering is arguably the costliest cyber-security issue today, but it is also the most preventable. Untold millions of dollars are lost every year due to social engineering with $3.7 million a year being spent on phishing alone for the average 10,000-person company.

Social engineering (SE) is defined as the deliberate application of deceitful techniques designed to manipulate someone into divulging information or performing actions that may result in the release of that information. During the engagement, victims are not aware they are being manipulated or that their actions may cause harm to themselves or their organization. By way of subterfuge, social engineers (SEs) convince victims to act against their best interests or against the interest of their organization. Unlike bribery or threats, a victim's motivation is based on trust and not necessarily reward or violence.

History

SE has been around for millennia. The Trojan Horse, of Greek mythology, wheeled into the secure gates of Troy was an SE (trust) ploy. In 1849, Samuel Williams, the original "confidence man" as he was known, conned the naïve into giving him their valuables by simply asking people to trust him with their jewelry until the next day.

In the early 20th century, Benito Mussolini was swindled out of $2 million dollars for phony rights to Colorado mining lands. Then in the 1960's, Frank Abagnale made a living using fake personas while kiting checks. It wasn't until hacker Kevin Mitnick arrived on the scene in the 1990's that the term "social engineering" entered into popular lexicon. Mitnick used the telephone as a tool to glean inside information needed to penetrate a network.

Professional penetration tester, Chris Roberts of One World Labs states that, "Whether breaking into buildings or slipping past industrial-grade firewalls, my goal has always been the same: extract the informational secrets using any means necessary." When given the mission for doing a penetration test for a high net-worth client, Roberts used the internet to find a phone number and an email the client had posted in a public forum for concert tickets.

The office number for the client (in this instance) allowed Roberts to gain access to personal cell phones numbers, mortgage info and a home address by posing as a publicist on the phone. According to Symantec, bad actors aren't targeting Windows vulnerabilities for exploit, they are going after people. Approximately 3% of malware used by perpetrators is used to exploit a technical glitch. The other 97% of malware is used to trick or as a ruse relating to a social engineering scheme.

Common Attacks

91% of breaches are the result of phishing. Phishing has been around for quite a while and may be the most common type of social engineering. Phishing uses threats, fear and a sense of urgency to motivate and manipulate victims to act immediately on spoofed websites or sites that have been shortened or embedded with links to suspicious websites. Ultimately, the actions, if successful, will provide the social engineer with personal information like names, addresses and credit card numbers. Phishing emails can run the gamut from mass produced, low quality emails (i.e. spelling errors and obvious misinformation) to focused emails (spear phishing) with detailed information and professional looking logos and signatures.

A McAfee Phishing Quiz found the most successful phishing email was spoofed from the United Parcel Service (UPS). The logo and branding matched and the website URL shown as UPS.com. Of note was the fact that the email contained only one malicious URL link. The first URL was a bona fide package tracking link. Only the second one, which encouraged the download and opening of an "invoice" (malware), was bad.

As we know, phishing, the (mostly) email based attack, gets its power from people clicking on an embedded link within an official looking email that can take them to a nefarious site or require victims to enter personal information under the guise of responding to a query from their bank or trusted institution. Vishing, phishing's lower tech cousin, uses the telephone to try and extract personal information from potential victims. This technique precedes phishing and dates back to the days when a social engineer attempted to get credit card numbers from trusting victims.

Pretexting relies on a social engineer's back story or scenario to gain the victim's trust. By using small amounts of actual, personal information (put together from various web sources) a social engineer can gain enough confidence to extract more information from the victim. SEs may advance their attacks to convincing victims to perform malicious acts without their knowledge to exploit a company or business. These attacks can be done online or in person. Impersonating a janitor who "lost his keys" is a perfect gambit for a social engineer to gain access inside a building or room for a seemingly authorized purpose.

Quid Pro Quo engagements offer an exchange of goods or services for information. Recent attacks include fraudulent Microsoft service desk tech impersonators who cold-call users offering to walk a victim through the process of removing phantom malware. These attacks can end up with the social engineers having access to a victim's computer and personal information or put them in a position where they can lock and encrypt the victim's information in order to ransom it for cash.

Baiting, like phishing, is based on a promise or likelihood of reward for cooperation. This type of SE is most common among freeware offers that entice users to enter personal information like name, addresses, emails, credit card numbers or banking information in exchange for free product.

The prevalence of social engineering attacks suggest that not only are the social engineers becoming more devious and improving their toolbox, but the human factor or "human firewall" is a continuous inherent weakness of a victim's inability to distinguish between bona fide requests and malicious communications . That being said, the obvious solution is knowledge.

Taking Action

Mitigation of the social engineering risk can best be done through awareness and training, focusing on the people and the processes. Companies should invest in training to make users aware of the potential threat (techniques, ploys and pitfalls) and educate them about how to deal with SE situations. Awareness and training combined with metrics help determine how close a company is to meeting its educational goal.

Employees who fail the tests or show elevated SE risk based on metrics should be retrained. Unfortunately, even though training, measurement and follow up are proven effective, they are not widely used. The Enterprise Management Association discovered that 56% of personnel had no SE training of any kind.

Personnel need clear boundaries established by guidance, policies and standard operating procedures from their employers. Thor Olavsrud, IT author and senior writer for *CIO* magazine, recommends some basic measures. These measures include education on the latest hacks/techniques, awareness of how important the information being released is and knowing which information is the most prized to bad actors. If there is data that can be monetized, it is valuable and worth a social engineering attempt to procure. Proper education and verification for employees will make them aware of the techniques used against them and train them to challenge would be impersonators.

Personnel need to change their paradigm about information. Information should be protected like the valuable resource that it is. Additionally, there should be no punitive measures against victims. Punitive measures create an atmosphere where employees will not share incidents and will, in fact, hide potential breaches for fear of employer retaliation.

Lastly, a "need to know" mindset is important for employees to implement. Asking "does this person need to know?" when fielding unsolicited requests is vital to avoiding SE losses. Most of

the time if an employee refers to a higher power (e.g. telling the caller they need to ask their manager or check the regulation before providing that info) a social engineer will break off and try an easier target.

Employer processes and policies provide a baseline of knowledge for the employee. To be effective they must be known by every user within the enterprise through education and training with consequences for violating the policies. To ensure a team approach, the policies and processes must also be distributed and embraced by top management as opposed to an edict from the IT department.

Typical policies include 1) procedures for verifying the identity of users to the IT department and IT personnel to users (secret PINs, callback procedures, etc.); 2) policies governing destroying (shredding) of paperwork, disks and other storage media; 3) prohibiting divulging passwords, to whom passwords can be disclosed and under what situations and procedures to follow if someone requests release of passwords; 4) requirements that personnel log off or password protect their desktop when away from keyboard; 5) physical security processes preventing outsiders accessing systems for nefarious purposes; and 6) strong password rules.

The Proactive Defense

In addition to training and definitive policies, a sense of employee ownership is imperative. If employees begin to take a personal stake in the welfare of their company, they will begin to make fewer errors and be more vigilant. Make no mistake, the technologies of penetration testing, patching, firewalls and the like are imperative to a proactive cyber-defense but without active engagement of company personnel against social engineering attacks, the biggest liability will remain.

About the Author

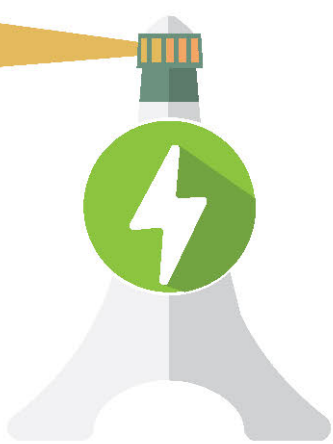
Daniel Jetton MBA, MS, MA, CISSP, CAP, PMP is the Vice President of Cyber Services for OBXtek, Inc., an Award-Winning Government Cybersecurity Service Provider providing Information Technology Engineering and Support, Program Management, Software Development, Testing, and Information Security services to the Federal Government. He is responsible for leading and defining cyber strategy while ensuring security, defense and risk mitigation for his clients.

Mr. Jetton is a former Army Medical Chief Information Officer with over 25 years of experience in cybersecurity, management, strategic planning and project management.

Daniel can be reached online at (djetton@obxtek.com). For more information on OBXtek, please visit their website at https://www.obxtek.com/aboutus

HACK IN PARIS

CYBER SECURITY CONFERENCE



EDITION

#7

2017

DISNEY'S NEWPORT BAY CLUB

TRAININGS: 19 - 21 JUNE

TALKS: 22 & 23 JUNE

www.hackinparis.com

Organized by

SYSDREAM IT SECURITY SERVICES

The Human in the Middle

Behavioral Design for Cybersecurity

by Alex Blau, Vice President, ideas42

In this ever-maturing digital era, using technology to solve our everyday problems feels like an obvious thing to do. Yet, in the realm of cybersecurity, a domain in which some of the best and brightest are applying their minds to build more adept and complex high-tech safeguards, we still find limitations in what our silicon chips and machine learning algorithms are capable of. Despite our obvious predilection towards innovation, one lament I continue to hear from experts is that we're not doing enough to deal with cybersecurity's weakest link, the human in the middle.

In 2014, IBM wrote in their Cyber Security Intelligence Index report that, "over 95 percent of all [security] incidents investigated recognize 'human error' as a contributing factor." However, to stem the growing cost of cybercrime, which is estimated to be more than $2 trillion globally by 2019, we continue to rely on technological solutions. Governments and private firms are rushing to invest billions of dollars in the next wave of hardware and software systems to protect institutions, organizations and citizens from the mounting global cyber threat. But, while building a better firewall, or smarter threat detection software is a necessary defensive tactic, it will most certainly not be sufficient in securing our digital boarders.

When we focus our attention on the power of technology, we may forget to consider how the behaviors of people can create the most persistent threats. Simple things like clicking on a bad link, opening the wrong email attachment, or inserting an insecure USB drive can be devastating to network security. And yes, while some technology investments have sought to prevent these sorts of problems from occurring in the first place, applying innovations like AI to detect a phishing email or identify malware in an attachment only goes so far—how many times has your spam filter missed a phishing email?

In practice, human beings must fill the gap between the limited capabilities of a given technology and a system's actual security needs, which ultimately relies on something humans are imperfect at using: their judgement.

Thankfully, there are entire fields of research that examine when human judgement fails, and can be used to help the designers of security systems predict when a user will act in less than safe ways. By applying insights from behavioral economics and psychology, we can begin to understand why users might fall for phishing attacks, click through browser warnings, or do any number of unsafe things with their computers.

Take updating, for instance. Security professionals frequently relay that applying security updates in a timely manner is probably one of the most important security measures any user can take. Many operating systems even prompt the user to install updates as soon as they are

ready. Yet, we often find that despite the ease and importance of updating, many users procrastinate on this critical step. Why? Part of the problem is that update prompts often come at the wrong time--when the user is preoccupied with something else--and provide the user an easy out in the form of various “remind me later” options. Because of this small design detail, users will be much more likely to defer on the update, no matter how important it is--how many times have you clicked “remind me tomorrow” before finally clicking on “update now”?

By understanding the factors that influence people’s decisions and actions, we can begin to identify solutions. For instance, instead of providing an option to push off the reminder to a later date, it might be prudent to get the user to commit to a specific time at which the update will take place. This way it is possible to prevent the endless stream of procrastination decisions, by getting the user to think critically about what a better time to update would be.

But, human error in cybersecurity is not limited to the decisions and actions of end users. Computer engineers may build errors into code that compromise the security of their software, IT administrators may not set up security systems properly, and C-level executives may not make the right kinds of investment decisions in their organization’s cyber infrastructure. However, by being able to recognize behavioral factors in cybersecurity, and identify their root causes, there is a rich vein of opportunity for making the system as a whole more robust.

Over the past year, ideas42, my behavioral science research and design firm, has been looking into what behavioral challenges exist in cybersecurity, and how we can use insights from the behavioral sciences to solve them. Through this effort, we wrote a cyber-novella, *Deep Thought: A Cybersecurity Story*, which tells the tale of how an extensive hack can be carried out by simply exploiting what we already know about the predictable errors in human behavior.

If you’re one of the people who have been seeking technological solutions to what you see as purely technological problems, then I recommend that you take a look at what we’ve learned, and see if there might be other ways of approaching the security challenges you’re trying to solve. And, if you’re one of those people who recognize that the person sitting between the chair and the computer is maybe one of the greatest threats to your cybersecurity system, than you’re already on the right track.

About the Author

Alex Blau is a Vice President at ideas42. He has extensive experience applying insights from behavioral science to solve design and decision-making challenges in a broad array of domains. His current foci at ideas42 are in the areas of cybersecurity, financial inclusion, public safety, and A/B testing. Alex Blau can be reached via email at ablau@ideas42.org, and on twitter at @unbofu and at our company website http://www.ideas42.org

Cyber Security Risks on Social Media

As technology advances, social media has gained popularity over time. It has provided a platform where people can freely express their feelings and get to interact with others, not forgetting to make new friends each passing day.

It has made communication quite easy, and news spread so fast thanks to the social media sites. However, while everyone is so keen to meet new people, form relations to feeling a sense of belonging, there is little time to worry about their security.

Cybercrimes are continually increasing with the internet adoption, and the more you let people in your life, the less safe you become. These people you interact with, “friends”, may have different motives as they send their requests to become your friends.

Cybercrimes With The Use Of Social Media

Identity Theft

This is the most common form of cybercrime. It occurs without you knowing, only to try and access your account and you find that you can’t get access to it. The next thing could be draining your bank accounts. With this in mind, you ought to be vigilant and use strong passwords to minimize the risk of identity theft occurring.

Leading Stalkers To You

In a bid to update your status, and post pictures on your page, people may connect the dots and get information that they ought not to and then find you. For stalkers, who in many cases are so keen to roughly examine what you post, may get hints of where you live or work, resulting in them tracking you down when you least expect it.

It is therefore advisable to reveal as little personal information as possible, and not to reveal the places where you stay to persons who you don’t even know.

Carelessness

Weekdays are usually the busiest days of the week. Everyone faces different challenges at their place of work, and at times, things don’t go as planned. In a bid to vent and express your frustrations, you may end up saying a lot that may not be necessary, more so where you are angered.

The information released may then be used later on against you, and it may cost you your job if you are not careful. This can be dealt with by minding what you say and post online. Moreover,

firms may put in place control measurements on social media, to prevent the release of vital information to competitors.

Corporate spies

Everyone has a way through which they earn their income. Some people are quite talented in spying, and when they seek to be your friends, you may not know about their motives. With time, they may gain access to your confidential information, through hacking. More so, if you don't have a strong password or don't regularly change the password, making it vulnerable. With time you may be accused of espionage, whereas you even know not about it. So play safe.

Corruption of passwords

A lot of people may be at high risk of their passwords being corrupted. To the hacker, this is an easy way to maneuver, and they have a lot of loopholes they can utilise. One of the ways that you ease their work is through remembering the password, which makes it so easy for them to bypass.

With time, a lot of your personal information is at their disposal. They end up acquiring a lot of information about you even regarding other accounts and your financial information as well. Be safe and input strong passwords, and also regularly change the passwords. Using different passwords for different accounts also makes it hard for people to connect and make relations between the accounts. Hence you remain protected.

Links to malware

Many people tend to fall victim of this. Upon logging into their accounts, some enticing links may emerge that lead you to click on them. On clicking on other links, it may require you to sign up giving more personal information. Well, most are malicious and are only there to enable you to reveal more information about yourself, and it may not work so well on your part. Avoid falling into the trap and only follow links from trusted sources.

The trick of remaining safe while using social media is knowing how much to let people know about you. Using strong passwords, and changing them regularly. To survive on the internet open only trusted links to avoid malicious links.

About the Author

This article was written by Simon Parker at Minerva Security. Minerva is an integrated fire & security service provider with a clear vision to create smarter environments, and to help its customers reduce their fire and security operating costs.

Cyber Attack Detection for Mobile and Web Technology

17 - 18 July 2017 | Singapore

Key Topics:

- Cyber-attack 'weapons' (0-days, Advanced Persistent Threats)
- Recognise a cyber-crime attack
- Prepare your protection from cyber-crime attack
- How to deploy a red team security testing program
- How to recover from an attack

LIVE Demonstrations:

- Blockchain
- Sniffing and hacking IoT
- Social engineering attack, including system take over (ransomware)
- Network detection
- Memory and network forensics

For more information, please contact us at marketing@openforum.sg

Proudly organised by

Open Forum Enterprise

Supported by

AISA

Media Partner

CDM
CYBER DEFENSE MAGAZINE
THE PREMIER SOURCE FOR IT SECURITY INFORMATION

QUOTE "CYBER DEFENSE MAGAZINE" FOR

15%

DISCOUNT OFF NORMAL RATE

PART II: DEFENDING YOUR AIRSPACE

WIPS vs. WIDS

by Ryan Orsi, Director Product Management, WatchGuard Technologies

In part one of this series: The Anatomy of a Wi-Fi Hacker, we addressed the ever-growing need for a digital connection and the risks associated with public Wi-Fi. Paramount among those risks is the man-in-the-middle (MiTM) attack, which allows a hacker to gain visibility into a device's traffic, and therefore launch other sophisticated attacks.

Think of the MiTM as a beanstalk that starts as a seedling and grows into something much larger. In this case, it grows into higher-layer attacks such as SSL Stripping with HTTS bypass, toxic proxies, or attacks that exploit vulnerabilities in WPAD. We want to kill this beanstalk (or the MiTM) before it grows, but how?

In part two of this series, we're going to explore that question. It all starts with the basics of Wireless Intrusion Detection Systems (WIDS) and Wireless Intrusion Prevention Systems (WIPS).

Both these systems were (and are) heavily driven by compliance standards like PCI DSS and HIPAA, which outline requirements for identifying rogue access points (APs) on Wi-Fi networks. WIDS works to detect existing rogue APs and uses traditional methods, such as:

- **CAM Polling**: A client connects to an AP (which needs to be in bridge network mode), and that AP is connected to a switch. The switch records the MAC address of the client connected to the AP and switch. The WIPS server then polls the switch and tries to get the MAC address. Meanwhile, the WIPS sensor is scanning the airwaves to correlate the AP MAC address from the client to the MAC address from the WIPS server/switch. If these addresses are found to be nearly the same, it's considered a rogue AP.
- **Passive MAC Correlation**: A sensor on the network looks at the wired and wireless network and finds the MAC addresses. If these are within a couple bytes of each other, there is a probability of them being the same device.

These two approaches suffer from complexity and scalability issues, and often result in false positives. Companies are now looking to solutions with marker packets, a new approach that effectively eliminates these challenges. Marker packets are essentially a small broadcast packet that flows through all the APs.

With this approach, the system can gather information that is then referenced against established policies to identify an AP as legitimate or rogue. Marker packets essentially

eliminate false positives for WIDS. But, detection is only part of the equation when protecting a Wi-Fi network.

How can we stop these rogue APs from getting access to, or getting on, the network in the first place? WIPS is the other half of the equation.

Historically, organizations have shied away from WIPS because the prevention features could accidentally shut down neighboring Wi-Fi networks, which can result in painful and costly repercussions.

For example, Smart City Networks was hit with a hefty $718,000 FCC fine for accidently shutting down a legitimate neighboring Wi-Fi network. According to Travis LeBlanc at the FCC, “All companies who seek to use technologies that block FCC-approved Wi-Fi connections are on notice that such practices are patently unlawful.”

But, new WIPS technology eliminates this problem by using automated *classification*. Automated classification goes deeper when classifying SSIDs and puts them into buckets such as authorized (good), rogue (bad), guest and external.

Once the SSIDs are classified, more granular policies can be applied to users to keep them safe. For example, a user can connect to an internal AP, but not an external malicious rogue AP by the same name.

This process is accomplished with sensors that constantly scan the airwaves and capture marker packet information. That information is then correlated with policy information and automatically classified. It ensures that legitimate external Wi-Fi networks are not accidentally taken down.

But, if this new WIPS technology exists, why aren’t more people using it? The reality is a lot of organizations are using WIDS, but these systems require dedicated teams to wade through alarms and false positives. So, it’s typically only larger organizations that have the resources to support them.

Unfortunately, because of the resource requirements and perceived risk, many companies stay away from the WIDS/WIPS solutions altogether. The good news is that cutting edge WIPS classification technology is making wireless defense more scalable, automatic and cost-effective for companies of all sizes.

In the meantime, while organizations play Wi-Fi defense catch-up, how can the everyday consumer tell if a hotspot is secure? Unfortunately, they can’t. While some organizations are trying to work toward offering secure Wi-Fi with accreditations like Friendly Wi-Fi, for the most part consumers are left to fend for themselves. This is another reason why brands should use automated systems to help keep consumers safe when connecting to public Wi-Fi.

The technology now exists to protect a Wi-Fi network and its users at reasonable cost, with solutions that require low maintenance, helping to reduce some of the major security issues facing organizations today.

According to a study from Javelin Strategy and Research, 15.4 million victims lost roughly $16 billion from credit card theft in 2016, which represents six percent of all consumers worldwide. And, it's only expected to increase in 2017.

The study also showed an increase in identity fraud via Wi-Fi attacks with hackers posing as the MiTM. So, these types of attacks continue to drive compliance mandates, like PCI DSS.

PCI has some specific, but not all too realistic, standards for securing Wi-Fi networks, such as my favorite: "performing regular scans for rogue APs on a quarterly basis." Really, we should just check for rogues every 90 days?

As you can see, compliance is not synonymous with security. And this speaks to the challenges companies and consumers face when dealing with Wi-Fi. Hackers are reaping the benefits of the industry's slow transition.

The standards are not strong enough, organizations don't yet realize how to automate Wi-Fi protection, and consumers roll the secure Wi-Fi connection dice.

