# CDM

**CYBER DEFENSE MAGAZINE**

THE PREMIER SOURCE FOR IT SECURITY INFORMATION

# CYBER WARNINGS


**DECEMBER 2014**

***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 Victor
stevinv@cyberdefensemagazine.com

EDITOR

PierLuigi Paganini, CEH
Pierluigi.paganini@cyberdefensemagazine.com

ADVERTISING

Jessica Quinn
jessicaq@cyberdefensemagazine.com

KEY WRITERS AND CONTRIBUTORS

Tom Scearce
Chris Rouland
Todd Weller
Tim Clark
Mav Turner
Gary Miliefsky
Daniel D. Brecht
Nate Lord
Ben Johnson
Dennis Lee
Milica Djekic
Calum MacLeod
Patrick Kehoe
William O'Brien
Paul Brubaker
Giorgio Bonuccelli
Stuart
Tal Klein
Arman Sidhu
and many more…

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®


# What Should We All Learn from The Sony Pictures Exploitation?

It's been splattered all over the news like a paintgun full of red ink. Sony Pictures Entertainment – exploited beyond reason. Some say this breach will cost them more than one hundred million dollars ($100M). They had five movies stolen and plastered all over the P2P file sharing sites. They had 47,000 records (or more) stolen. Very embarrassing executive emails leaked. Is this Sony's fault? Some would blame their CISO, but he actually left the job in September, 2014. Many say their policies were insufficient and that makes a lot of sense. But ultimately, even the FBI has stated that 90% of businesses in the USA would have been easily exploited like Sony. Why is this?

Most organizations don't have centralized security event information management. Most do not have up to date information security training for best practices, to be mandatorily taken by all their employees. Most organizations don't have proper password management, backup policies, encryption polices and on top of that, they don't know how to deal with zero-day malware including the newest remote access Trojans (RATs). Our executive producer predicts 2015 will be the Year of the RAT and I sadly must agree with him – when so many organizations don't know they are already being exploited, they are already infected, it's only a matter of time for them to end up on the front page news or on the PrivacyRights.org database list of recent breaches.

Isn't it about time we start looking for the more innovative solutions to these problems? Why not manage risk with next generation solutions – maybe from smaller, more nimble vendors. I look to the many new kids on the block who show up at RSA Conference 2015 with a new idea for password management or a better way to bring your own device (BYOD) or real-time encryption and backups that don't bog you down. I'm not looking for the big names to help us because their tools are the top visible and easily exploited. Firewalls don't cut it anymore. Antivirus is dead. It's time to take a new and more bold approach to information security. The basic lessons we can learn from Sony Pictures are that policies must be best practices, in place, under review and audit constantly, if we are to avoid being infected by RATs and losing our data. This breach was a wakeup call. Please enjoy this edition of CDM focused on getting one step ahead of the next threat.

To our faithful readers, Enjoy

Pierluigi Paganini

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

# Will the Public Cloud Ever be Safe for Enterprise Files?

*By Tom Scearce, Senior Product Marketing Manager, Attachmate and Novell*

Controlling corporate data. It's the number one priority for enterprise IT. Several recent breaches into public consumer cloud services (significantly among them Dropbox, JPMorgan Chase, PayTime, Inc., Deltek, and many more, including Goodwill Industries) have proven that security concerns for enterprise files are justified. So what's the solution?

Obviously better security systems, but choosing among the many offerings often comes down to which vendor is the cleverest marketer, and that's a dangerous trend. As the enterprise file-sync-and-share (EFSS) market continues to heat up – there are now more than 120 third-party vendors vying for market share, many leveraging the public cloud – many vendors have created clever marketing campaigns that promise innovative solutions with top-notch security, but they are often fraught with peril.

In a nutshell, here's how these vendors work:

- Target tech-savvy consumers and mobile professionals with free, easy-to-use file sharing software.
- Give generous amounts of free storage to these users, who in turn recruit their friends, collaborators, and clients to use the software.
- As these network effects take hold, monitor the platform for accumulations of users within large enterprises.
- Pitch a company-wide license to these enterprises, presenting active user counts as proof that "the people have spoken, and our product has won."

Unfortunately, IT leaders are put in the awkward position by top management: Choose a "winner" among several EFSS products that often genuinely lack adequate, enterprise-grade security and management features. If you're one of the IT leaders being asked to make these uncomfortable trade-offs, pay attention to what follows.

**It's popular, so it must be secure. Right?**

As has been proven time and again, just because everyone is doing something doesn't make it a good idea. Take late-1920s America, and the rush to buy stocks on margin, or the lax real estate market before the financial crisis of 2008. History reminds us that rising tides eventually fall. And when it does, many ships are left stranded.

There's a parallel in the current EFSS market. It is extremely risky for enterprise management to assume, despite the claims of some EFSS vendors, that end-user adoption numbers have any bearing on a product's readiness to meet enterprise security requirements. This is particularly true for enterprises in highly regulated industries like healthcare, finance, and education.

The aforementioned Dropbox is just one EFSS public cloud vendor that, having accumulated end users on a "freemium" basis, is attempting to gain traction in the enterprise segment. With recent breaches as proof, Dropbox and other cloud-based file sharing tools, including Google Drive and Box, have some security issues to overcome before becoming truly enterprise-ready.

Here are just a few examples that highlight these concerns:

- In 2011, Dropbox disclosed that all of its users' files were publicly accessible for almost four hours. As VentureBeat reporter Sean Ludwig noted, this snafu underscored the security risks of cloud services. When all of your files are stored on another company's servers, can you trust that company to keep your data safe?
- In August 2012, Dropbox announced that some usernames and passwords were stolen from other websites and their accounts were accessed. Since this security breach came on the heels of Dropbox's snafu just three months earlier it led many to question whether the cloud is secure enough for the enterprise. Karsten Strauss at Forbes stated in his article on the security breach that, "This type of central intel hub – these server facilities and their contents – may require more than tweaked third-party security software to assure safety."
- This past May – just one month after Dropbox released its enterprise-facing product Dropbox for Business product – BBC announced that users of some cloud-based file storage services such as Dropbox and Box could be at risk of inadvertently leaking their own files as a result of a sharing function that creates a public link. Intralinks uncovered the problem when it found links to documents including bank statements and mortgage applications during routing use of Google's Adwords and Analytics services.
- In May 2014 Google announced a security hole in Google Drive where clicking hyperlinks within a document sent referrer data to a website, meaning the owners of the site could see the document's URL. Even though the issue was fixed quickly, a weak spot remains because anyone who has or guesses a private link can still access it.
- Dropbox has also been battling an ongoing malware problem – black hats have discovered how to use Dropbox's features to spread malware, particularly the kind that holds your files hostage until you pay a fee. Dropbox tests for viruses and malware using a variety of different anti-virus and anti-malware programs, but Slashgear reported on June 23 that these abuses of Dropbox's services are still happening.
- And most recently, an anonymous Pastebin user claimed to have hacked 7,000,000 Dropbox accounts and posted several hundred username-password pairs as proof of the claim. Dropbox issued a confusing statement in which they said they had "not been hacked," but that the credentials were stolen from third party services and used to attempt to gain access to Dropbox. Dropbox then went on to say they had "previously detected these attacks and the vast majority of the passwords posted have been expired for some time now." So, apparently they were not hacked. But they were attacked, and they fended off the "vast majority" of those attacks "some time" ago. But it's not yet clear what we should call the not-vast minority of attacks that were not thwarted.

**Still not ready for enterprise prime time**

Dropbox recently took steps to improve matters by announcing Dropbox for Business API, which connects Dropbox for Business with a variety of third-party enterprise tools that can

provide an extra layer of security. The move is meant to ease IT managers' security concerns, but will it be enough to earn the trust of enterprise customers, who have more to lose than their smaller counterparts?

Dropbox Vice President for Enterprise Strategy Ross Piper confirmed that the company does not take security as seriously as enterprises when he said in an interview with FierceEnterprise Communications, "If you can get five times the number of users to use it, it's OK to give up a little bit of security control."

I wonder how many CIOs and IT Directors at large enterprises share Mr. Piper's view?

In an interview with TechCrunch, 451 Research analyst Alan Pelz-Sharpe sums up why Dropbox's strategy isn't suitable for enterprises: "Dropbox has been so successful to date by being end-user friendly and largely ignoring IT." He added that Dropbox is going to have to find a way to balance the needs of both, but that will be much easier in SMBs than in large enterprises. "In the much bigger small and mid-sized business market," he said, "it's much easier to meet their administrative and security requirements without compromising ease of use – these buyers don't typically have the complex integration, process or compliance requirements that Fortune 1000 firms do."

This statement can easily be applied across the board – all of the popular cloud-based file sharing vendors offer intuitive user interfaces and experiences, but most are seriously lacking in the security department. In order to be enterprise-ready, the two sides must be balanced out.

**About the Author**

Tom Scearce is a senior product marketing manager at Attachmate and Novell, two leading providers of advanced software that helps make the workplace more productive, secure and manageable. Over the span of his career, Tom's experience in marketing strategy, business development, sales operations and program management has helped companies grow revenue, predictably and profitably. Tom can be reached online on LinkedIn at www.linkedin.com/in/tomscearce, on Twitter at @ TLOTL and at the companies' websites http://www.attachmate.com and https://www.novell.com.

# Why Visibility is Critical to Securing the Internet of Things

*By Chris Rouland, Founder & CEO, Bastille*

Depending on which analyst firm you tend to believe, it is estimated that there are currently between 10-13 billion connected devices worldwide. In addition, projections forecast an explosion of devices will hit the mass market– everything from wearables and Bluetooth to home appliances and medical devices – adding up to 50 billion connected devices or more by 2020.

As the world becomes increasingly more connected, there is a rising fear over the security of corporate and personal privacy within our hyper-networked environments.

The majority of the world is still adapting to threats using the Internet as a means to exploit device vulnerabilities. In fact, businesses and consumers are paying more attention to cybersecurity concerns than ever before, as evident by the projected growth of the Information Security Market, which is largely expected to exceed $125 Billion in 2015, according to Global Industry Analysts.

But a recent study from Israel's Ben-Gurion University paints a different picture; one that suggests we might not be securing all of the right networks and devices in all of the right places, as environments once considered impenetrable are now at realistic risk of falling victim to malicious cyber activity.

The Ben-Gurion University researchers, Mordechai Guri and Professor Yuval Elovici, recently created Airhopper, an application that can read keystrokes from an isolated network machine, also referred to as an air-gap environment.

Using a compromised cell phone and a connected set of ear buds acting as an antenna, Airhopper was successful in using a cell phone's built-in FM radio receiver to intercept radio frequencies (RF) coming from a computer's video display.

What does this mean? Essentially, it means that critical data can be stolen, in real-time, from a machine that is **completely offline.**

Of course, there are limitations to Airhopper's capabilities. For one, it has a short range of transmission at only 7 meters; and it is also very slow, only capable of transmitting at 13-60 bytes per second. Despite its current range and speed confines, Airhopper and other technologies warrant real concern from information security executives.

Critical and sensitive data, such as passwords and credentials, are now at 24/7 risk of penetration, whether the devices they reside on are offline or on.

So if cyber threats no longer require an Internet connection to cause havoc, what can be done to keep a company's assets and infrastructure safe? How can companies ensure the personal privacy of their employees, vendors and the thousands of daily visitors coming in and out of their offices?

It might surprise you to hear that the answer goes back to the old adage: an ounce of prevention is worth a pound of cure.

As we've discovered, cyber threats are no longer distinct to wired outlets. Thus companies – big and small - are beginning to understand that cell phones, tablets, and the thousands of other wirelessly connected devices pose real, non-linear risks that are continuously evolving in sophistication and frequency over relatively short periods of time.

While reaction to this *Wild West* of vulnerabilities, outside of the world's largest corporations, has been slow; the vast majority of companies are finally responding by implementing Bring Your Own Device (BYOD) policies.

Unfortunately, many of these policies only secure what goes *out* through devices and pays little attention to what these devices may be *bringing in*. A fix here is to develop a more comprehensive Internet of Things (IoT) policy; yet to date, there has been little discussion and virtually no implementation of such policies.

In 2014, workplace cyber crime will account for over $100 billion. In addition, IDC predicts that within the next 2 years, 90% of all IT networks will have an IoT-based security breach, although many will be considered "inconveniences."

Whether an inconvenience or a catastrophe, these statistics are staggering, and illustrate the immediacy needed to create policy that can detect and mitigate what defines the vast diversity of f 21st century cyber threats.

Airborne security, for example, will rely heavily on detection - knowing what devices are supposed to present in an environment and what devices should not. As with Airhopper, today's most common methods of security and detection would not see the FM transmission signal responsible for facilitating a data breach – and an attack using these protocols would have been successful.

The Airhopper study also illustrates the importance of utilizing the technology that exists to passively read electromagnetic leakage with a simple smart phone. Of course, hardware exists that can remove the speed and data transmission barriers illustrated in the Airhopper study and allow for RF data collection from much further distances.

With the emergence of the IoT and the proliferation of devices in corporate airspaces, the world is quickly approaching a whole new way in which the bad guys can compromise enterprise infrastructure.

Solutions empowering corporate security professionals with greater insight into situational awareness, both in and around their cyber environments, are being developed. As the Airhopper study revealed, the IoT makes it imperative that RF emission detection be a major component of cybersecurity solutions moving forward.

But hackers and threat actors won't wait for these technologies to be perfected, so CISOs and corporate executives need to take notice, and most importantly, action to secure the new world – one comprised of the Internet of Things.

**About the Author**

Chris Rouland founded Bastille Networks in 2014 after more than 25 years in the information security industry. Most recently, Chris founded Endgame Systems, which provides cyber security solutions to the defense, civilian and national security communities.

As founder and CEO of Endgame, in just three years, he grew the company from his basement to nearly 100 employees with offices in Washington, Atlanta and San Antonio and from revenues of $0 to more than $10 million. Chris also put together a world-class team of investors and board of directors investing over $58 million in venture capital - making Endgame a name brand in cyber security. His innovation and leadership combined with Endgame's rapid growth, earned Chris the Metro Atlanta Chamber's Business Person of the Year in 2011.

Prior to founding Endgame, Chris served as chief technology officer at Internet Security Systems Inc. (ISS) where he was responsible for the overall technical direction of its product and services portfolio. In 2006, IBM Corp. purchased ISS, where Chris remained CTO and was appointed an IBM Distinguished Engineer.

From 1994 to 1998, Chris served as vice president of distributed technology at Lehman Brothers. A noted information security expert, Chris is a sought after speaker and has been featured in national publications, including Forbes and Wall Street Journal.

# Are Your Files Protected From The Cloud?


**GoAnywhere™** is a **managed file transfer solution** that tightens data security, improves workflow efficiency, and increases administrative control across diverse platforms and various databases, with support for all popular protocols (SFTP, FTPS, HTTP/S, AS2, etc.) and encryption standards.

With robust audit logs and error reporting, GoAnywhere manages file transfer projects through a browser-based dashboard. Features include Secure Mail for ad-hoc file transfers and NIST-certified FIPS 140-2 encryption.

**Visit GoAnywhere.com for a free trial.**

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

**GoAnywhere.com 800.949.4696**

SAVES US A LOT OF TIME AND HEADACHE


"It's helpful every single day as the lifeline for communications with our customers."

Matt Booher
*President*
*WIS:DOM Information Systems*

# You've Been Hacked- Now What?

*By Todd Weller, VP, Corporate Development, Hexis Cyber Solutions*

One of the main reasons the Target data breach received so much attention -- and was able to cause so much damage -- was because it took place over the holiday season, the most heavily trafficked online shopping time of the year.

Over the past year, we have seen countless other major retailors become victims of cyber-attacks and we see how easy it is for adversaries to compromise networks and steal important information. It's only a matter of time before you experience the same. Why? Because hackers only need to exploit one vulnerability and defenders need to cover all of them.

It typically just takes a single user unknowingly clicking on a link and the hacker is in. Once this happens, the damage can be extensive.

As we cross the one year mark from the Target breach, we are reminded of the valuable lesson these breaches have taught us this year: **it is a matter of *when, not if*, you will be breached**.

Organizations need to constantly be on the defense against cyber attacks and be prepared with the proper systems in place for when they are breached. This will help them effectively and efficiently handle the attack and minimize the damage done.

To help mitigate the impact of an attack now and in the future, the following five-step plan outlines a methodical approach your IT team should have in place to reduce the amount of time a breach can live and wreak havoc in your network.

1.) **Detect and Identify:** Once the IT security team has validated that the organization is faced with a malicious situation and not just 'noise,' they need to react quickly and establish a cross-functional team to oversee all aspects of the response process.
2.) **To Contain or Not to Contain?** After identifying the nature, extent, and severity of the attack, team members are faced with two options: contain it or proceed directly to removal.
3.) **Remove and Recover**: To remove the threat and recover, the team must identify all infected hosts on the network and then must take necessary precautions to effectively stop and kill all active processes of the attacker.
4.) **Be Proactive:** APTs often return with nuanced versions of the attack, so it is absolutely critical that organizations take a proactive stance to break the cycle.
5.) **Automate Incidence Response:** Automation goes hand in hand with a proactive approach. Automation eliminates the need to perform manual work provides an opportunity for huge cost savings.

Will your organization know how to react in the event of a Holiday data breach? Visit the Hexis Information Center for case studies on companies that already have the tools in place to identify and remediate attacks.

If you feel or know you've been attacked, take a look at our eGuide, "Five Things To Do After You've Been Hacked," which provides you with a plan of action to take, and what actions you should avoid taking, to ensure no further damage happens.

**About the Author**

Todd Weller, VP, Corporate Development, joined Hexis Cyber Solutions in March 2014. His responsibilities include analyst relations, competitive and market intelligence, corporate visibility, M&A, and strategic partnership development. Todd draws on his 17+ years of experience as an equity research analyst where he covered the security industry for much of that time. In his equity research career Todd provided research coverage of over 60 companies across several technology sectors, including security, infrastructure software, data center/cloud hosting, and healthcare IT.

*Connect with Hexis online: http://www.hexiscyber.com/*

*Hexis Blog: http://www.hexiscyber.com/blog*

*Twitter: @hexis_cyber*

*LinkedIn: https://www.linkedin.com/company/hexis-cyber-solutions*

# Help Avoid Hacking This Holiday

*By Tim Clark, The FactPoint Group, on behalf of Hexis Cyber Solutions*

With the holiday season in full swing, and online shopping activity more popular than ever, it's important that everyone remain vigilant about their cyber security habits. Cybersecurity is a shared responsibility and it's important that everyone do what they can, even by taking a few simple steps, to help make the internet (and your corporate network) safer from cyber threats.

As IT, security or business executives, don't make the mistake of thinking that consumer oriented cyber threats as irrelevant to your enterprise. Your users—employees, customers, partners—also utilize the Internet for personal reasons, so the same tips and messages for consumers apply equally to your own eco-system.

A smartphone infected with malware at a consumer website is still infected when it logs onto your corporate network. Think your bring-your-own-device policy protects you? Think again. Your users are actively trying to circumvent your BYOD policy because it's faster and easier for them to use their software (or device) than yours.

What guidance should you offer your users? Start with these:

1. **Set strong passwords**: combine numbers, symbols, and letters (uppercase and lowercase). Don't share them with anyone.
2. **Install updates**: keep your operating system, browser, and other critical software optimized on all your devices: laptops, smartphones, tablets, desktops.
3. **Keep it to yourself**: limit the personal info you post online and use privacy settings to avoid sharing information widely. This includes posting anniversary dates, birthdays, your home address, vacation dates or details, etc.
4. **Stranger danger:** Don't open emails, links, or attachments from unknown aliases, strangers, or if the subject line seems suspicious.
5. **Back up:** or copy sensitive and critical information and databases. Sync your contacts, photos, videos and other mobile device data with another device or cloud service weekly.
6. **Make a list** and inventory of your most critical equipment, hardware and software.
7. **Watch out for prying eyes**: when using a public, unsecured wireless connection (coffee shop wi-fi, airlines, library, hotel), avoid using apps or websites that require you to enter a password.
8. **When in doubt, turn it off**: for mobile, switch off your Wi-Fi and Bluetooth connections when not in use to help prevent malicious parties from connecting to your device without your knowledge. A 3G or 4G connection is safer than an unsecured Wi-Fi connection.
9. **Lock it up**: on mobile, activate key-lock features and/ or use a passcode. If your device allows for a complex password, take advantage of the feature.