But it doesn't have to be that way. Any organization can now afford to proactively defend their airspace and eliminate the Wi-Fi network risks for employees, partners and customers.

So, make sure that you're protecting your Wi-Fi network with WIPS technology that utilizes the marker packet detection method and eliminates false positives and automatically assess connected APs and Wi-Fi clients to determine if they're authorized, rogue or external.

Now that we've covered how Wi-Fi hacks happen and how organizations can protect themselves with automated WIPS/WIDS, our final installment will look at how to protect a network from connected devices and IoT.

Join me next month as I explore how the world of connected devices and rapidly evolving IoT threats will impact Wi-Fi security.

About the Author

Ryan Orsi is Director of Product Management at WatchGuard, a global leader in network security, providing products and services to more than 75,000 customers worldwide. Ryan leads the Secure Wi-Fi solutions for WatchGuard. He has experience bringing disruptive wireless products to the WLAN, IoT, medical, and consumer wearable markets.

As VP Business Development in the RF industry, he led sales and business development teams worldwide to success in direct and channel environments. He holds MBA and Electrical Engineering degrees and is a named inventor on 19 patents and applications.

Ryan can be reached online at @RyanOrsi and at our company website www.watchguard.com/wifi

Time to Get Serious About Internet of Things Cybersecurity

The Internet of Things (IoT) is made up of everyday objects built with the ability to sense, analyze, and communicate information about themselves and their environment. In smart homes and offices, these devices measure air quality, secure against intruders, and listen for verbal instructions to play music or order pizza. IoT devices are also deployed in industrial applications to do things like monitor the flow of oil through pipes, track public transit vehicles, and control robotic arms on assembly lines. IoT even includes simplistic sensors that do everything from measuring temperature to counting how many times a door is opened or how many times a customer tries on a pair of shoes. There are already billions IoT devices deployed around the world, and most estimates put that number at 25-50 billion by 2020.

While the promise of near omniscience continues to fuel this rapid growth, IoT cybersecurity appears to still be an afterthought. The capabilities that would help protect IoT devices, and those that would protect the rest of the world from IoT devices, are severely lagging. This reality came to a head when hackers secretly searched for, found, and compiled a list of millions of easily hacked IoT devices. The unprotected devices were combined into a botnet dubbed Mirai, which was unleashed on the world in a massive Distributed Denial of Service (DDoS) attack that brought down some of the biggest Internet sites in the world. Twitter, Spotify, SaneBox, Reddit, Box, Github, Zoho CRM, PayPal, Airbnb, Freshbooks, Wired.com, Pinterest, Heroku and many others were knocked offline for hours. Level 3 put out a report that explains in detail how the Mirai botnet worked.

The source code for the Mirai bots was subsequently released, allowing others to use the same technology to build their own IoT botnets. While the release of malware source code isn't uncommon, it usually follows the widespread availability of a patch to close the hole the malware exploits. The fact that IoT devices are often difficult or impossible to patch, makes the release of the Mirai source code particularly dangerous.

One good thing about the Mirai attack was that it generated a lot of data from which we have learned a couple of very interesting things. First, the attack had little to do with the capabilities of the devices themselves, only their massive numbers combined could generate such traffic. Second, and most importantly, this attack was almost completely avoidable.

Most IoT devices were not designed to be secure, and their production reflects that. For example, most security cameras which became part of Mirai had hard coded default passwords, so they were all operating with known backdoors. Certainly, the "build security in" crowd can find a lot of support in Mirai examples, but organizations that deploy devices with weak security bear significant responsibility for how those devices are used.

Had the organizations deploying the devices that were caught up in the Mirai botnet adhered to cybersecurity risk management best practices, much of the impact of these attacks could have been mitigated. When considering a new device deployment, organizations should consider the

impact of an attack that causes a device to: a) misbehave; b) attack other parts of the enterprise; and c) launch attacks outside of the enterprise. In the case of utility or industrial IoT, these attacks could compromise critical infrastructure and endanger lives or harm the national economy.

Users can take steps to control their IoT environments following security best practices like changing device default passwords, connecting devices to secure networks, and enforcing rules about how, when and with whom IoT devices can communicate. The Cloud Security Alliance has also published guidelines specific to the securing of IoT devices. Their top five suggestions include the need to:

1. Design and implement a secure firmware/software update process for IoT;

2. Secure product interfaces with authentication, integrity protection and encryption;

3. Obtain an independent security assessment of all IoT products;

4. Secure any companion mobile applications and/or gateways that connect IoT products to networks

5. And implement a secure root of trust for root chains, and private keys on each device.

Unfortunately, many of these common security best practices such as secure roots of trust, network security, firmware updates, and even maintaining unique certificates are challenging to implement when it comes to IoT. Additionally, the limitations of many IoT devices, makes their integration into enterprise security capabilities (e.g. network access controls, address whitelisting, key management) a difficult or impossible task. The good news is that many in the security community are hard at work on this problem - building the tools and services to secure the IoT.

About the Author

Nate Lesser is the Managing Director of MasterPeace LaunchPad, an advanced technology startup studio in Maryland, and has spent the last 15 years driving innovation at the nexus of technology and business. He has held technical and executive positions in government and the private sector. He works with cybersecurity technology builders, buyers, and investors to improve the efficiency of the innovation ecosystem.

Nate is a strategic leader, cybersecurity expert, and advisor to numerous startups and non-profits. He serves as a Senior Fellow at the George Washington University Center for Cyber and Homeland Security, a mentor at the Mach 37 cybersecurity accelerator, CEO at Cypient, and Advisor at Zuul IoT.

5 ACTIONS TO TAKE NOW!

To Avoid Common Third-Party Risk Management Pitfalls...

Navigating the third-party management jungle while trying to avoid its many risk and compliance pitfalls is a dangerous business for CISOs. It's critical for companies to keep sensitive data safe and comply with industry regulations.

EVALUATE YOUR VENDORS

DOES YOUR CURRENT SECURITY PROGRAM INCLUDE THIRD-PARTY RISK MANAGEMENT (TPRM)?

77% of companies expect a breach **because of vendor activity** in the next 2 years...

...meaning your vendors' vulnerabilities are likely **your vulnerabilities.**

Download the full infographic:
http://go.prevalent.net/PitfallsInfographic

PREVALENT®

ENGAGE WITH ALL STAKEHOLDERS

A TPRM PROGRAM IMPACTS ALL ASPECTS OF A BUSINESS, INCLUDING THE BOTTOM LINE.

62%

of businesses say their boards **don't require** third-party management.

GET EDUCATED ABOUT YOUR VENDORS

USE A TPRM PLATFORM TO IDENTIFY WHICH OF YOUR VENDORS HAVE ACCESS TO YOUR SENSITIVE DATA AND WHICH ONES HAVE THE CONTROLS IN PLACE TO PROTECT IT.

2/3

of companies **simply don't know** how many third-parties have access to their systems.

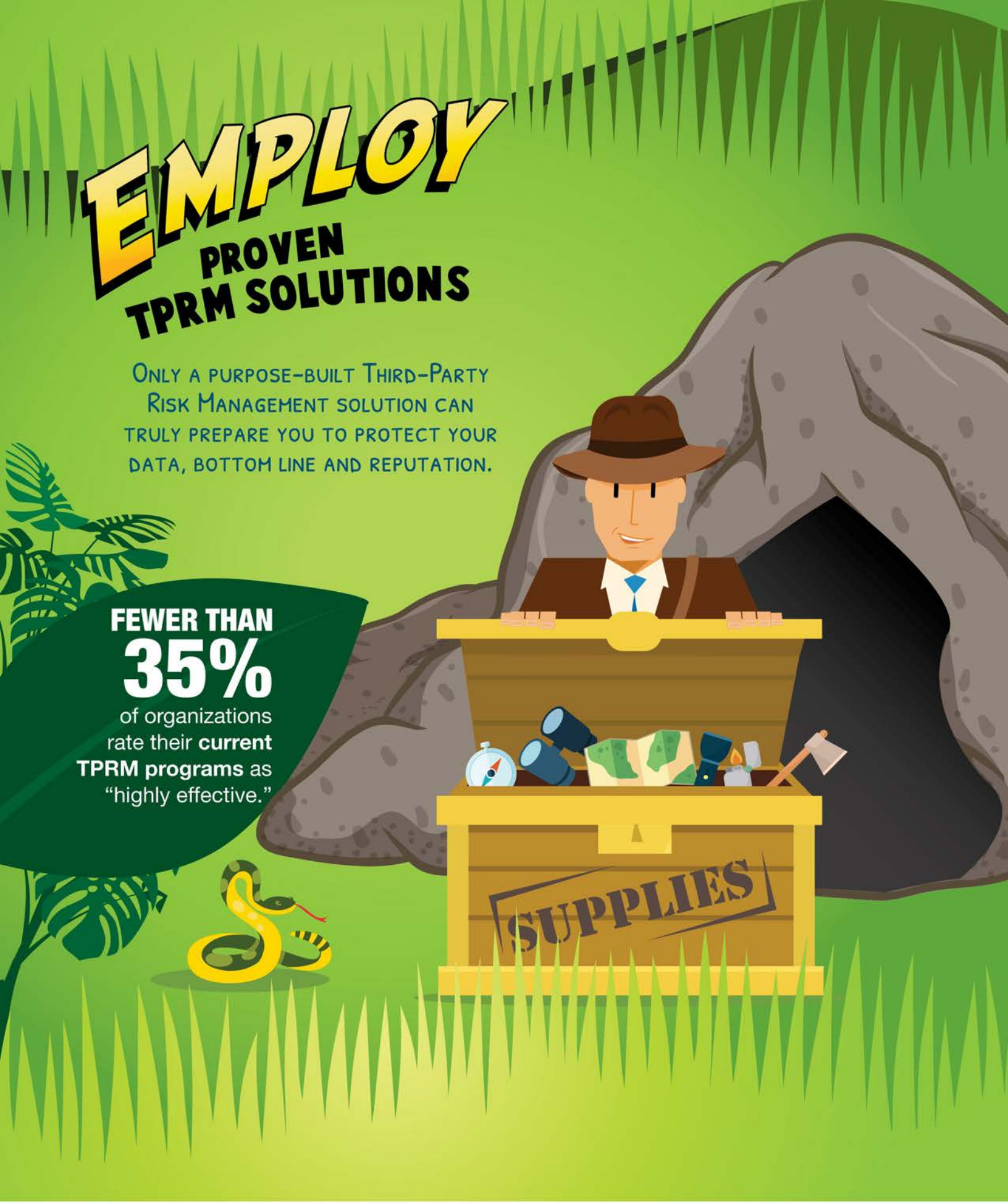
Download the full infographic:
http://go.prevalent.net/PitfallsInfographic

PREVALENT®

EMPLOY PROVEN TPRM SOLUTIONS

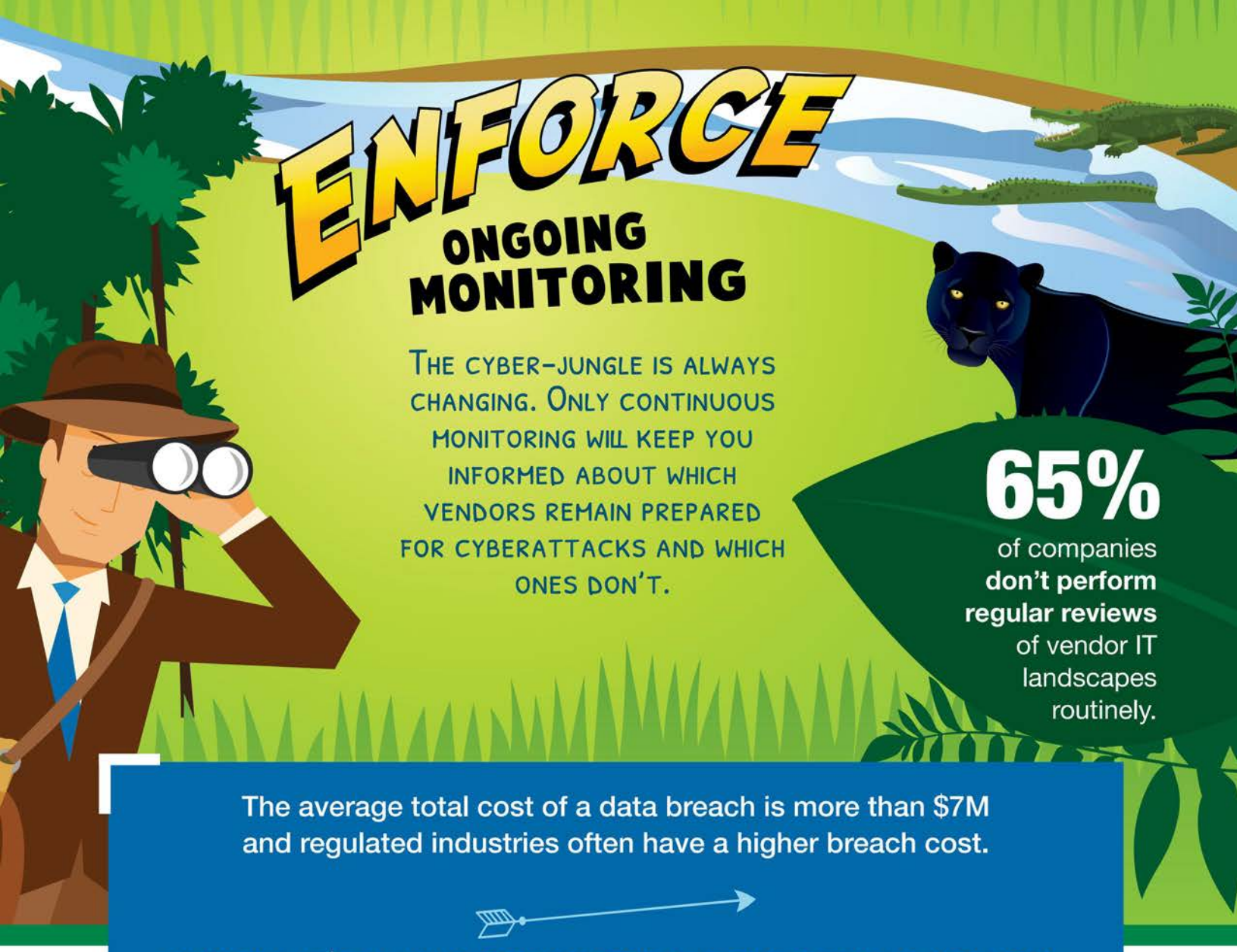
Only a purpose-built Third-Party Risk Management solution can truly prepare you to protect your data, bottom line and reputation.

FEWER THAN 35% of organizations rate their **current TPRM programs** as "highly effective."



Download the full infographic:
http://go.prevalent.net/PitfallsInfographic

PREVALENT™



The average total cost of a data breach is more than $7M and regulated industries often have a higher breach cost.

CLEARLY, IT'S A JUNGLE OUT THERE AND THE PITFALLS ARE DEEP.

CAN YOU AFFORD NOT TO ACT?

PREVALENT®

Named the only Visionary for a second time in a row on Gartner's Magic Quadrant for IT Vendor Risk Management, Prevalent delivers comprehensive third-party risk management solutions to companies across industries and markets.

Visit **PREVALENT.NET** to learn more.

Download the full infographic: http://go.prevalent.net/PitfallsInfographic

INFOGRAPHIC DATA SOURCES:

Data Risk in the Third-Party Ecosystem; Ponemon Institute LLC, April 2016
Cost of Data Breach Study: United States; Ponemon Institute LLC, June 2016
Vendor Vulnerability Index; Bomgar, 2016

Why today's university students pose a massive cyber threat — and what to do about it

By François Amigorena, CEO, IS Decisions

To any IT security person working within a university, students are one heck of a headache. Old enough to make adult decisions but young enough to make naïve judgements, students pose a security challenge akin to holding water in a sieve.

Despite being digitally savvy and the future of the workforce, students often regard IT security as a barrier rather than a safeguarder — much in the same way as perhaps they view their parents in some situations. While mom and dad may know best, children will often do what they want to until something bad happens.

Arguably, it's the same with cybersecurity. Until a student personally experiences the theft of their own data, which costs them money or causes any kind of hindrance, convenience is likely to be much more important than security.

And then the IT practices that are taken for granted by most employees by the time they turn 30 fall to the wayside.

The stats back up these assumptions. While 70% of higher education students are aware of the threats of cyber crime, most (80%) aren't concerned by cyberattacks, and 65% don't see cybersecurity as their concern.

These findings go some way to explaining students' poor security habits. Many problems stem from poor password practice. For example, many students will use the simplest and easiest-to-crack passwords — sometimes the same one for all their accounts.

Indeed, a report analysing more than 5 million stolen passwords in 2016 found a huge number of "ridiculously insecure" passwords, including '123456' and even 'password'.

And even when they may use simple passwords, those same students will forget or lose their login details, meaning they borrow their friends' logins to do their work. IS Decisions research, for example, found that nearly 35% of those aged 16–24 have shared their password with at least one other person, compared with the average figure across all ages of 23%.

Aside from password practice, many students may also feel that it's ok to leave their laptop logged in unattended in the library when they go out to take a break.

They're not necessarily bothered about how they access their files and systems, provided they can do it quickly — and you can hardly blame them for the practices they adhere to if they've neither been trained nor had to suffer the consequences of a breach.

When many of today's cyberattacks occur as a result of compromised credentials, this kind of lax security poses a real worry to IT teams within universities.

University systems are likely to hold the healthcare records, university files, bank details, addresses, phone numbers and much more for each student — and the practices by the students themselves are risking that data to exposure.

This combination of slack security and valuable information is a gold mine for cybercriminals, and a nightmare for IT professionals working in universities to protect students.

To put things into context, a recent report by Dark Reading uncovered that thousands of stolen and fake student, faculty and alumni email credentials were available to buy on the dark web.

The usernames and passwords were linked to 300 of the largest and most well-known universities in the US. And with prices ranging from anywhere between $3.50 to $10 per email address, it's clear that these credentials are in high demand.

University IT teams therefore must do more to protect their students, which is hard enough when the students barely help themselves.

Education with regards to cybersecurity is obviously key, but there's only so much students will take in before lapsing back in to bad habits. And those who do change their ways are still human.

They're still prone to making mistakes like clicking on a link in a phishing email and giving up their university login credentials unknowingly.

So, what can you *really* do to better protect students?

Prevention is better than cure

In the past, IT teams within the education sector have only implemented security policies as a reaction to a breach, rather than pro-actively and pre-emptively put policies in place. That needs to change — in particular to protect against compromised logins.

To better protect education institutions and monitor for potential threats, IT teams must take preventive measures to implement a network access control and identity management system that stops hackers in their tracks.

The future of identity management is therefore context-aware security. Context-aware security verifies the legitimacy of a login based on more information than just the correct username and

password. This type of security analyses the time, the location, the device, the IP address and other contextual factors surrounding a login.
Based on that information, IT administrators can set rules that restrict logins to only those that don't look suspicious.

For example, if the login details of a student at Harvard falls into the hands of an attacker based in China, the system can deny access because the login attempt is happening outside of Massachusetts — even if the attacker is using the right username and password.

This kind of security protects students against the consequences of phishing attacks and halts dangerous concurrent login practices, all without hindering the student or slowing them down.

It stops attackers from gaining entry and stealing valuable data or uploading ransomware. It provides the same strength security as multi-factor authentication without any of the hassle because the security simply acts in the background.

It protects against lax behaviour and gives the university's IT team peace of mind that those logging in to university systems are exactly who they say they are. It's a win-win situation for both students and IT teams.

Context-aware security is therefore the future of protecting university IT. It's the form of protection that students want, and IT teams need.

About the Author

François Amigorena is the founder and CEO of IS Decisions, and an expert commentator on insider threat issues.

IS Decisions is a provider of infrastructure and security management software solutions for Microsoft Windows and Active Directory. The company offers solutions for user-access control, file auditing, server and desktop reporting, and remote installations.

Its customers include the FBI, the US Air Force, the United Nations and Barclays — each of which rely on IS Decisions to prevent security breaches; ensure compliance with major regulations; such as SOX and FISMA; quickly respond to IT emergencies; and save time and money for the IT department.

Gartner Summits

Gartner Security & Risk Management Summit 2017

June 12 – 15 / National Harbor, MD
gartner.com/us/securityrisk

Manage Risk. Build Trust. Embrace Change.

Key benefits

- Reinvent your approach to security and risk for the digital age
- Embrace new ways of protecting vital assets without slowing interactions
- Learn how to shift to more adaptive, dynamic, people-centric approaches to security
- Build a trusted, resilient environment for digital business

For more information and to register, visit gartner.com/us/securityrisk. Use promotion code GARTMP4 to save $300 on the standard registration rate.

"I was impressed with the forward-looking nature of the topics covered at the summit."

Steve Logan, GTAS Senior Project Manager, Security & Privacy, Vanguard

WannaCry Ransomware: Dangerously Different

by Jason Matlock, Security Analyst, Sword & Shield Enterprise Security

This article originally appeared on Sword & Shield Enterprise Security blog on May 15, 2017.

Friday, May 12, 2017, will be remembered for what was the largest ransomware attack in internet history.

The world watched as critical systems were affected by a piece of ransomware called WannaCry or Wcry for short.

By the time the dust settled, more than 200,000 computers in 150 different countries were infected by WannaCry ransomware.

Thanks to a security researcher named MalwareTech, a kill-switch was discovered that effectively stopped Wcry from spreading further. But, is it over?

As the weekend ended, the fear, when people returned to work to power on their computers, was that the WannaCry Ransomware would again begin spreading. In addition to this, there is a strong possibility that new versions of either Wcry or another similar piece of ransomware will show up without the kill-switch available and cause another widespread infection.

Let's take a quick look at how Wcry is spreading. For this, we need to turn back in time a bit to the Shadow Brokers' release of NSA exploits back in April, specifically to one named "EternalBlue", which we explained in a previous blog.