10. **Activate locator apps**: many mobile manufacturers have free apps you can download to help you locate your device in the event it gets lost or stolen. These apps may allow you to remotely lock the device or wipe data.
11. **Think before you app**: only download apps from reputable sources, like verified app stores. Understand what information (i.e., location, social networking profiles, etc.) the app would access and share before you download.
12. **Record the serial number**: by dialing these five characters – *#06# – you can access your phone's unique, 15-digit International Mobile Equipment Identity (IMEI) number. Write this number down and store in a secure location, so you can report it if your phone goes missing.

These tips are simple and may seem obvious to some, but they are also easy to disregard when not top of mind. By sharing these ideas with your users, you can help keep their holiday, and your business, cyber hack free.

**About the Author**

Tim Clark is a partner at industry research firm The FactPoint Group. Follow Tim on Twitter: @TimClark

*Connect with Hexis online: http://www.hexiscyber.com/*

*Hexis Blog: http://www.hexiscyber.com/blog*

*Twitter: @hexis_cyber*

*LinkedIn: https://www.linkedin.com/company/hexis-cyber-solutions*

# Don't Believe the Hype – The Sony Snowball

*By Todd Weller, VP, Corporate Development, Hexis Cyber Solutions*

Sony Corp. is not having a great year. Over the past few weeks, we've learned that Sony Pictures Entertainment suffered a cyberattack that brought down the company's corporate email systems.

Last week, we learned that they fell victim to another attack – a major hacking breach that exposed over 25 gigabytes of sensitive data on tens of thousands of employees at the company, including Social Security numbers, medical and salary information.

Earlier in the year, we also learned that Sony's network operations were disrupted for almost a week's worth of time and that unreleased films from the industry giant were leaked online.

It was disclosed that Sony Corp's PlayStation Network and Sony Entertainment Network had been disrupted by hackers via a DDoS attack. You can read an overview of the hack here.

Following this turbulent series of events, many have pointed a finger at North Korea, citing that their motive lies behind the release of a Sony-produced film, "The Interview," featuring Seth Rogen and James Franco.

The comedy follows two media workers who are asked to assassinate the leader of North Korea, Kim Jong-Un.

While it's easy to draw parallels between Sony's hacking incidents and the releasing of this film, we as security experts must warn the general population, "Don't Believe the Hype" – not yet, at least.

While it may be easier to lay the blame on an organization or country that certainly appears as though it fits the criteria of the perpetrator, the general population as a whole should take a step back and allow those investigating the details of the attack to do their jobs.

Instead of playing the blame game, perhaps what we as an industry should do is recognize that there is in fact a bigger problem at hand.

Until recently, organized cyber criminals were targeting industries that played major roles in the way our country is run – government, financial institutions, healthcare organizations, etc.

However, as of just a few weeks ago, it appears as though the entertainment industry is at risk now, too.

In today's cyber battlefield, it's clear that no one is untouchable. Tighten up your security initiatives and know that the best offense is a strong defense.

**About the Author**

Todd Weller, VP, Corporate Development, joined Hexis Cyber Solutions in March 2014. His responsibilities include analyst relations, competitive and market intelligence, corporate visibility, M&A, and strategic partnership development. Todd draws on his 17+ years of experience as an equity research analyst where he covered the security industry for much of that time. In his equity research career Todd provided research coverage of over 60 companies across several technology sectors, including security, infrastructure software, data center/cloud hosting, and healthcare IT.

*Connect with Hexis online: http://www.hexiscyber.com/*

*Hexis Blog: http://www.hexiscyber.com/blog*

*Twitter: @hexis_cyber*

*LinkedIn: https://www.linkedin.com/company/hexis-cyber-solutions*

# Is a False Sense of Security Putting Your Organization at Risk?

*By Mav Turner, Director, Security, SolarWinds*

Target, Home Depot, Sony and Jennifer Lawrence. Just a year ago, most would be hard-pressed to think of a commonality between these besides the fact that they are all well-known entities. Now, however, the answer is obvious—all have been victims of cyber-attacks resulting in loss of sensitive information.

As security breaches persist in the headlines day after day, business leaders and the public at large feel less confident about where their data is stored, how it is transmitted and what steps companies are taking to ensure sensitive information is secure.

So, it may be perplexing to learn that a recent SolarWinds survey found that 84 percent of IT professionals believe their organizations are "very secure"—that is they fall in at least the 30$^{th}$ percentile of the most secure organizations. Even more stunning is that 15 percent of those said their organizations are in the top 10$^{th}$ percentile. In addition, 87 percent said they feel their IT departments currently have sufficient resources to keep their organizations secure.

Where is this confidence stemming from? Increased budget, man-power and integration between security and other IT processes and operations, such as network and system administration, are likely driving it.

For example, 74 percent of those surveyed reported their departments' security budgets increased from last year to this year. Moreover, only 1 percent said their organizations do not have at least one staff member responsible for security, and 97 percent said they have more than one. This man-power could explain why 61 percent said they are able to test their defenses at least monthly. Finally, 47 percent said their IT departments tightly integrate security and other IT processes and operations, while all others reported at least some level of interaction

However, this begs an obvious question: Does this confidence indicate a false sense of security, thereby increasing organizations' risk and vulnerability, or are the measures organizations are taking really that effective?

Unfortunately, the survey results indicate the former is more likely. For example, though nearly 30 percent of respondents do not believe their organizations are a target for an attack and another 27 percent said they feel they are at low risk of a successful attack, 82 percent reported their organizations have experienced a significant attack, with approximately one-third of those reporting that it took at least one month to discover the attack. Furthermore, approximately one-third also said it took at least one month to recover from the attack. Underscoring this is that nearly 40 percent said their organizations either do not have defined security best practices or if they have them, do not regularly follow them.

This all underlies the dangers of falling into the trap of over-confidence. IT should do everything it can to ensure the best defences possible, but never actually think everything needed to create a secure infrastructure is done. In order to do this, IT should consider the following:

- *Get back to basics:* First of all, confirm your organization has security best practices established. If not, create them. By maintaining records of procedures, every IT employee—not just the security admins—can immediately pick up the playbook and help out if necessary. These best practices should go beyond just testing and incident response policies, they should also include internal contact information, vendor and security tool information and more. Also, once developed, follow the security best practices. This is where the rubber meets the road—in the operationalization of the guidelines and policies that the organization should adhere to.
- *Take a data-centric approach rather than a network-centric approach:* Instead of thinking in terms of the number of VPNs or where to install firewalls, IT should think in terms of where and how data is stored, and how attackers will try to access and use it. Break it down in terms of most sensitive data first and work out from there.
- *Assign a dollar value to risk in order to show direct impact of how security success—or failure—directly impacts the business:* This will not only gain corporate buy-in toward more resources and personnel, but showcase the value of IT security as a true revenue protector within the organization.
- *Consider what kind of IT tools are really needed according to business needs:* High-end, complex enterprise-grade security tools are only helpful if they're being utilized correctly and to capacity. IT tools are far more effective when they directly meet business needs, aren't constantly scrutinized from a budgetary perspective and are easily implemented and used on an ongoing, regular basis.

In summary, while IT professionals' confidence in their organizations' security readiness is high, likely as the result of several positive developments, these same organizations continue to suffer from damaging attacks, indicating the confidence could be a false sense of security preventing them from more closely following security best practices and safeguarding their organizations' infrastructure. However, by following the best practices outlined here, they can ensure they are proactively taking all the steps necessary to truly protect their organizations' sensitive data.

**About the Author**

Mav Turner is the director of SolarWinds' security portfolio. He has worked in IT management for over 14 years, including roles in both network and systems management prior joining SolarWinds in 2009.

AccoladeTechnology

# Advanced Application Acceleration & Host Offload

## Dual Port 100 Gbps NIC for:

Network Security & Forensics | Network Monitoring | In-Line DPI | Test & Measurement | Network Probes | Application Performance Management & more…

View Dual 100 Gbps NIC Specifications

## 200 Gbps Packet Capture NIC for Cyber Security & Network Monitoring Applications

### OEM Customer Applications:

- Network Security & Forensics
- Network Monitoring
- Application Performance Monitoring
- Next Generation Firewalls
- In-Line DPI
- Network Probes

### Key Features:

- Line Rate Packet Capture
- Packet Filtering & Header Slicing
- Packet Classification
- Load Balancing
- Deduplication
- Flow Classification

View ANIC-200K (2 X 100 Gbps NIC) Specifications

### Other ANIC Advanced Packet Analysis NICs:

| | |
|---|---|
| ANIC-100K | 1 X 100 GigE |
| ANIC-40K3 | 4 X 10 GigE |
| ANIC-20KH | 2 X 10 GigE |
| ANIC-4KL | 4 X 1 GigE |

### OEM Customer Software Development Guide (SDG) And Support:

Software Reference Manual & Sample Code | Comprehensive API Documentation | Firmware Customization | Dedicated Product Integration Support | Linux, FreeBSD & Windows Drivers

For More Information: info@accoladetechnology.com

# 2015: THE YEAR OF THE RAT – THREAT REPORT

## Reflecting on the Sony Pictures Entertainment Breach

While the Chinese Zodiac calls 2015 the "Year of the Sheep" (how apropos), I predict that 2015 will be the Year of the Remote Access Trojan (RAT). It all started in November, 2014, when Sony Pictures Entertainment (SPE) was hacked. Many speculated it was a 'malicious insider' but the facts show it was something very different and something you should expect when you least expect it.

Let's take a quick look at the SPE attack and realize that it's the tip of the iceberg for what's coming our way in 2015. If you don't take actions and head my warnings to get more proactive in protecting your personal privacy (see: http://www.snoopwall.com/halting-hackers-on-the-holidays/) and also in your business environment, avoid being phished and infected with RATs, then you might actually be one of the sheep losing your fleece in 2015.

### How Sony Pictures Entertainment Was Hacked – Maliciously From the Outside

The story is an 'internal administrative' password was used to take down Sony Pictures Entertainment (SPE). That is a tiny piece of the real story. It's easy to get an admin password, especially when it's stored in a file called "Usernames&Passwords" in clear text on an adjacent system in the same computer network, if you've already deployed a RAT.


### Antivirus is Dead

The first problem is that so many computers throughout the globe are infected with zero-day (new) malware. In fact, when NTT tested the top antivirus products for a year, in their recent report, they concluded that between 50-70% of the malware made it passed their antivirus scanners. That means, and I've been saying this for years, that Antivirus is dead.

Just look at this May 4, 2014 Wall Street Journal article, where Symantec's senior vice president for information security, Brian Dye, told the *Wall Street Journal* that antivirus "is dead." If you

can't detect the malware and you're already infected, then what can it do? How about controlling your computer and using it as one of many 'hops' in the chain to obfuscate the source of an attack? If you get infected with one of these Zero-day RATS (Remote Access Trojans), you're not only a victim, you are an accidental accomplice.

### Remote Access Trojans

Remote Access Trojans (RATs) that make it onto a computer, undetected, give someone far away all the control they need of the victim's computer. RATs are generally sent through emails by 'riding' what looks like as a trusted file attachment such as a PDF, Excel spreadsheet or Word doc.

Once the victim opens the email and clicks on the attachment, they may actually see a useful or trustworthy looking PDF, XLS or DOC open up but at the same time the RAT is being installed. Some less sophisticated RATs will display a fake error message 'file corrupted' so you think the attachment didn't come through completely and didn't open.

Many RATS can disable antivirus and firewall software or create covert channels to bypass them, when sending and receiving information, commands, data and files.

RATs can do just about anything you can think of – this is a sampling of what they are capable of:

- Watch you type and log your keystrokes
- Watch your webcam and save videos
- Listen in on your microphone and save audio files
- Take control of your computer
- Download, upload and delete files
- Physically destroy a CPU by overclocking
- Install additional tools including viruses and worms
- Edit your Windows registry
- Use your computer for a denial of service (DoS) attack
- Steal passwords, credit card numbers, emails and files
- Wipe your hard drive completely
- Install boot-sector (very hard to remove) viruses

A well-designed RAT will allow the operator the ability to do anything that they could do with physical access to the machine. RATs can be used to install additional tools so a program to upload or download files can be installed secretly – what a great way to move an entire electronic copy of an upcoming movie onto a peer to peer file sharing network?

### Phishing Attacks – Social Engineering 101

According to Phishme.com, "Phishing can be defined as any type of email-based social engineering attack, and is the favored method used by cyber criminals and nation-state actors to carry out malware and drive-by attacks.

These are fraudulent emails disguised as legitimate communication that attempt to trick the recipient into responding – by clicking a link, opening an attachment, or directly providing sensitive information. These responses give attackers a foothold in corporate networks, and access to vital information such as intellectual property.

Phishing emails are often carefully crafted and targeted to specific recipients, making them appear genuine to many users.


Phishing is effective, low-cost, bypasses most detection methods, and offers criminals little chance of capture or retribution. It's little wonder then that several prominent security firms have confirmed it to be the top attack method threatening the enterprise today, with security firm TrendMicro noting that spear phishing accounts for 91% of targeted attacks, incident response consultant Mandiant citing spear phishing as Chinese hacking group APT1's most common attack method, and Verizon tracing 95% of state-affiliated espionage attacks to phishing."

### Lex Parsimoniae: Here's What Most Likely Happened

Understanding the means, the motives and the capabilities of the 'actors' involved, and using Occam's razor - the least assumptions, problem solved:

1) SPE puts out a teaser in June, 2014

2) A Nation state reacts in June, 2014 and asks both The Whitehouse and UN to halt release of the movie “The Interview”
3) No response to their request and threat to pull “The Interview”, to them an ‘act of war’.
4) Between July, 2014 and October, 2014, a crack team from a large cyberarmy is charged with Reconnaissance (RECON) on Sony Pictures Entertainment for the deployment of a highly targeted Phishing attack that deploys a RAT.
5) Internal network RECON takes place, files are stolen by being transferred (uploaded) to other RAT victims, not directly to the attacker, in this case most likely a cyberarmy.
6) File uploads, email and records pilfering along with hard drive wiping tools were most likely controlled by Command and Control (C&C) RAT servers located outside of the US with other computers controlled remotely inside the US.
7) Pilfered files are leaked, threats are made through spoofed IP addresses accessing gmail accounts to make tracing difficult.
8) 9-11 type threats are made to trick Sony and Movie Theaters into blinking. They blinked.
9) US Government and top security forensic professionals (FBI.gov, Mandiant, Fireeye) figure this all out as well and share some of this information including the fact that the malware was developed on Windows in the Korean language (most likely using WINE running Windows on a linux derivative OS). The Whitehouse reacts, now that the initial forensics is complete and the POTUS is fully briefed.

## Can We Protect Against This Type of Attack?

If my analysis is correct then any organization could defend against this attack, in spite of the FBI’s statement that 90% of businesses would have been victimized (this is probably true, sadly).

To defend against this attack, even though “Usernames&Passwords” was one of the files discovered, with plaintext passwords like the word “password”, that’s not what triggered the attack, changing those passwords would have made it a longer and harder RECON and pilfering period but it wouldn’t have stopped them. It’s very embarrassing for SPE to have used such foolish passwords and file names.

But that’s not the heart of the problem. Here’s my view:

1) We're all infected and don't know it. Assuming you are infected positions you better to proactively harden your systems and remove zero-day infections. With this key assumption, you need to backup all your data files, wipe and reimage your computers and install only legally owned copies of software.

2) You can't let Smartphones and Tablets onto corporate networks (bring your own devices – BYOD dilemma) unless they can be managed. This also means deleting all apps and then starting to install trustworthy apps from sources you know and trust. How many apps do we have installed without knowing if they have backdoors or they, themselves, are not just tools and games but are also RATs in disguise?

3) Employees at Sony are not trained like employees at Coca Cola. This company hasn't had a breach or lost a secret formula in 100 years. Cyberarmies could attack Coke for the formula and most likely would never succeed in getting it, using the means they used on Sony. Why? Because Coke practices Employee Training (for social engineering), has frequently tested and updated security policies (including physical security, people security and network security) and they don't leave the secret formula out in the open – they practice COUNTERVEILLANCE (see http://www.snoopwall.com/free to take my free beginner's course on this subject matter).

## Best Practices for 2015

Working backwards, reviewing this Sony Pictures breach, we can see lots of reactive behavior. Why not get proactive instead of reactive by:

a) Training Employees Better
b) Hardening Systems (see: http://nvd.nist.gov)
c) Detecting and Removing RATs
d) Deploying Full Disk Encryption and Real-time Backups
e) Defending Against Phishing Attacks
f) Managing the BYOD Dilemma

Of course it's easier said than done. The biggest weakness at SPE was their employees and if you can't train them to behave better and understand phishing attacks, proper password

management and leverage full-device encryption, storing important information always encrypted and frequently backed up, then what can you expect but another successful breach from the inside out.

I would suggest we all start writing emails as if everyone in the world can see them. Sony Pictures executives have learned this lesson the hard way. But, again, that's not what caused the breach, that's data that was stolen and used against them – that's just throwing salt in the wound. The real issue is that all employees need better security training.

**How Do RATs Travel Behind Corporate Firewalls?**

While most folks think it's the phishing attack (through the email port – the front door) as the only and key point of entry, you need to start assuming that most of your **smartphone or tablet apps are creepware** – malware that spies on you and your online behavior – **many free apps are RATs**. Do you really need them? Delete all of the apps you aren't using that often. Replace those apps that take advantage of too many of your privacy settings like GPS, phone & sms logs, personal identity information, with similar apps that don't.

If you don't manage this bring your own device (BYOD) dilemma then expect RATs on your portable devices to invade your corporate network.

**Coca Cola Practices Counterveillance – You Should Too**

How old is the Coca Cola recipe? Has it been hacked or stolen in over 100 years? So what is Coca Cola doing better than everyone else?

They are doing steps a) through f) above and frequently checking and rechecking their security posture. If you don't have a plan, expect to be a victim in the Year of the RAT. If you can make the important information "invisible" to the malware – the RAT, then they can't steal it.

Practicing Counterveillance, like Coca Cola could be the most important thing you do for privacy and security. Think about it. If you could be invisible, no one could see you. They wouldn't know when you are browsing the web or using your smartphone.

If you could make all the private information about yourself become completely invisible, no one could every steal it. That's right – your personally identifiable information (PII) could not be stolen if no one could see you or your data.

It's so simple – it sounds too good to be true. Right? If you could make yourself invisible, if you could hide your PII from prying eyes, you would be practicing counterveillance. That's right – you would be countering surveillance.

## What makes the US B2 Stealth bomber so unique?

It disperses its radar signature so that it becomes invisible to traditional radar – the design of the 'skin' of this aircraft is a counterveillance technology.

It is possible to become nearly invisible but you're right to think it's very challenging – many would say nearly impossible.

However, if you start out with this as a goal 'how do I make my data invisible to criminals and hackers?' then each day you should be working to reach this goal – to build your own B2 Steath bomber – a more secure and encrypted database, better password management, real-time backups, defense against RATs and phishing attacks and ultimately better trained employees who realize that 'loose lips sink ships.'

### About SnoopWall

At SnoopWall, we invented the world's first counterveillance technology and filed an international patent on it. This technology is very very hard to implement on computers and mobile devices – but we're doing it anyway.

We have some of the best programmers in the world working hard every day, building our counterveillance solution. We're going to help your computer and mobile device become

'nearly' invisible. That means hackers, cyber criminals, online predators, cyber terrorists and other ne'er do wells won't be able to find you or your confidential information. It won't matter how advanced their malware becomes – advanced persistent threats (APTs)? No problem! Zero-day Malware? No problem! If they can't see you or your data, they can't steal it. Hard to implement but simple to understand.

**About The Author**

Gary is the Founder of SnoopWall and the sole inventor of the company's new technology. He has been extremely active in the INFOSEC arena, most recently as the Editor of Cyber Defense Magazine and the cover story author and regular contributor to Hakin9 Magazine. He also founded NetClarity, Inc., an internal intrusion defense company, based on a patented technology he invented. He is a member of ISC2.org, CISSP® and Advisory Board of the Center for the Study of Counter-Terrorism and Cyber Crime at Norwich University. He also advised the National Infrastructure Advisory Council (NIAC) which operates within the U.S. Department of Homeland Security, in their development of The National Strategy to Secure Cyberspace. Miliefsky is a Founding Member of the US Department of Homeland Security (http://www.DHS.gov), serves on the advisory board of MITRE on the CVE Program (http://CVE.mitre.org) and is a founding Board member of the National Information Security Group (http://www.NAISG.org). Email him at: ceo@snoopwall.com.

Sources: SnoopWall.com, FBI.gov, CIA.gov, wikipedia.com, USCERT, and public domain information.

# Are Cyber Threats the New Terrorism Frontier?

*by Daniel D. Brecht, IT Freelance Writer*

Today, we live in a high-tech world of uncertainty. The more we become dependent upon technology in our everyday lives, the more threats are developed. The perception for end users is that the Internet is no longer a safe and secure avenue for research and development, to communicate, find information, send/receive email, engage in file sharing, conduct online chat and collaboration.

The Internet has unfortunately been a playground for cybercriminals who employ increasingly sophisticated methods to carry out their agenda. Newly emergent attacks have become more frequent, dangerous and complex these days; this is shown by the upswing in hacking incidents targeting the US financial system as well as government agencies.

The rise of security threats also involves, increasingly, the Internet of Things. Physical systems that interface with digital networks are vulnerable to online cyber-criminals who look to turn a connection-oriented machine into a possible threat against intended targets.

An interesting trend, however, relates sudden increases in threats to political events. The rise of threats against financial systems in the US, such as the theft of gigabytes of data from JPMorgan Chase's system, coincided, for example, with the escalation of tensions between Russia and the US over the crisis in the Ukraine. Was this just a coincidence?

Given the number of high-profile cybersecurity incidents, IT/IS experts say the level of sophistication of targeted attacks suggests that cyber-based terrorist threats are becoming more real; cyber-terrorism may become a critical element in people's lives over the next decade. It is believed that the risk of cyber-terrorist attacks is likely to exceed the danger posed by current terrorist networks.

**Cyberterrorism: how real is the threat?**

Although real cyber terrorism attacks have not been launched in full scale yet, a number of incidents have demonstrated the potentially devastating effects of concerted large scale strikes. The fact that many attacks seem to be directly related to political objectives highlights the increasing interest of terrorists for the digital world, and for a good reason.

While conventional attacks, in fact, are carried out necessarily on the spot and represent a risk for those who perpetrate them (think about the use of kamikaze for example), cyber-attacks are potentially risk-free as they can be carried out from anywhere, against any target.

Effects can be even more devastating than traditional attacks as the target is not necessarily a single group of people, a building, a city, but can actually be an entire infrastructures and

system to affect millions of people at a time. Affected systems could be of financial nature, classified information databases, utilities, and air travel-related security systems. It is easy to imagine how devastating would be a hacking attack to a missile ballistic defense system.

Terrorism through the Internet is a war unlike any other; the use of cyber technology against systems to disable communications, install malicious code, infect with malware, damage or place out of service for a period of time can be carried out at any time an in way that leave few traces and are hard to track.

The mediatic appeal of such attacks not only increases cyber fear in users but also creates a perfect sounding board for terrorists looking for maximum exposure. However, have threats been exaggerated? How safe are national infrastructures? What kind of damage would it take to qualify as cyberterrorism? Nevertheless, the threat posed by cyberterrorism has grabbed the attention of politicians, security experts, and the public.

With cyberspace constantly evolving so is our expectation of security of digitized information that is stored, shared, and communicated online over computer networks. The way attackers have exploited end users' systems to cause damage or disruption even in organizations known to be employing maximum security (government agencies, Apple, Microsoft, etc.) shows that much needs to be done still to secure our digital systems.

What makes things harder is the knowledge that secure systems can actually be easily compromised by a single careless end user, a disgruntled employee, through the exploitation of a basic security loophole or the simple failure of following basic security procedures. It's that easy.

**Today's cyber-security landscape**

Cybersecurity experts say the road to establishing a truly safe Internet in unclear. Fears over the potential threat of cyberterrorism is increasing and leading to what is described as a "cyber world war," a new global arms race against international countries that engage in any cyber threat acts and attacks. International relations are already becoming more active in both cyber offense and defense.

The implications of cybersecurity go well beyond cyberspace; it influences everything from cybercrime to unimaginable threats and attacks that affect our online freedom to engage in instant messaging, obtain specific web content, send and receive data. IT experts say that people do care about keeping their computer systems secure, but behave otherwise and continue to ignore web security warnings and proceed anyway online without considering safe security techniques in order to minimize the number of successful cyber security attacks. Humans are considered to be the weakest link in any security chain.

**Agitation in cyberspace**

While cyberspace has grown to be loved and needed for Internet-connected devices, it is increasingly becoming a place of risk and danger, vulnerable to hacks and cyber warfare. People may question if cyberwar can ever actually be called a war but, from a cyber-security perspective, the simple answer is yes. Although cyber warfare has never formally taken place yet, a cyberwar is a significant threat and may take place in the near future.

Some experts believe that the mere hacking of critical systems does not count as cyber warfare but are simply security loopholes that outside hackers often exploit. However, as the motivation of malicious hackers will go from economic or social to purely ideological, there is a potential for an escalation of attacks that can potentially affect the military and intelligence functions of world governments and aid high-level spying; therefore the threat is real and it is to be considered a war, albeit of a newer, technological kind.

**Anxiety over of Cyberwar and Cyberdefense**

The notion of cyberterrorism has sparked several studies on the potential risks. As the cyberspace consists of systems and technologies that are typically connected to other information systems on the Internet, it is an excellent breeding ground for attacks.

Over and over again, weaknesses are exposed that are giving end users the impression that no one is safe.

In some cases, weaknesses in America's industrial control systems have allowed intruders unauthorized access to networks routed through the cyberspace infrastructure. Cyber Risk Intelligence says the increasing interconnectivity of Industrial Control Systems (ICS) to the Internet should be secured and tested to ensure vulnerabilities are mitigated and risks minimized, as they have become vulnerable to cyber-attacks.

Recently, the Department of State has been the target of a massive attack that has led to the complete shutdown of its e-mail system and a complete overhaul of its cyber security stance. Hackers had breached their security perimeter and its unclassified system. Another unforeseen breach that was discovered at the White House computer systems (in October) has been tied to a criminal group in Russia.

Nations like China have conducted massive electronic probing of networks in the U.S., say cybersecurity experts. Nevertheless, cybersecurity issues challenge literally everyone.

Even more recently, a security service firm has published a report outlining the cyber activities of Iranian hackers who allegedly penetrated the systems of a number of government agencies and infrastructure companies in several countries, including the United States.

The attack was carried out against targets in a variety of industries and sectors from education to technology, defense, chemical and aerospace, and it supposedly led to the theft of highly sensitive material.

As the news is released, it's easy to see how anxiety over a possible cyberwar attack builds up and is actually fueling tensions between nations. Leaders are beginning to recognize the potentials of a coordinated cyber-attack.

President Barack Obama, lately, indicated cyber terrorism as one of the biggest threats to national security and called for heightened attention on cybersecurity. The president believes that attacks similar to those already perpetrated against government agencies and banking institution (like JPMorgan) can not only lead to massive theft of sensitive data or money, but can also generate a dangerous state of chaos in any nation, United States included. It seems many cybersecurity experts agree.

Recently, it has been reported by the media that a top intelligence chief has highlighted that a major vulnerability is in the U.S. power grid. Normally attacks to utilities are not as glamorous and interesting from a media standpoint, but they could potentially be more destructive than data loss and privacy breaches as they would affect massive numbers of people and impair activities in a much more pervasive way.

As unlawful attacks and threats of attacks against computers, networks and the information stored therein continue, nations are organizing concerted efforts to create defenses and recovery strategies by pulling efforts together. Organizatins like the European Advanced Cyber Defence Centre (ACDC) or the Internet Engineering Task Force (IETF) work towards the creation of protocols and mechanism to minimize threat while governments appoint ad-hoc committees and task forces to review current vulnerabilities and solve them. IT/IS professionals need to deploy advance technology to protect systems and services from the risk of security breaches, threats and malicious attacks.

However, without proper security features built into Internet-related technology, end users will need to become "experts" to better understand and handle cybersecurity issues at their office or home. In essence, they must learn to fight battles in their online domains.

**Terrorism-based Cyberwar**

So, does cyberwar make sense for terrorists? Definitely; at least until target countries will find foolproof, effective ways to secure their system even when connected to networks and to easily identify, track and quickly locate the perpetrators of the attacks.

Without a way to avoid terrorism-based cyberwar attacks, then the Internet could be turned into a weapon used against citizens by terrorists hidden in cyberspace and physically located elsewhere.

Who knows what is yet to come, but the prospect of cyber war looms ahead of us and remains unclear. In a sense, we are all in some way cyber warriors that engage in protecting cyberspace domains to defend against those who wish to attack our networked systems. It's easy to be afraid not knowing much about the enemy, but technology is so much a part of our life and lifestyle that it is virtually impossible to step back and minimize its impact. This pervasiveness in everyone's life is what makes cyberwar so palatable to terrorists. Cyberspace is a warfighting domain, and once that is clear, nations can effectively prepare themselves proactively and effectively.

**About The Author**

Daniel Brecht has been writing for the Web since 2007. His interests include computers, mobile devices and cyber security standards. He has enjoyed writing on a variety of topics ranging from cloud computing to application development, web development and e-commerce. Brecht has several years of experience as an Information Technician in the military and as an education counselor. Brecht holds a graduate Certificate in Information Assurance and a Master of Science in Information Technology.

CI Energy Group's Inaugural Summit on

# Cyber Security *for* Energy

January 21 – 22, 2015 » TELUS Convention Centre » Calgary, AB

## *The intelligence and tools you need to protect critical assets from cyber attacks*

Global cyber-attacks on critical infrastructure continue to increase in frequency and Canada's energy sector is by no means exempt. Hacktivism, state sponsored attacks, cyber terrorism and industrial espionage are but a few of the emerging threats facing the oil, gas and utility sectors. Antiquated strategies, such as anti-viruses and firewalls are no match for the sophisticated hackers of today. Senior executives and their respective organizations must take a proactive and technologically-advanced approach towards cyber security if they hope to safeguard critical assets and avoid damaging and costly liability claims.

**CI Energy Group's Inaugural Summit on Cyber Security for Energy** was designed in tandem with the country's leading experts and promises to deliver the up-to-the minute information and critical strategies your organization needs to make sound security planning decisions.

### Hear from Leading International Experts including:

- Shell Canada
- North American Electric Reliability Corporation (NERC)
- Enbridge Inc.
- Nexen Energy ULC
- ENMAX Power Corporation
- TransCanada

### Hear Vital Information to Inform your Security Planning:

- Understand the latest threats targeting the Canadian energy sector
- Conduct thorough vulnerability assessments for oil, gas & utilities
- Learn innovative and effective approaches for planning, preparing and responding to cyber incidents
- Protect SCADA systems from emerging cyber threats
- Evaluate the Board of Directors' oversight into cyber security
- Assess Canada's cyber security regulatory framework and understand how it can be improved

### Benefit from hands-on workshops:

A **A Step-by-Step Guide to Conducting Vulnerability Assessments**

B **A Primer on Planning, Preparing and Responding to Cyber Attacks**

PRESENTED BY: CI Energy Group

SPONSORED BY: CGI, Check Point Software Technologies Ltd., iON Secured Networks, Fortinet, intel Security, Symantec, TELUS, THALES

MARKETING PARTNER: CDM

Priority Service Code: 270DX02

REGISTER NOW » 1-877-927-7936 » **www.CanadianInstitute.com/CyberforEnergy**

# The CISO's Job: Untangling the Wild Web of Security Vendors

As we reflected on all the buzz from October's National Cyber Security Awareness Month, the sheer amount of vendors in the information security space was starting to make our heads spin! From software vendors and service providers to analysts, conferences, and organizations, the information security industry has grown into quite a large and noisy space. As one of those vendors there are certainly pros and cons: more attention from venture capital firms, but at the same time, more competition in the market.

As National Cyber Security Awareness Month passed, we recognized how difficult this makes the CISO's job. In a time when companies are under constant attack, they're left with a plethora of security vendors that all seem to be saying the same thing. One can't blame a CISO for feeling overwhelmed by all these options. Further complicating matters is the fact that many of these companies offer complex networks of different solutions designed to handle different security functions. Can you imagine beginning an RFP process only to have multiple companies come back with products falling outside of the initial scope?

Adding another layer of complexity is the industry debate about the best approach to protecting data. For many years, a layered approach to security has been most popular, with the majority of investment going to the network layer. Lately, however, this thinking has started to shift; Forrester Research has recently championed a data-centric approach to security. This philosophy turns the security stack on its head by focusing on the very thing that attackers (whether inside or outside the organization) are after: sensitive data.

So, after putting ourselves in the shoes of a CISO, we worked through many of the leading industry analyst reports and created the Information Security IndustryScape – a helpful little infographic designed to give a snapshot look at who's who in the security zoo. We've tried our best to be as exhaustive as a 1200x900 pixel space will allow, but it's inevitable that a graphic like this will never be comprehensive in such a rapidly moving industry. Think we left someone out? Let us know! This is only the first edition of our Information Security IndustryScape and there will certainly be more to come.

**About the Author**

Nate Lord oversees the social media and SEO programs at Digital Guardian. His work includes creating blog and multimedia content that provides unique insight into the information security industry.


## WHAT TO EXPECT

EXHIBITION SPACE

27,000 SQM

EXPECTED NUMBER OF EXHIBITING COMPANIES

250

EXPECTED NUMBER OF TRADE VISITORS

8,000

450
KEY DECISION-MAKERS FROM INTERPOL'S

190
MEMBER COUNTRIES

Contact us TODAY at +65 6389 6614 or sales@interpol-world.com

Event Owner: INTERPOL

Supported By: Ministry of Home Affairs; Singapore Exhibition & Convention Bureau

Supporting Knowledge Partner: Frost & Sullivan

Held In: YourSingapore

Managed By: MP international

# Unwelcome Guests:

## The Internet of Things and Wireless Networks

*By Cricket Liu, Chief Infrastructure Officer, Infoblox*

Earlier this year, Infoblox commissioned a survey of network managers and administrators on the Internet of Things. We were curious to find out whether enterprises were actually introducing non-traditional devices to their networks, and if so, where and how they were connecting them. After all, "Things" can have unique access requirements.

To use just my home as an example, my thermostat and smoke alarm need to connect through the Internet to Nest so that I can turn off my heat or AC when I inevitably forget to do so before leaving the house. My digital video recorder needs to talk to TiVo to make sure I've paid my monthly bill, to see whether I want to record anything new, and to download new TV schedules and code. And my car—even my car!—wants to create a VPN back to the manufacturer to download updates.

The sorts of Things enterprises are deploying boast an even wider variety of access requirements: security systems monitored by third parties, cafeteria cash registers uploading sales data to concessionaires, and remotely managed HVAC systems.

We learned that businesses certainly are connecting Things to their networks—a whopping 75 percent of those surveyed reported adding Things in the general category of "office equipment" to their networks, and 70 percent said they'd added "security" Things.

However, one finding of the survey that I found alarming was the increasing tendency to connect these "Things" to guest wireless networks. On the one hand, that trend is understandable: Many of these devices support 802.11 wireless, and many also require connectivity to the Internet to work. Guest wireless networks generally support both.

But in many ways guest wireless networks aren't at all suitable for IoT devices. In addition to requiring Internet connectivity, some devices need access to internal resources, too. For example, a security "Thing" might need access to a Domain Controller to authenticate users, and permitting that will probably require poking a hole or two in your firewall. But you probably don't want to allow any device on your guest wireless network access to a Domain Controller.

Guest wireless networks are, after all, used by a wide variety of users and devices. By definition, most of those users aren't employees (who presumably have access to your production wireless network). Simply knowing that you use a particular type of device and understanding this kind of device requires access to an internal server might induce a Bad Guy to search for a way through your firewall. Even if firewall reconfiguration isn't necessary, are you sure the traffic your Things send back to home base is encrypted? Does that traffic need prioritization? What effect would a misbehaving guest device have on your wireless network, and therefore your Things' ability to phone home?

The alternative, though it may sound onerous, is to create separate logical or physical networks for Internet of Things devices and traffic. These networks can support different authentication requirements from guest wireless networks and can support the access and prioritization requirements of IoT devices. Unfortunately, our survey showed that only 30 percent of respondents planned to implement separate IoT networks.

Things get trickier (literally) when different species of device have very different access requirements and can't easily or securely be mixed on the same network. For example, a third party might require remote access to one type of Thing, while another type of device might need to communicate with an internal database server to function—but you might not trust the third party to access that database server. How you handle that scenario is up to you, but you might consider creating different Internet of Things networks based on patterns of access: Things that need access to internal resources, Things that third parties on the Internet need access to, and so on.

Providing appropriate network access to the Things on your network is far from the only security challenge you'll face as we deploy the Internet of Things—there are the limited security features of some Things, the need to manage them and keep them upgraded—but at least you can use the networking tools you have at your disposal to address the problem.

**About the Author**

Cricket Liu is a leading expert on the Domain Name System (DNS) and Infoblox's Chief Infrastructure Officer. With more than 25 years of experience with enterprise-scale DNS infrastructure, technical writing, training and course development experience, Cricket serves as a liaison between Infoblox and the DNS community.

Prior to joining Infoblox, Cricket worked for HP for nearly 10 years, where he ran hp.com, one of the largest corporate domains in the world, and helped found HP's Internet consulting business. Cricket later co-founded his own Internet consulting and training company, Acme Byte & Wire. After Network Solutions acquired Acme Byte & Wire and later merged with VeriSign, Cricket became director of DNS Product Management.

Cricket is the co-author of all of O'Reilly's Nutshell Handbooks on the Domain Name System, DNS and BIND, "DNS on Windows NT," DNS on Windows 2000, DNS on Windows Server 2003, the DNS & BIND Cookbook, and DNS & BIND on IPv6, and was the principal author of Managing Internet Information Services.

# Preparing For 2015: Hindsight Is 20/20

**Five top global cybersecurity trends from 2014 can help companies prepare as they brace themselves for the "year of the endpoint"**

*By Ben Johnson, Chief Security Strategist, Bit9 + Carbon Black*

The information security market endured quite a year in 2014, with high-profile breaches compromising record-setting amounts of customer data.

While some would argue it's been a year for the record books, it's clear that things are not going to slow down anytime soon. Gartner research predicted the cybersecurity market would exceed $73 billion in 2014, while Market and Markets estimated it to now be worth more than $96 billion. Looking ahead, those figures are expected to nearly **double** over the next five years.

As the cybersecurity landscape continues to evolve, it's important to examine some emerging trends. While attackers continue to become more advanced and continually change their tactics, evolved security teams are now keeping pace…*if* they have the right approach.

As 2014 comes to a close, five key trends stand out that organizations should be aware of as they determine their security strategy and investments for 2015:

**1) Security is a process, not a technology.**

Companies are increasingly realizing that they can't just buy a security appliance or piece of software to become safe, or even defensible. As the saying goes: "There's no silver bullet." As a result, companies must invest in their teams and their overall security posture, going beyond just point solutions.

Trying to piece together best-of-breed solutions, leveraging APIs, and ultimately embracing a culture of "always on" security are some ways to act on this trend.