"EternalBlue" attacks a vulnerability in SMBv1, allowing a malicious person to remotely execute code on the victim's computer.

It seems that Wcry's authors are using this vector as the initial entry into a computer where the ransomware is then delivered and executed, infecting the machine.

Once a machine is infected, Wcry then looks at other computers on the network to infect. This method of propagation is what allowed Wcry to infect so many computers in a relatively short amount of time.

In March, Microsoft released security update MS17-010, which addresses this SMB vulnerability. At that time, the patch was only available to current versions of the Windows operating system, so anyone who was using Windows XP, Server 2003, or Windows 8 was still vulnerable.

Because of the widespread infection of Wcry, Microsoft revised their policy to support end-of-life software and released patches for those operating systems on Friday.

So, how should people protect themselves? In addition to the tips my colleague, Rick Cantrell, gave in his blog, here are a few to protect your personal computers, as well as those in a corporate environment:

- If you can't patch a system due to legacy software, disable SMBv1 and segregate those devices from other systems on the network. Microsoft's support article 2696547 details how to disable SMBv1.
- Do not expose SMB ports to the internet (TCP 445, 139); properly configure your perimeter firewall rules.
- Have known good backups; it isn't enough to just do a backup; perform regular restore tests to make sure you can recover your files.

There will almost certainly be copycat actors who will release new variants of WannaCry Ransomware, so always remain vigilant. Stay safe!

About The Author

Jason Matlock is a security analyst and penetration tester for Sword & Shield Enterprise Security. As a trusted security professional since 2005, Jason brings expertise in internal/external security assessments, wireless security, help desk, and endpoint security.

For more information about Jason and Sword & Shield, visit https://www.swordshield.com/.

ALL ACTIVE MILITARY & GOVERNMENT EMPLOYEES CAN ATTEND FOR ONLY $25!

3RD ANNUAL CYBER SECURITY FOR DEFENSE

Protecting Our Nation Against Faceless Enemies

NEW SPEAKERS FOR 2017:

SHERRILL NICELY
Chief Information Security Officer
Central Intelligence Agency

STEVEN SHIRLEY
Executive Director, Defense Cyber Crime Center
Air Force Office of Investigations

TONYA UGORETZ
Director, Cyber Threat Intelligence Integration Center
Office of the Director of National Intelligence

TRENT TEYEMA
Section Chief (SES)
Federal Bureau of Investigation

CHRISTIAN LIFLANDER
Head of the Cyber Defence Section
NATO

200+
Attendees

20+
Defense Cyber Security Speakers

10+
Hours Of Networking

Expert Presentations From The Military, Government, Law Enforcement, And International Military & Government

Receive An Exclusive 20% Discount Off Standard Rates

Use Code: **'CyberDefenseMagazine_20'**

www.CyberSecurityForDefense.iqpc.com

Threats and Enemies: The 10 Most Dangerous Threats to Your Network and How to Combat Them

By Summer ParkerPerry, Product Evangelist, ManageEngine

With data breaches and security threats on the rise, protecting your network has become virtually impossible. In 2016 alone, a recorded 1,093 data breaches occurred (according to the Identity Theft Resource Center and CyberScout). With this peak in data breaches, it's more critical than ever to make sure your system is protected.

It's important to stay educated on the latest and most dangerous threats to your network to make sure you have the right tools to keep your system secure. The following list details the most commonly used attacks and threats to your network.

Threat 1: SQL Injection Attack

- An SQL injection attack, commonly known as an attack vector for websites, uses malicious SQL statements to control a web application's database server. These types of attacks are dangerous because they allow attackers to tamper with (and even destroy) data, spoof identities, access administrator rights, and alter transactions and balances.

- WordPress, unfortunately, fell victim to an SQL injection attack that affected their WP_Query, which is used to access variables, checks and functions coded into WordPress' core. Though the issue did not affect the core, it did introduce further vulnerabilities. (January, 2017)

Threat 2: DDoS Attack

- A DDoS attack floods a machine or network with endless requests, overloading the system. This type of attack is intended to disrupt the host's services and prevent requests from being fulfilled.

  Some DDoS attacks can result in backscatter, which restricts the victim's machine from being able to distinguish between legitimate and spoofed packets.

- In 2016, DNS provider Dyn Inc. fell prey to a DDoS attack that took down their service for nearly 24 hours, impacting popular services that rely on Dyn, including Netflix, Twitter, Airbnb and PayPal.

Combat: Shield Your Network from DDoS and SQL Injection Attacks

To protect networks from SQL injection attacks, DDoS attacks, phishing attacks and more, IT teams need to pinpoint breach attempts, insider threats, and policy violations with no manual

intervention necessary. Drag-and-drop correlation rule builders allow users to define attack patterns and proactively prepare for any security threat with mitigation and vulnerability scanners. More than ever, it's important to be able to identify the cause and perpetrator of a breach.

Threat 3: Insider Attack

- Insider attacks on an organization are orchestrated by someone within that organization, such as a former employee, contractor or even a current employee. This person typically takes valuable (often confidential) information, alters that information on security practices and data, and can even sabotage computer systems.

- One of the most famous insider attacks occurred when Edward Snowden (computer professional and former Central Intelligence Agency employee) leaked classified information from the National Security Agency in 2013.

Threat 4: Pass-the-Hash Attack

- A pass-the-hash attack is defined by an attacker obtaining the password or password hashes to an account through LM or NTLM authentication. This type of attack allows the password hash to remain static for each session, until the password is changed.

- Pass-the-hash was one of the methods used in Yahoo's 2016 breach, in which up to one billion accounts were compromised.

Threat 5: Stolen Password

- Stealing passwords is essentially the process of extracting a password from data that has been stored in or transmitted by a computer system. A stolen password gives someone unauthorized access to a system that often contains confidential information.

- In 2012, 117 million passwords were stolen from LinkedIn, compromising user accounts. In 2016, those passwords and other critical account information, including password hashes, were published online. Following the 2012 breach, LinkedIn implemented two-factor authentication and salted hashes to avoid future calamity.

Combat: Defend Your Network from Internal Threats and Password Attacks

- The best way to protect your system from insider threats, pass-the-hash attacks and stolen passwords is to create a secure, centralized vault for password storage and access.

- In addition, preventative and detective security controls are extremely important and can be implemented with real-time alerts on password access and approval workflows.

Threat 6: Malware Attack

- A malware attack uses software to disrupt a computer system by stealing sensitive information, spying on computer users, displaying unwanted advertisements and gaining access to private systems. These attacks can also be used to extort money and even harm a system.

- 97 percent of public and private companies surveyed by Ponemon in 2015 reported to be victims of a malware attack.

Threat 7: Privilege Escalation Attack (EoP)

- In a privilege escalation attack, otherwise known as an EoP, an attacker creates a bug that tricks the system into believing that they have legitimate administrative privileges. In turn, the hacker can gain access to protected resources, open files, change user accounts, destroy an Active Directory and more.

Threat 8: IP Attack

- In an IP attack, the attacker overloads targets with traffic from multiple spoofed addresses, sending the system more data than it can handle. IP attacks can also transmit a packet to the sender when another machine receives a packet, flooding the target's IP address.

Combat: Defeat Malware, IP and EoP Attacks

- One of the most useful features to combat malware, IP and privilege escalation attacks is a context-rich audit trail, which investigators can use to monitor AD users and actions.

  It juxtaposes important information (such as the admin actions on the account, the account's remote access from an unfamiliar IP, and the account lockout) to differentiate related security events and expose insider jobs.

Threat 9: Botnet Attacks

- A botnet attack consists of a group of compromised computers that are remotely controlled by a hacker who attempts to infect and control machines by hitting them with malware and sending spam emails, viruses, etc. Usually a botnet cybercriminal controls the machines through a covert channel, such as Internet Relay Chat.

- In 2016, the Mirai botnet took down the internet for many in the U.S. The attack was reported to be "likely the largest of its kind in history ... [and] roughly twice as powerful as any similar attack on record."

Threat 10: Brute Force Attack

- A brute force attack is when a hacker attempts to crack a password using a program to decode encrypted data (such as passwords or Data Encryption Standard keys) with manual, repetitive effort.

- GitHub fell victim to one of the largest brute force attacks in 2013, when 40,000 unique IP addresses attempted brute force logins.

Combat: Eliminate Brute Force and Botnet Attacks

- A critical defense against brute force and botnet attacks is to centrally collect, archive and analyze security device logs to generate forensic reports. From there, it's key to inform users of all possible network attacks and security breaches in your network, active viruses in the network, anomalies in the firewall policies, and how to rectify them all.

  Beyond that, use a wide range of reports for external threat monitoring, change management, and regulatory compliance.

Conclusion

As you can see, network security faces endless enemies and threats, making proper monitoring software more critical than ever. But beyond that, it's important to stay aware of what security threats your network faces to proactively prevent disaster and to effectively restore service when it does occur.

Security in 2017 is no easy feat, but with the proper knowledge and awareness, enabled by reporting and monitoring tools, anyone can secure their network and combat the ever-growing minefield of cyber threats.

About the Author

Summer ParkerPerry is a product evangelist at ManageEngine, the real-time IT management company and division of Zoho Corporation.

For more information on ManageEngine, the real-time IT management company, please visit www.manageengine.com; follow the company blog at http://blogs.manageengine.com, on Facebook at http://www.facebook.com/ManageEngine and on Twitter @ManageEngine.

INTERPOL WORLD 2017

FOSTERING INNOVATION FOR FUTURE SECURITY CHALLENGES

Congress: 4-6 July 2017 | Exhibition: 5-7 July 2017

Suntec Singapore Convention & Exhibition Centre

AN EVENT BY: INTERPOL

INTERPOL World 2017 Congress

Register now before 31 May 2017 to enjoy early bird rates

Shedding light on the "Dark side"– Cyberspace and the future of security

Prevention – Getting smarter, faster and more precise

Identity management and detection in a borderless world.

World Economic Forum (WEF) addresses cybercrime

WEF's 'Recommendations for Public-Private Partnership against Cybercrime' highlighted the need for information-sharing and cooperation platforms between businesses and law enforcement, with the INTERPOL Global Complex for Innovation (IGCI) in Singapore recognized as such a model.

A workshop dedicated to the implementation of the initiative's recommendations will be held in IGCI on 3 July, followed by a Dialogue on cybercrime on 4 July at INTERPOL World 2017 Congress.

INTERPOL World Dialogue, 4 July 2017 moderated by

Dr Jean-Luc Vez
Head of Public Security Policy and Security Affairs
Member of the Executive Committee
World Economic Forum

WORLD ECONOMIC FORUM

SPEAKERS INCLUDE

Arthur Holland Michel
Co-Director
Center for the Study of the Drone, Bard College

Christian Karam
Director and Global Head of Cyber Threat Intelligence
UBS AG

Dr John Coyne
Head of Border Security Program
Australian Strategic Policy Institute

Commander Jorge R. Rodriguez
Commander
Los Angeles Police Department

Michael Hershman
Group CEO
International Centre for Sport Security (ICSS)

Rob Leslie
Chief Executive Officer
Sedicii Innovations Limited

INTERPOL World 2017 Exhibition

EXHIBITION HIGHLIGHTS

- PUBLIC SAFETY TECHNOLOGIES
- BIOMETRICS
- IDENTITY SOLUTIONS
- FORENSICS AND INVESTIGATIONS
- CYBERCRIME

Register at **www.interpol-world.com** or contact us at **visitor@interpol-world.com**

EVENT OWNER: INTERPOL

SUPPORTED BY: Ministry of Home Affairs Singapore; World Economic Forum

INDUSTRY INSIGHTS BY: pwc

HELD IN: YourSingapore

MANAGED BY: ümp

Nation State Cyber Attacks Emerge from the Shadows

Leo Taddeo, CISO at Cyxtera Technologies

Nation-state hackers are increasingly targeting government agencies, critical infrastructure facilities, and businesses with powerful, sophisticated techniques that interrupt business operations, leak confidential information resulting in massive data and revenue loss.

Today, public and private organizations unwittingly leave sensitive, monetizable data, such as intellectual property (IP), unprotected, making cyberattacks a high stakes, low risk game for nation-states.

These groups can apply seemingly limitless time, money, and hacker talent to achieve their objectives, while cybersecurity professionals on the other side are challenged to deploy limited resources most efficiently.

Many mature cybersecurity programs use a risk-based approach to maximize security value for dollars spent. This requires an understanding of the adversaries targeting your networks and the data they seek. And if the last year provides any lessons, the top takeaway is that almost all executive communications have value for hackers.

For example, last year much of the news was dominated by reports of Russian agencies using cyber attacks to extract information to influence the U.S. presidential election. In June, the Washington Post reported that Russian government hackers penetrated the Democratic National Committee's network and gained access to the entire database of opposition research on GOP presidential candidate Donald Trump.

In December it was reported that Russian hackers tried to penetrate the computer networks of the Republican National Committee, using the same techniques. And just this month, we learned the Russians were again suspected of trying to influence the presidential election in France by leaking hacked emails.

As state-sponsored cyber attacks grow in scale, frequency and sophistication, understanding hacker motivations and capabilities is the first step towards a risk-based approach to mitigating threats.

'State-backed' cyber attacks rise

The fact that nation-states are actively deploying cyber weapons against commercial interest in the West has been well-known over the last decade in the law enforcement and intelligence communities.

In the last few years, state-sponsored cyber attacks have come out from the shadows. Companies of all sizes have found themselves face-to-face with military and intelligence agencies, without much protection from the government.

This has left them essentially alone to contend with the significant challenge of ensuring that they can detect and protect against such serious threats.

Russia and China are two of the most sophisticated players in this high stakes game. They deploy both custom, sophisticated malware as well as simpler, off-the-shelf tools to achieve their objectives. In many cases, the common element of the attack is the exploitation of the human element within an organization, which is increasingly growing more sophisticated and targeted.

Motivations

Let's look at the top two players. First, the Russians. While they remain committed to hacking business information that will assist their competitive standing in the world, their first priority is collecting military and diplomatic information. They have put significant talent and resources into targeting U.S. government networks to collect the kind of diplomatic information that gives them an advantage in negotiations or strategic decisions, to predict U.S. strategic positions and decisions.

For cybersecurity professionals, it is important to know what type of information is stored on or passing through your network. Media companies, academics, law firms, and companies that deal in strategic commodities are all potential targets. A risk-based approach will account for the threat and layer more advanced (and expensive) defenses around sensitive information.

In comparison, the primary objective of Chinese cyber collection capability is to enable State Owned Enterprises (SOEs) to compete and dominate in the global economy.

Cybersecurity professionals have noted an increasing number of network intrusions that result in exfiltration of business information, including IP and executive communications. That's a hallmark of Chinese hacking groups, particularly Group 61398, known for stealing trade secrets from companies such as Westinghouse and US Steel.

Group 61398's efforts to target technologies and information that advance China's strategic industrial sectors are emblematic of the Chinese hacking initiative. Cybersecurity analysts have directly correlated key industries China seeks to grow with the sectors they target with attacks.

It pays to understand what the Chinese are after, and develop a risk-based approach to protecting the information in your network that may be of value to a sophisticated economic adversary.

Are you ready for a "State-Sponsored Attack"?

One of the main challenges for organizations is moving from a perimeter-based strategy to a risk-based approach is a rapidly expanding, amorphous infrastructure.

Deploying a software defined perimeter (SDP) model to protect highly sensitive information, such as IP, contracts, business processes, and communications, can help meet these challenges by effectively making the infrastructure invisible.

For years many have argued that you can't secure what you can't see, however the reverse is also true - you can't hack what you can't see!

The approach is simple – provide access to the least amount of network-based resources for the least number of individuals, who are then granted the lowest level of privileges required to perform their job. Access privileges are set, defined and updated by user-centric policies, which leverage multiple aspects of server and user context, including device integrity as part of the authentication process.

About the Author

Leo Taddeo

Chief Information Security Officer, Cyxtera Technologies

Leo Taddeo is responsible for oversight of Cyxtera's global security operations, investigations and intelligence programs, crisis management, and business continuity processes. He provides deep domain insight into the techniques, tactics and procedures used by cybercriminals, to help Cyxtera continue to develop disruptive solutions that enable customers to defend against advanced threats and breaches.

Taddeo is the former Special Agent in Charge of the Special Operations/Cyber Division of the FBI's New York Office. In this role, he directed over 400 special agents and professional support personnel conducting cyber investigations, surveillance operations, information technology support, and crisis management. Previous responsibilities focused on FBI international operations, including service as a Section Chief in the International Operations Division, where he managed operations in Africa, Asia, and the Middle East.

Taddeo received a B.S. in applied physics in 1987 from Rensselaer Polytechnic Institute. After completing his studies, Taddeo served as a tank officer in the US Marine Corps. In 1991, he was awarded a Purple Heart and Bronze Star Medal for valor for his service in the Gulf War. Following his service, Taddeo earned a J.D. from St. John's University. Upon graduation, he joined the law firm of Mound, Cotton & Wollan in New York, where he practiced in the field of civil litigation until entering duty with the FBI.

Taddeo is a graduate of the CISO Executive Program at Carnegie Mellon University. He maintains the Certified Information Systems Security Professional (CISSP) and GIAC Certified Incident Handler certifications.

The Strategic CISO: Learning from the Masters of War

There are seven useful strands of military strategic thought useful for modern CISOs. The first is the importance of ensuring that CISO's objectives are always tied to the larger business objectives. The second is that adversaries will respond dynamically and often in unexpected ways to every action taken by defenders and the third that a defender must understand and focus on the right center of gravity. The fourth suggests that an indirect approach is often more fruitful than charging straight into every problem and the fifth principle of flexibility and resiliency is most often needed to enable that indirect approach. The sixth lesson from military strategy is on the importance for a CISO to understand both their actual situation and that of their adversaries as accurately as possible and the final seventh lesson is on the importance of measurements and metrics.

The Chief Information Security Officer or CISO is a relatively new phenomenon. In medium and large firms they have gone from almost unheard of in the early 2000's to very common in less than a decade.[1] While a CISO's role and scope of responsibility can vary from firm to firm, generally they are responsible for the defense of business and enterprise networks from attackers of all levels from unsophisticated attackers running tools or "script kiddies" up through nation state level attackers.[2] The responsibilities of a typical CISO have also started to expand to cover not just Information Technology (IT) but also Operational Technology (OT) as the importance and vulnerability of those systems has become more broadly understood.[3] CISOs most often come from an IT background as that is where the bulk of their responsibility has traditionally been. Because of their technological focus, CISOs are often admonished to be "strategic" instead of tactically focused on technology. But, what does it mean for a CISO to be strategic?

There are few words in the English language abused as often as "strategic."[4] Official definitions abound but for many people a "strategy" has become almost synonymous with a plan and is simply a concept of how something is to be accomplished. Military thinkers, on the other hand, have drawn a firm distinction between planning and strategy with strategy being more about the "why" and planning about the "how." Is there something for CISOs in the thousands of years of carefully recorded thinking about military strategy that would apply to their business focused strategies?

Physical warfare can be thought of as analogous to attacks in cyberspace since in both cases humans in conflict are at the heart of the matter. Accordingly, there are useful strands of strategic thought that can be extracted from military strategy and repurposed to great effect by modern CISOs. Before pulling out specific strands of use to CISOs, it is worthwhile to briefly look at some well-known concepts of what strategy is, and how those concepts might apply to the problems faced by a CISO.

Academics who study strategy and warfare like nothing more than to endlessly debate the definition of strategy, however, for a CISO, I think that Colin Gray's definition is the most useful when coupled with additional elements from J. C. Wylie. Gray's definition of strategy is essentially that it is the, "bridge that connects the worlds of policy and military power."[5] Good

strategy ensures that military force is applied in such a way as to further the political policy of the state.[6] This almost seems so obvious as to not be worth saying unless you consider any number of historical examples where military operations took precedence over policy with disastrous results for the nations involved.[7] When applied to a CISO, Gray's definition can be modified to state that a strategic CISO should be the bridge that connects the two worlds of business objectives and cybersecurity. Security should serve and enable business objectives, never the other way around. Wylie adds one useful element missing from Gray's definition when he adds that strategy should also include a systematic way to measure its success.[8] Defining the goals, ensuring they are achievable and time bound while developing the metrics to achieve them is a critical, but too often overlooked, aspect of organizational leadership.

Establishing what are often referred to as SMART goals is an essential element. SMART goals are Specific, Measurable, Attainable, Reportable and Time bound.[9] There are many benefits to specifying and defining strategic goals. Lower echelons of your organization are empowered to focus and organize their efforts to achieve the goals and prioritization becomes more achievable because the tradeoff decisions can be evaluated in terms of goal achievement. This is just as true of a CISO who should be able to determine if a given strategy is successful in supporting the business objectives and then have the ability to demonstrate that level of success to the leadership of the company.

While the basic concept of strategy is similar between modern business and traditional military strategy, is that as far as it goes? What can a long dead 19th century Prussian philosopher of war possibly have to say to a 21st century CISO that will be relevant and useful? Wherever people have fought, whether on land, sea, or air the heart of the matter has been humans in conflict who act, and react, in similar ways. As conflict has extended into space and cyberspace, that still appears to hold true. Carl von Clausewitz, the aforementioned 19th century Prussian, observed that war's, "grammar, indeed, may be its own, but not its logic."[10] An interesting development in cyberspace is that unlike the other domains, private companies have thus far been expected to largely defend themselves in cyberspace, whereas in the physical domains a business was not expected to defend itself from hostile aircraft or tanks.[11] Some similarity may be seen in merchant ships that were subject to attack, but in the modern era they were generally defended by military members put on board for that purpose.