**2) Threat intelligence – security teams want it.**

"Threat intelligence" is the buzzword of the year. A good security posture starts with intelligence. Intelligence starts with information.

Individual security teams around the world are increasingly realizing that the security community as a whole can benefit if the right threat information is shared. Teams are becoming more educated about feeds, clearing houses, and types of threat intelligence, including protocols and formats. Organizations are collecting, analyzing and comparing information to understand not only their risks, but also the capabilities and techniques of the malicious threat actors targeting them.

Understanding the enemy enables organizations to adjust their defensive strategies and techniques appropriately. Leveraging threat intelligence is a key factor in that.

**3) The investment in cybersecurity personnel is on the rise.**

As the cybersecurity landscape evolves, teams are ripping out antiquated defenses (and people) and introducing new solutions and teams designed to accomplish two things:

1) Create defensible postures

2) Achieve cyber resiliency

Good leaders understand the need for a strong core of people, supported by technology that enables the team to be effective and fast. The goal is to create an environment where unauthorized code or unauthorized access does not lead to a massive, headline-making breach.

Additionally, organizations are increasingly hiring experts with law enforcement or defense community backgrounds and empowering them to build out a team comprising full-time programmers and other resources. Such practices were extremely rare even just a couple of years ago.

**4) Data and intelligence analytics are very popular**

It seems that security is not to be left out of the big data bandwagon, and with good reason. It is becoming increasingly difficult to pick out the suspicious traffic or malicious executables from the volumes of enterprise noise. Combine this with attackers' ability to "live off the land," (use built-in Microsoft and other tools) means that defenders have to move faster to compare current and historical activity to find anomalies.

While analytics isn't a new concept, the security community's discussion about them, the number of thought leaders pushing them, and the number of vendors trying to provide an analytics solution is exploding.

**5) The endpoint is the new perimeter.**

Security teams are beginning to assume that ALL of their assets, especially endpoints, are not adequately protected behind traditional, penetrable perimeters such as antivirus. Building a higher wall will no longer suffice. The perimeter, while still important, is deteriorating. By focusing on endpoint protection, security teams are putting their defenses where critical data resides.

Integrating network and endpoint defense (i.e., "layered" security) is an approach the many security teams are moving toward. The fact that more employees are working remotely or often traveling means organizations need to do more than just slide a network appliance into their rack to be secure. Before this year, the endpoint had been largely overlooked. 2015, however, will be the "year of the endpoint."

Recognizing and learning from these five 2014 trends will provide an advantage for companies across all industries navigating what's sure to be another rapidly evolving year in the world of cybersecurity. Don't let yours be the record-breaking breach of 2015. Take a look back; hindsight can be 20/20.

**About The Author**

**Ben Johnson** is the chief security strategist of Bit9 + Carbon Black. Prior to the merger, Johnson was cofounder and chief technology officer at Carbon Black. Johnson has extensive experience building complex systems for environments where speed and reliability are paramount. His background also includes a lot of technical "agility," having worked on advanced operational teams supporting U.S. national security missions and writing complex calculation engines for the financial sector. Johnson has degrees in computer science from the University of Chicago and Johns Hopkins University, and is a 35th Generation Shaolin Kung Fu Disciple.

*You can follow Ben on Twitter @chicagoben and read more on the Bit9 + Carbon Black website: https://blog.bit9.com/.*

# Actionable Approach to Fighting Cybercrime using Cyber Threat Intelligence

Actionable Approach to Fighting Cybercrime using Cyber Threat Intelligence

*By Dennis Lee, Territory Manager North America, Blueliv*

## Introduction

Organizations are finding themselves in a world where having defensive controls like a firewall, secure datacenter and stringent security policies is simply not enough. In 2014, we've seen companies like JP Morgan Chase, Sony Pictures and eBay pour millions into security programs, yet they still suffered from devastating and very public security incidents.

These organizations including private and public entities are getting tired of deploying layers of defenses, waiting for an attack. They want to take action and stop cybercriminals and state sponsored hackers by looking beyond their network.

One of the first steps in enabling an actionable security program is to use Cyber Threat Intelligence to uncover threats that are lurking in the shadows. This can be accomplished by:

- Acquiring raw feeds from the Government and other private organizations.
- Knowledge sharing with other Information Security teams in your industry.

Unfortunately, this leads to having too much data which becomes difficult to manage and ultimately non actionable. The solution is to use a Cyber Threat Intelligence platform that can identify cyber threats targeted to your organization in real time.

Let's explore the types of threat intelligence essential to know by using one of my customers who's a Global Life and Financial services entity– let's call them XYZ Corp.

## Botnet Intelligence

Entities need to identify bad cyber actors that threaten them. Many of these actors operate command-and-control servers that can issue commands to Botnets. Botnets can passively wait in silence or actively wreak havoc by:

- Launching dynamic and unpredictable DDoS attacks.
- Conduct large scale E-mail Spam campaigns.
- Serve as collection points for stolen data.

XYZ Corp can take action by:

- Initiating a botnet takedown to eliminate or paralyze criminal networks.
- Feed the botnet large amounts of false and unreliable data.
- Recover stolen data such as compromised passwords, credentials, credit card numbers, documents and much more. Afterwards, the entity can remediate the exposure.
- Proactively block, track and monitor a list of known crime servers.

**Hacktivism Awareness**

Organizations should be aware of what's being posted on social media sites, websites known for sharing stolen data and operations conducted by Hacktivist groups. XYZ Corp closely monitors this by analyzing real-time alerts and reports generated when keywords they specify are triggered.

For example, an alert is sent when a Hacktivist group like Anonymous uses Pastebin to expose information about XYZ Corp such as:

- Credentials to servers and websites.
- Personal details about corporate executives and officers.
- Trade secrets and other documents.

Organizations can also track campaigns such as #OpRemember which recently used Facebook, Twitter and Pastebin to coordinate cyber-attacks against dozens of companies in the financial sector. Stolen data is posted daily under #OpRemember since going live in November 2014. Organizations can take action by following established procedures to have the stolen data removed and trigger internal forensics investigations to mitigate further seizures.

There's seemly little you can do today about Hacktivist threatening or openly coordinating an attack against your organization. The unpleasant truth is they probably already breached your environment. However, intelligence provides you with the early warning needed to prepare and hopefully locate any previously undetected vulnerabilities and exposure.

**Brand Abuse Monitoring**

XYZ Corp tracks brand abuse which can damage their reputation by putting its employees, customers and others at risk. For years Internet users knew that misspelling the address of a popular website meant you would probably be sent to a malicious website. Criminals now use a combination of social engineering and spear phishing tactics to lure users into visiting malicious websites designed to steal information.

Cybersquatting and Phishing websites designed to look like your brand can be identified using threat intelligence. Once discovered, an entity can take action by:

- Releasing public or private notices alerting users of the threat.

- Initiate legal procedures to control domain ownership.
- Block access to malicious websites using URL filters.
- Report URLs to anti-phishing companies.

With the rise of Mobile computing, rogue mobile apps portrayed to be associated to an organization are a real threat. XYZ Corp found numerous apps that used their company name and logo available on several Appstores. An investigation concluded that the Apps weren't actually harmful scamware in this particular incident. However, do you really want an App out there which could pose as a potential liability?

- A future update to the application could reveal its true criminal intent.
- Your customer service line may receive calls regarding the application.

XYZ Corp learned of the existence of these Apps through Mobile App Monitoring intelligence and took action by having them removed from the Appstores.

**Malware Intelligence**

The industry has seen Malware spread stealthy and harmlessly, in some cases for years until it found its way into a target's environment.

Unfortunately, Antivirus products don't offer enough protection because the existence of these threats remains unknown until it's too late. Malware Threat intelligence allows organizations to proactively identify these threats. This is accomplished when Malware analysis or reversing discovers parameters associated to an entity such as their:

- Domain name and Domain SID
- Internal IP and IP Ranges
- Network naming conventions

An entity can work with law enforce to try and locate benefactors of the malware in order to take legal action. The entity can also work with security software companies to make the threat recognizable by their products.

**Conclusion**

In 2014, we've all witnessed or fell victim to some of the most sophisticated cyber-attacks ever seen. These attacks brought large organizations and governments down to its knees and subsequently caused billions of dollars in damage.

Threat intelligence is no longer just a military approach. Companies, small and large, should seek timely, high-quality insight and actionable intelligence for protecting their assets.

The days of being blind to external threats are over. It's time to take action– Follow XYZ Corp and contact companies like Blueliv to obtain Cyber Threat Intelligence. The platform addresses botnets, command & control, targeted malware, credit card theft, rogue mobile apps, hacktivism, data leakage, phishing, cybersquatting, brand abuse, and much more to turn global threat data into predictive, actionable intelligence specifically for each enterprise and the unique threats it faces.

**About The Author**

Dennis Lee has more than 14 years of cyber security experience and is currently Territory Manager North America of Blueliv, responsible for implementing the company's strategy in sales, partnerships and technology in the United States. He currently attends Lewis University in pursuit of a Master of Science in Information Security.

As a hobby, Dennis organizes the NY Information Security Meetup group which is currently the largest non-affiliated information and cyber security group in the United States.

Dennis was previously a Principal Systems Engineer at Symantec Corporation where he successfully worked in technical presales on the User Authentication team. He joined Symantec through the acquisition of PasswordBank Technologies. Under his leadership at PasswordBank, Dennis managed Engineering efforts in Sales and Product which contributed to the successful acquisition in 2013. In 2012, he was awarded by Microsoft the Most Valuable Professional (MVP) title for his work in Forefront security. He is also recognized as a reviewer to several Network Security publications by Packt Publishing written by Erez Ari from Microsoft.

Dennis can be reached online at LinkedIn and at our company website http://blueliv.com.

# INFOSEC WORLD 2015

Conference & Expo

March 23-25, 2015 | Disney's Contemporary Resort | Orlando, FL
Bonus Workshops March 21-22, 25-27


## Cyber Defense Magazine readers save 10%!

Register with discount code **OS15/CDM** and save **10% off the main conference pass.**
Call MISTI Customer Service today to secure your spot **508-879-7999 ext. 501**

WWW.MISTI.COM/INFOSECWORLD

# Cyber Security Today

*Milica Djekic, an Online Marketing Coordinator at Dejan SEO and the Editor-in-Chief at Australian Science Magazine*

*Cyber security is not a part of our future. It's something that is happening right now and today. Even if you do not move from your home, you can become a victim of cybercrime or, if you are on the opposite side, you can get the one who will commit a crime. It appears there is no safe place if you got an appropriate device and an internet connection. So, is that the fact for real? How could security support us in such a case? In this article, we plan to discuss the challenges of cyber defense of today and to review some models and approaches that will make a cyber security more efficient and comprehensive in practice.*

**Everyone Can Make a Cybercrime**

Nowadays it is easier than ever before to commit a crime. Billions of people worldwide got an access to the internet and all of them are a part of one big *cyber community* that is sometimes called *a global village*. In other words, we all are correlated with each other; we all can get in touch with each other and we all can affect each other though the cyberspace.

The global village is a very effective way to maintain communication between people, to make the information available to everyone, but also to expose a lot of IT systems to a certain cyber risk. It seems we cannot enjoy the benefits of our technological development without being concerned for our safety.

Cybercrime is something that can wait for us just behind the corner and cause us a lot of nightmares and worries. It's not any longer about a computer or data breach, but rather about the true financial, political or military harm.

Cyber criminals are very motivated when it comes to their business. It is their method to make a money, simply sitting in front of their computers and taking a minimum risk to get discovered. Seems so attractive, ha? Who could reject such an amazing opportunity, bad guys believe.

Well, we can get their point of view and we agree that in the world there are still concerning areas that will offer to cybercrime professionals to commit a crime and to stay unpunished. Those parts of the world should seriously think about the drawbacks in their legal system and try to develop mechanisms to respond to such a threat.

Many developing countries still miss efficient cybercrime laws and security procedures, so that could be one of the greatest challenges to cyber security of today, because those spots are not a problem on its own, but rather an issue to the rest of the world.

Everyone from such an region could threaten develop countries and make harm to our civilization. For that reason, we say that everyone could make a cybercrime.

**Cyber Security at the Moment**

These days a cyber security is facing up a new stage in its development. A modern cyber defense can be seen as a mix of monitoring, prevention and incident response. The accent of current cyber systems is still on a monitoring and mainly on a prevention, while an incident response appears as a field that needs a lot of effort and time invested in to get developed to full.

Let us try to explain why a monitoring and prevention are so important in modern security and how a progress of the incident response procedures could benefit this area.

Firstly, a monitoring is about tracking a situation in cyberspace and getting the information how the things inside a cyber system are linked to each other. It is a quite passive factor in cyber security, because it includes only an observation with a minimum action applied.

On the other hand, a prevention is a process of invoking measures and techniques that can help us avoid some undesirable conditions in the future. For instance, if we install an anti-malware software to our computer, we can avoid specific sorts of malware to infect our machine. In other words, it is a combination of passive and active principles in cyber defense.

Finally, we came to an incident response. It's a completely active factor in cyber security and covers a set of measures, techniques and procedures that are created to support a system that is under attack.

Further, we will talk about an actual cyber defense model that can assist us in having a better and more comprehensive insight into the situation within an IT infrastructure.

**Ways to Understand the Issue**

The best way to understand the problem is to make a good - either graphical or mathematical representation of the issue. You would agree with us that math seems as too complex to many, but a good drawing of your model can make things very simple and approachable to everyone.

For such a reason, in *Figure 1* we offer this simple and clear model of cyber security that can explain all we mentioned through this article and help us to have a better insight and an efficient observation of this area.

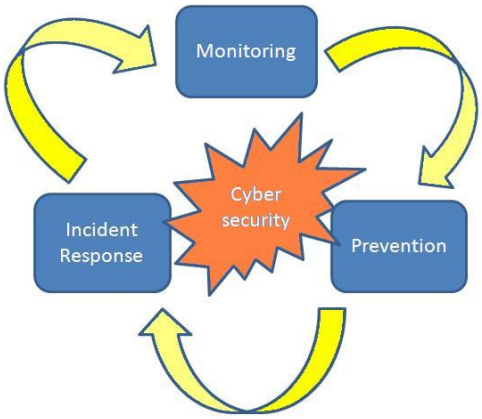



**Figure 1.** A cyber security flow chart

In this flow chart, we can see that monitoring, prevention and incident response are something that make cyber security and we can also notice how all of these elements are in correlation or, in other words, how they make a cycle or a flow.

You will agree with us that is a very elegant way to describe a problem and to make some steps forward in understanding its essence.

**Some Words at the End**

In this article, we make an attempt to provide a good graphical model of cyber security of today and consequently make you easier to see only through one picture something that normally needs to get described using many words. We hope this contribution is a good way to make a cyber defense clearer to a very broad audience and represent a quite complex concept in a pretty simple and "on the ground" manner. It's not that easy to get familiar with a cyber security of today, but, at least, we believe this representation was still a good approach.

**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. Currently, she's the Editor-in-Chief of Australian Science Magazine, as well as an Online Marketing Coordinator for Dejan SEO. She also serves as a Reviewer at the Journal of Computer Sciences and Applications. She writes for Australian and American security magazines. Milica is based in Subotica, Serbia.

American Conference Institute's
15th Advanced Global Legal & Compliance Forum on

# Cyber Security & Data Privacy and Protection

Inquire about in-house, government, and group rates

**January 15–16, 2015 | Washington Plaza Hotel | Washington, DC**

Pre-Conference (early a.m.) Workshop – January 15 • Post-Conference (p.m.) Workshop – January 16

Earn CLE Credits

***Featured Speakers From:***

FTC
U.S. DHS
FBI
NIST
U.S. EEOC
U.S. DOJ
U.S. CFTC
California DOJ
Missouri AG Office
Vermont Office of the AG
Illinois Office of the AG
Pennsylvania Office of the AG
MA Consumer Affairs and Business Regulation
TX Comptroller of Public Accounts
Interactive Advertising Bureau
Network Advertising Initiative

***Be sure to also book for Workshops A and B:***

A Privacy & Security 101

B Fundamentals of Cyber & Data Risk Insurance

This conference is approved for CPE credits, as an Approved Privacy Education Provider and Activity.

## Sessions Include:

- Federal Regulatory, Legislative, and Enforcement Landscape: Changes on the Horizon and Integrating New and Anticipated Initiatives Into Your Privacy and Compliance Program
- Unique Regulatory and Enforcement Insights by State Attorneys General and Consumer Protection Agencies on Emerging Privacy Initiatives, Settlement and Enforcement Trends, Security Breach Notification Requirements, and More
- INTERNATIONAL: Managing a Global Privacy Program and Preparing, Collecting, Using and Transferring Data Across Borders
- The Intersection of Healthcare and Data Security: OCR, HHS, and HIPAA Cyber Security and Data Privacy and Protection
- The Internet of Things: Privacy, Security, New Risks and Developing Threats
- Practicing Privacy by Design: Ensuring Cyber Security and Data Privacy & Protection Don't Become an Afterthought
- Cyber Security Preparedness: Best Practices for Data Breach Incident Response Teams With a Focus on Preemptive Measures to Take and Rehabilitating Your Image
- The Cloud: Best Practices on Third-Party Vendor Compliance and Negotiating Terms of Cloud Services Contracts and Service Level Agreements
- Privacy on Mobile Platforms and Privacy Disclosures for Mobile Apps: Best Compliance Practices
- Ensuring Compliance With Privacy Requirements for Online Behavioral Advertising and Marketing Initiatives: Cookies, "Do-Not-Track", and Other Behavioral Targeting Nuances
- Big Data in the Cyber Security and Privacy Protection Context: Aggregating Data, Data Analytics, Data Mining, and Privacy Rights
- Class Actions & Litigation Roundup: Recent Data Breach Cases, Mega Privacy Actions, TCPA and Texting Suits, and Assessing What Claims Are Worth

## Conference Co-Chairs

**Russell Schrader**
Visa, Inc.

**Ashley Taylor, Jr.**
Troutman Sanders LLP

***as well as:***

Prudential Financial
McKesson Corporation
NeuStar, Inc.
Motorola Mobility
Epsilon
GE Healthcare
Farmers Group, Inc.
SCOR Reinsurance Company
Northwestern Mutual
KAYAK Software Corporation
Marriott International
Hewlett-Packard Company
W.R. Grace
BNY Mellon
PPD
The Coca-Cola Company
Viewpost
Microsoft
PrizeLogic
Google
Freedom Specialty Insurance Co.
Condé Nast
Advocate Health Care
University Hospitals
Foursquare Labs, Inc.
AIG
IBM
Avon
Nationwide
AppNexus
Unum
Wyndham Worldwide

Register Now | 888-224-2480 | AmericanConference.com/Privacy

**Subscribers are entitled to $200 off registration with Discount Code: CDM200**

# Cyber Armageddon

## Is The Internet Spiraling Out of Control?

*By Calum MacLeod, Director, Behaviosec AB*

The doorbell rings and two lovely ladies are waiting for me, asking if I'm concerned about world events, and if I'm uncertain about the future. They offer me a small leaflet that's intended to provide the answers that I need to rest easy, and then they are on their way. No question they are well meaning, but they've been knocking on my door for years, seeking to calm my fears about the ozone layer, bird flu, climate change, global warming, global terrorism, and today it's Ebola.

And in cyber space the same holds true. Daily we have to deal with news about more breaches, identity theft, APTs, advanced malware, and cyber warfare threats. We are warned that we are rushing head on to a cataclysmic scenario where society itself may be thrown into chaos due to imminent attacks on everything from the financial system to the very physical infrastructure our lives depend on. Scenarios that show the complete breakdown of social order, resulting from sustained attacks on critical infrastructure which will bring everything from the banking system to the road haulage infrastructure that ensures our supermarket shelves are filled.

While preparing this article, news has broken of a second major breach at Sony, which implicates the North Korean government, and a report published by cyber security firm Cylance says Iranian state-sponsored hackers have hacked critical infrastructure of more than 50 organizations in 16 countries worldwide in a cyber-espionage campaign that could allow them to eventually cause physical damage.

### Living In A Virtual World

The majority of us spend most of our lives in a virtual world. We no longer visit our bank, because it's no longer there. Many of the goods we buy come from virtual stores, and in many cases our lives center on social media. And as a result, every day we share our identity and personal details in millions of locations.

My cell is no longer primarily used for phone calls. Today it's used for mobile banking, and various other services that offer convenience. My car is now accessible online. I can follow its location, turn on and off various features, simply by accessing an application on my cell.

But each and every one of these services require that they can identify me. And this is where it opens up a Pandora's Box. How many services does the average individual subscribe to, and how do they authenticate?

Each of us have potentially hundreds of subscriptions online, and we identify ourselves with an email address and a password. And in order to ensure that we can use the services, most

people will reuse the same credentials across multiple sites. I am probably pretty averages in having twenty plus services that I regularly use, and two factors are common on most of them – the username and password. My imagination and my intellect simply don't permit me to remember twenty unique passwords containing uppercase, lowercase, a numeric and a special character. So breaching my Target account and gaining access to my credentials simply opens up the door to probably every other service I subscribe to.

The problem is exasperated with the explosive growth of business cloud based services. Again the dependence on usernames and passwords means that the business users will frequently use the same password for their business applications as they use for their social media and consumer services. The only modification is likely to be their username which goes from a personal address to a business address, but the passwords stay the same.

**Breach Pandemic**

The sheer scale of cyber-attacks has become overwhelming. Millions of customers have seen their information stolen in attacks on companies including Target, Home Depot and JPMorgan Chase & Co. Banks and retailers are popular targets because of the access they have to consumer financial information. A recent report PWC estimated that more than 117,000 cyber-attacks hit businesses each day.

Breaches such as those just discovered at Target, the NSA, or wherever, all follow a set pattern. Breaches are not a shot in the dark, but require careful planning and execution.

In the first instance, the attacker has to identify the target, essentially looking for the weakness in the defense. Multiple tools are available on the Internet that allows anyone to scan for systems or components that have vulnerabilities. Once the point of entry is identified, the next step is to gain entry. In other words, looking for access to a system which can then be used as an escalation point.

In the book "Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners by Jason Andress and Steve Winterfeld", they clearly describe the attack process. The attack process is usually focused on a particular system, or set of systems, which an attacker attempts to access, either by using an outright attack or using credentials that have been discovered somewhere in the environment, through social engineering, or other means. Once access to a system is achieved, the next step is to escalate the account on the system in order to escalate the level of access that the attacker has in order to accomplish their goals. The target for such privilege escalation is often root or administrator level access, giving the attacker relative freedom on the system. Given the needed level of access to the system, the attacker can then remove any information that they wish to, cause damage to the environment in any way that benefits them, and install any measures that they need to in order to ensure future access.

**Is Two Factor Authentication The Answer?**

Many of us are familiar with the use of 2FA technology, and many of us carry a fob with us to gain access to our business systems. But as the migration away from the corporate data center

to the cloud continues, we increasingly are using IT infrastructures almost as a utility, similar to the electricity grid.

These has also coincided with the increased use of soft tokens, or using cellular devices for OTP services.

But as has been proven on several occasions, all OTP systems share the same inherent flaws. The OTP passwords are generated as either time-synchronized or counter-synchronized codes and often require the user to carry a small hardware device. Some solutions generate and send OTPs to the customer's mobile phone via SMS. There have been several well documented attacks against OTP systems and since they all remain reliant on browser-based communications, it means that a phishing site mimics the webserver or the browser is otherwise compromised, the customer's credentials and the OTP can be harvested by fraudsters and immediately used to gain access to accounts and authenticate fraudulent transactions.

The increased use of SMS is even more alarming and even the Telcos have openly stated that "SMS is not designed to be a secure communications channel and should not be used by banks for electronic funds transfer authentication," http://www.itnews.com.au/News/322194,telcos-declare-sms-unsafe-for-bank-transactions.aspx

Another approach that has recently come under increasing scrutiny is the use of digital certificates. The combination of breaches resulting the theft of private keys, to the recent Heartbleed vulnerability has demonstrated that certificates are no longer a guarantee that the user is who they say they are. And in any case, an increasing number of organizations are recognizing that device identity is no longer sufficient to guarantee a user's identity

**Are Passwords Dead?**

So how can we reduce the risk associated with authentication given that the evidence demonstrates that most commonly used systems are vulnerable?

The password still continues to offer the most convenient method both for users and the industry at large, and to a certain extent it is not dependent on technology. A password has in certain respects a biometric element in that it is a cognitive choice by an individual as to what it is.

However they are vulnerable as demonstrated daily, although they are well qualified for their purpose. So although they are of little value, they do have a purpose.

Authentication relies on three cornerstones, what I know, what I have, and what I am. What I have can be stolen or duplicated, and what I know can be guessed or shared or stolen.

What I am has two key elements, physical and behavioral attributes. The increased used of physical biometric technology such as fingerprint, facial recognition, etc., are unique to each of us and although no one will chop of your finger without you noticing, we have now designed technology that has the capability of stealing digital representations of those features.

Physical biometrics has the additional complication that it requires that an individual has the necessary technology to allow their physical biometrics to be recognized, and this presents several challenges such as the requisite technology, and the legal challenges related to data protection and privacy. Additionally once we have shared our physical biometrics, then our data is on the internet and can be stolen.

Behavioral biometrics are another thing entirely. Our behavior is virtually as unique as our fingerprint, and in independent analysis has proven to have a higher accuracy of detecting the individual than fingerprint technology due to fingerprint being very susceptible to the quality of the technology being used.

Additionally what behavior biometrics provides is continuance verification. In other words it is comparable to a user having their finger on a fingerprint reader through the duration of a session. MITB attacks become much harder to perpetrate because any significant change of the user's behavior during a session will result in the anomaly being immediately recognized. And behavior is not something that we are able to copy. Everything a user does on the phone, browser or computer consists of user patterns. Behavioral biometrics identifies these patterns by collecting information, not on what the user is doing but rather how they are doing it. As a result it prevents unauthorized access by authenticating user patterns of typing, swiping, mousing, or switching between applications.

According to Bruce Schneier , "The idea — and I think this is a good one — is that the computer can continuously authenticate people, and not just authenticate them once when they first start using their computers."

What Behavioral Biometrics offers is the ability to ensure that an individual's "credentials" cannot be stolen or hijacked. And as more devices are being modified to "know their users", the devices will be qualified to confirm their identities. By combining this confirmation with a traditional password, it will be possible to authenticate users more effectively and in a manner that will be transparent to them. Additionally it provides an organization with the ability to use passwords in combination with behavior to provide extremely high levels of accuracy in identifying the real user as opposed to an impostor, without the need to deploy any software or technology to the user!

Behavioral biometrics has a unique side property that solves a security problem where traditional security solutions fall short. A scenario where the user has an incentive to be part of the fraud - by sharing account details or disregarding the need to protect the security token. For example, software licensing of SaaS services where users share credentials to access hosted ERP and CRM, as well as to pay walls for news and media services.

Such credential abuse is commonplace and an issue in 'desktop sharing' environments such as trader floors and inside health/government services. In the healthcare sector convenient authentication is a must-have in all clinical situations and the push to electronic health records is driving a need for both patient-level and clinician-level strong authentication. Behavioral biometrics can determine not only if there is abuse of privileges, but who the person using the credentials actually is.

**Alliances Are Key To Winning**

One of the exciting features of a behavioral biometric solution is its ability to see the user and not just the security token. Repeat fraudsters can be marked and placed on a 'watch list'. Subsequently suspicious transactions can be compared against repeat offenders allowing for faster (real-time), cost effective fraud prevention.

Obviously a fraudster does not limit himself to one target, but by enabling the sharing of intelligence, across institutions, it provides institutions with means to quickly identify fraudsters and protect their clients, and their own interests.

**About The Author**

Calum Macleod is Business Development Director for Behaviosec www.behaviosec.com. With over 40 years' experience in the IT industry, he has have been involved in leading edge technologies and developments in the industry for many years. He is also a regular contributor to journals such as Sarbanes-Oxley Compliance Journal, Computer World UK, and many other journals.

Calum can be reached online at cmacleod@behaviosec.com and at our company website http://www.behaviosec.com/

MARCH 24th-25th, 2015 | TEL AVIV, ISRAEL

CYBERTECH2015
THE EVENT FOR THE CYBER INDUSTRY

ISRAELDEFENSE

PRIME MINISTER'S OFFICE
NATIONAL CYBER BUREAU

Ben-Gurion University of the Negev

# THE INTERNATIONAL CONFERENCE & EXHIBITION FOR CYBER SOLUTIONS


WITNESS AND EXHIBIT THE LEADING CYBER INNOVATIONS FROM AROUND THE WORLD!

## CYBERTECH 2015

MARCH 24th-25th, 2015 | TEL AVIV, ISRAEL


ORGANIZED BY:

ISRAELDEFENSE

FOR MORE INFORMATION:

**E:** cyber@israeldefense.co.il | www.cybertechisrael.com | **T:** +972-74-7031211

# Apps Under Attack

## New Research Demonstrates Increase in App Hacks for Top 100 Mobile Apps

*by Patrick Kehoe, Chief Marketing Officer, Arxan Technologies*

Increasingly, the news we hear about hacks is dealing with mobile apps. Whether it is WireLurker, Masque, or one of the other recent exploits, both iOS and Android apps alike are falling prey to hacks and being exploited for malicious gain. Given this, the findings from a recent State of Mobile App Security report are not surprising.

**How protected are mobile apps?**

The findings from the report clearly illustrate that unprotected mobile applications are vulnerable to reverse-engineering, repackaging, republishing and susceptible to becoming malicious weapons – and that most apps are, in fact, *not* well protected. The analysis, for example, revealed that the following had been hacked:

- 97% of top paid android apps
- 87% of top paid iOS apps
- 80% of the most popular free Android apps
- 75% of the most popular free iOS apps

The research also revealed that hacks are occurring on apps across verticals. In financial services, for example (where research has shown that hacking or malware has been the predominant method of credit card data breaches that occurred from 2005 to 2014* **source** Privacy Rights Clearinghouse), most apps have been hacked. Specific findings related to financial services apps – as well as retail and healthcare apps - are summarized in the attached infographic.

The 360 apps analyzed in the study were identified in the iOS App and Google Play stores, and a number of techniques and sources were used to identify hacked versions of these apps. The techniques to find hacked versions included, but were not limited to:

- Searching unofficial app stores
- Examining app distribution sites
- Reviewing the top torrent sites
- Examining file download sites

**The numbers are staggering and frightening – can this really be the case?**

When you consider a few points, you realize how we've gotten to the "state" we're in:

- First, securing mobile apps hasn't been a significant focus for many organizations; rather, most organizations have focused on network and device-level protection.
- Second, those who are focused on application layer security are not typically protecting their binary code (which is the code you download from an app store) – and a mobile application whose binary code is not protected is at risk, and can potentially jeopardize your other security work as well. (Note: you can learn more

about the risks associated with unprotected binary code in this "How to Hack an App" Video )

- Finally, once an application's hacked, there's no shortage of outlets for distribution. In fact, there are hundreds of app stores and websites around the world, many of which are legitimate, but have limited security controls, and unfortunately many others are focused solely on the distribution of torrents and hacked apps

**So what do we do about it?**

To combat the unique threats that mobile apps are susceptible to, organizations must adopt pre-emptive and proactive measures:

- Applications with high-risk profiles running on mobile platforms should be made tamper-resistant and capable of detecting and defending themselves against threats at runtime. Note: You can learn more about how to maintain the confidentiality of code and establish runtime application self-protection in this brief video.
- The software that's used to enable mobile wallets/payment applications (e.g., Host Card Emulation software for Android platforms) should leverage cryptographic key protection and application hardening.
- As part of the mobile application development lifecycle, your organization should conduct penetration tests that assess your level of vulnerability to reverse-engineering and tampering that can result from unprotected binary code.

These and other recommendations are detailed within the full State of App Security report.

Hopefully the proliferation of recent mobile attacks and findings from the research are eye-opening for developers and security practitioners alike. However, I suspect that a dramatic shift in focus toward application protection and making applications self-protecting at runtime won't occur any time soon, and that the "state of app security" won't change much in the near term. Hopefully I'm proven wrong!

**About The Author**

Patrick Kehoe is the Chief Marketing Officer of Arxan Technologies. He and the team at Arxan are in the business of understanding application security vulnerabilities and deploying approaches to protect applications—building on over 10 years of research and intellectual capital on this topic. Patrick brings over twenty years of experience working with software, hardware, and service providers in the High Tech industry. He holds a degree in Computer Science from Vanderbilt University and a MBA from the Darden Graduate School of Business at the University of Virginia. In his spare time, he enjoys triathlons and traveling with his family. Patrick can be reach at (310) 968-4290 and at the Arxan website http://www.arxan.com.

# A Guide to Cloud Compliance in the Defense Industry

*By William O'Brien, COO, Brainloop Inc.*

Defense contractors do not differ from other industries in seeking fast, efficient and cost-effective technology solutions to most efficiently run their businesses. This process often leads contractors to rely on free or low cost, low functionality public cloud storage solutions to store, exchange and collaborate on data with colleagues and third parties.

While this may seem like standard business practice (as well as quite convenient), the defense industry – out of all sectors – *must* consider security and compliance regulations when implementing such technology into their day-to-day workflow.

This reality is no more acute than when they are handling sensitive and export-controlled information and technical data where mere promises of security and half-hearted attempts to achieve security will not suffice.

**Don't Ignore "The Important"**

Traditionally – and surprisingly – security compliance when dealing with sensitive information too often isn't at the forefront for defense contractors. Perhaps it is only human nature at play, but until businesses fail to meet certain policies and are sanctioned, the issue of data and document security is more often acknowledged in theory rather than honored in practice.

But once that penalty is imposed and a company must pay a significant fine, which can range from tens of thousands to millions of dollars due to regulatory violations, then the issue and need for airtight solutions become a primary goal.

Perhaps even worse, once fined, the reputation of that contractor is immediately tarnished within its supply chain, its customers and the public.

Any company can opt out of this cycle. Companies can learn the lessons of security and institute appropriate practices before it's too late to avoid adverse consequences. They can, as others have, stop ignoring compliance once and for all, *before* the breaches and resulting punishments occur.

Just the thought of sensitive technical data landing in the hands of an uninvited, unlicensed third party poses far too much of a risk for companies to do otherwise.

The threat is more common than most think. Just consider the following situation: an employee at a U.S. defense contractor stores a file containing sensitive data onto a free or near free cloud storage platform, for the sake of expediency.

After just a few clicks of the user or perhaps due to data mining by the storage company, a link to that file is shared with a third-party vendor.

Once that file breaks out in such an unsupervised manner, no one knows exactly who is viewing it or its ultimate destination – a major risk when handling important, government-related technical data and, too often, a major regulatory violation.

**Just what is ITAR Compliance?**

Each year, several well-known enterprises are charged for not adhering to the International Traffic in Arms Regulations (ITAR), a subset of the Federal Government's export regulations. These cases can arise even when actual illegal exports are not alleged, but sloppy practices have resulted in "deemed" exports.

Under ITAR, the U.S. government requires *all* manufacturers, exporters and brokers of defense articles, defense services and technical data to follow stringent compliance guidelines to protect certain confidential and technical information related to national defense from unlicensed non-citizens or transfer outside the country.

This means that recipients, or even viewers, of this data must be U.S. persons – a guideline that standard public cloud solutions can't ensure or track.

In just three years' time, nine large companies have been sanctioned for ITAR violations. The penalties are made public on government websites (even a simple Google search can yield this information), meaning companies are unable to hide and immediately suffer a hit to their reputation.

Recent fines for not adhering to these export regulations have ranged from $20,000 to as much as $78 million per company. Looking back to 2007, one company had to pay $100 million in fines and forfeitures as a result of an ITAR violation.

In addition to the substantial sum of the monetary penalties, companies investigated for potential ITAR violations are subject to being decertified as an exporter by the government with the obvious devastating impact of that sanction.

**ITAR's Impact in the Cloud**

ITAR regulations don't necessarily restrict a company from using the public cloud, but a business should be more cognizant of the technology decisions made prior to implementation and exercise an extreme level of due diligence in the selection.

As more organizations exchange and collaborate on technical data via the cloud, ITAR compliance will need to be considered and adhered to in the virtual solutions provided by third-party vendors.

Always verify if the technology is ITAR compliant, or if the vendor is also ignoring "the important." This means ensuring that there is no access, involvement or control by non-U.S. persons on the backend of the technology an enterprise is considering.

To fully protect your company from compliance violations and reputation loss, don't assume your business operations are fully compliant from the beginning nor that vendor claims of compliance exist unless verified, especially when handling something as sensitive as defense-related data. Regularly research, ask questions, monitor and conduct audits of the collaboration technology within a company, to ensure technical information is kept in safe hands.

For more information on ITAR, including recent violations, please view this infographic here.

***About the Author***

*William O'Brien is the Chief Operating Officer of Brainloop Inc., a provider of SaaS technology for the secure storage, collaboration, and exchange of confidential documents and files including those containing technical data. For more information on the Brainloop Secure Dataroom in relation to ITAR compliance, please visit www.BrainloopITAR.com or contact Brainloop via Twitter: @BrainloopInc.*

# The UK Energy Cyber Security Executive Forum

## A one-day conference

## London, 5th February, 2015

## 20% Discount for CDM subscribers

### An exceptionally strong speaker panel includes:

- **Ciaran Martin,** Director General for Government and Industry Cyber Security, GCHQ
- **Graham Wright,** Group CISO and Digital Risk Officer, National Grid
- **Stephanie Daman,** CEO, Cyber Security Challenge UK
- **Dr Gal Luft,** Senior Advisor, The United States Energy Security Council & Chairman, Nation-E
- **Raj Roy,** Legal Director, British Gas
- **Iowa Carels,** Senior Cyber Security Advisor, The National Cyber Security Centre, The Dutch Ministry of Security and Justice

…. and many others

*This conference will:*

- *Provide insights into the latest cyber security developments in the UK, Europe and the US*
- *Offer C-level executives guidance to minimise the risks, avoid cyber security breaches through proper adherence to standards, develop resilience, protect and strengthen your business in the UK and globally*
- *Supported by Cyber Security Challenge UK, IISP, ISSA, The Journal of Energy Security, The Energy and Cyber Security Center, this strategic and practice-driven summit will give you an excellent opportunity to network with the best of the energy cyber security sector and learn how to actively engage with the cyber security issues at the board level.*

*As demand for attendance at the event is likely to be high, early booking is recommended.*

*Visit www.cityandfinancialconferences.com/CyberEnergy2015*

*Obtain a double discount when booking by 10th January and using code CYSENCDM.*

# Cutting Through the Red Tape: Why the Benefits of Going Mobile Outweigh the Risks for Government Agencies

*Paul Brubaker, director of government solutions, AirWatch® by VMware®*

At a recent conference in Washington, D.C., government and industry experts convened to discuss how mobility is transforming security and intelligence around the world. Among the many topics at the conference, it was clear that mobile technology could be the next frontier for greater government productivity and effectiveness.

However, questions still exist about the security, privacy and regulation of mobile devices, stalling their adoption across the government sector. Unfortunately, this means that, while agencies wait for a perfect solution, they are missing prime opportunities to take advantage of mobility.

To help with these concerns, the Department of Defense (DoD) has been tasked with creating multiple mobile device focused initiatives, including the Mobility Unclassified Capability (DMUC) and Defense Mobility Classified Capability (DMCC) guidelines.

These plans include establishing clear encryption and security standards for deploying applications, email and content to employee-accessible devices. Additionally, the plans also call for selecting an enterprise mobility management platform that meets the standards of the Security Technical Implementation Guide (STIG), a resource meant to outline parameters for devices accessing DoD networks.

Although these initiatives are promising starting points, agencies overall have yet to embrace mobility for two main reasons. The first reason is how technology is approved by the DoD for government use.