In our systems of systems world, both national defense and private industry are arguably more codependent than ever before. Akin to the military protecting merchant vessels in WWII, civilian industries and transportation have become more dependent on systems that are vulnerable to cyber-attacks. Is there an emerging need to support and defend these vessels during times of high threat or known attacks? Or does private industry fend for themselves with the persistent cyber threats in the modern information age? Industry and military leaders are evaluating these questions and seeking the appropriate balance. The necessity of providing military protection to private industry was clearer in the industrial age such as the example of escorting merchant vessels in WWII, but the dependence of cyberspace challenges the historical approaches to these situations.

Military personnel don't defend factories and businesses in cyberspace, and today CISOs face increasingly dangerous threats. While everyone was paying attention to the Sony hack, which did create a great deal of media publicity, a potentially far more groundbreaking cyber-attack took place in Germany. In December of 2014 cyber attackers caused "massive physical damage" to a German steel mill through a social engineering attack that then bridged across to production systems.[12] These types of attacks cause physical damage similar to what aircraft bombs or dynamite from a saboteur would. The attacks on the Ukrainian power grid were another example of complex and high-level attacks where a business came under direct attack that had wide reaching physical effects.[13] These attacks are only the beginning, as the importance of cyber-physical systems increases in the often mentioned term "Internet of Things," the importance of attacks on those "things", whether or not they are traditional IT also increases. If CISOs are going to have to defend their business systems, not just from cyber-criminals, but also against nation state level cyber attackers, what can be learned from the traditions of military strategy?

Lesson 1: Operations Must Support Policy

The first major lesson from the great strategic theorists is the importance of ensuring that operations always serve the larger policy purpose. This is already evident from the definition of strategy given above by Gray.[14] Clausewitz famously stated that war is a, "continuation of policy with other means."[15] Security should be a continuation of business of objectives and security for its own sake makes no more sense to a business than battles fought with no connection to a the overall policy objective of a nation. Of course, the policy objectives of business generally revolve around profit, although long term profitability vice short term profit is normally a wiser objective. It may help the balance sheet in the short term to cheat on environmental regulations, but the hit on long term profitability when the cheating is discovered will normally be much larger than the short term boost. For the CISO, staying connected to business objectives often involves finding the right balance of security, functionality, and finance.

Finding the right level of security that protects the business, while enabling connectivity and the pursuit of business objectives is one of the most difficult challenges faced by a CISO. The default answer for most security professionals when confronted by a threat is "lock it down" but that is often unacceptable to functional business units trying to accomplish their tasks. Communication is risky, but it is also the whole point of most business systems.16 "Vulnerabilities" are often inherent in the design of systems whose purpose is communication and closing them down can have significant negative effects.[17] Of course, CISOs can fail just as easily by leaving systems too open, finding the right balance and ways to be secure while still enabling business processes is the key.

Furthermore, every person with access to the network must become the equivalent of sentries who are trained to identify the threats and take immediate action to minimize them. Individuals must become trained to identify threats such as phishing as well as behavior that inadvertently introduce threats to systems. Sometimes plugging in a phone to the network with the intent only to charge the device could potentially introduce malware that could compromise critical systems. Strategic CISOs must ensure training and education are part of their plans. The first point of connecting tactical actions to business objectives is well understood but is important

enough as to be worth repeating anyway, unfortunately the next lesson from the strategic masters is far less widely understood.

Lesson 2: Action and Reaction

CISOs should never forget that they contest continually with active and maneuvering enemies who will react to every move and countermove. It is a well-known military truism that, "the enemy gets a vote" which is to say that the enemy will react to whatever a combatant does, often in unexpected ways. Clausewitz said this more elegantly when he compared war between nations to a wrestling match with each wrestler constantly reacting to what the other wrestler is doing in a continuous interaction.[18] Edward Luttwak takes this concept even further and states that the entire realm of strategy is driven by this interaction which generates a paradoxical logic where combatants often get the opposite of whatever they are seeking due to the enemy's response.[19]

Further, once malicious code is released and detected, the defended organization will likely remediate the threat quickly. After an attack is detected, the defender can perform forensics on the malicious code and then modify their own systems as required to counter it.

Once the attacker determines that they have been detected, they will respond by changing the nature of their attack. This maneuver dynamic makes responding to a cyber-attacker very different from responding to a natural disaster. An earthquake or hurricane may do tremendous damage, but it isn't trying to defeat your defenses, it just is what it is and would be the same if your facility happened to be in the way or not. Natural disasters are mitigated through good risk management and engineering, but some of that methodology breaks down with cyber attackers. The odds of a hurricane striking a particular area can be well modeled using probabilistic methods, not so for a cyber-attacker who is responding to incentives and countering what the defender is doing. Closely monitoring an incoming hurricane does nothing to change its trajectory, closely monitoring your IP space and attackers trying to get in, will change a cyber-attacker's trajectory.

Vulnerabilities in IT systems represent opportunities for the enemy to inflict their desired effects on your systems. Both hardware and software added or altered in your system environment introduces additional potential vulnerabilities. Routine updates to your software as well as adding even simple devices such as mice, keyboards, printers etc., all add potential new security weaknesses that attackers can exploit. There are also always "zero day" or unknown vulnerabilities that exist in every system. The number of potential vulnerabilities in just IT systems is overwhelming, when you consider Operational Technology (OT) systems such as water treatment, electrical power generation, or production systems, the enormity of the problem becomes hard to even grasp. The bottom line is that a determined and competent attacker will eventually be able to find an opportunity to enter and create their desired effects.

Enemy forces will be able to maneuver and evaluate opportunities, but CISOs should never forget that they can maneuver as well. Because modern cyber maneuver represent largely keystrokes versus large personnel and equipment movement, attackers are agile in their ability

to quickly probe and pursue targets. CISOs need to be able to respond quickly by monitoring their systems to detect and react to intruders in real time. Attackers use automated systems to rapidly search for vulnerabilities, defenders can use automated detection systems to determine that scanning is underway and dynamically adjust their environment to confound scanning. A continuing issue is that many organizations do not establish software lifecycle programs to deal with software that is no longer supported. Most of these systems' vulnerabilities are no longer patched which makes them static targets that can no longer easily maneuver which often leaves these systems open to easy compromise. Because threats are so dynamic, CISOs have to be very agile and dynamic as well.

Lesson 3: Identify the Correct Center of Gravity

The next major lesson from classical military theorists for a modern CISO is the importance of focusing on the correct center of gravity. In cyberspace terms, this center of gravity is also often referred to as cyberspace key terrain. There are many thousands of devices on any medium sized network, which ones does a CISO pay attention to first? There are always limited resources so prioritization is a key question for any CISO. Clausewitz identified the center of gravity as the, "hub of all power and movement" which is notoriously difficult to understand and apply to a practical situation.[20] For a CISO, their center of gravity should encompass only the most critical business systems and what those systems are will depend on the nature of the business and the strategy of the firm. As a simple example, for a bank, e-mail servers are presumably of far less importance to the survival of the bank than the systems that transfer money. For a major manufacturing firm the cyber key terrain might be the computer systems controlling manufacturing.

There are several key characteristics of cyber key terrain that are worth exploring. One factor is that cyber key terrain can change very quickly. Gregory Rattray identified that the geography of cyberspace is extremely mutable and the cyberspace equivalents of mountains and oceans can be shifted, deleted, or inserted with the flick of a switch.[21] However, cyberspace is not endlessly mutable as it is tied to the physical world. The physical devices that create cyberspace matter, and defending them is a critical element of an effective defense in depth.[22] Many a CISO has learned this the hard way when an attacker gains physical access to inadequately protected hardware or someone with a backhoe digging a trench accidentally takes down a critical data center.

Both the physical and virtual portions of cyberspace matter and should be mapped to a comprehensive enterprise architecture if it is going to be defended properly. A good enterprise architecture is the first step, but if a CISO is going to identify what is truly critical, they will have to also do a mission analysis of what elements are most important to the organization.

There are numerous methodologies that enable this type of analysis available from numerous organizations and it is hard work to sort out, but absolutely imperative if a CISO is going to understand their center of gravity and cyber key terrain.

Lesson 4: Use an Indirect Approach

The fourth major lesson for CISOs from the world of military strategy is not to take on every challenge head on. Often a more indirect approach that comes at a problem from the side is far more effective and less costly. In military terms, often that maneuver is literally to the side as in a flanking maneuver that goes around a strong enemy defense to attack from a much weaker point at the side or rear. One of the strongest proponents of this approach was Sir Basil Liddell Hart who wrote at great length about the indirect approach and also emphasized the psychological versus just the physical element of coming at the enemy in an unexpected way.[23] A CISO will not normally be physically moving to the side of an attacker, but can surprise them by having unexpected defenses or monitoring in place.

The Chinese strategist Sun Tzu placed a heavy emphasis on trying to deceive your foes to bait and lure them.[24] A modern CISO can accomplish much the same with honey nets, virtualization, and software defined networking among other techniques. It does take more than technology; to deceive an attacker, a defender must understand what the defender expects to see and feed those expectations.[25] If an attacker is occupied by attacking systems that are not really there, it is relatively easy to understand and contain them.

A CISO can also do more than build honey nets, a CISO controls the physical hardware and architecture and so can deliberately create a geography and environment hostile to attackers. Miyamoto Musashi, a famous Japanese Samurai, advised that a warrior should strive to force the enemy into inconvenient situations.[26] A CISO can accomplish this in cyberspace by architecting business systems so they allow necessary business functions while making life extremely difficult for attackers, even once they penetrate the outer defenses. There are many promising technologies and approaches on the horizon that can accomplish this from a technical perspective.

Lesson 5: Flexibility and Resiliency Often Bring Success

A fifth major lesson for CISOs from military strategy is the importance of flexibility and resiliency. Flexible forces are required if a CISO is going to be able to respond dynamically to an attacker much like a defender on the ground in a combat situation must be able to rapidly shift forces from point to point to respond to different enemy probes and attacks. Sun Tzu went so far as to state that a commander should have normal and exceptional forces that can change roles in the middle of a battle from fixing an enemy force to maneuvering and vice versa.[27] For a CISO this could involve personnel who can transition to different roles as crises and attacks develop.

Critical systems must be evolved and developed to “know” when they are in a secure state, and when they are not. This is being done today by establishing a baseline for the system that is monitored and alerts when the state is altered.

By building a dynamic ability to perform root cause analysis of what has caused the deviation, systems will be able to potentially suspend activities for a time and return itself to the secure baseline. The result of the analysis would be fed to an intelligence center for analysis and subsequent action for other systems if required.

Lesson 6: Know Your Enemy and Know Yourself

The sixth thing that a CISO can learn from military strategy is the importance of intelligence. Sun Tzu focused extensively on intelligence and famously stated that if you, "Know the enemy and know yourself; in a hundred battles you will never be in peril."[28] For a CISO, knowing yourself starts with enterprise architecture and mission analysis, knowing the enemy involves staying up to date on what the threats to the organization are doing. Most CISOs do not have the resources to engage in serious intelligence work so this is an area where hiring this role out to one of the firms that specializes in this work can be very helpful. CISO's should not just care about what is being said on the dark web about who is thinking about attacking who, but should seek out the latest technical based intelligence and profiles that may not have made it into commercial signature based scanners yet.

Dynamic cyber intelligence collection has become paramount. Microsoft has adopted this concept and receives notifications from their operating systems when they detect new potential threats. Defense and intelligence organizations should develop a joint center with partnerships of private companies to protect the critical systems and government policy is clearly headed in this direction. Strategic CISOs across various organizations should partner to build a security council and sponsor joint capabilities where that makes sense for their business. Most organizations agree that you must understand your threat. With the cyber threat becoming so dynamic and persistent, more partnership to collect the threat and intelligence data is important and becoming more so every day. The cyber intelligence center would both collect and disseminate information to trusted organizations with a need to know to include private industry. Both software and hardware manufacturers would be potential recipients of some of the collective intelligence.

Lesson 7: You get what you Measure so Choose Wisely

A final major lesson from military strategy is the importance of measurement and assessment; without it a combatant or CISO has no idea if what they are doing is moving them closer to their desired end state. J.C. Wylie rightly tied measurement to the heart of strategy and included a system of measures at its center. It is discouraging to see how many organizations do not even routinely count and track the number of patches that have not been applied and report the results to senior management. These are very easy and basic measurements readily available to any CISO, but they are not necessarily the best measurements available.

Metrics should always link back to the business mission and the easiest things to measure may not be the most important things. It has long been understood that measurement influences behavior and in business. Just as in quantum physics, the presence of an observer will alter reality. If the key security metric reported to management is the percentage of systems that are fully patched, an organization may have very well patched systems, but are they secure? And what does "secure" mean anyway within the context of the business mission and objectives? The U.S. military tries to address these issues by having two different types of metrics, Measures of Performance (MOP) and Measures of Effectiveness (MOE). An MOP measures how well a task is being accomplished while an MOE measures how close the organization is to its desired objectives.[29] An example of a MOP might be the percentage of IT systems that are

fully patched, while an MOE might be how well protected the company's Intellectual Property (IP) is. MOP tend to be much more specific and under the control of the CISO while MOE are harder to measure but are the measurements that really matter. Good MOP's will contribute to MOE's but it is always tempting for CISOs to measure the things that are easy to measure vice the important things. Patching systems is a good thing, but does not guarantee that IP is protected, numerous other things will need to be done as well. The mission analysis done to identify cyber key terrain will help guide the development of meaningful MOEs that can help a CISO understand how well they are doing in a similar way to military strategists.

There are seven useful strands of strategic thought that can be extracted from military strategy and repurposed to great effect by modern CISOs. That there are so many useful lessons applicable to CISOs should not be that surprising; cyberspace attacks on businesses are similar to physical warfare because in both cases humans in conflict are at the heart of the matter and this human dynamic has great impact. The first lesson that CISOs can pull from the strategic theorists is the importance of ensuring that their objectives are always tied to the larger business objectives and that security for its own sake should never be pursued. The second lesson is that the adversaries attempting to attack or disrupt business systems will respond dynamically and often in unexpected ways to every action taken by defenders.

This dynamic maneuvering is available to defenders as well who need to be agile and responsive while defending the most important cyber terrain that should be identified via the third lesson that a defender must understand and focus on the right center of gravity. The fourth lesson suggests that an indirect approach is often more fruitful than charging straight into every problem and the fifth principle of flexibility and resiliency is most often needed to enable that indirect approach. The sixth lesson from military strategy is on the importance for a CISO to understand both their actual situation and that of their adversaries as accurately as possible and the final seventh lesson is on the importance of measurements and metrics. An organization will normally get more of whatever it values and measures so it is critical that a CISO measure the right things that lead to the desired objectives and end state. All of these seven principles and lessons can help a CISO be more effective in the fast moving and technologically grounded world of today's organizations, and when the principles are combined, the synergy amongst them is even more powerful.

[1] Todd Fitzgerald and Micki Drause, ed. "What You Told Us: A CISO Survey" in *CISO Leadership: Essential Principles for Success*, (Amazon: Auerbach Publications, 2008), 3.
[2] William D. Bryant, *International Conflict and Cyberspace Superiority: Theory and Practice* (London: Routledge, 2015), 208-210.
[3] A good definition of OT is, "hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices, processes and events in the enterprise." Gartner, "Operational Technology (OT)" Gartner, http://www.gartner.com/it-glossary/operational-technology-ot.
[4] The top definition from Merriam-Webster is, "of or relating to a general plan that is created to achieve a goal in war, politics, etc., usually over a long period of time." Merriam-Webster Dictionary, "strategic" Merriam-Webster, Incorporated. http://www.merriam-webster.com/dictionary/strategic. That type of definition is very broad and not very specific.

[5] Colin S. Gray, *Fighting Talk: Forty Maxims on War, Peace, and Strategy* (London: Praeger Security International, 2009), 48.
[6] Carl von Clausewitz, *On War*, ed. and trans. by Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1976), 579.
[7] A classic example can be seen in Germany's performance in World War II. Throughout the war, German tactical and operational art was generally very good, but it was coupled with strategic blunders such as attacking Russia while England was still fighting that made it nearly impossible for them to win. Another example of a brilliant operational success that produced strategic failure was the Japanese attack on Pearl Harbor, where the very success of the attack doomed Japan to strategic failure as it hardened the resolve of the United States and made it impossible to achieve the negotiated settlement that was the Japanese policy objective.
[8] J. C. Wylie, *Military Strategy: A General Theory of Power Control* (New Brunswick, N.J.: Rutgers University Press, 1967), 13.
[9] Jacob Gudger, *SMART Goals: The Ultimate Goal Setting Guide*, Kindle Edition, 2011, 14-30.
[10] Clausewitz, *On War*, 605.
[11] Paul Rosenzweig, *Cyber Warfare: How Conflicts in Cyberspace are Challenging America and Changing the World* (Santa Barbara, CA: Praeger, 2013), Kindle Location 3660.
[12] Robert M. Lee, Michael J. Assante and Tim Conway, *German Steel Mill Cyber Attack*, SANS ICS Defense Use Case (Washington D.C.: SANS, 30 December 2014,) 1.
[13] Robert M. Lee, Michael J. Assante and Tim Conway, *Analysis of the Cyber Attack on the Ukrainian Power Grid*, SANS TLP: White Report (Washington D.C.: SANS, 2016,) 20.
[14] Gray, *Fighting Talk*, 48.
[15] Clausewitz, 69.
[16] Majory S.Blumenthal and David D. Clark, "The Future of the Internet and Cyberpower." In *Cyberpower and National Security*, edited by Franklin D. Kramer, Stuart H. Starr and Larry K. Wentz, 206-240. (Washington, DC: Potomac Books, 2009), 229.
[17] Rosenzweig, Kindle location 441.
[18] Clausewitz, 75.
[19] Edward N. Luttwak, *Strategy: The Logic of War and Peace* (Cambridge, MA: Belknap Press, 2003), 2.
[20] Clausewitz, 595.
[21] Gregory J. Rattray, "An Environmental Approach to Understanding Cyberpower." In *Cyberpower and National Security*, edited by Franklin D. Kramer, Stuart H. Starr and Larry K. Wentz, 253-274. (Washington, DC: Potomac Books, 2009), 256.
[22] Martin C. Libicki, *Conquest in Cyberspace: National Security and Information Warfare* (Cambridge: Cambridge University Press, 2007), 66.
[23] B. H. Liddell Hart, *Strategy* 2nd ed., (New York: Penguin Books, 1967), 5.
[24] Sun Tzu. *The Art of War* Trans by Samuel B. Griffith with Forward by B. H. Liddell Hart. (Oxford University Press: Oxford, 1971), 66.
[25] Gray, 35.
[26] Miyamoto Musashi, *The Book of Five Rings* (Start Publishing LLC: Amazon Kindle, 2012), Kindle Location 797.
[27] Sun Tzu, 91.
[28] Sun Tzu, 83.
[29] Department of Defense, *Joint Publication 5-0*, 11 August 2011, D-3.

New Year New Techniques to Prevent Your Website from Hackers

When your website goes live, you are opening the doors to customers as well as hackers. The internet, though very useful in most instances, can bring in people with malicious intent. These hackers are often intelligent enough to outsmart any basic techniques which you may be using to protect your website. This is why it is imperative that you have the proper locks which protect and safeguard your valuable information and data.

Because hackers are invisible and generally very quick, you won't have the time to catch them in the act. And if you fail to integrate these new techniques, these electronic thieves will be able to get away with the details of your customer's accounts like credit card information or get away with confidential data which you don't want to reveal.

Moreover, remember that theft may not always be the reason behind the actions of a hacker. Some of them simply want to create destruction and chaos and in such a situation, they won't just destroy company and business records but can also hamper your reputation with your clients by sending them malicious emails and messages.

This is why it is necessary that you take some steps to prevent the damage that a hacker can cause. Remember that though even basic protection will discourage amateur hackers, it is a good idea to keep yourself prepared with the big guns if someone is really out to get you.

So, don't let all your hard work go to waste and integrate these fool-proof techniques to protect your website and business from potential hackers. Though there are many other methods you can try out, these are some of the tried and tested ones which provide a higher level of protection than your basic security.

Be Careful About Admin Access

One of the easiest ways for a hacker to get into your website is through the admin level. This gives the hackers easy access to your files which they can manipulate. To toughen up and protect this control, make sure you have a strong password which can't be guessed. Also, limit the number of times you or anyone else with access can login within a specific time.

You should also look into hiding your admin pages because if they aren't indexed by search engines, they'll be much harder to find and manipulate. Finally, if you are sharing the admin access, make sure you don't send details through email because hackers can easily gain access to these accounts.

Update Software Regularly

Though we are all very aware of the risks of keeping our website unprotected, most companies fail to realize the importance of keeping their software updated. Most companies do it only when necessary and this ends up costing them a lot more than if they would've taken the right step and updated. Those these updates do cost money, they save you from hassle.

Delaying updates, especially when there is a security vulnerability will expose you to an attack which could have been prevented. Remember, hackers spend days and browse thousands of websites looking for weaknesses that'll allow them to attack and damage your website. Updating software regularly will give you an extra shield and may even end up being the reason why your website wasn't hacked.

Invest in a Web Application Firewall

WAF or a web application firewall is a software or hardware which is set between the server of your website and the data connection. What makes it valuable for you, especially in terms of protection is that it reads every single bit of data which passes through the portal. Though these web types of firewalls will cost you, they can provide an added level of security.

You can find these applications in cloud form or as a plug-and-play service which can be used for a monthly fee. Once the WAF is installed, it will block all attempts of hacking also help you filter out spammers and bad bots. This is one of the best options which you should start exploring especially if you have a website which has a lot of competition.

Limit Uploads

If you aren't new to the industry and the internet, you already know that file uploads are probably the first culprit when it comes to hacking. It doesn't matter how thoroughly your website checks out the system because very secretly hidden bugs can still come through and allow a hacker to damage your website's data. If you run a website where uploads cannot be stopped completely, you should prevent direct access to the files and store them outside the main directory to avoid bugs from getting inside.