Because current government technology is built to be incredibly secure, new devices and software must go through rigorous testing and numerous approvals before being integrated, creating a bottleneck in the adoption process.

The second reason concerns the DoD's approach to mobility as a whole. As an organization that continuously prepares for potential technological threats, the DoD employs detailed planning procedures to predict where technology is headed.

However, the rapidly changing technology industry is nearly impossible to predict, leaving complicated DoD procedures unable to readily address new innovations. Agencies end up hitting a wall of red tape, and new technologies are left unexplored.

Despite the gap between mobility and agency adoption, there is still a demand for it among government employees. The reality is that despite their employers' best efforts, many employees are already working in ways that may not be secure.

A Cisco-sponsored survey from Mobile Work Exchange found that 41 percent of government employees are engaging in risky mobile behavior, including accessing unsecure Wi-Fi networks, refraining from using device encryption and not configuring a device passcode.

If agencies choose to ignore the need for a secure platform to facilitate file sharing, workplace collaboration and mobile email access, employees will continue to seek out free and often unsafe alternatives to achieve their work goals.

Fortunately, government agencies have solutions for bringing secure mobility to their employees. There are three major ways agencies can safely begin to adopt mobile devices in the workplace:

1. **Simplify the bureaucratic process of adopting new technologies.** Many solutions in the mobility industry already provide the functionality that government standards require, including stringent device encryption, certificates for authentication and secure application containers for email. By simplifying the approval and technical processes, new technologies can be incorporated faster, boosting national defense effectiveness and putting agencies at the forefront of innovation.

2. **Deploy mobile devices in extensive pilots for testing in real-world scenarios.** Instead of waiting for the perfect solution in theory, agencies should begin testing mobile devices in practice. With devices on the ground, agencies can gather real-world statistics, track actual use cases and fine-tune employees' capabilities while mobile. This will enable agencies to make informed decisions about what mobility can actually do for them. For example, the United States Army Corps of Engineers (USACE) adopted mobility to assist with disaster relief efforts. With iPads and a custom application, USACE replaced pen and paper with mobile kiosks for resident information collection, reducing a 2-3 day waiting period to mere minutes.

3. **Provide transformative mobile technologies to some of the most valuable employees in the public sector.** Embracing mobile devices, including smartphones, tablets and laptops, in government will improve communication, strategy and operational choices for workers in the field. As threats from all corners of the world put countries at risk, it's imperative to stay one step ahead with technology. Getting mobile devices in the hands of service members and administrative staff will keep them informed in the line of duty. For instance, the UK-based defense company Chemring uses iPads to secure electronic board documents, ensuring board members have updated information when making strategic decisions.

With the current government approach toward mobility, agencies cannot effectively adopt mobile devices.

Government organizations should make a conscious effort to revisit mobility, carefully evaluate the current standards and begin implementing small but efficient mobile device pilots.

Balancing mobility and security will not be an easy undertaking, but it will empower employees and government agencies to be effective in the ever-evolving technological world.

**About the Author**

Paul Brubaker, Director of Federal Government Solutions, AirWatch by VMware

Paul Brubaker is the director of federal government solutions at AirWatch by VMware, the leading enterprise mobility management (EMM) provider. In this role, Brubaker oversees all federal government activities, includes sales, marketing, events and strategy.

Brubaker, a two-time presidential appointee, has held a number of leadership positions in government and the private sector. Most recently, he served as director at the United States Department of Defense, where he was responsible for planning and performance management activities for the Office of the Secretary of Defense. A former GAO evaluator, he served as the Republican staff director of the Senate Subcommittee on Oversight of Government Management where he led the passage of the Clinger-Cohen Act for then-Sen. William S. Cohen (R-ME). Brubaker was the deputy CIO of the Defense Department under President Bill Clinton and in 2007, he was confirmed by the U.S. Senate to become the research and technology administrator at the Transportation Department under President Bush.

In the private sector, Brubaker served as CEO, president, CMO and at the executive level of several successful small and mid-sized technology-focused companies, including Silver Lining, Synteractive and Procentrix. Additionally, he was the general manager for the North American Public Sector Internet Business Solutions Group (IBSG) at Cisco Systems, developing innovative applications and creating market expansion opportunities across the enterprise.

He received the Department of Transportation Secretary's Gold Medal in 2009 and the Department of Defense Medal for Distinguished Public Service in 2001. He was also recognized with numerous awards for his contributions to public service and his collaborative work with the public sector and private industry.

Brubaker earned a bachelor's degree in political science from Youngstown State University and a master's degree in public administration from Kent State University.

# How Secure is Your BYOD Environment?

Bring your own device or BYOD is a revolutionary innovation in networking, and it is here to stay. It can broadly be defined as a program that provides device-independence to end-users. Due to the increased use of smartphones, organizations have inevitably implemented the BYOD concept in their networking strategies. According to Gartner, it is expected that by 2016, four out of 10 organizations shall rely exclusively on BYOD, meaning that the organizations won't provide any devices to their employees. Moreover, 85% of companies are expected to have some form of BYOD in place by 2020. Interestingly, small- and medium-sized businesses are taking advantage of this growing trend. In 2013, 62% of small- and medium-sized businesses had an official BYOD policy in place, as reported by iGR.

## BYOD Rewards

With the ability to access corporate resources from anywhere, at any time, BYOD brings an array of benefits to organizations. When employees use their own devices for personal and business use, productivity increases while employee attrition rate decreases.

Businesses can transfer operational expenses to the user while optimizing revenues. At the same time, BYOD offers mobility to corporate resources. Overall, BYOD is a win-win situation for employees as well as businesses.

Along with the benefits come the risks. The versatility in models and operating systems makes it more difficult for IT staff to manage each device with a comprehensive policy. Most of the time, the employee owns and maintains the device, and the company has less control over it than if it were company-owned.

## Data Management Issues

The past few years have seen rapid implementation of both BYOD and cloud networks in organizations of all sizes. With mobile and cloud data storage solutions, it has become difficult to manage and track data. New devices come with large storage capacities and have the ability to connect instantly to the internet and social networks.

Huge volumes of data - over which organizations have little control - are stored on these devices. It is not easy to distinguish between work data and personal data. Organizations that do not have the infrastructure to monitor data movement rely on third-party solutions to do so.

## Data Compliance Issues

With the increased incidence of identity theft and phishing scams everywhere, government authorities have come up with strict regulations for data management. The UK Data Protection Act of 1998 is an example. This Act regulates data collection and storage. While there is no

such law in the United States, organizations have to be compliant with other regulations such as the PCI DSS (Payment Card Industry Data Security Standard), which is related to credit card transactions, and the Health Insurance Portability and Accountability Act (HIPAA), which offers privacy protection for personal health. When these data are stored and managed on an employee-owned device, complexity increases.

## Malicious Apps

Employee-owned devices are vulnerable to malware and malicious apps. This is why some have labeled the phenomenon BYOM (Bring Your Own Malware).

According to Lookout, Google Store contained 32 apps that were infected with a malicious program called BadNews. Interestingly, these apps were downloaded 9 million times in 2013. Bit9 reports that 100,000 apps on the Android store are suspicious.

Today, hackers are finding innovative ways to access information on a device. According to researchers at The University of Alabama at Birmingham (UAB), hackers even use music to trigger mobile malware in a device.

Another concern for businesses is the unauthorized access to corporate data via mobile apps. When employees download malicious apps on their cell phones, they give outsiders unauthorized access to critical corporate data. It is a headache to impose security software and add updates and patches on these devices.

Employees can easily uninstall the software if they feel that these apps are impacting device performance and degrading the end-user experience.

## Lost or Stolen Devices

Owing to their small form and also because they are always carried around by users, mobile devices can easily be lost.

According to IDG research, more than 3 million handsets were stolen in 2013. Out of these devices, 44% were left in a public place. The BBC reports that 314 mobile devices are stolen in London every day. When devices that are registered in a BYOD network are lost or stolen, sensitive corporate data can fall into the hands of an outsider.

## Fired Employees

Another important way in which corporate data become compromised is through disgruntled or fired employees. Employees may retain a certain amount of data even after they leave an organization. Typically, a fired employee does not inform the HR department about data residing on his smartphone, and this information can easily be leaked to a rival organization.

Companies should have a written BYOD policy ensuring that employees do not retain data owned by the company when they leave an organization.

## Hacking Issues

Protecting smartphones from hacking attacks is a big challenge for organizations. According to CBS News, smartphones have recently become the prime targets for hackers. With password-cracking software available for download on the internet, anyone can purchase a password-hacking tool and hack mobile devices. When a device is hacked, it can be used to connect to a corporate network to access business-critical information.

## How Can You Secure Your BYOD Environment?

Firstly, organizations should not implement a BYOD policy unless they are fully prepared to handle it. By weighing drawbacks and benefits along with compliance issues, organizations can prepare a written BYOD policy that addresses BYOD security issues comprehensively.

This policy should include compliance aspects such as how and when corporate data should be deleted from a device, what type of data can be accessed through a personal device, how data are moved between personal devices and business servers, and what type of encryption should be in force.

Business data and personal data have to be differentiated, and access to corporate data must be privilege-based. Most importantly, employees need to be educated about their responsibilities, and instructed on safe practices for smartphone use within corporate networks. Without proper co-operation from employees, it is not easy to manage a BYOD environment.

By performing an audit on access to personal data and the types of devices used, organizations can add an extra layer of security.

Secondly, the BYOD policy should provide clear password specifications for employees. The password should have a minimum length and should be locked after a time lapse.

Based on the number of specified failed password attempts, the device should be reset to factory settings. It should be possible to lock the device remotely, change password, or wipe off its entire content with ease.

Thirdly, businesses need a comprehensive mobile device management suite. With an array of versatile mobile devices, hybrid networks and multiple business procedures, it is not easy for businesses to manually manage and monitor each and every device within the network.

A powerful mobile device management (MDM) solution provides a centralized dashboard to manage and monitor the entire range of devices effectively.

## Remotely Control Devices

With a comprehensive MDM solution, you can remotely monitor and manage files on your device from any browser. It is very easy to drag and drop files between a device and your browser. From a centralized location, you can remotely edit contacts and take control of the device's camera. When a device is stolen, you can use the device camera to take a picture of the thief, and submit it to the relevant authorities before remotely wiping the data from the device.

## Mobile Security

In a BYOD environment, it is very important to have a strong password policy. However, it is a tedious task to enforce this policy on multiple devices manually. With an MDM program, you can automatically apply password policies on multiple devices, saving time.

You can enforce password specifications such as the length of the password, as well as number of failed attempts and time lapse before auto-lock. When a device is lost or stolen, the password can be changed remotely, data and settings can be remotely wiped off, and the device can be reset to factory settings. The device can be controlled even through an SMS.

MDM solutions allow you to remotely monitor apps installed on any device, and easily remove rogue applications. With an app whitelist, you can allow specific apps to be installed on a device.

You can create a blacklist of apps for the entire organization or for a specific group of employees. When a blacklisted app is installed, IT administrators and the user are immediately notified; an instant alert is generated along with the details of the devices involved.

## Find & Track Devices

With a comprehensive MDM solution, the location of each device can be tracked and a complete location history created. While this feature facilitates staff routing and improves customer service, it also allows businesses to keep track of device location and be in compliance with government regulations.

Location history can be enabled for a group, department or role, and the time periods during which records should be logged can be specified as well.

## Easy Management

The mix of BYOD and cloud networks creates a high level of complexity for IT staff. However, by means of a centralized dashboard an MDM solution makes it easy to manage thousands of mobile devices. By grouping devices according to a department, role or job function, security settings can be customized according to group policies.

WiFi network settings can be easily deployed to multiple devices. Device and SIM card details can be stored. Using the MDM program, email settings can be remotely configured.

## Conclusion

BYOD is here to stay. For a secure BYOD environment, IT and security staff must work together to implement advanced security solutions such as sandbox apps and data containerization.

Employees have a key role to play here. Starting from the creation of a BYOD policy to its enforcement and execution with proper support, every step has to be planned carefully. With a sound and security-focused BYOD policy in place, businesses can mitigate the risks of BYOD while taking full advantage of its benefits.

2X MDM is a complete software solution for your company's BYOD policy. Password security, track and locate are just a few of the advanced features of this solution. 2X MDM can secure your corporate data and fully support your remote workforce using their own devices.

**References**


How Secure is Your BYOD Environment | BYOD/BYOA: A Growing, Applicable Trend | inc.com

http://www.inc.com/comcast/byod-byoa-a-growing-applicable-trend.html

How Secure is Your BYOD Environment | BYOD: an emerging market trend in more ways than one | us.logicalis.com http://www.us.logicalis.com/globalassets/united-states/whitepapers/logicalisbyodwhitepaperovum.pdf

How Secure is Your BYOD Environment | People Are Willing To Go To Extreme Lengths To Retrieve Their Stolen Smartphones

http://www.businessinsider.in/People-Are-Willing-To-Go-To-Extreme-Lengths-To-Retrieve-Their-Stolen-Smartphones/articleshow/34790154.cms

How Secure is Your BYOD Environment | 314 mobile phones 'stolen in London every day' | bbc.com

http://www.bbc.com/news/uk-england-london-21018569

How Secure is Your BYOD Environment | Payment Card Industry Data Security Standard | wikipedia.org

http://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard

How Secure is Your BYOD Environment | BYOD: Many Call It Bring Your Own Malware (BYOM) | blogs.cisco.com

http://blogs.cisco.com/security/byod-many-call-it-bring-your-own-malware-byom

How Secure is Your BYOD Environment | BYOD Security: 5 Risk Prevention Strategies | smallbusiness.foxbusiness.com

http://smallbusiness.foxbusiness.com/technology-web/2014/08/07/byod-security-5-risk-prevention-strategies/

**About the Author**

Giorgio Bonuccelli is the Marketing and Communication Director for 2X Software. Giorgio has extensive experience in cloud computing and virtualization, with a background of many years in multinational corporations (Dell, EMC and McAfee). In his career he has filled different roles, from sales to training and marketing. This wide-ranging experience and flexibility helps him simplify concepts and write content that is easy to read and understand even by newcomers to the subject. As a blogger and technical writer he has published more than 1000 papers.

# CYBER SECURITY FOR OIL AND GAS CANADA

**January 26-28, 2015 | Calgary, Alberta, CA**

## Building the Foundation for Advanced Information & Cyber Security Practices

**Don't miss the Live hacking Demonstration and analysis to demonstrate defense-in-depth strategy and identify risk mitigation best practices by Chris Shipp, CISO, at Fluor Federal Petroleum Operations**


## Featuring in-depth discussions leading industry experts will cover best practices:

**Craig Coughlan**
Supervisor Incident Response Threat Assessment
**ENBRIDGE**

*Review case studies of the benefit threat intelligence can drive to your security operations*

**Hani Mansi**
Director, Risk & Information Security
**ATCO**

*Information security program maturation, planning and implementation strategy*

**Staff Sergeant Ryan Jepson**
Electronic Surveillance Unit
**CALGARY POLICE SERVICE**

**Senior Constable Shafik Punja**
Technological Crimes Team (TCT)
**CALGARY POLICE SERVICE**

**Sgt Corey Dayley**
Cybercrime Support Team (CST)
**CALGARY POLICE SERVICE**

*Development of a digital forensics team and reviewing the means to start, develop process & protocols, team oversight and the technical details of enacting digital forensic analysis in your organization*

**Zoltan Palmai**
Team Lead, Network Security - Security & Access Operations IRSM
**CHEVRON**

*Management of joint ventures and vendor partnerships to ensure security protocols are adhered to and network connections are secured across the supply chain*

**Chris Shipp**
CISO
**FLUOR FEDERAL PETROLEUM OPERATIONS**

*Management of joint ventures and vendor partnerships to ensure security protocols are adhered to and network connections are secured across the supply chain*

## Top Benefits of Attending:

- Access an intimate industry forum to discuss the most effective strategies to harden your information / cyber security practices
- Develop knowledge of industry trends for the implementation of cyber defense, incident response, risk management, governance & forensics plans
- Identify advances in global cyber threat trends, vulnerabilities, outlets for support and best of breed solution providers/partners to ensure development of your security practices
- Expand your network of industry contacts to create potential opportunities for secure threat intelligence sharing
- Interface with government agencies and regulatory experts for assurance on your GRC plans

***"Excellent conference to bring oil and gas industry together and share cyber security issues and solutions"***

**– Patrick McNallen, Vice President, Elbit Systems**

**Get 20% OFF with discount code: CSO_CDM. To register call 1-800-882-8486, email EnquiryIQPC@iqpc.com or visit www.cybersecurityoilgas.com**

**Sponsors:**

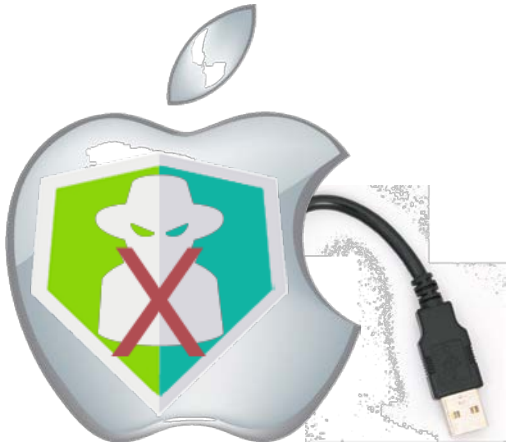
paloalto networks. FireEye SECURITY REIMAGINED Check Point SOFTWARE TECHNOLOGIES LTD. iON SECURED NETWORKS (ISC)² WATERFALL IBM

**Media Partners:**

CIPS Canada's Association of Information Technology (IT) Professionals www.cips.ca | Oilfield Conference | Oil & Gas iQ | Mission CRITICAL | Cyber Defense Magazine | OFFCOMM NEWS

# Mobile Device Security: Don't Be Naïve

I woke up this morning at my normal 4:30AM. This getting old stuff really whacks your sleep! Turned on the news and the first two stories were on yet another set of cyber security breaches. In fact, there is not a single day that goes by that you don't hear about the latest cyber security breach or credit card hack or personal data theft or even identity theft. This week, a story broke where Sony Pictures had their Enterprise system hacked and unreleased films stolen and placed on the internet for free downloads. Last week, the US Post Office Enterprise got hacked and more than 750k USPS employees' personal information stolen.



WireLurker Malware

But, it isn't just the Enterprise being attacked. Ask Apple. In the past 3 weeks, 2 very nasty attacks were directed at the Apple mobile operating system, iOS. The first is called the "Masque Attack" which poses as a very popular game app and users unknowingly install it. The Masque Attack then steals your banking and credit card transaction information. The other is named "WireLurker", which attacks your Apple mobile device while charging from a USB port. It is an extremely sophisticated program that also steals personal information such as the device serial number, iTunes information, and phone number and sends it to another server.

It struck me that there are just some things that a lot of people just haven't quite grasped yet. The cyber security criminals are very organized. And, there is a distinct shift in their targeting. With the move to more and more mobile device dependency, the criminals are targeting mobile devices more than our desktop and laptop computers. Yes, our mobile devices have become the primary target for cyber criminals.

And the consequences are dire. Think of all the stuff you have on your mobile device. Now think about this. Think about a company of 10 or 20 or 30 thousand criminals. They have the money, the resources, and the expertise. They attack indiscriminately, looking for opportunities, making opportunities, and they no longer have to break into your back door or your vault. They can attack thousands, hundreds of thousands, even millions of potential victims with a keystroke. No one is immune. No operating system is completely secure.

I'm no chicken little. But, honestly, the volume and severity of attacks has me on high alert, especially when it comes to my mobile devices. I have a bunch of them, all Apple. You need to be aware of the ever-present and very REAL threat. You also need to exercise common sense and be smart about protecting yourself from these malicious criminals and their ever-increasing, sophisticated, clever attacks meant to do harm to anyone and everyone. The bad guys don't discriminate.

First, recognize that mobile devices are the new primary target. Be alert. Be cautious. If you receive an email with a link in it that you don't recognize, don't click on it. Doesn't matter if it is your laptop or your iPhone. Seriously, don't do it.