If you aren't sure how you can make this happen, you can always ask your web host to help you set this up. Doing this will give you a considerable amount of protection so don't make the mistake of skipping this valuable technique.

Backup Everything

Much like you need to update your system software regularly, you must also make sure that you backup every frequently. This is important because sometimes, even the toughest security measures can't stop adamant hackers and this is when you need be sure that everything is backed up.

Your backup should be so aggressive that every time a user saves something on the website, it is automatically saved on multiple platforms. The best policy is to backup several times a day because if you are saving once a day, you will lose data when the hard drive fails.

Changing passwords and logins regularly and using HTTPS are some other ways you can protect your website from malicious hackers. All the techniques discussed here will help you go a long way in protecting your website, so don't forget to apply and integrate them immediately if you plan on making your website live soon. However, remember that some threats are inevitable and if you do get a breach, acting quickly is one of the first things which will stop further damage.

PERCEPTION MEETS REALITY: COMBINING TECHNOLOGY AND TRAINING TO CREATE A MORE RELIABLE CYBERSECURITY SYSTEM

LESSONS LEARNED FROM THE US DEPARTMENT OF DEFENSE

By Bob Heckman, Vice President and Chief Information Security Officer, Cybersecurity Center of Excellence, Criterion Systems, Inc.

In recent years, IT executives have justified and received capital funding from their boards to purchase a plethora of cybersecurity products promising to be the silver bullet that will solve all their security-related problems. One look at the 2017 RSA Conference list of exhibitors and sponsors reveals thousands of companies offering products and services from access control, anti-malware, anti-spam, and firewalls, to analytics, intelligence, response, application security, and how to secure the Internet of Things (IoT).

Given this wealth of solutions, it is not surprising that a recent report and accompanying panel at that conference unveiled a substantial difference in how confident IT executives are in their current cybersecurity defenses (high) versus how effective those defenses actually are (they are, in fact, struggling to keep up).

From the IT executive's perspective, they have invested a substantial amount of money acquiring technology to enhance the organization's cybersecurity defenses, thus ensuring their security. Unfortunately, there are no silver bullets, and adding even more technology is not the solution. This is also a people problem. For one, most organizations lack the qualified and experienced cybersecurity resources necessary to effectively manage their security infrastructures.

It's like purchasing a very expensive Formula One (or NASCAR) race car and not having a mechanic to maintain it or driver to race it. While there is a vigorous debate in the industry on the subject, the current perception is that a shortage of qualified cybersecurity resources is impacting all aspects of the industry.

A second "people-related" factor compounding the issue of weak defenses is that most organizational workforces don't understand or abide by a corporate culture of cybersecurity. There is a funny quote making the rounds on the Internet, attributed to Einstein, "Two things are infinite: the universe and human stupidity; and I'm not sure about the universe!" This explains why phishing remains a major problem for organizations. What, then, can IT executives do to address the perceived shortage of cybersecurity talent and encourage their employees to be more cybersecurity conscious? These two problems need to be solved in concert, and the US Department of Defense has made a good start in doing so.

A Holistic Approach to Cybersecurity: Bringing Together Technology and Training

Department of Defense (DoD) security education, training, and certification programs, including cyber awareness training, have been in place for years. Every military member, government civilian employee, and contractor must complete annual security awareness training to continue being granted access to DoD systems and networks.

There are a variety of mediums available for individuals to receive training; one of the more recent approaches is the DoD Cyber Awareness Challenge offered online to DoD employees. Everyone is required to take the Challenge and must pass an exam at the end in order to meet their annual training requirement.

In addition, through the implementation of the DoD 8570.01-M Directive in 2005, the Department established an Information Assurance Workforce Improvement Program that provides guidance for the identification and categorization of positions and certification of personnel conducting Information Assurance (IA) functions within the DoD workforce supporting the DoD Global Information Grid (GIG). This program includes a list of DoD-approved IA baseline certifications aligned to each category and level of the IA workforce.

Personnel performing IA functions must obtain one of the certifications required for their position, category/specialty, and level. This program has been augmented by DoD Directive 8140, Cyberspace Workforce Management, which unifies the overall cyberspace workforce and establishes specific workforce elements (cyberspace effects, cybersecurity, and cyberspace information technology (IT)) to align, manage, and standardize cyberspace work roles, baseline qualifications, and training requirements.

With these programs, the DoD maintains a total force management perspective to provide qualified cyberspace government civilian, military, and contractor personnel to identified and authorized positions. These personnel function as an integrated workforce with complementary skill sets, and provide an agile, flexible response to DoD requirements. Although the DoD is not perfect, the combination of these initiatives has improved the Department's culture of cybersecurity and demonstrably reduced the impact of the human stupidity factor.

From providing average employees with cyber awareness training to delivering sophisticated specialized training (Bootcamps, SANS, CompTIA, ISC2, etc.) to Computer Network Defense Service Provider (CNDSP) Cyber Operators, their efforts have helped mature DoD's cyberspace workforce.

Commercial companies can apply DoD's approach and lessons-learned to enable or fast-track their cyber awareness and workforce improvement initiatives. It is important to establish a true culture of cybersecurity, and this needs to be driven from company leadership throughout the organization.

Instilling a culture of cybersecurity will also entail proper training for all employees, not just IT and security staff. It's important to note that DoD's requirements are applicable to contractors. This raises another concern for IT executives working for a commercial company: Does your organization hold the independent contractors providing services to your company to the same standards as your own employees? Are they forced to comply and meet the same cyber requirements and security awareness standards?

Improving Employee Security Awareness: An Example.

Let's revisit the problem of phishing. Several cost-effective tools exist today that allow you to routinely phish everyone within your organization. Conducting phishing campaigns against your own employees – and contractors -- will allow you to consistently reinforce the importance of security by educating the right people at the right time and by applying targeted training that changes employee behavior.

As phishing attacks become increasingly sophisticated and highly targeted, an anti-phishing program is a good first step – but that is all it is. It should be coupled with training on how to prevent phishing attacks and the mandatory reporting of suspected phishing emails to your security team. To be effective, anti-phishing learning objectives must be part of your overall security awareness training program.

You can then benchmark your phishing results, identify and track your repeat offenders for additional training, and demonstrate the impact of your awareness training with detailed metrics on risk exposure. Reporting capabilities from these tools will allow you to identify susceptible users by tracking individual behavior, system information, and other related data, and then determine future assessment and targeted training needs.

Solving the Cybersecurity Skills Gap: Some Proposals

In addition to adopting DoD's approach to cyberspace workforce management, here are a few proposals for addressing the cybersecurity talent shortage and ensuring you have the qualified and experienced resources necessary to effectively manage your security infrastructure and program. They include organic efforts like:

- Improved education and training, e.g., the implementation and funding of a corporate continuous education program;
- Innovative hiring, e.g., encouraging individuals in other departments to pursue cybersecurity careers even if their primary tech specialty lies somewhere else; and,
- Investment in existing IT teams to help solve the skills gap.

Another way to address the skills shortage is through outsourcing, primarily for areas that are easily automated. For example, tier-1 24x7x365 glass watching (a.k.a. network monitoring and notification) is a function that could probably be outsourced.

From an overall cybersecurity community perspective, spending more on education, promoting gaming and technology exercises, and pushing for more practical learning via hands-on cybersecurity programs in trade schools would better prepare our kids for the real world. Computer science and cyber-related curriculum should be taught in middle-school and high-school to pique their interest in this exciting field.

In one good example, Carnegie Mellon University's CyLab hosts a virtual capture-the-flag competition called picoCTF that is teaching middle- and high-school students the basics of hacking. Participants learn to reverse engineer, break, hack, decrypt – anything necessary -- to solve a series of challenges centered around a storyline.

Challenges start out easy and become increasingly difficult, helping to develop the participants' critical thinking skills and uncover their hidden talents. Also, enhancing and increasing the number of cyber programs within higher education and creating clear paths from undergraduate to graduate school cyber degrees – and promoting them so students actually know they exist – would be a huge help.

None of this will be easy, nor inexpensive. Recent reports have demonstrated that most IT executives simply don't have time to implement a holistic innovative cyberspace workforce management program given day-to-day tasks.

Their leadership does not allocate sufficient funds for security training efforts and their corporate culture is simply not change-oriented . Regarding the longer-term proposals around education mentioned above, we all know the current pitiful state of education funding and the challenges associated with education reform. But the status quo simply cannot continue; the stakes are too high.

To be successful in getting the time and money they need, IT executives must show their project's impact and delivered value to the organization. By using Return-on-Investment (ROI)-backed innovation techniques, they should demonstrate how not doing something about the problem could have severe consequences.

To revisit our example, a successful phishing attack could result in:

- loss of competitive advantage and financial stability due to theft of sensitive information such as intellectual property, trade secrets, or research data;

- reputational damage as compromised accounts can be used to target individuals or other organizations;

- disruption of business operations due to the confidentially, integrity, and availability of data being compromised; and

- significant financial costs relating to the investigation, response, and recovery from a potential compromise or incident.

Conclusion

Today's problems in cybersecurity cannot be addressed by technology alone. Organizations must also address two key "people-related" problems in concert: recruiting and retaining cybersecurity talent and creating an effective culture of cybersecurity in their workforce. The Department of Defense has made some important headway in this holistic approach to cybersecurity, and commercial companies can learn from these experiences.

Hands-on learning, for both IT and general workforce members is critical. Ideally, this kind of education will start early in a child's education. As we have seen, there is no silver bullet that will solve the cybersecurity problem; it is going to take time and financial investment. However, the stakes are too high if we don't make these changes: companies will be attacked and will collapse.

Using ROI-based innovation techniques and combining technology with training to improve your cybersecurity infrastructure management will help companies more quickly bring the reality of their cybersecurity program's effectiveness into alignment with their perception of its strength.

About the Author

Mr. Heckman is the Vice President and Chief Information Security Officer (CISO) for Criterion Systems. As the lead for Criterions Cyber Security Center of Excellence (COE), he is responsible for the operation of the company's strategic and comprehensive information security program that defines, develops, maintains, and implements policies and processes that enable consistent, effective information security practices which minimize risk and ensure the integrity, confidentiality, and availability of information that is owned, controlled and processed by the organization. He monitors the external threat environment for emerging threats, and advises relevant stakeholders on the appropriate courses of action. Mr. Heckman liaises with external agencies, such as law enforcement and other advisory bodies as necessary, to ensure that the organization maintains a strong security posture.

Bob can be reached online at Bob.Heckman@Criterion-sys.com, at his LinkedIN profile: https://www.linkedin.com/in/bobheckman/ and at our company website http://www.criterion-sys.com.

Defense Strategies Institute's 4th Annual

MOBILE SECURITY FOR DEFENSE AND GOVERNMENT SUMMIT

FREE for Military and Government Attendees

JUNE 7 & 8, 2017 | ALEXANDRIA, VA

Summit Speakers Include:

- Mr. Gary Wang, Deputy CIO, HQDA Chief Information Officer / G-6, US Armyg Security and Innovation for the Mobile Ecosystem
- Mr. Bill Marion, SES, Deputy Chief, Information Dominance & DCIO, US Air Force
- Mr. Frontis B. Wiggins, SES, Chief Information Officer, US Department of State
- Mr. Manish Patel, CIO, PEO EIS, US Army
- Mr. Jacob Marcellus, Acting Mobility Portfolio Manager, DISA
- CAPT Michael Dickey, Commander, C4ITSC, USCG

To Register, Download Agenda & Learn More Visit

MOBILESECURITY.DSIGROUP.ORG

The mighty have fallen: how even the unlikeliest targets are going down to DDoS attacks

Informative sources on distributed denial of service (DDoS) attacks will often include at least one warning that nearly every website on the internet is a potential target.

With the current ubiquity of DDoS attacks this is not a needlessly dire warning.

Nearly every website *is* a potential target.

Yet there is a certain subset of website owners that might just assume these warnings don't apply to them because their internet technology and online security knowledge is so far above that of the average website owner.

Relatedly, there is also a certain subset of website owners that might just end up tremendously embarrassed when their websites go down to distributed denial of service attacks despite that impressive knowledge.

Widely distributed attacks

DDoS attacks are used to either slow a target website down to the point that it is no longer usable, or take the target offline altogether.

Either way the end result of a successful attack is the same: the legitimate users of the website are denied its services while the attack is ongoing.

DDoS attacks are made possible by botnets, which are networks of internet-connected devices that have been infected by malware in order to allow attackers to control them remotely.

Using the firepower of all these infected devices, the attacker can overwhelm the resources or use up the bandwidth of the target website.

These attacks have been an issue for websites and businesses for over 15 years and the issue is only getting bigger thanks to innovations like DDoS for hire services, DDoS ransom notes and massive Internet of Things (IoT) botnets.

Successful attacks can now cost larger organizations anywhere from $20,000 and $100,000 per hour, and that isn't factoring in the costs associated with the software damage that can accompany the attacks, the data breaches that can occur while DDoS attacks are used as a smokescreen, and the loss of user trust and loyalty that so often stems from DDoS-caused outages.

Even the experts

The past six months have seen a series of high-profile distributed denial of service attacks dominate headlines, not only because of the size of the attacks and the extent of their damage but because of the websites that have been targeted.

First up was Brian Krebs, a renowned internet security blogger who has made his career breaking stories on data breaches, online fraud and hackings.

His website was among the first major victims of the massive Mirai botnet, powered by hundreds of thousands of IoT devices.

In the face of what was then the biggest DDoS attack in history, weighing in at 600 Gbps, Krebs' website went down for days, and his hosting company revoked their services as a result of the attack.

Soon after the Krebs attack, the Mirai botnet struck again in a major way, taking down DNS provider Dyn with a reported 1 Tbps attack.

As a result of this attack, internet giants Netflix, PayPal, Twitter and Spotify, among many others, disappeared from the internet for hours despite presumably having top of the line security measures implemented.

Another unlikely target buckled under a DDoS attack in February when Stack Overflow, the internet's biggest question and answer site for programmers and a favorite of tech experts the

world over, was taken down on a Monday.

Amusingly enough, a search on the Stack Overflow site for DDoS-related topics turns up a page in which a question asking for information on the best way to protect against DDoS attacks was closed for being off-topic.

The only specifics released in regards to the attack have come from Stack Overflow's site reliability engineer Nick Craver, who reported that the site was receiving 40,000-50,000 requests per second for six plus hours.

The requests apparently came from a botnet made up of compromised webcams, CCTV and DVRs – likely one of the absurdly sized IoT botnets currently dominating the DDoS landscape.

Craver indicated that neither he nor the rest of the Stack Overflow team would be forthcoming with more information on the botnet behind the attack, stating that the secrecy was for the greater good as some of the efforts being made to stop such botnets cannot be publicly discussed for legal and privacy reasons.

Getting on-topic

It may have been off-topic for Stack Overflow, but it's on-topic here: the best way to protect against distributed denial of service attacks is by investing in professional DDoS mitigation.

Cloud-based protection provides scalable mitigation for websites and organizations of all sizes, protecting effectively against network layer, application layer and protocol attacks by inspecting traffic at a granular level in order to keep malicious traffic from reaching the protected website's network while allowing legitimate traffic through to the website uninhibited, even during an attack.

As the high-profile attacks of the last six months have shown us, not only is there no shame in needing professional DDoS protection, there might just be some shame in not having adequate DDoS protection. Everyone is a target, no matter how unlikely it may seem.

About the Author

Anna Jones is an experienced freelance writer specializing in the latest cyber security trends and news. She is keen to share her knowledge and expertise in the field and loves taking on a writing challenge!

Illuminating Innovation: A Roadmap for Incubating and Advancing Technologies

It is said that necessity is the mother of invention, and it's true that good ideas are often born as a response to opportunities for improvement, or when there is a stark necessity.

Far too often however, the cost, time and effort required to develop, test and implement those new ideas or innovations are outside the capabilities of an organization.

As a result, those freshly born ideas, however revolutionary and regardless of potential, don't get the opportunity to advance.

In terms of technology, this is an especially acute problem, with the result being that many software applications, platforms, and solutions remain void of the innovation needed to catapult them to the next level of performance.

Even research labs, which are a natural hotbed for idea creation, often lack the ability to capitalize on many of the innovative products and services they create. Many wonderful innovations with great potential never get the opportunity to evolve into usable forms, or become productized for the wider commercial market.

Whether it's due to a lack of resources, time, money or executive sponsorship, the chips are stacked against any invention making it much beyond the concept phase.

But there may be hope for good ideas yet, especially if an organization fosters an environment of innovation that includes a champion to support and help infant technologies become disruptive innovators.

One recent example of a successful technology transfer occurred at Pacific Northwest National Lab (PNNL).

PNNL, part of the Department of Energy (DoE), was able to help spur the support of a start-up business based on an innovation that was developed at the Lab. In fact, this technology has since been spun out, refined and then adopted by PNNL.

In this case, PNNL became a customer of the innovation that they helped seed.

PNNL has been operated by Battelle and its predecessors since its inception in 1965 and has over 50 years of experience advancing the frontiers of science and engineering.

The national lab makes fundamental scientific discoveries that solve the mysteries of the Earth and the universe, and is able to apply their scientific expertise to tackle some of the most challenging problems in energy, the environment and national security.

Like many organizations, PNNL faces the challenge of analyzing growing volumes of security data without the human resources necessary to match demand.

Quickly recognizing this challenge, they put their support behind an artificial intelligence system that had been incubated at the Lab and successfully transferred to a commercial entity, Champion Technology Company.

By choosing this path, PNNL overcame the hurdles and resource constraints inherent with developing new products and services while benefitting from the outcome.

The result of this successful technology transfer will deliver value to the host organization for years to come.

DarkLight, Champion Technology's core product and the newly evolved company name, is now commercially available. With sights set on cybersecurity, DarkLight models the behavior of a seasoned analyst, performing the "sense-making" and "decision-making" that's required of the human analyst when applying his or her tradecraft.

By fusing information from disparate sources, DarkLight enables organizations to understand and respond to the threat within the context of its enterprise.

Capturing and scaling this analytic tradecraft goes a long way to closing the cyber-security talent gap that most organizations face.

Augmented intelligence helps organizations make determinations on what threats are most important and what threats need the most attention.

"DarkLight captures the analytical processes of a human analyst in order to enable automated reasoning, prioritization and action on a network, effectively acting as an analyst itself," said John Shearer, CEO and Co-Founder at DarkLight.

"The cybersecurity industry is past the point of throwing bodies at the 'data deluge' problem to solve it. We saw this gap, and knew that with the right commercial sponsorship, the solution developed at PNNL could solve the problem."

DarkLight and PNNL are consummate examples of how entities like government agencies can take great strides in infusing innovation to overcome the barriers, which exist within their own environments.

By following the example set by PNNL and its support of DarkLight, the sky is the limit to growing innovative products and ideas, both for the benefit of the host agency, and possibly for everyone else as well.

Tesco Bank

Oversight

by Charles Parker, II; Information Security Architect

And the hits keep coming. The Swift issue involving over $100M in thefts has recently been not in the news nearly as much. The Swift system is currently being updated and upgraded so this does not occur again.

Just as the banking industry begins to move back into its normal, conservative stance, another issue in the industry occurs and is well-placed in the news.

This recent issue occurred with Tesco Bank, located in the UK. Tesco Bank noted suspicious activity and transactions with 40K accounts of their total 136K accounts. These transactions occurred over a weekend. In approximately half of these accounts, there was money missing. What triggered the suspicious activity flag was the bank's fraud algorithm.

The bank is presently working with the National Crime Agency to investigate this. This has been reported as one of the larger breaches in recent history.

Method

As with most attacks, this has been labelled as "sophisticated". The attack and thefts occurred over a 24-hour period with the varying amounts. This was probably meant to gather/steal as much as possible prior to being caught, much like structuring transactions to avoid being detected.

The bank's actions indicate the attack did not involve the bank's core computer system. Had more of the functions facing the clients been locked down, it would have been more likely the enterprise would have been compromised.

With the timing, it also appears the attack was automated. With the number of accounts with stolen money involved experiencing this within the 24-hour period, the automated attack is probable. The attack also appears to be website-oriented. With any maintenance or updates, there can be new errors or bugs that were not present previously.

Even with the best, detailed planning, evening if a DFMEA process were to be utilized, there may be issues. These issues provide for an attack point. The attackers do consistently scan the websites on their reader for changes and new vulnerabilities. This could also be directly from a third party, who had access to their system, being compromised. This may have allowed the

third party's infected system to infect Tesco Bank's system. This is much like person A, who has the flu, shaking hands with person B and passing the virus.

There had been issues in the past with their web-based systems. In 2014 thousands of Tesco Bank accounts were deactivated after the client's login IDs and passwords were shared online.

Reaction

Outwardly facing, the bank's reaction to this was limited. The bank did not limit the funds to be drawn from ATMs, use of most debit or credit cards, and pay bills. A relative few of the client's cards were shut down. The bank did however suspend its online transactions.

Guidance for Customers

If your bank is a victim of this, there are many steps available to follow to protect yourself, your money, and personal, confidential information. With passwords, the password should be challenging. The 12345678 or 23456789 would not be recommended. There should be the upper and lower case, numbers, and special characters.

Any personal information, such as the street you grew up on or your first pet's name, should not be included in the password. This information could be secured from other online resources.

The same password should not be used for the various websites. This may be tempting, however the attackers know it is also. The client would not want to provide access to all of their websites by using one password for them all.

When possible if offered, two factor authentication should be used. Granted this is one more step, but it will however add a new level of security and complexity the attackers may not want to deal with.

About The Author

Charles Parker, II can be reached online at charlesparkerii@gmail.com and InfoSecPirate (Twitter).

THE SKILLS SHORTAGE WITHIN CYBERSECURITY

WHAT ARE THE ISSUES?

by Jonathan Stock, Information Security Recruitment Consultant, IntaPeople

According to a recent global study of employer demand for cybersecurity expertise, the UK was identified as the second worst in the world.

Employer demand outweighed candidate interest by more than a third, with only 31% of the cybersecurity jobs posted being searched for by candidates.

So what are the issues creating this skills shortage?

Diamond in the rough

Clients are looking for the finished article instead of looking for the diamond in the rough. Job specifications are a shopping list of everything they want; from hard to soft skills.

If the candidate has everything why would they want a similar job, they want to progress their career?

Companies should reassess what they actually need and ensure they are looking for a diamond in the rough. Junior candidates might not be able to hit the ground running but they will show a loyalty to the company for giving them a chance to develop.

Talent conveyor belts

The best way to solve a skills shortage is to promote from within, creating a conveyor belt of talent.

If you are looking for a Senior Malware Analyst is there someone internally who could make the step up?

You can then look to replace these people with candidates at the start of their career. This creates a positive culture where employees are rewarded for dedication and loyalty.

Graduates, graduates everywhere

Approximately 100 students, all eager to get into cybersecurity companies, attended a recent event at the University of South Wales to gain an insight into the industry and what employers look for in graduates.

This is one university, so across the country there is an abundance of talent looking to find their first role.

These graduates won't have all the commercial and technological experience required, however they will have a passion to learn and develop, giving you talent you can mould to fit your company.

Think outside the box

Candidates are becoming disengaged with traditional recruitment methods after applying for countless roles and not necessarily getting feedback.

Therefore it is essential companies seek out talent in different areas, e.g. social media, networking events or hacking challenges.

Do you think candidates who like hacking as a hobby would be offered a role as an Ethical Hacker within a corporate environment or would they be discarded because of their lack of commercial experience?

Recently there have been companies like the Cyber Security Challenge UK creating competitions for candidates, maybe the skill set you are looking for can be found here rather than by traditional recruitment methods.

It is clear there is a skills shortage within the UK cybersecurity sector but the best way to combat this is to reassess your recruitment strategy.

There are other avenues for sourcing candidates, and companies have to engage with non-traditional recruitment methods, or use someone who knows about them, to help them bridge the gap.

Ultimately, the talent is available, it is just about knowing where to look.

About The Author

Jonathan Stock is an Information Security Recruitment Consultant for IntaPeople. He contributes to several cybersecurity online magazines, is a member of the UK Cyber Security Cluster and an event co-ordinator.

Jonathan can be reached online at j.stock@intapeople.com, www.twitter.com/jonathanstock86 and at our company website http://www.intapeople.com/

Defense Strategies Institute's 3rd Annual

ELECTROMAGNETIC SPECTRUM OPERATIONS SUMMIT

Delivering EW and Cyber Capabilities for Multi-Domain Operations

JUNE 20 -21, 2017 | ALEXANDRIA, VA

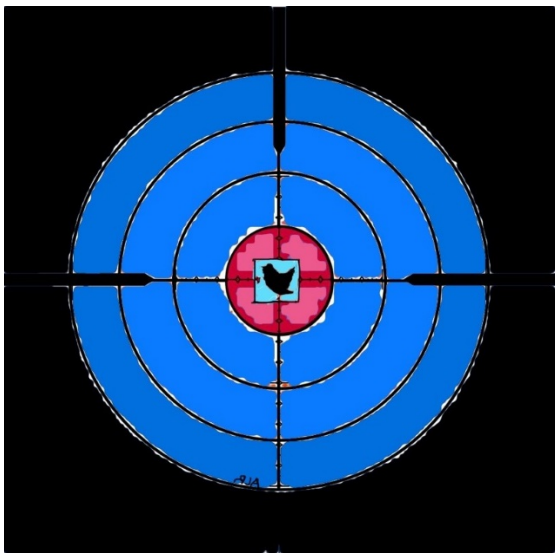
FREE for Military and Goverment Attendees

To Register, Download Agenda & Learn More Visit **EW.DSIGROUP.ORG**

Is Social Media Today's Newest Platform for Weaponry?: The Kurt Eichenwald Story

Not all weapons are guns…

By: Andrew L. Rossow, Esq.



You receive a *Twitter* message. You open it to find a still image with a "play" option. You hit play. All of a sudden, an image flashes at you, continuously, displaying the words, "*YOU DESERVE A SEIZURE FOR YOUR POSTS!"* Next thing you know, you regain consciousness on the floor listening to your significant other calling the police because you just experienced a seizure…from a *tweet*. Who is responsible?

Not all weapons are tangible objects, such as guns and knives. Some can be as simple as the manipulation of a series of words or even a Graphic Interchange Format (*GIF*). Social media has been the millennial generation's newest and quickest source of information, both real and "fake", giving society the power to communicate and exchange information over short and long distances.

But what happens when a social media platform such as Twitter is manipulated in such a way that it is then used to cause physical harm, or even deadly harm to another individual? What happens when a user sends a tweet, containing words, images, videos, and/or a *GIF* to a user who is a known epileptic, with the intent of causing them to experience a seizure or even die? Should these manipulated behaviors be regulated? Victims of social media crimes such as cyberbullying and stalking would most likely answer in the affirmative. As of late, Kurt Eichenwald, a Dallas journalist and senior editor with *Newsweek,* would answer abruptly in the affirmative.

Enter the pending case of *United States vs. John Rayne Rivello*,[1] recently filed in the United States District Court for the Northern District of Texas.

A. Can the Use of a Social Media Platform Such as *Twitter* Be Modified in Such a Way That It Could Be Construed as a "Deadly Weapon?"

Not all weapons are tangible items like a gun or a knife. Distance does not, and should not change the analysis here. The effect is the same. The distinction to be made here is that the platform itself is not the weapon. It is the manner of use and/or the manipulation of that platform in such a way that it becomes an instrument of inflicting harm. The *Rivello* case which will set this distinction out, has roots reaching back to October 2016.

1. A Seizure Heard 'Round the World: How a GIF Sent Via Twitter Induced a Seizure from Dallas Journalist, Kurt Eichenwald

Kurt Eichenwald, a Dallas journalist and senior writer with *Newsweek*, gained national attention back in October 2016, resulting from an article exploiting then, presidential candidate, Donald Trump's conflicts of interest internationally as it pertained to allegations that Russia has manipulated U.S. information to gain political advantage. [2] Resulting from critiques he was receiving in response to his article, Mr. Eichenwald then followed up with an article about how Donald Trump supporters attack journalists on a daily basis. [3] He revealed publicly, that he has "intractable epilepsy." [4] However, he pointed out that one pro-Trump supporter, or "deplorable", took a potentially dangerous step further. [5] Mr. Eichenwald, explained that he had received a tweet from a Twitter user with the Twitter handle "*@Mike's Deplorable AF"* which referenced his known seizures and included a small video of Pepe the Frog, a cartoon character that has been identified as a hate symbol. [6] Logged into his Twitter account on his iPad, Mr. Eichenwald hit the play button on the still video which opened to a 'sort of strobe light, with flashing circles and images of Pepe flying toward the screen.' [7] Luckily, he was standing and dropped the iPad to the ground, avoiding any potential trigger of a seizure." [8] Mr. Eichenwald made note that this [was] not the first time a journalist such as himself has been targeted by a 'deplorable', but indicated that [he] would be extra careful and not push play on any unsolicited videos he receives." [9]

---

[1] *See Criminal Complaint, United States of America v. John Rayne Rivello,* 3-17MJ192-BK
[2] http://www.newsweek.com/2016/09/23/donald-trump-foreign-business-deals-national-security-498081.html
[3] http://www.newsweek.com/epileptogenic-pepe-video-507417
[4] *Id*.
[5] This word was coined from Hillary Clinton's statement on September 9th, 2016, at a New York fundraiser: "*To just be grossly generalistic, you can put half of Trump supporters into what I call the basket of deplorables. Right? Racist, sexist, homophobic, xenophohic, Islamphobic, you name it."* The term as depicted in the dictionary is used as an adjective, but as of this statement, it's now starting to be used as a noun; see for reference https://www.merriam-webster.com/news-trend-watch/clinton-says-half-of-trump-supporters-are-in-a-basket-of-deplorables-20160910
[6] http://www.newsweek.com/epileptogenic-pepe-video-507417
[7] *Id.*
[8] *Id*.
[9] *Id*.

On December 15th, 2016, another attempt made, later revealed to have been successful, centered around another Twitter user who used *Twitter* to send a *GIF* to Mr. Eichenwald, in hopes that he would experience a seizure and/or death. [10] A *GIF* is an animated image that plays automatically upon receipt and only stops when the recipient clicks it to pause or stop it. [11] Mr. Eichenwald revealed the nature of what happened, to the best of his recollection, on *Good Morning America* with George Stephanopoulos. [12]

Mr. Eichenwald fell victim to the Twitter user, "*@jew_goldstein"*, a 'deplorable'. [13] The user sent a tweet to Mr. Eichenwald, containing a *GIF* of a flashing, strobing image playing the message, "YOU DESERVE A SEIZURE FOR YOUR POSTS." The post, which has since been removed from Mr. Eichenwald's account, caused Mr. Eichenwald to experience a seizure, where his wife found him on their bathroom floor.[14] At that point, his wife took a screen shot of the *GIF,* although when depicted below, is shown to simply be a still image. According to reports, Mr. Eichenwald was bed-ridden for twenty-four (24) hours and was unlikely to drive for months.[15]

Credit: *MediaIte[16]; Twitter (now removed from the account)*

In response to the user's tweet, Mr. Eichenwald's wife sent out a tweet from his profile announcing that her husband had indeed suffered a seizure and the account information was being turned over to the police for potential claims of assault. [17] Since the incident, Mr.

---

[10] https://www.nytimes.com/2017/03/17/technology/social-media-attack-that-set-off-a-seizure-leads-to-an-arrest.html; http://www.businessinsider.com/kurt-eichenwald-twitter-strobes-epilepsy-seizures-2016-12; https://www.theguardian.com/technology/2016/dec/20/newsweek-kurt-eichenwald-twitter-epilepsy-seizure;

[11] https://smallbiztrends.com/2016/03/what-is-a-gif.html

[12] http://abcnews.go.com/GMA/video/newsweek-reporter-twitter-induced-seizure-claim-44297849

[13] http://www.dallasnews.com/news/crime/2017/03/17/fbi-arrests-man-accused-trolling-dallas-journalist-kurt-eichenwald-tweet-triggered-seizure; http://www.newsweek.com/kurt-eichenwald-twitter-seizure-arrest-john-rivello-569813;

[14] http://abcnews.go.com/GMA/video/newsweek-reporter-twitter-induced-seizure-claim-44297849

[15] *Id*.

[16] http://www.mediaite.com/online/kurt-eichenwald-claims-twitter-troll-gave-him-seizure-taking-social-media-hiatus/; please note that this image can no longer be found on *Twitter*, as it was immediately removed by Mr. Eichenwald.

[17] https://twitter.com/kurteichenwald/status/809616876011749376?ref_src=twsrc%5Etfw&ref_url=http%3A%2F%2F

Eichenwald had for safety reasons, decided to take a short break from Twitter to spend time with law enforcement and lawyers to see if he could go after the individual behind the account, which took away from one of his main responsibilities of working for *Newsweek*.[18]

As of today, the user behind the Twitter account has been identified as John Rayne Rivello, living in Maryland. He currently in custody and suspended from Twitter indefinitely. Mr. Eichenwald has been working with law enforcement and lawyers pursuing the now active case against Mr. Rivello. As of late, the Criminal Complaint was unsealed and made available to the public.

B. Did Mr. Rivello "Cyber Stalk" Mr. Eichenwald Under the Federal Cyber-Stalking Statute 18 U.S.C. §2261?

The Complaint filed on March 10th, 2017, charged Mr. Rivello under the federal cyber stalking statute ("Statute"). [19] The Statute reads as follows:

> *Whoever…*
>
> *(2) with the intent to kill, injure, harass, intimidate, or place under surveillance with the intent to kill, injure, harass, or intimidate another person, uses…an interactive computer service or electronic communication service…to engage in a course of conduct that—*
>
> *(A) places that person in reasonable fear of the death of or serious bodily injury to…that person, an immediate family member of that person, or a spouse or intimate partner of that person or*
>
> *(B) causes, attempts to cause, or would be reasonably expected to cause substantial emotional distress to a person described in (A)*
>
> *shall be punished as provided in section 2261(b) of this title.*

- 18 U.S.C. §2261(A)(2)(A)/(B).

www.mediaite.com%2Fonline%2Fkurt-eichenwald-claims-twitter-troll-gave-him-seizure-taking-social-media-hiatus%2F

[18] *Id*.

[19] 18 U.S.C. §2261(A)(2)(A)/(B)

1. **Did Mr. Rivello Intend to Kill, Injure, Harass, and/or Intimidate Mr. Eichenwald Under 18 U.S.C. §2261(A)(2)(A/B)?**

The issue in this case is whether Mr. Rivello had sufficient 'criminal intent' to cyber stalk Mr. Eichenwald? Generally, criminal intent refers to a 'criminal or wrongful purpose.'[20]

First, Mr. Rivello created a fake Twitter account on or around December 11th, 2016. By using the fake username "*AriGoldstein@jew_goldstein",* or shortened on Twitter as "*@jew_goldstein",* he was able to contact Mr. Eichenwald. In response to law enforcement's search warrant, Twitter produced the following messages from Mr. Rivello's Twitter account:

- **December 13th, 2016** – "[*Mr. Eichenwald] deserves to have his liver pecked out by a pack of emus*"

- **December 16th, 2016 at 1:42 p.m**. –"*I hope this sends him into a seizure*"
- **December 16th, 2016 at 2:30 p.m**. –"*Spammed this at [Mr. Eichenwald], let's see if he dies*"

- **December 16th, 2016 at 5:00 p.m.** –"*I know he has epilepsy*"
- **December 16th, 2016 at 5:30 p.m**. –"*If I haven't been banned yet, check my feed when you wake up. @[Mr. Eichenwald]".* [21]

It appears that from these messages, these messages depict Mr. Rivello's intent to cause serious physical harm to Mr. Eichenwald, mentioning to other Twitter users in direct/private messages that he hopes his message(s) causes him to go into a seizure, or die. Furthermore, the messages indicate that Mr. Rivello knew that Mr. Eichenwald was epileptic, and despite Mr. Rivello's potential to be banned from Twitter, continued to send similar messages out to the public.

2. **Is Twitter Considered to be an "Interactive Computer Service" or "Electronic Communication Service Pursuant to 18 U.S.C. §2261(A)(2)(A/B)?"**

The second element of the Statute requires the use of "*any interactive computer service or electronic communication service*." Mr. Rivello used the social networking platform, Twitter to contact Mr. Eichenwald. *Twitter* is a free-access social media platform/dashboard that allows users[22] with Twitter accounts to create, share, and read 140-character messages called "*tweets*".[23] During the registration process, a user must create a unique Twitter username, also known as a "*Twitter Handle*", indicated by the "@" followed by their username. Users are able to "favorite" or like other messages, "*retweet"* or share other messages, and even reply to the tweets of other users. Additionally, users can directly tweet to or send a message directly to the page of the recipient user by starting their tweet off with the "@" and typing the intended recipients' username. Lastly, a user can also send a direct message or privately message another user, which appears in their inbox, rather than their public page, so long as they have not been blocked by Twitter or that user.

[20] Black's Law Online Dictionary (2nd ed. 2009), http://thelawdictionary.org/criminal-intent/
[21] (Case 3:17-mj-00192-BK; Hopp Aff. ¶ 17)
[22] The term "users" used throughout this article refers to all individuals with a registered *Twitter* username and uses the service to communicate and exchange information.
[23] *Hopp Aff. ¶¶ 8-13;* see also www.twitter.com

Users can also embed visual files, such as photographs or still images in their tweets.[24] These files can include animated or moving images known as *GIFS*. Unlike *Facebook* or *Instagram* where you can click the *GIF* to play it, by default, Twitter will automatically play the *GIF* when the recipient hovers over it or simply views it on the page.[25] Based off the site's guidelines and terms of service, it appears that Twitter would most likely fall under the statute's definition of an interactive computer service or electronic communication service.

3. Did Mr. Rivello Engage in a "Course of Conduct", or Was this an Isolated Incident pursuant to 18 U.S.C. §2261(A)(2)(A/B)?

The third element of the Statute requires an individual to have engaged in a "*course of conduct*" while using a service such as Twitter. The Statute further defines course of conduct as a "*pattern of conduct composed of two or more acts, evidencing a continuity of purpose*."[26]

Looking at the results of the search warrant Twitter provided to law enforcement and the Prosecution, Mr. Rivello contacted Mr. Eichenwald at a minimum of five times, with the same tone and goals in mind. Mr. Rivello used Twitter, to create a fake account registered under the Twitter handle *@jew_goldstein*.

Mr. Rivello then composed and sent messages that included both words and a *GIF* directly to Mr. Eichenwald's Twitter page. At the same time, Mr. Rivello had composed and sent messages to other users informing them to "follow" the prior tweets he had sent. He then sent a tweet informing all of his followers to check his Twitter feed, or history to see all the previous tweets he had sent to Mr. Eichenwald's page.

Next, Mr. Rivello took it a step further and visited the official epilepsy website at www.epilepsy.com to find out statistics and triggers for seizures. It was this point that he had created a fake *Wikipedia* page for Mr. Eichenwald, altering the obituary date of death to show December 16th, 2017*,* the day after the *GIF* was sent to Mr. Eichenwald.[27]

After viewing some of Mr. Rivello's actions and messages sent out on Twitter, it is likely that this was not an isolated event, but many steps taken in hopes of inducing a seizure from Mr. Eichenwald.

4. Did Mr. Rivello's Conduct "Place Mr. Eichenwald in Reasonable Fear of Death or Serious Bodily Injury Pursuant to 18 U.S.C. §2261(A)(2)(A/B)?"

The fourth element of the Statute looks at whether Mr. Rivello's conduct "*placed* [*Mr. Eichenwald*] *in reasonable fear of death* or *serious bodily injury*." Due to Mr. Eichenwald's publicity and verified Twitter profile page, he receives thousands of tweets, comments, and critiques on his page daily. While Mr. Rivello could argue that Mr. Eichenwald should have known something like this was coming, due to the incoming flood of messages not just from him, but from other users, it would seem unlikely that the *GIF* placed Mr. Eichenwald in reasonable fear of death or serious bodily injury, simply because he could argue he had no idea this particular threat was coming.

However, as this relates to Mr. Eichenwald's wife, the analysis could change. Applying this same element when either his wife witnessed her husband experiencing a seizure, or after Mr.

[24] *Id*.
[25] *Id*.; see also www.twitter.com
[26] *Hoff Aff.* ¶ *5*.
[27] *Hoff Aff.* ¶¶ *18, 28.*

Eichenwald became conscious, it would appear possible that his wife could have thought her husband was going to die, as she watched him fall to the floor. Upon Mr. Eichenwald regaining consciousness, it could be argued that it was likely that Mr. Eichenwald was placed in reasonable fear of death. Indeed, it's also likely that he was placed in fear of serious bodily injury, because after viewing the *GIF*, he experienced a seizure that lasted for approximately eight minutes.[28] His wife explained to law enforcement that he experienced a complete loss of his bodily functions and mental faculties, as he had no recollection of the incident other than waking up on the bathroom floor with his wife holding him.[29]

While part of his job with *Newsweek* is to actively use Twitter to share and communicate relevant information, Mr. Eichenwald told *Good Morning America* that [he] has continued to experience impairment to [his] bodily functions and mental faculties, as [he] is careful on the length of time [he] [drives] and how often [he] spends on Twitter.[30] Mr. Eichenwald's neurologist informed sources that because of this seizure, Mr. Eichenwald could experience other seizures in the near future.[31]

Lastly, the Statute indicates that crimes falling under this section, could subject an individual like Mr. Rivello to imprisonment, ranging from 10-20 years. While briefly set out, the Statute seems adequate enough in addressing a scenario such as this.

C. A States' Point of View: Assault With a Deadly Tweet?"[32]

The Texas Penal Code[33] and Ohio Revised Code assault statutes are almost harmonious, therefore, the following legal analysis will be pursuant to the Ohio Revised Code ("Code").[34]

1. Did Mr. Rivello "Assault" Mr. Eichenwald When He Sent Him a GIF Through Twitter?

Under the Restatement (Second) of Torts, "*an actor is subject to liability to another for assault if:*

> *(a) He acts **intending to cause a harmful or offensive contact with the person of the other…or an imminent apprehension of such a contact,** and*
>
> *(b) The other is thereby **put in such imminent apprehension**"* [35]
>
> ■ Restatement (Second) of Torts, emphasis added

Applying the *Restatement* to the case at hand, Mr. Rivello intended to send a *GIF* when he sent a tweet to Mr. Eichenwald, a known epileptic, containing a strobing message flashing, "*YOU DESERVE A SEIZURE FOR YOUR POSTS*."

---

[28] *Hoff Aff. ¶ 14.*
[29] *Id*.; see also http://abcnews.go.com/GMA/video/newsweek-reporter-twitter-induced-seizure-claim-44297849
[30] http://abcnews.go.com/GMA/video/newsweek-reporter-twitter-induced-seizure-claim-44297849
[31] *Id*. at ¶ *18.*
[32] This phrase was coined by Attorney and Author, Keith Lee on his blog, *The Associate's Mind* http://associatesmind.com/2016/12/16/can-you-sue-someone-for-a-tweet-that-induces-epilepsy/ ; see also *Parts II-VI*
[33] Tex. Penal Code §22.02
[34] Ohio Rev. Code §2903.11(A)(1)/(2)
[35] Restatement (Second) of Torts §21 (1965).