Second, keep your virus protection up-to-date on your computers even though it may be annoying to purchase annual licenses and we are all a little suspicious of the virus protection vendors. But, in the likelihood that you need to connect to your computer with your mobile devices, you don't want to leave an open door for criminals to infect your devices from your laptop.

Third, recognize that juice-jacking is the number one opportunity for mobile device infections - so, when you plug your phone into any USB port, you are extremely vulnerable to attacks. Read up on the recent WireLurker juice-jacking virus and your knees will rattle a bit. You are especially vulnerable while on travel - when you often have no choice but to charge through a USB port and have no way of knowing what you are plugging into. ChargeDefense's product, the Juice-Jack Defender® is guaranteed to block identity theft code and malware when connected to a USB outlet. It's a $15.95 no-brainer. If you don't have a Juice-Jack Defender® and must connect to an unknown USB port, at least keep your mobile device locked. And for goodness sake, put a password on your device! But, even those precautions are no guarantee that a hacker can't find a way in.

The bottom line is this: Don't be naïve. YOU ARE THE TARGET OF CYBER CRIMINALS. Be smart. Protect yourself. Use common sense precautions. And, remember that it isn't just computers anymore. That wonderful mobile device that you carry around with you everywhere needs the same level of protection and precaution as your laptop computer. Be safe.

**About the Author**

Stuart McCafferty, ChargeDefense
Like us on FaceBook and get special discount deals: www.facebook.com/chargedefense

# Shadows of Things That Have Been

*Tal Klein*

> *"Spirit!" said Scrooge in a broken voice, "remove me from this place."*
>
> *"I told you these were shadows of the things that have been," said the Ghost. "That they are what they are, do not blame me!" – from Charles Dickens'* A Christmas Carol

The holiday season is traditionally a time of reflection. As the year draws to a close and another looms on the near horizon, it makes sense to both look back on what was and what may yet be. In Charles Dickens' classic holiday yarn A Christmas Carol, Ebenezer Scrooge endures a night's reflective haunting and is changed for the better because of it. When it comes to the way enterprises address Shadow IT, let us hope 2015 see us put things in their proper perspective and stop wasting time and money fretting over Shadow IT.

If you don't want to take it from me, Verizon's 2014 State of the Market: Enterprise Cloud report pronounced Shadow IT dead as a business risk. Instead, the report touted the adoption of cloud services as essential to efficiency and innovation.

The fear behind Shadow IT has been rooted in the idea that armies of rogue users are hunkered down in their cubicles downloading applications willy-nilly and storing petabytes of sensitive corporate data in the cloud, unprotected. This just isn't the case. In their Cloud Adoption and Risk Report, Skyhigh Networks found that, while the average enterprise used 831 cloud services, 80 percent of corporate data uploaded to the cloud was stored in just one percent of those applications. Adallom's own annual Cloud Usage Risk Report confirmed this finding, identifying four primary services used for storing enterprise files in the cloud: Box, Office 365, Salesforce, and Google Apps.

Not one of these respected and broadly adopted services, comprising the largest attack surface for data in the cloud, fits the definition of Shadow IT. To the contrary; the status quo has pivoted so profoundly that these services are more likely to be sanctioned by IT than traditional IT services.

This is not to say that cloud applications are risk free. The proliferation of third party applications built on top of these and other dominant SaaS platforms constitute a real and measurable risk requiring that enterprises understand what is happening within their cloud ecosystem in order to identify potential risks to corporate data and IT systems.

The Adallom Cloud Usage Risk Report identifies actual scenarios in which hackers took advantage of common application vulnerabilities and tricked privileged users into forfeiting sensitive corporate data. Such scenarios demonstrate the difficulty in governing third-party SaaS applications with cross-platform functionality creating attack vectors from one service into another.

Considering the risks inherent with mainstream cloud applications, resolve in the New Year to stop chasing the shadows of what had been and address the threats to cloud security as they are. If you fail to do so, *do not blame me!*

**About the Author**

Tal Klein is vice president of strategy at cloud computing and SaaS security provider Adallom, based in Palo Alto, Calif. Previously, Tal was senior director of products at Bromium where he led a product marketing strategy that helped build that company into a multi-million dollar business. He has managed integrated product strategy at Citrix and also spent more than a decade in the webhosting industry developing managed infrastructure services.

# User Friendliness is Making Us Vulnerable

*By: Arman Sidhu*

"A Short History of the Internet," is a piece authored by Bruce Sterling, penned in 1993, more than two decades worth of technology has eclipsed since the article was written and much of Sterling's predictions hold true. For example, he mentions how the Internet's spread will be unprecedented and near the end produces this concluding statement: "By the turn of the century, "network literacy," like "computer literacy" before it, will be forcing itself into the very texture of your life.

Flash forward twenty years, and our technology and utilization of the Internet has exploded with social media, electronic commerce, mobile application, and the much heralded "Internet of Things." As our technology has evolved, so has our behavior with technology, we constantly starve for the newest innovation, and we demand much from the developers, programmers, and engineers that always seem to cater to our needs as users in growing digital universe. Our communication with others is faster, information on anything and everything is more accessible than ever, and we just can't wait till the little annoying tasks we go through in our lives, whether at home or work, are automated at a level where we no longer worry about them.

Running parallel with our praises, we saw a rapidly developing dark side to our technology. We worried about our privacy and security being vulnerable, either to Big Brother's surveillance or from hackers looking to profit from our fragile "security" practices.

Yet as we've passed through the Sony Hack, PRISM leaks, the Heartbleed Bug, the Password heist by a Russian cyber gang, infiltration of private photos of celebrities, and the attacks on Target and Home Depot, the gap between secure systems and those hell-bent on intrusion has hardly decreased in size. Social media reports the attacks but seldom spread information to beef our security as vulnerable users. When we deem it time for our occasional password change, we gain a false sense of relief. For even the simple task of a password change has managed to become a hassle and even rendered useless. The trend of two-factor authentication might have caught on for some, but many of us still avoid it when we can. Anti-virus companies give us a sense of security, but they have their faults, and few of us maintain the recommendations that IT administrators in our workplace.

The reason probably isn't (and shouldn't) be because we don't feel vulnerable, but instead stems from the double-edged sword known concisely as Usability, or interchangeably known as User Friendly, a phrase that dominates the planning stages of virtually every consumer tech product, and while it provides us with the quick learning curve, it also leads us to a state of disbelief when our apps crash, don't respond, and fail to fulfill us with the utility we downloaded them for.

Thanks to the surge in mobile and tablets, our interaction is consistently being judged by companies looking to deliver the best product available. With this, we lose out on basic security practices, many aren't capable of troubleshooting the most basic of errors, and we silently lose out on control of securing the data and information we transmit each and every day.

The best traps are the most convincing, the Nigerian royalty email scams had a good run, but phishing has gotten the best of thousands, if not millions, of internet users because it dupes us with convincing emails and login pages from authorities we trust, like our banks. It takes our human element of the fast-paced, get-it-done, environment we are so accustomed to with the updates, emails, and messages that clutter our devices and makes us susceptible to social engineering. By the time we have even noticed it, the damage is and has been done, sometimes with irreversible consequences. The worst part might be finding and bringing the perpetrators of the attacks to justice. In December, the Target breach celebrates an anniversary, and the number and severity of such hacks has increased and been brought to the public's attention. Even though we've chose to vilify and caricaturize the basement hackers and G-men who hunt our devices, we do little to make their jobs even slightly more difficult. Backing up files, implementing tougher passwords, ensuring we sign into encrypted websites, and properly reviewing our installations are easy, relatively quick ways to insure our security.

Yet, few could hardly say things are looking up in the security world. This isn't because we don't fear hackers, or the possibility of our data being stolen and at the helm of other individuals, who have a slim probability of being caught for their crimes. It's our dependency on opening, closing, saving, and using our products at the fastest rate possible. Passwords themselves are a hassle, encryption is another obstacle between us and our work, two-factor authentication doesn't have enough utility for its "safety," and reliance on software, prone to the same vulnerabilities as our own systems, to detect our threats has rendered the general populace "security illiterate."

Scapegoats have included Congress and Corporations, but the solution to adequate cybersecurity ultimately rests with consumers themselves, who must make it a priority for users to familiarize themselves with the most basic of security practices, only then can we maintain reasonable assurance for our information.

If we've learned anything from the countless cyber-attacks, crime, and espionage that has ensued in the past year, we know that no one, not governments, not corporations, and certainly not any of us, are immune to the growing and resilient vulnerabilities that our technology faces. The problem cannot be attributed to a single source, as users we demand efficiency, and at the fastest rates possible. The developers and product managers in the security industry are hustling to reinforce the same stronger protective systems, of which many become obsolete and face pricey updates and fixes. What is needed is a new form of security, a pioneering system that allows every party, from the product designers to the end users to compromise their time for security. Until then, expect side-by-side linear increases in user efficiency and cyber-attacks.

**About the Author**

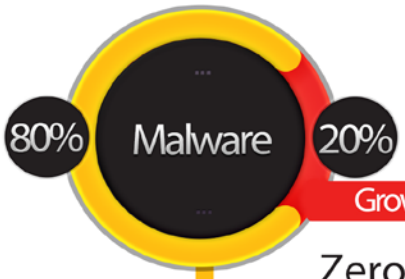
*Arman Sidhu is a political commentator based in Phoenix, AZ, USA, he writes with a focus on contemporary issues ranging from technology governance to international relations. He is a former Reagan Fellow at the Goldwater Institute.*

SnoopWall

RECLAIM YOUR PRIVACY ™

## TRADITIONAL MALWARE

Virus
Blended-Threat
Botnet
Zombie
Worm
Spyware
Trojan




## MODERN MALWARE

Growing by 30,000 New Samples Daily

Zero Day
Advanced Persistent Threats
Command & Control Channels
Eavesdropping
Remote Control Threats on Smartphones, Tablets, iPhones & iPads

Anti-Virus programs can detect and protect you from **Traditional Malware** and only a small fraction of **Modern Malware**

SnoopWall protects you from **Modern Malware** - puts you in control

## Get SnoopWall for

Windows (COMING SOON!)

iPhone (COMING SOON!)

Android

## DID YOU KNOW

Less spying means longer battery life for your devices!

Increase Battery life!

# RECLAIM YOUR PRIVACY ™

# 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

# 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 or 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.

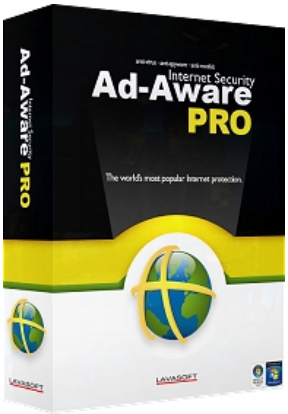
So use it by going here:

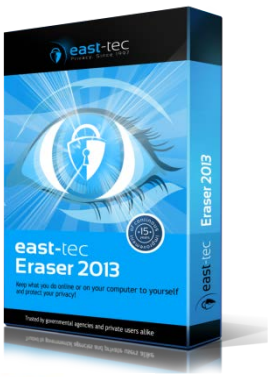
http://www.naisg.org/techtips.asp

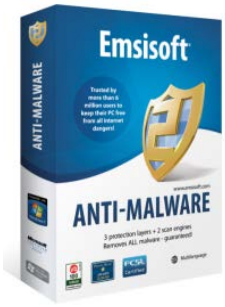
SOURCES: CDM and NAISG.ORG

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 December 2014

**Sample Sponsors:**



**To learn more about us, visit us online at http://www.cyberdefensemagazine.com/**

# Cyber Warnings Newsflash for December 2014

## *Highlights of CYBER CRIME and CYBER WARFARE Global News Clippings*

Get ready to read on and click the titles below to read the full stories – this has been one of the busiest months in Cyber Crime and Cyber Warfare that we've tracked so far. Even though these titles are in **BLACK**, they are active hyperlinks to the stories, so find those of interest to you and read on through your favorite web browser…

Oops: After Threatening Hacker With 440 Years, Prosecutors Settle for a Misdemeanor
http://www.wired.com/2014/11/from-440-years-to-misdemeanor/

Brain Science and Browser Warnings
http://threatpost.com/brain-science-and-browser-warnings/109615

Ex-counter-terror chief: criticism of Facebook over Rigby murder is unfair
http://www.theguardian.com/uk-news/2014/nov/26/lee-rigby-former-counter-terror-chief-criticism-facebook-unfair

Adobe tries to fix Flash vulnerability (again)
http://www.computerworld.com/article/2852124/adobe-tries-to-fix-flash-vulnerability-again.html

The rise of account takeovers
http://net-security.org/secworld.php?id=17690

AV Firms Defend Regin Alert Timing
http://www.govinfosecurity.com/av-firms-defend-regin-alert-timing-a-7614

New online tool ACORN allows Australians to report cybercrime in real time
http://www.theage.com.au/digital-life/consumer-security/new-online-tool-acorn-allows-australians-to-report-cybercrime-in-real-time-20141125-11u0v1.html

Cyber security poised to be China's next social campaign
http://www.wantchinatimes.com/news-subclass-cnt.aspx?cid=1204&MainCatID=12&id=20141126000043

Senate Cybersecurity Vote Not Likely in Lame Duck
http://blogs.rollcall.com/technocrat/senate-cybersecurity-vote-not-likely-in-lame-duck/?dcz=

Regin: 'cyberspy' malware from 2003, snooped on Saudis, Russians, Belgians...
http://www.computerworld.com/article/2851060/security0/regin-state-sponsored-malware-itbwcw.html

Craigslist DNS hijacked, redirected at infamous "prank" site for hours [Updated]
http://arstechnica.com/security/2014/11/craigslist-dns-hijacked-redirected-at-infamous-prank-site-for-hours/

Cybersecurity for the holidays: A non-stop job
http://www.usatoday.com/story/tech/2014/11/25/cybersecurity-holiday-shopping-black-friday-cyber-monday/70015208/

Army Cyber branch offers Soldiers new challenges, opportunities
http://www.army.mil/article/138883/Army_Cyber_branch_offers_Soldiers_new_challenges__opportunities/

Hacking cars: Automakers put high priority on cybersecurity
http://www.mercurynews.com/business/ci_27002897/hacking-cars-automakers-put-high-priority-cybersecurity

Are ex-hackers the answer to addressing the cyber security skills gap?
http://www.computerweekly.com/opinion/Are-ex-hackers-the-answer-to-addressing-the-cyber-security-skills-gap

Poll: Many concerned over online privacy, but few acting for security
http://thehill.com/policy/technology/225275-poll-many-concerned-about-online-privacy-but-few-acting

Why you should protect your wireless connection
http://net-security.org/secworld.php?id=17686

Breach Reported After Vendor Dispute
http://www.govinfosecurity.com/breach-reported-after-vendor-dispute-a-7605

16 arrested in European bust over RAT spyware
http://www.zdnet.com/16-arrested-in-european-bust-over-rat-spyware-7000036090/

Making law enforcement more difficult with mobile-device locks
http://www.newsobserver.com/2014/11/21/4342361_making-law-enforcement-more-difficult.html?sp=/99/108/&rh=1

Stealthy, sophisticated 'Regin' malware has been infecting computers since 2008
http://www.pcworld.com/article/2851472/symantec-identifies-sophisticated-stealthy-regin-malware.html

U.K. Terrorism Law to Force Internet Providers to Give User Data
http://www.bloomberg.com/news/2014-11-23/u-k-to-propose-terror-law-on-internet-user-data-as-threat-grows.html

Fears grow of Iran cyber attack
http://thehill.com/policy/cybersecurity/225045-fears-grow-of-iran-cyber-attack

Now e-cigarettes can give you malware
http://www.theguardian.com/technology/2014/nov/21/e-cigarettes-malware-computers

Cybersecurity lapses leave government agencies vulnerable to hackers
http://www.washingtontimes.com/news/2014/nov/23/cybersecurity-lapses-leave-us-government-agencies-/

Cybersecurity was missing in action on Election Day
http://thehill.com/blogs/pundits-blog/technology/225143-cybersecurity-was-missing-in-action-on-election-day

ENISA guidelines on cryptographic solutions
http://net-security.org/secworld.php?id=17678

Researchers Uncover Government Spy Tool Used to Hack Telecoms and Belgian Cryptographer
http://www.wired.com/2014/11/mysteries-of-the-malware-regin/

Civil liberties groups vow to fight on after Senate kills NSA reform bill
http://www.theguardian.com/us-news/2014/nov/19/senate-kills-nsa-reform-bill-civil-liberties-groups

Cyber war games held
http://www.washingtontimes.com/news/2014/nov/12/inside-the-ring-cyber-war-games-held/

Hacker Lexicon: What Is the Dark Web?
http://www.wired.com/2014/11/hacker-lexicon-whats-dark-web/

New House Intel chief viewed NSA reform as unnecessary
http://thehill.com/policy/technology/224627-new-house-intel-chief-viewed-nsa-reform-as-unnecessary

WhatsApp Adds Encryption by Default to Android App

http://threatpost.com/whatsapp-adds-encryption-by-default-to-android-app/109442

DDoS attacks continue to fall in size and frequency
http://net-security.org/secworld.php?id=17657

10 hottest IT skills for 2015
http://www.computerworld.com/article/2844020/careers/10-hottest-it-skills-for-2015.html

IG: DHS Struggles to Manage Privacy
http://www.govinfosecurity.com/ig-dhs-struggles-to-manage-privacy-a-7574

Unscheduled Windows update kills critical security bug under active attack
http://arstechnica.com/security/2014/11/unscheduled-windows-update-kills-critical-security-bug-under-active-attack/

DOJ scores two cyber crime wins
http://thehill.com/policy/cybersecurity/225450-doj-scores-two-cyber-crime-wins

Siemens pushes out emergency SCADA updates
http://net-security.org/secworld.php?id=17695

Researchers identify POS malware targeting ticket machines, electronic kiosks
http://www.scmagazine.com/researchers-identify-pos-malware-targeting-ticket-machines-electronic-kiosks/article/385558/

This Artist's Images Integrate Code From Malware Like Stuxnet and Flame
http://www.wired.com/2014/11/malware-art/

Intelligence authorities 'fail to understand data', say ISPs
http://www.theguardian.com/technology/2014/nov/27/intelligence-authorities-fail-to-understand-data-isp

How to evaluate national cyber security strategies
http://net-security.org/secworld.php?id=17694

Bracing for Breaches This Holiday Season
http://www.govinfosecurity.com/bracing-for-breaches-this-holiday-season-a-7612

Obama facing uphill battle in curbing NSA snooping
http://www.washingtontimes.com/news/2014/nov/27/obama-facing-uphill-battle-in-curbing-nsa-snooping/

AHA: Medical Device Makers Should Be Accountable for Cybersecurity

http://www.ihealthbeat.org/articles/2014/11/26/aha-medical-device-makers-should-be-accountable-for-cybersecurity

The Week Ahead: Cybercrime, Telecommunications Law and the Internet of Things
http://blogs.rollcall.com/technocrat/the-week-ahead-cybercrime-telecommunications-law-and-the-internet-of-things/?dcz=

Why is Facebook Flaw Still Unpatched?
http://www.govinfosecurity.com/is-facebook-flaw-still-unpatched-a-7619

2014: The year everyone's security took a hit
http://www.zdnet.com/2014-the-year-everyones-security-took-a-hit-7000036224/#ftag=RSS86a1aa4

The persistent threat of data breaches
http://net-security.org/secworld.php?id=17700

Companies must act quickly to tackle cyber crime
http://www.computerweekly.com/feature/Companies-must-act-quickly-to-tackle-cyber-crime

NSA Opens Up Data Automation Software For Public Use
http://www.forbes.com/sites/adrianbridgwater/2014/12/01/nsa-opens-up-data-automation-software-for-public-use/

Commerce takes bigger oversight role in its bureaus' cybersecurity
http://www.federalnewsradio.com/523/3753468/Commerce-takes-bigger-oversight-role-in-its-bureaus-cybersecurity