Secondly, Mr. Rivello knew Mr. Eichenwald was epileptic based off Mr. Eichenwald's prior announcement in a *Newsweek* article indicating he had epilepsy. Indeed, the information Twitter provided to law enforcement in response to the search warrant, revealed several of Mr. Rivello's tweets indicating he knew Mr. Eichenwald was epileptic. The results further revealed that Mr. Rivello's search history contained extensive research and visits to informational sites such as www.epilepsy.com explaining different triggers for seizures.

Lastly, Twitter's default settings of video playback as it pertains to *GIFS*, automatically load and play the *GIF* without having the user click on it to load or play it. Consequently, when Mr. Eichenwald logged into his Twitter account, Mr. Rivello's tweet, containing only the flashing *GIF* was the first thing he saw, to which he immediately experienced a seizure for approximately eight minutes.

In light of the foregoing, it appears that Mr. Rivello's actions directed towards Mr. Eichenwald are likely to constitute assault under the *Restatement*. However, this conclusion is based off a very *particular* set of facts, such as this case. Not every tweet that verbally attacks another individual can be considered assault.

2. Did Mr. Rivello Commit Felonious Assault Under Ohio Revised Code §2903.11(A)?

In Ohio, felonious assault is second-degree felony[36] with a prison sentence anywhere from 2-8 years. The statute reads as follows:

> *(A) No person shall knowingly do either of the following:*
>
> *(1) Cause serious physical harm to another;*
>
> *(2) Cause or attempt to cause physical harm to another…by means of a deadly weapon or dangerous ordnance.* [37]

As discussed earlier in the article, Mr. Rivello knowingly caused serious physical harm to Mr. Eichenwald by inducing approximately an eight-minute seizure when he used Twitter to send a tweet containing a *GIF* of a flashing strobe message to an individual who he knew was epileptic. Indeed, it is likely that Mr. Rivello could be charged with felonious assault under Ohio's Revised Code.

3. Did Mr. Rivello Commit Aggravated Assault Under Ohio Revised Code §2903.12(A)?

In Ohio, aggravated assault, is a fourth-degree felony and has a potential prison sentence of 6-12 months.[38] The statute reads as follows:

> *(A) No person, while under the influence of sudden passion or in a sudden fit of rage, either of which is brought on by serious provocation occasioned by the victim that is reasonably sufficient to incite the person into using deadly force, shall knowingly:*
>
> *(1) Cause serious physical harm to another…;*

[36]

[37] Ohio Rev. Code §2903.11(A)(1)/(2)

[38] Ohio Rev. Code §2903.12

(2) Cause or attempt to cause physical harm to another…by means of a deadly weapon or dangerous ordnance, as defined in section 2923.11 of the Revised Code. [39]

Similar to Ohio, except for the degree, in Texas, aggravated assault is a second-degree felony, with possible imprisonment from 2 – 20 years and/or a fine of up to $10,000.[40] Attorney Keith Lee[41] has published a series of blog posts on his blog, *The Associate's Mind*", discussing the *Rivello* case, entitling his six-part series, "*Assault With a Deadly Tweet."*[42] Texas categorizes a "deadly weapon" into two categories[43]: *weapons by design* and *weapons by manner of use*.

Under the Penal Code, a deadly weapon by design includes a (1) firearm and/or (2) anything specifically made to cause death or serious bodily injury. [44] A weapon can also be considered deadly based off the manner in which it is used. [45] This includes (1) *anything that is used in a manner that is capable of causing death or serious bodily harm*[46] and/or (2) *objects one would not ordinarily think to be considered weapons*. [47]

The purpose or design of these objects is not to hurt another individual, but if manipulated in such a way, can cause serious bodily harm or death to another. For example, these objects could include a pillow, glass bottle, golf club, hammer, car, or even a person's hands.[48] Historically, Texas courts have held belt-buckles[49], dustpans[50], the floor[51], a hand[52], and underpants[53] as deadly weapons.

When social media platforms such as Twitter are manipulated in a way outside of its intended design and purpose to then inflict serious bodily harm or deadly harm upon another, the platform then has the potential for being construed as a deadly weapon. This case illustrates a scenario where in limited circumstances, a person could be found guilty of felonious assault for using Twitter in a particular way that removes the "distance of the parties" argument.

D. With Great Broadband, Comes Great Responsibility: Has Social Media Become the Next Platform for Cyber Warfare?

---

[39] Ohio Rev. Code §2903.12(A)(1)/(2)
[40] Tex. Penal Code §22.02
[41] **CITE TO KEITH LEE'S ASSAULT BY GIF PART 6;** see also http://hamerlawgroup.com/attorneys/keith-r-lee/
[42] http://associatesmind.com
[43] http://associatesmind.com/2017/03/21/assault-by-gif/
[44] Tex. Penal Code §1.07(a)(17) (1994); see also http://www.pacefirm.com/faq/assault-deadly-weapon.html
[45] Tex. Penal Code §1.07(a)(17) (1994); see also http://www.pacefirm.com/faq/assault-deadly-weapon.html
[46] *Id*.
[47] *Id*.
[48] See Case No: 02-15-00419-CR/ 02-15-00420-CR, (Tarrant County Grand Jury indicted Jamual Edward Parks, an MMA fighter, concluding his hands are considered deadly weapons); see also *Turner v. State*, 664 SW 2d 86, 90 see also http://www.bjpenn.com/mmanews/the-man-whose-hands-are-deadly-weapons-in-the-lone-star-state-a-cautionary-tale/
[49] *Garza, 695 S.W.2d 726, 729 (Dal. 1985), aff'd, 725 S.W.2d 256 (Tex. Crim. App. 1987); see also http://associatesmind.com/2017/03/21/assault-by-gif/*
[50] *Quintana*, 777 S.W.2d 474, 478 (C.C.1989M ref'd); see also *http://associatesmind.com/2017/03/21/assault-by-gif/*
[51] *Stanul*, 870 S.W.2d 329, 335 (Aus. 1994, dism;d); see also *http://associatesmind.com/2017/03/21/assault-by-gif/*
[52] *Morales, 792 S.W.2d 789, 791 (Hous. [1st] 1990, no pet.); Cooper, 773 S.W.2d 749, 750 (C.C.1989M no pet.);* see also *http://associatesmind.com/2017/03/21/assault-by-gif/*
[53] *Id*. ; see also *http://associatesmind.com/2017/03/21/assault-by-gif/*

1. "Sticks and Stones May Break My Bones, But Words Will Never Break Me"[54]

Words do cause harm, sometimes, they can even cause physical harm or even deadly harm to another. We have seen proof of the potential harm electronic messages can cause over the years. It started with one of the very first cases of cyberbullying, Monica Lewinsky. While the gossip, rumors, and soon to be admitted truth of former President Clinton and Ms. Lewinsky's infamous affair was spread across dial-up internet, it still reached the population of the entire country, causing harm and damage to both Ms. Lewinsky and former President Clinton, still to this day. The *Rivello* case presents several questions as to how social media platforms are used to commit crimes against another.

First, *how narrowly does this particular analysis apply*? Will the holding of this case apply specifically to a situation where someone uses a *GIF* or *video* posted on social media to exploit another's pre-existing medical condition, such as Mr. Eichenwald's?

Secondly, the next step is to look to the *jurisdiction* of where the harm is being transmitted to, and the *effect of the harm* being communicated to the recipient. [55] While a *minimum contacts* analysis is used to determine the jurisdiction for most crimes, the analysis differs when it comes to crimes taking place in cyberspace.[56] It becomes difficult to determine the jurisdiction of a state court when you have two parties from different states conducting activities through electronic mediums such as smartphones and computers. In cyberspace, the *Effects Principle* is used. Under the Effects Principle, we would simply look to the *effect* of the harm and how frequent the transmission(s) occurred.[57]

Next, how has the social media platform been *manipulated*? The social media platform itself is not a weapon. By design, Twitter's only purpose is to share, exchange, and communicate information (words, audio, images, videos) across a community of users. In the *Rivello* case, Mr. Rivello took substantial steps in manipulating the design and purpose of Twitter from simply communicating and sharing information, to using Twitter to exploit Mr. Eichenwald's epilepsy for public show.

Finally, the analysis ends with the *characteristics of the potential victim*. Mr. Eichenwald was a known epileptic who was known for his articles, critiques, and interviews in the media. By conducting background information on a potential victim, a perpetrator has a better chance of unlocking and understanding the potentially fragile nature of their victim.

E. What Defenses, If Any, Does Mr. Rivello Have Available?

1. Does the First Amendment Shield Mr. Rivello's Messages to Mr. Eichenwald?

---

[54] *The Christian Recorder, African Methodist Episcopal Church, March 1862;* see also http://www.phrases.org.uk/meanings/sticks-and-stones-may-break-my-bones.html

[55] See Susan W. Brenner, NCR Distinguished Professor of Law and Technology at the University of Dayton School of Law; she has published various articles dealing with cybercrime; see also http://globalcyberrisk.com/our-team/susan-brenner/; http://cyb3rcrim3.blogspot.com; https://papers.ssrn.com/sol3/papers.cfm?abstract_id=786507; https://fas.org/sgp/crs/misc/R42547.pdf; http://euro.ecom.cmu.edu/program/law/08-732/Jurisdiction/GrayMinimumContacts.pdf; http://corporate.findlaw.com/law-library/jurisdiction-in-cyberspace.html; http://euro.ecom.cmu.edu/program/law/08-732/Jurisdiction/GladstoneDeterminingJurisdiction.pdf;

[56] International Shoe Co. v. Washington, 326 U.S. 310 (1945), where the Supreme Court of the United States held that a party…may be subject to the jurisdiction of a state court if it has "minimum contacts" with that state.

[57] https://www.asil.org/sites/default/files/benchbook/jurisdiction.pdf

Congress shall make no law…prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press…[58]

■ U.S. Constitution, First Amendment

The U.S. Constitution gives every citizen the freedom to speak their mind, so long as it does not constitute certain types of speech, such as hate speech. [59] Hate speech is…any form of intimidation…that [is] most likely to inspire fear of bodily harm.[60] In an ordinary case, the standard of care a court will look to is that of a reasonable person in like or similar circumstances. However, in this case, the standard of care shifts to that of a person in like or similar circumstances who suffers from epilepsy.

It appears from this case, that Mr. Rivello would not be shielded under the First Amendment because the tweet could be considered hate speech. The *GIF* was created and sent to Mr. Eichenwald with the purpose of causing the fear of potentially having a seizure. While words alone cannot make anyone do something, a person who may not have complete control over their physical impairment(s), the analysis changes.

2. **Did Mr. Eichenwald Assume the Risk of Receiving Any Form of a Message, Even a Strobing GIF?**

Assumption of risk refers to situations in which an individual acknowledges the risks associated with any activity, but chooses to take part regardless.[61] In other words, the individual knew the activity could result in a particular end result, but decided to proceed with it regardless.[62]

Mr. Rivello could first argue that Mr. Eichenwald assumed the risk of being exposed to potentially dangerous tweets such as his own because of his public status as a reporter and the nature of his job which invites critiques and unsolicited messages at times. However, Mr. Rivello could rebut that on the basis that maintaining an active social media account as part of their daily reporting routine journalist does not automatically subject the individual to the infinite number of potential solicitations or unsolicited messages.

Mr. Rivello could next argue that he was not the only one to send Mr. Eichenwald messages of this kind and he should have known that because of his criticized articles and/or interviews with the media, that he was bound to receive a similarly-styled unsolicited message from the general public. To counter, while the nature of Mr. Eichenwald's job requires him to maintain an active online presence, that does not at the same time, open every door to every possible risk that may present itself online in the realm of social media. Mr. Eichenwald has a large number of *followers* on Twitter that it is almost impossible for him to predict each and every result of reading every tweet and/or message he receives.

While Mr. Rivello's argument seems logical, it does not seem likely that Mr. Eichenwald could be said to have invited himself into a situation where he assumed the risk of suffering a seizure because he logged into his account and viewed tweets he receives on a daily basis.

---

[58] U.S. Const. amend. I
[59] This is only one of the exceptions to the First Amendment protections to Free Speech; these are used simply for relevance to the particular scenario.
[60] Virginia v. Black, 538 U.S. 343 (2003)
[61] https://legaldictionary.net/assumption-of-risk/
[62] Id.

3. Is Twitter Liable Under 47 U.S.C. § 230 of the Communication Decency Act?

Section 230 of the Communication Decency Act ("CDA") states that *"No provider or user of an interactive computer service shall be treated as a publisher or speaker of any information provided by another information content provider*". [63] Put differently, a social media platform such as Twitter cannot be held liable for the content its users publish or send out on a daily basis.

While the CDA is quite clear, Mr. Rivello could argue that Twitter should be held liable under the CDA because it violated its continuing obligation to monitor its platform to ensure users comply with its Terms and Service, or simply, did not do enough. If that argument were to stand, Mr. Rivello could potentially argue that Twitter should be the Defendant in the lawsuit, not him, to which Twitter should be joined as a necessary and indispensable party. However, both Mr. Eichenwald and Twitter could argue that Twitter has policies in place that set the parameters for which its service should and should not be used for; that there is no way for Twitter to actively monitor each and every post for content that potentially violates the Terms and Services.

Twitter, if joined as a party in the lawsuit, could argue that under the CDA, it is a provider and/or an interactive computer service. While it does take steps in monitoring heavily reported accounts or for certain posts that post topics or keywords that have been flagged for certain keywords, for all intents and purposes, its platform is populated by users around the globe, and it would be next to impossible to monitor every single user throughout any given day. For example, Twitter for some time now has been taking *GIF*s and converting them into a .mp4 format before posting it. This allows for the user or recipient of a video to *choose* to play the video without the risk of it playing undesired content. It is likely that Twitter would succeed under the safe-harbor provisions of the CDA.

F. Case Study: Pokemon Shock

Today's millennial generation grew up with one of the hottest animated cartoons of all time, *Pokémon*.[64] However, one episode in Japan was removed from the air as a result of reports that young viewers were experiencing seizures and temporary blindness. [65] The episode, entitled, Electric Soldier Porygon, or known internationally as Computer Warrior Porygon, depicted Pikachu, a yellow-moused Pokémon with electric abilities, using his lightning attack to blow up some virtual missiles in a cyber-space environment. [66] However, since the episode was taking place in cyberspace, the animators did not think a regular explosion would do the trick.[67] Instead, the animators used a rapidly-strobing technique that flashed red and blue lights on the screen, making the explosions look more "virtual". Reports indicated that as a result of this episode, there was a connection between the flashing, strobes on the television and viewers who suffered from certain physical impairments such as epilepsy. Health professionals reported that it was a combination of the strobe lighting effects along with the popularity of the program.[68]

---

[63] 47 U.S.C. § 230.
[64] https://en.wikipedia.org/wiki/Pokémon
[65] http://kotaku.com/5757570/the-banned-pokemon-episode-that-gave-children-seizures; see also http://www.nejm.org/doi/full/10.1056/NEJM200407223510424#t=article
[66] http://www.cnn.com/WORLD/9712/17/video.seizures.update/; see also http://www.nejm.org/doi/full/10.1056/NEJM200407223510424#t=article; see also http://www.nejm.org/doi/full/10.1056/NEJM200407223510424#t=article
[67] *Id*.
[68] *Id*.

Sources claimed that around 1 in 4,000 people are vulnerable to photosensitive seizures and other health issues.[69] Japan labeled the incident as "Pokemon Shock."

[70]

*****WARNING*****

A YOUTUBE LINK TO THIS SEGMENT OF THE BANNED EPISODE IS FEATURED IN THE FOOTNOTES OF THIS ARTICLE, WITH A SIMILAR WARNING.

IF YOU SUFFER FROM EPILEPSY OR A SIMILAR CONDITION INVOLVING PHOTO-SENSITIVITY OR POTENTIAL FOR SEIZURES, DO NOT CLICK THE YOUTUBE LINK!!

G. How Could This Case Be Applied in the Future?

The holding of this case could potentially dictate in limited instances, how an individual could be guilty of assault simply by modifying the intended use of a platform such as Twitter, to cause physical harm or even deadly harm to another individual. This case provides a situation where a social media platform was modified into being used as an instrument for psychological warfare through cyberspace.

About the Author

Born and raised in Dallas, Texas, Andrew Rossow is a Cyber-Space and Technology Attorney in Ohio with Gregory M. Gantt Co. L.P.A. To see more of Mr. Rossow's publications and updates, please follow him on Facebook at www.facebook.com/drossowlaw and on Twitter at @CyberEsqRossow

This article was written for purely educational purposes and is strictly the opinion of its writer. In no way does this article lend itself to give legal advice to its reader(s), but to provide its readers with a legal analysis of a limited situation where social media was used to cause physical harm or even deadly harm to another individual. If you wish to find out more information about epilepsy, please visit www.epilepsy.com.

[69] *Id*.
[70] Youtube: *Pokemon Shock* (still image of the video), (https://www.youtube.com/watch?v=q4dDaxHtQDU)

SECURITY IT SUMMIT

4 July 2017
Hilton London Canary Wharf

Start your planning for 2018 at the **Security IT Summit.**

Meet with the most trusted solution providers, learn from industry thought leaders and connect with peers over the course of the Summit, which is entirely **FREE to attend** for security professionals.

Topics covered include: Access Control • Anti-Virus Browser • Security Data • Theft/Loss • Malware • Mobile Security • Network Security Management • Trojan Detection • UK Cyber Strategy



For more information and to register, please contact **Liz Cowell** on:
01992 374072 or **l.cowell@forumevents.co.uk**.

@SECIT_SUMMIT #SITSUMMIT

SECURITYITSUMMIT.CO.UK

MEDIA & INDUSTRY PARTNERS:

HOSTED BY:

The Top Four CISO Data Security Concerns and Deployment Trends: 2017 RSA Survey Findings

For the third straight year, STEALTHbits Technologies surveyed attendees to the RSA Conference, the cyber security industry's top event.

STEALTHbits researchers and data security and governance experts gathered insights on five key points from more than 300 security professionals, from several vertical industries including technology, finance, government, healthcare, services, and education.

It will come as no surprise that the survey results reflect the challenges faced by security teams today, the most important of which is securing sensitive data. The biggest issues that emerged in the 2017 poll were:

- discovery of unstructured data,
- the massive amount of unclassified data,
- the lack of proper tools to mitigate risk,
- lack of budget, and hand-in-hand, the lack of resources.

1. Chief Information Security Officer Priorities:

Respondents ranked the following as their top six CISO priorities for 2017:

1. Threat Analytics
2. Identity and Access Management (IAM)
3. Active Directory (AD) Management and Security
4. Data Access Governance (DAG)
5. Compliance
6. Security Information Event Management (SIEM)

2. Deployment Maturity Δ 2015 - 2017

Respondents indicated the deployment phase of key security technologies, and for each solution category, the leading answer was "not planned." Solutions included in the Development Maturity question included:

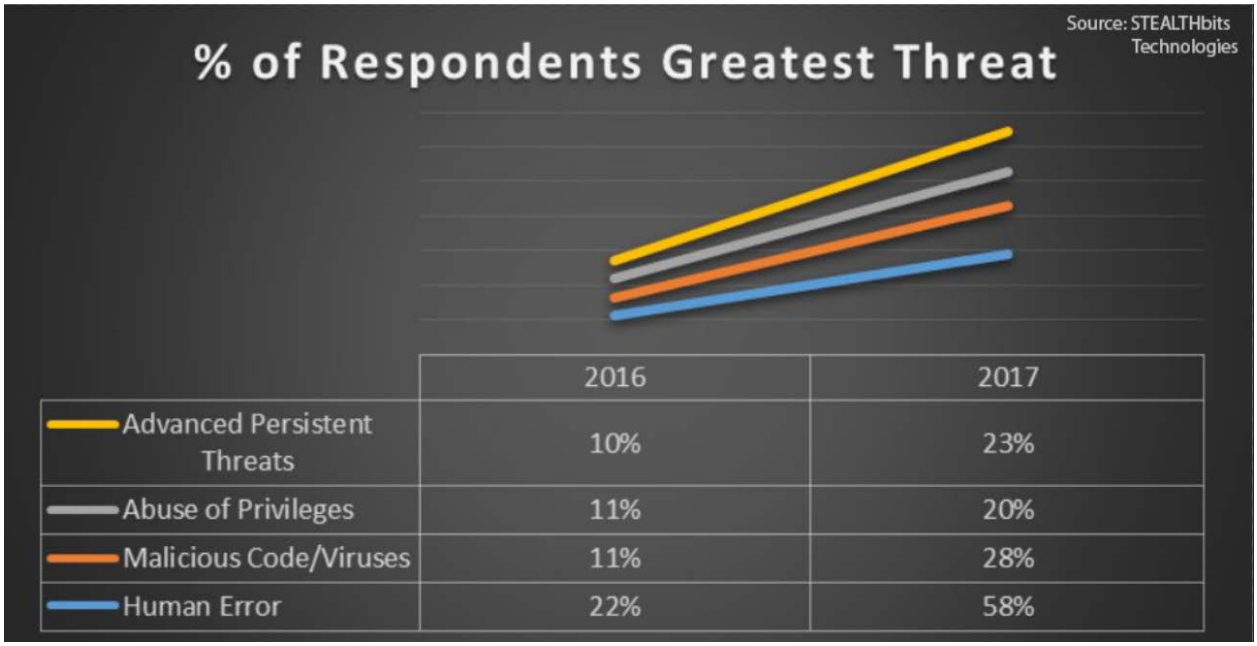
- Data Loss Prevention (DLP):
  - Deployment not planned: 24% in 2015, 29% in 2016, 37% in 2017
- Identity and Access Management (IAM):
  - Deployment not planned: 26% in 2015, 32% in 2016, 29% in 2017
- Privileged Identity Management (PIM):
  - Deployment not planned: 28% in 2015, 42% in 2016, 35% in 2017
- Security Information and Event Management (SIEM):
  - Deployment not planned: 32% in 2015, 36% in 2016, 29% in 2017
- User Entity Behavior Analytics (UEBA):
  - Deployment not planned 49% in 2016, 44% in 2017

Of those five security technologies, IAM and SIEM were the most widely accepted/deployed at this time, while, unsurprisingly, UEBA is the least mature.

3. Greatest Threats to Organizational Data

STEALTHbits found that from 2016 to 2017, the four most prevalent threats -- Human Error, Abuse of Privileges, Malicious Code/Viruses, and Advanced Persistent Threats -- continued to grow in concern at a steady rate. However, unlike previous years, respondents did not rank Massive Amount of Data as being a highly-ranked threat. Instead, Advanced Persistent Threats emerged as a priority-level concern.

Despite the amount of security tools and educational materials that have flourished over the last year, Human Error continued to grow as a threat.



4. European Union General Data Protection Regulation (EU GDPR) Preparation

The European Union (EU) General Data Protection Regulation (GDPR) regulation will fully take effect on May 25, 2018, forcing organizations around the world to comply with the broad range of stringent security, privacy and data location/protection mandates, or incur onerous penalties.

When asked, “Is your organization preparing for the EU GDPR?” a full 67% of respondents said that their organizations were busy preparing.

For more information on GDPR requirements and preparation, see “Preparing for the GDPR Time Bomb.”

STEALTHbits Technologies is a cybersecurity software company focused on protecting an organization's credentials and data. By removing inappropriate data access, enforcing security policy, and detecting advanced threats, we reduce security risk, fulfill compliance requirements, and decrease operations expense. Identify threats. Secure data. Reduce risk. http://www.stealthbits.com.

Jeff Steuart is an IT professional in a commercial real estate analysis practice.

Anti-Abortion Ads Plague Women-Online Privacy Lies in Peril

If the recent anti-privacy bill's existence was not enough, it has sparked numerous debates resulting in internet users resorting to different tactics and tools to safeguard their privacy.

Unfortunately, online privacy lies in peril for everyone, as the basic right to protecting one's privacy seems like a farfetched dream.

Women Targeted by Anti-Abortion Ads

Recently, the attorney general of Massachusetts brought to light an alarming predicament, which involves women being hounded by anti-abortion ads as soon as they visit reproductive health facilities.

Come to think of it, this is not only a breach of privacy, but it is illegal as such information should not be available to anyone, except for one's physician.

The Fate of Illegal Advertising in Massachusetts

The good news is that legal action is being taking against any and all advertising agencies who used health data illegally.

The attorney general, Maura Healey, went so far as to settle the matter once and for all, by barring one such Boston advertising agency for using health data illegally.

At the same time, she has offered full support to those women looking for pregnancy help and she assures them they have complete choice to do so as they please.

Identifying the Cause for the Breach

What is truly alarming is how such advertising agencies managed to get hold of such information, all the while being accurate at delivering targeted ads.

So far, location based apps have been determined to be the cause for such a breach.

Analyzing the Anti-Privacy Bill in Light of Recent Developments

Healey's actions as commendable as they may be, have come under scrutiny. She is being criticized for barring an activity which is in fact protected by the first amendment for advertisers.

But then again, this incident has revealed how disastrous Trump's and the Republicans' in Congress decision to overturn Obama-era legislations in regards to privacy really is.

If those legislations did in fact remain in place, such invasive advertising would not have been possible.

Defeating the Anti-Privacy Bill - No matter who is to be held responsible, internet users are still at risk and hardly have any legal protection to prevent such breaches of privacy, as they are considered 'creepy' but not illegal, which is absurd to say the least.

It goes without saying the anti-privacy bill is and will remain controversial, due to how it works against American internet users and how it's favoring ISPs and their right to do whatever they see fit with the information they gather.

As frightening as the whole ordeal has turned out to be, internet users are not entirely out for the count.

Taking recent events into account, numerous privacy advocates have recommended using encryption tools to counter such breaches of privacy, that too for good reason.

About Author:

Anas Baig is a Cyber Security Expert, a computer science graduate specializing in internet security, science, and technology. Also, a Security Professional with a passion for robots & IoT devices.

Follow him on Twitter @anasbaigdm, or email him directly by clicking here.

NSA Spying Concerns? Learn Counterveillance

Free Online Course Replay at www.snoopwall.com/free

"NSA Spying Concerns? Learn Counterveillance" is a 60-minute recorded online instructor-led course for beginners who will learn how easily we are all being spied upon - not just by the NSA but by cyber criminals, malicious insiders and even online predators who watch our children; then you will learn the basics in the art of Counterveillance and how you can use new tools and techniques to defend against this next generation threat of data theft and data leakage.

The course has been developed for IT and IT security professionals including Network Administrators, Data Security Analysts, System and Network Security Administrators, Network Security Engineers and Security Professionals.

After you take the class, you'll have newfound knowledge and understanding of:

1. How you are being Spied upon.
2. Why Counterveillance is so important.
3. What You can do to protect private information.

Course Overview:

How long has the NSA been spying on you?
What tools and techniques have they been using?
Who else has been spying on you?
What tools and techniques they have been using?
What is Counterveillance?
Why is Counterveillance the most important missing piece of your security posture?
How hard is Counterveillance?
What are the best tools and techniques for Counterveillance?

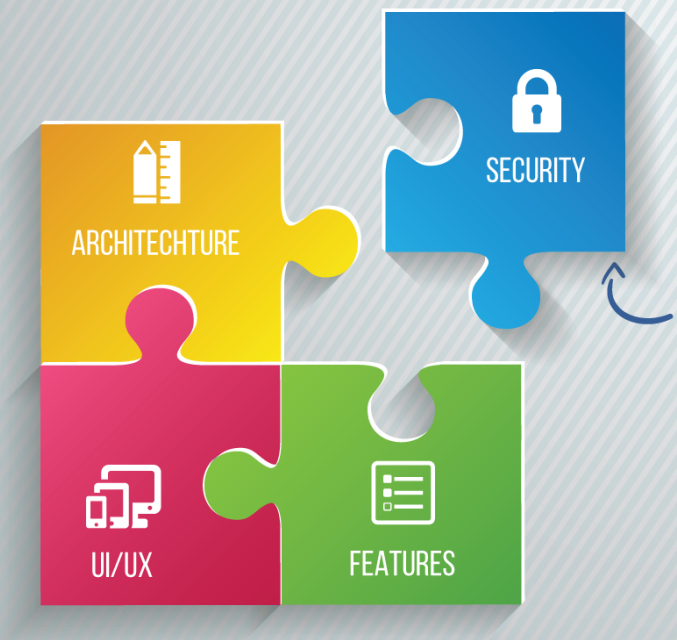
Your Enrollment includes :

1. A certificate for one free personal usage copy of the Preview Release of SnoopWall for Android
2. A worksheet listing the best open and commercial tools for Counterveillance
3. Email access to the industry leading Counterveillance expert, Gary S. Miliefsky, our educator.
4. A certificate of achievement for passing the Concise-Courses Counterveillance 101 course.

Visit this course online, sponsored by Concise-Courses.com and SnoopWall.com at http://www.snoopwall.com/free

AppSHIELD™ SDK

MOBILE APP FIREWALL & CLOAKING TECHNOLOGY



You have built a great app with an amazing team.

Let us help you secure it.

SnoopWall's patents-pending AppShield™ SDK can secure any mobile app on all major platforms. Our AppShield SDK makes your app invisible to any other app on the mobile device which might otherwise eavesdrop on it, just like the B2 Bomber employs stealth technology to evade radar detection. With 24/7/365 active monitoring, regular updates and a dedicated team of cybersecurity experts, you can be assured that your app's security and customer data are safe, all the while providing a non-intrustive customer experience.

KEY FEATURES

- Cloaking Technology (patents-pending)
- Dynamic Port Management (patents-pending)
- No Need for Code Obfuscation
- No Malware Scanning Required
- No Backend Database Required
- Root & Jailbreak Detection
- Secure Storage for Data Hiding
- Application Hardening Technology
- No Known Way to Exploit
- Detects & Blocks Tomorrow's Threats
- Apple iOS, Google Android, Microsoft Windows
- No Sysadmin, no Reboot, no special Privileges
- Tiny Deployment Size & Rapid Integration
- Most Cost Effective Per Deployment Pricing

GET IN TOUCH

Toll Free: 1-800-991-3871 x1000 www.snoopwall.com securitysolutions@snoopwall.com

SW-GEN-2015-0205

AppSHIELD™ SDK

MOBILE APP FIREWALL & CLOAKING TECHNOLOGY

Firewalls are essential for security

Does your mobile app have built-in next generation firewall technology to safeguard customer data?

Mobile apps are critical and vulnerable touchpoints in most companies networks. Just like the firewall which protects your IT network, an app firewall is needed to protect your mobile app. However, most app development teams do not have this expertise, nor are they dedicated to this mission.

DO IT YOURSELF TO BUILD A MOBILE APP FIREWALL

- HIGH RISK OF PATENT INFRINGEMENT $$$$$
- MAJOR DISTRACTION FROM CORE DEVELOPMENT FOCUS
- HIGH REPUTATIONAL RISKS
- POSSIBLY NOT SECURE
- UPDATED WHEN YOU CAN FIND THE TIME
- FULL BLOWN SOLUTION WILL TAKE YOU 20,000 CODER HOURS (10 CODERS FOR 12 MONTHS)
- LIGHTWEIGHT RISKY SOLUTION WILL TAKE YOU 10,000 CODER HOURS (10 CODERS FOR 6 MONTHS)
- MAINTENANCE AND SUPPORT WILL TAKE YOU 5200 HOURS PER YEAR (2 CODERS FOR 12 MONTHS)
- HIGH RISK TO BREAK YOUR AWESOME APP AND USER EXPERIENCE
- HIGH RISK TO CAUSE USER CONFUSION AND LOSS OF CUSTOMERS
- MAY LOSE SOME OR ALL CUSTOMER RECORDS
- MAYBE SSL PINNING IS THE MOST YOU CAN DELIVER
- MAY PROTECT SOME OF THE PORTS SOME OF THE TIME
- TIME TO DEVELOP AND DEPLOY: 6-12 MONTHS
- **COST TO DO IT YOURSELF: $1.2M**
- **ANNUAL COSTS TO KEEP IT UP TO DATE: $650k**
- **COSTS TO AVOID PATENT INFRINGEMENT: $500k-1.5M**

vs.

LICENSE OUR AppSHIELD SDK

- ✓ PROTECTED ACCESS TO PATENTED AND PATENT PENDING SOLUTIONS
- ✓ LEVERAGE YEARS OF MOBILE SECURITY EXPERTISE
- ✓ LOW REPUTATIONAL RISKS
- ✓ EXTREMELY SECURE AND PROVEN SOLUTION
- ✓ 7x24x365 CYBERSECURITY PROTECTION
- ✓ THE SOLUTION IS DONE
- ✓ THE SOLUTION HAS BEEN PROTECTING MILLIONS OF TRANSACTIONS SINCE 2014
- ✓ MAINTENANCE AND SUPPORT IS INCLUDED
- ✓ INCLUDED IN THIS SYSTEM:
  - → ZERO DAY MALWARE PROTECTION
  - → ADVANCED PERSISTENT THREAT PROTECTION
  - → FEATURES INVISIBLE TO CONSUMER EXPERIENCE
  - → ALL MOBILE APP CUSTOMER PII PROTECTED
  - → MILITARY GRADE ENCRYPTION
  - → REAL-TIME DATA LEAKAGE PROTECTION
- ✓ **TIME TO INTEGRATE AND DEPLOY: 3-5 BUSINESS DAYS**
- ✓ **NO INFRINGEMENT RISKS ONCE LICENSED: FIRST OF ITS KIND IP**
- ✓ **ANNUAL UPDATE COSTS A FRACTION OF DO IT YOURSELF**
- ✓ **PRICING IS A NO-BRAINER (MUCH MUCH LOWER)**

GET IN TOUCH

Toll Free: 1-800-991-3871 x1000 www.snoopwall.com securitysolutions@snoopwall.com

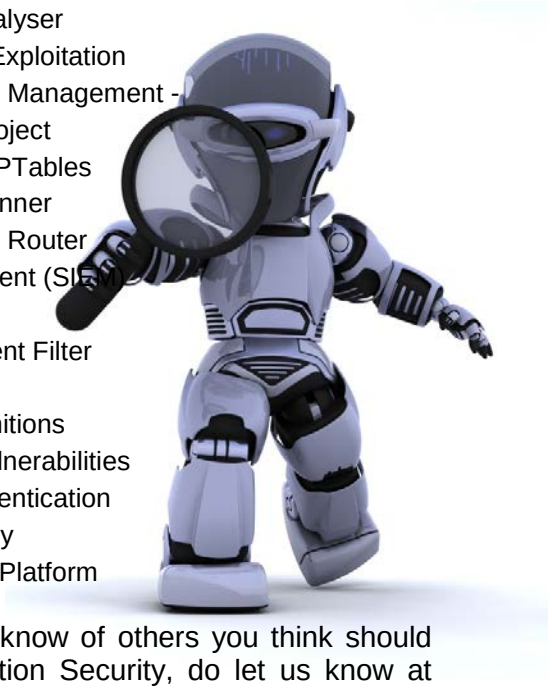
Top Twenty INFOSEC Open Sources

Our Editor Picks His Favorite Open Sources You Can Put to Work Today

There are so many projects at sourceforge it's hard to keep up with them. However, that's not where we are going to find our growing list of the top twenty infosec open sources. Some of them have been around for a long time and continue to evolve, others are fairly new. These are the Editor favorites that you can use at work and some at home to increase your security posture, reduce your risk and harden your systems. While there are many great free tools out there, these are open sources which means they comply with a GPL license of some sort that you should read and feel comfortable with before deploying. For example, typically, if you improve the code in any of these open sources, you are required to share your tweaks with the entire community – nothing proprietary here.

Here they are:

1. TrueCrypt.org – The Best Open Encryption Suite Available (Version 6 & earlier)
2. OpenSSL.org – The Industry Standard for Web Encryption
3. OpenVAS.org – The Most Advance Open Source Vulnerability Scanner
4. NMAP.org – The World's Most Powerful Network Fingerprint Engine
5. WireShark.org – The World's Foremost Network Protocol Analyser
6. Metasploit.org – The Best Suite for Penetration Testing and Exploitation
7. OpenCA.org – The Leading Open Source Certificate and PKI Management -
8. Stunnel.org – The First Open Source SSL VPN Tunneling Project
9. NetFilter.org – The First Open Source Firewall Based Upon IPTables
10. ClamAV – The Industry Standard Open Source Antivirus Scanner
11. PFSense.org – The Very Powerful Open Source Firewall and Router
12. OSSIM – Open Source Security Information Event Management (SIEM)
13. OpenSwan.org – The Open Source IPSEC VPN for Linux
14. DansGuardian.org – The Award Winning Open Source Content Filter
15. OSSTMM.org – Open Source Security Test Methodology
16. CVE.MITRE.org – The World's Most Open Vulnerability Definitions
17. OVAL.MITRE.org – The World's Standard for Host-based Vulnerabilities
18. WiKiD Community Edition – The Best Open Two Factor Authentication
19. Suricata – Next Generation Open Source IDS/IPS Technology
20. CryptoCat – The Open Source Encrypted Instant Messaging Platform



Please do enjoy and share your comments with us – if you know of others you think should make our list of the Top Twenty Open Sources for Information Security, do let us know at marketing@cyberdefensemagazine.com.

(Source: CDM)

National Information Security Group Offers FREE Techtips

Have a tough INFOSEC Question – Ask for an answer and 'YE Shall Receive

Here's a wonderful non-profit organization. You can join for free, start your own local chapter and so much more.

The best service of NAISG are their free Techtips. It works like this, you join the Techtips mailing list.

Then of course you'll start to see a stream of emails with questions and ideas about any area of INFOSEC. Let's say you just bought an application layer firewall and can't figure out a best-practices model for 'firewall log storage', you could ask thousands of INFOSEC experts in a single email by posting your question to the Techtips newsgroup.

Next thing you know, a discussion ensues and you'll have more than one great answer. It's the NAISG.org's best kept secret.

So use it by going here:

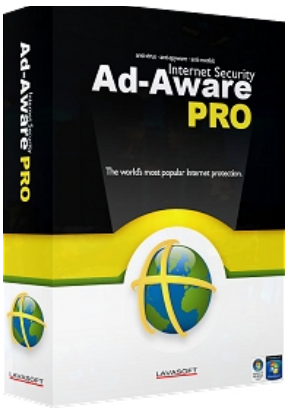
http://www.naisg.org/techtips.asp

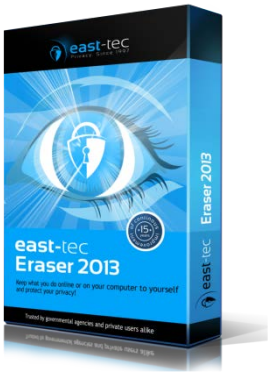
SOURCES: CDM and NAISG.ORG

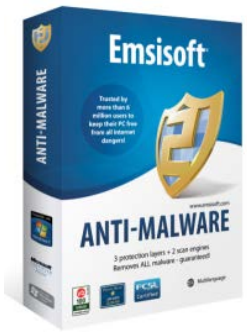
SIDENOTE: Don't forget to tell your friends to register for Cyber Defense Magazine at:

http://register.cyberdefensemagazine.com

where they (like you) will be entered into a monthly drawing for the Award winning Lavasoft Ad-Aware Pro, Emsisoft Anti-malware and our new favorite system 'cleaner' from East-Tec called Eraser 2013.







Job Opportunities

Send us your list and we'll post it in the magazine for free, subject to editorial approval and layout. Email us at marketing@cyberdefensemagazine.com

Free Monthly Cyber Warnings Via Email

Enjoy our monthly electronic editions of our Magazines for FREE.

This magazine is by and for ethical information security professionals with a twist on innovative consumer products and privacy issues on top of best practices for IT security and Regulatory Compliance. Our mission is to share cutting edge knowledge, real world stories and independent lab reviews on the best ideas, products and services in the information technology industry. Our monthly Cyber Warnings e-Magazines will also keep you up to speed on what's happening in the cyber crime and cyber warfare arena plus we'll inform you as next generation and innovative technology vendors have news worthy of sharing with you – so enjoy.

You get all of this for FREE, always, for our electronic editions.

Click here to signup today and within moments, you'll receive your first email from us with an archive of our newsletters along with this month's newsletter.

By signing up, you'll always be in the loop with CDM.

CDM

CYBER DEFENSE MAGAZINE™

THE PREMIER SOURCE FOR IT SECURITY INFORMATION

Cyber Warnings E-Magazine May 2017

Sample Sponsors:

To learn more about us, visit us online at http://www.cyberdefensemagazine.com/

Cyber Warnings Newsflash for May 2017

Highlights of CYBER CRIME and CYBER WARFARE Global News Clippings

Here is a summary of this month's cyber security news. Get ready to read on and click the links below the titles to read the full stories. So find those of interest to you and read on through your favorite web browser…

New 'Judy' malware on Android may have infected 36 million devices

http://bgr.com/2017/05/29/judy-malware-android-infections/

Microsoft patched more Malware Protection Engine bugs last week

https://www.theregister.co.uk/2017/05/29/microsoft_out_of_band_patches/

Chipotle releases information on malware attack; Utah locations impacted

http://kutv.com/news/local/chipotle-releases-information-on-malware-attack-utah-locations-impacted

MICROSOFT QUIETLY PATCHES ANOTHER CRITICAL MALWARE PROTECTION ENGINE FLAW

https://threatpost.com/microsoft-quietly-patches-another-critical-malware-protection-engine-flaw/125951/

This is the easiest way to prevent malware on your Android device

https://www.cnet.com/how-to/the-best-way-to-prevent-android-malware/

The silver lining of a global malware attack

https://www.csindy.com/coloradosprings/the-silver-lining-of-a-global-malware-attack/Content?oid=5582687

MALWARE NETWORK COMMUNICATION PROVIDES BETTER EARLY WARNING SIGNAL

https://threatpost.com/malware-network-communication-provides-better-early-warning-signal/125874/

Hackers are hiding malware in subtitle files

https://techcrunch.com/2017/05/24/hackers-are-hiding-malware-in-subtitle-files/

Malware strike underscores need to protect computer data

http://www.houstonchronicle.com/business/jaylee/article/Malware-strike-underscores-need-to-protect-11177003.php

Hackers upgrading malware to 64-bit code to evade detection

https://www.scmagazineuk.com/hackers-upgrading-malware-to-64-bit-code-to-evade-detection/article/664526/

More malware is making the rounds -- but this time it's invisible

http://money.cnn.com/2017/05/18/technology/windows-adylkuzz-cryptocurrency/

How a $10.69 purchase may have sidelined the global malware attack

https://www.washingtonpost.com/news/worldviews/wp/2017/05/13/a-british-researcher-says-he-found-a-kill-switch-for-the-malware-crippling-computers-worldwide/?utm_term=.2c786e052778

Federal Computers Dodge Global Malware Attack ... This Time

http://www.npr.org/2017/05/22/529518708/federal-computers-dodge-global-malware-attack-this-time

Network analysis can find malware before it strikes

http://www.networkworld.com/article/3197949/security/network-analysis-can-find-malware-before-it-strikes.html

Cyber Defense Magazine
848 N. Rainbow Blvd. #4496, Las Vegas, NV 89107.
EIN: 454-18-8465, DUNS# 078358935.
All rights reserved worldwide.
marketing@cyberdefensemagazine.com
www.cyberdefensemagazine.com

Cyber Defense Magazine - Cyber Warnings rev. date: 05/30/2017