If anything shouldn't be taken for granted, it's Information Security Management
http://net-security.org/secworld.php?id=17696

Securing Federal Data on Nonfederal Systems
http://www.govinfosecurity.com/securing-federal-data-on-nonfederal-systems-a-7593

Are hackers playing the stock market?
http://thehill.com/policy/cybersecurity/225562-are-hackers-playing-the-stock-market

FBI warns of 'destructive' malware following Sony hack
http://www.zdnet.com/fbi-warns-of-destructive-malware-following-sony-hack-7000036313/

New point-of-sale malware on underground markets for $2,000
http://www.computerworld.com/article/2854154/new-point-of-sale-malware-on-underground-markets-for-2000.html

Hacker Group Claims Credit For Taking Xbox Live Offline
http://www.forbes.com/sites/davidthier/2014/12/01/hacker-group-takes-credit-for-taking-xbox-live-offline/

Edward Snowden wins Swedish human rights award for NSA revelations
http://www.theguardian.com/us-news/2014/dec/01/nsa-whistlebloewer-edward-snowden-wins-swedish-human-rights-award

US establishes Counter Intelligence and Security Center
http://economictimes.indiatimes.com/news/international/world-news/us-establishes-counter-intelligence-and-security-center/articleshow/45341440.cms

DOJ wants Apple to help unlock iPhones
http://thehill.com/policy/cybersecurity/225621-inside-the-dojs-requests-for-apple-to-unlock-iphones

The 10 Biggest Bank Card Hacks
http://www.wired.com/2014/12/top-ten-card-breaches/

Report Connects Iran to Critical Infrastructure Hacks Worldwide
http://threatpost.com/report-connects-iran-to-critical-infrastructure-hacks-worldwide/109666

Training kids to become infosec superheroes
http://net-security.org/secworld.php?id=17705

How to recover a stolen Twitter ID from Russian-speaking Bruce Willis impostor
http://www.csmonitor.com/Innovation/Tech/2014/1201/How-to-recover-a-stolen-Twitter-ID-from-Russian-speaking-Bruce-Willis-impostor

Fear of Mobile Device Evidence Collection?
http://www.officer.com/article/12023577/fear-of-mobile-device-evidence-collection

Obama's pick to lead the Pentagon is big on cybersecurity

http://www.washingtonpost.com/blogs/the-switch/wp/2014/12/02/obamas-pick-to-lead-the-pentagon-is-big-on-cybersecurity/

How the world's powers are preparing to defend themselves against cybercrime
http://www.telegraph.co.uk/technology/internet/11268693/How-the-worlds-powers-are-preparing-to-defend-themselves-against-cybercrime.html

Microsoft's futuristic cybercrime computer lets you see and hear botnet activity
http://www.geek.com/microsoft/microsoft-futuristic-cybercrime-computer-lets-you-see-and-hear-botnet-activity-1610635/

Trainee cyber-criminals wanted to help solve skills shortage
http://phys.org/news/2014-12-trainee-cyber-criminals-skills-shortage.html

Likely DOD pick helped drive Cyber Command buildup
http://thehill.com/policy/cybersecurity/225780-likely-dod-pick-helped-drive-cyber-command-expansion

Cyber Threats to Increase in Scope and Complexity in the New Year as Black Hat Hackers Become More Sophisticated, According to Fortinet 2015 Threat Predictions
http://www.broadwayworld.com/bwwgeeks/article/Cyber-Threats-to-Increase-in-Scope-and-Complexity-in-the-New-Year-as-Black-Hat-Hackers-Become-More-Sophisticated-According-to-Fortinet-2015-Threat-Predictions-20141203

Making the business case for cybersecurity
http://www.federaltimes.com/article/20141201/CYBER/312010020/Making-business-case-cybersecurity

For China, Cybersecurity Is Part of Strategy for Protecting the Communist Party
http://sinosphere.blogs.nytimes.com/2014/12/03/for-china-cybersecurity-is-part-of-strategy-for-protecting-the-communist-party/?_r=0

This Guy's Hacked Hearing Aids Let Him Listen to Wi-Fi Networks
http://www.wired.com/2014/12/guys-hacked-hearing-aids-let-listen-wi-fi-networks/

Justice Department Plans New Cybercrime Team
http://www.npr.org/2014/12/04/368351872/justice-department-plans-new-cybercrime-team

Digital Forensics Can Use Facebook to Solve Cases

http://www.baselinemag.com/security/digital-forensics-can-use-facebook-to-solve-cases.html

Did North Korea Really Hack Sony?
https://www.bloomberg.com/politics/features/2014-12-04/did-north-korea-hack-sony-theories-on-sony-hacking

Inside the "wiper" malware that brought Sony Pictures to its knees

http://arstechnica.com/security/2014/12/inside-the-wiper-malware-that-brought-sony-pictures-to-its-knees/

The Real Cost of Cyber Incidents, According To Insurers
http://www.darkreading.com/the-real-cost-of-cyber-incidents-according-to-insurers/d/d-id/1317851

Bank-funded cyber info sharing software released

http://thehill.com/policy/cybersecurity/225872-banks-release-cyber-info-sharing-software

Defense contractors fighting cyber threats can share information through new Information Security and Analysis Center
http://www.al.com/business/index.ssf/2014/12/defense_contractors_fighting_c.html

Avoiding Data Breaches with Context Aware Behavioral Analytics
http://threatpost.com/avoiding-data-breaches-with-context-aware-behavioral-analytics/109679

Best practices in knowledge-based authentication
http://net-security.org/secworld.php?id=17715

Cybersecurity Seen as DoD Priority Under Carter
http://www.govinfosecurity.com/cybersecurity-seen-as-dod-priority-under-carter-a-7634

Inside the "wiper" malware that brought Sony Pictures to its knees [Update]
http://arstechnica.com/security/2014/12/inside-the-wiper-malware-that-brought-sony-pictures-to-its-knees/

What is on the Pentagon Cyber Chief's Holiday Shopping List?
http://www.nextgov.com/cybersecurity/2014/12/what-pentagon-cyber-chiefs-holiday-shopping-list/100539/

In surprise, Senate may bring up cyber bill
http://thehill.com/policy/cybersecurity/225994-senate-may-move-soon-on-cyber-bill

Judge: Give NSA unlimited access to digital data
http://www.pcworld.com/article/2855776/judge-give-nsa-unlimited-access-to-digital-data.html

Health insurance online threats revealed
http://net-security.org/secworld.php?id=17718

NH-ISAC Offers Cyber-Intelligence Tool
http://www.govinfosecurity.com/nh-isac-offers-cyber-intelligence-tool-a-7642

DOJ Launches New Cyber Unit, Claims Privacy is Mission Critical
http://threatpost.com/doj-launches-new-cyber-unit-claims-privacy-is-mission-critical/109732

Detecting the Insider Threat - how to find the needle in a haystack?
http://www.computerworld.com/article/2854636/security0/detecting-the-insider-threat-how-to-find-the-needle-in-a-haystack.html

Lizard Squad performs a 'RIGHTEOUS' Sony HACK
http://www.computerworld.com/article/2856472/lizard-squad-performs-a-righteous-sony-hack-

itbwgk.html

It's Computer Science Ed Week And It's Time To Do Something
http://techcrunch.com/2014/12/08/its-computer-science-ed-week-and-its-time-to-do-something/

Data from wearable devices could soon land you in jail
http://www.networkworld.com/article/2856479/big-data-business-intelligence/data-from-wearable-devices-could-soon-land-you-in-jail.html

The cybersecurity skills gap
http://www.scmagazine.com/the-cybersecurity-skills-gap/article/385079/

Police 'failing to train key staff to fight growing threat of cyber crime'
http://www.independent.co.uk/news/uk/crime/police-failing-to-train-key-staff-to-fight-growing-threat-of-cyber-crime-9909334.html

Teams gain computing, life skills in cybersecurity competition
http://www.mercedsunstar.com/news/local/article4334666.html

We are in a war with no boundaries, warns cyber security expert
http://www.thenational.ae/uae/technology/we-are-in-a-war-with-no-boundaries-warns-cyber-security-expert

What will create cybersecurity challenges in 2015?
http://www.net-security.org/secworld.php?id=17727

Largest school districts vow computer science classes, WH says
http://thehill.com/policy/technology/226287-largest-school-districts-vow-computer-science-classes-wh-says

Enacting Cyber Law Remains Possibility
http://www.govinfosecurity.com/blogs/enacting-cyber-law-remains-possibility-p-1779

Senate Dem plans 'botnet' bill for 2015
http://thehill.com/policy/cybersecurity/226425-senate-dem-plans-botnet-bill-for-2015

Meet the hacking prodigy you definitely want on your side
http://www.pri.org/stories/2014-12-08/meet-hacking-prodigy-you-definitely-want-your-side

Here Are The FBI's Most Wanted Cyber Criminals
http://www.businessinsider.com/fbis-most-wanted-cyber-criminals-2014-12?op=1

New DOJ Cybersecurity Unit to advise on Internet crime
http://www.federaltimes.com/article/20141205/CYBER/312050020/New-DOJ-Cybersecurity-

Unit-advise-Internet-crime?odyssey=nav|head

Security Expert Says Antivirus Vendors Must Disclose Threats Sooner
http://blogs.wsj.com/cio/2014/12/08/security-expert-says-antivirus-vendors-must-disclose-threats-sooner/

A new strain of "ransomware" is striking
http://www.cbsnews.com/news/warning-issued-over-new-strain-of-ransomware/

Hackers hit Playstation, Sony Entertainment Network
http://nypost.com/2014/12/09/hackers-hit-playstation-sony-entertainment-network/

Rock Veteran Gets Jail Time for Participating in Anonymous Hack
http://www.billboard.com/articles/business/6386028/jake-commander-anonymous-operation-payback-jail-federal-court

Molly Sauter's quest to make political DDoS legitimate
http://www.csmonitor.com/World/Passcode/2014/1208/Molly-Sauter-s-quest-to-make-political-DDoS-legitimate

Senate looks to move on DHS cyber bill
http://thehill.com/policy/cybersecurity/226395-senate-expected-to-move-on-cybersecurity-bill

Pirate Bay Down Following Police Raid In Sweden
http://www.huffingtonpost.com/2014/12/10/pirate-bay-down-raid-sweden-internet-piracy_n_6299936.html?utm_hp_ref=technology

A huge intelligence screw-up turned the government and private companies into cyberwarfare partners
http://wgbhnews.org/post/huge-intelligence-screw-turned-government-and-private-companies-cyberwarfare-partners

Sony attackers also stole certificates to sign malware
http://arstechnica.com/security/2014/12/sony-attackers-also-stole-certificates-to-sign-malware/

'Inception' malware, dropped clues have hacker experts stymied
http://www.stripes.com/news/europe/inception-malware-dropped-clues-have-hacker-experts-stymied-1.318317

Healthcare Security In 2015: 9 Hotspots
http://www.informationweek.com/healthcare/security-and-privacy/healthcare-security-in-2015-9-hotspots/d/d-id/1317867

FISMA, cyber workforce bill clear hurdles - Cromnibus hits a speed bump - Sony latest: Hackers

demanded money before attack
http://www.politico.com/morningcybersecurity/1214/morningcybersecurity16382.html

Funding bill boosts cybersecurity spending
http://thehill.com/policy/cybersecurity/226577-funding-bill-boosts-cyber-spending

NIST Tardy on Cryptography Standards Report
http://www.govinfosecurity.com/nist-tardy-on-cryptography-standards-report-a-7651

Microsoft released seven advisories, three are critical
http://net-security.org/secworld.php?id=17744

FBI doubts North Korea link to Sony Pictures hack
http://www.theguardian.com/technology/2014/dec/10/fbi-doubts-north-korea-link-sony-pictures-hack

Senate passes DHS cyber bill
http://thehill.com/policy/cybersecurity/226639-senate-passes-dhs-cyber-bill

Why DC is Getting a $35M Cybersecurity Campus
http://inthecapital.streetwise.co/2014/12/10/dc-35m-cybersecurity-campus-gsa/

Is the game finally up for The Pirate Bay? Site knocked offline following police raid

http://www.digitaltrends.com/computing/game-finally-pirate-bay-site-knocked-offline-following-police-raid/

Standards: The superglue for security systems
http://www.securityinfowatch.com/article/12026739/axis-steve-surfaro-examines-how-standards-serve-as-the-superglue-that-binds-security-systems-together

'Hackers are a serious threat to aircraft safety': Aviation chiefs warn of the devastating consequences of a cyber attack

http://www.dailymail.co.uk/sciencetech/article-2869827/Hackers-threat-aircraft-safety-Aviation-chiefs-warn-devastating-consequences-cyber-attack.html

Today's multiheaded malware needs a multipronged solution
http://www.infoworld.com/article/2858313/endpoint-protection/predictive-execution-inspection-detecting-malware-designed-to-hide.html

Sony Hackers Nabbed Digital Cert to Evade Malware Filters
http://www.infosecurity-magazine.com/news/sony-hackers-stole-cert-to-evade/

Sony uses hacker techniques to fight back over stolen data
http://www.theguardian.com/technology/2014/dec/11/sony-uses-hacker-techniques-to-fight-back-over-stolen-data

Senate's torture report will provoke hacktivist reprisals
http://www.computerworld.com/article/2857784/senates-torture-report-will-provoke-hacktivist-reprisals.html

Big Data analytics to the rescue
http://www.net-security.org/article.php?id=2181

Streamlining the Digital Forensic Workflow: Part 3
http://www.dfinews.com/articles/2014/12/streamlining-digital-forensic-workflow-part-3

Young hacker trains cops in tackling cyber-crime cases in Punjab
http://zeenews.india.com/news/punjab/young-hacker-trains-cops-in-tackling-cyber-crime-cases-in-punjab_1514558.html

FBI: Iran Hackers May Target U.S. Energy, Defense Firms
http://recode.net/2014/12/13/iran-hackers-may-target-u-s-energy-defense-firms-fbi-warns/

Ransomware criminals turn to virus technique to spread infection
http://news.techworld.com/security/3590984/ransomware-criminals-turn-to-virus-technique-to-spread-infection/

Voice Biometrics Improve Transaction Monitoring Fraud Detection
http://www.banktech.com/security/voice-biometrics-improve-transaction-monitoring-fraud-detection/a/d-id/1318145

Cyber breakthrough eludes lawmakers
http://thehill.com/policy/cybersecurity/227017-cyber-breakthrough-eludes-lawmakers

Agencies Mold Regulations around 'Voluntary' Cyber Standards
http://www.nextgov.com/cybersecurity/2014/12/agencies-mold-regulations-around-voluntary-cyber-standards/101217/

Sony hacked in February, knew about security flaws before data leak
http://www.networkworld.com/article/2859473/microsoft-subnet/sony-hacked-in-feb-knew-about-huge-security-flaws-before-cybersecurity-train-wreck.html

AP source: US probe links NKorea to Sony hacking
http://www.mysanantonio.com/business/technology/article/AP-source-US-probe-links-NKorea-to-Sony-hacking-5964004.php

Ars Technica readers urged to change passwords in wake of hack
http://www.net-security.org/secworld.php?id=17768

ICANN data compromised in spearphishing attack
http://www.computerworld.com/article/2860408/icann-data-compromised-in-spearphishing-attack.html

State-sponsored or not, Sony Pictures malware "bomb" used slapdash code
http://arstechnica.com/security/2014/12/state-sponsored-or-not-sony-pictures-malware-bomb-used-slapdash-code/

Is ISIS Trying To Unmask Syrians With Malware?
http://www.forbes.com/sites/thomasbrewster/2014/12/18/is-isis-trying-to-unmask-syrians-with-malware/

A look at North Korea's cyberwar capabilities
http://www.sanluisobispo.com/2014/12/18/3404101_a-look-at-north-koreas-cyberwar.html?sp=/99/102//&rh=1

London teen pleads guilty to Spamhaus DDoS
http://www.theregister.co.uk/2014/12/17/london_teen_pleads_guilty_to_spamhaus_ddos/

Cybersecurity 2014: The battle for mindshare
http://fedscoop.com/year-cybersecurity/

Connected cars: a cyber-security nightmare on wheels
http://www.techradar.com/news/world-of-tech/connected-cars-a-cyber-security-nightmare-on-wheels-1277541

Romney: Release 'The Interview' for free online
http://thehill.com/policy/cybersecurity/227521-house-dem-release-the-interview-on-dvd

South Korea steps up cyber security at nuclear plants
http://www.reuters.com/article/2014/12/23/us-southkorea-cybersecurity-park-idUSKBN0K106620141223

DHS Releases Destover Wiper Malware Indicators of Compromise
http://threatpost.com/dhs-releases-destover-wiper-malware-indicators-of-compromise/110025

North Korea and cyberterrorists won big in Sony hack, researcher says
http://arstechnica.com/information-technology/2014/12/how-north-korea-won-the-sony-cyber-war-even-if-they-didnt-start-it/

U.S. coy about North Korea Internet failure as retaliation speculation swirls
http://www.washingtontimes.com/news/2014/dec/22/us-coy-about-north-korea-internet-failure-as-retal/

As North Korea Loses Internet, Anonymous, Others Question Whether It Really Hacked Sony
http://www.huffingtonpost.com/2014/12/22/north-korea-internet_n_6367654.html

Gang Hacked ATMs from Inside Banks
http://krebsonsecurity.com/2014/12/gang-hacked-atms-from-inside-banks/

What Is Wrong With 'Legal Malware'?
http://www.forbes.com/sites/eugenekaspersky/2014/12/22/what-is-wrong-with-legal-malware/

Cyber Command investment ensures hackers targeting U.S. face retribution
http://www.washingtontimes.com/news/2014/dec/22/us-cyber-command-investment-ensures-hackers-target/

Watchdog: Secret Service refused to hand over cybersecurity data
http://thehill.com/blogs/blog-briefing-room/227929-watchdog-secret-service-refused-to-hand-over-cyber-security-data

The Year's Worst Hacks, From Sony to Celebrity Nude Pics
http://www.wired.com/2014/12/top-hacks-2014/

When Does Cyber Crime Become an Act of Cyberwar?
http://townhall.com/columnists/rachelmarsden/2014/12/23/when-does-cyber-crime-become-an-act-of-cyberwar-n1935158

SoakSoak Malware Campaign Evolves
https://threatpost.com/soaksoak-malware-campaign-evolves/110081

POS malware crooks hack IP cams to validate targets
http://www.theregister.co.uk/2014/12/24/opendaylight_vulnerability/

Were hackers behind North Korea outage?
http://www.politico.com/story/2014/12/north-korea-internet-113746.html

North Korean Web goes dark days after Obama pledges response to Sony hack
http://www.washingtonpost.com/business/economy/north-korean-web-goes-dark-days-after-obama-pledges-response-to-sony-hack/2014/12/22/b76fa0a0-8a1d-11e4-9e8d-0c687bc18da4_story.html

Nuclear plant hack resembles past North Korea attacks
http://thehill.com/policy/cybersecurity/228013-nuclear-plant-hack-resembles-past-north-korea-attacks

Cybercrime will continue to evolve
http://net-security.org/secworld.php?id=17778

Feds Enhancing Cloud Security Vetting Process
http://www.govinfosecurity.com/feds-enhancing-cloud-security-vetting-process-a-7687

China is key to North Korean Internet, but maybe not hackers
http://www.computerworld.com/article/2862854/china-is-key-to-north-korean-internet-but-maybe-not-hackers.html

DoJ's new cybersecurity office to aid in worldwide investigations
http://www.federalnewsradio.com/489/3769859/DoJs-new-cybersecurity-office-to-aid-in-worldwide-investigations

European Hackers Found New Method to Bypass Fingerprint Authentication
http://www.utahpeoplespost.com/2014/12/european-hackers-found-new-method-to-bypass-fingerprint-authentication/

Degree profile: Criminal justice & cyber crime
http://www.militarytimes.com/story/veterans/careers/civilian/jobs/2014/12/28/cyber-crime-mendez-jobs-careers/20489271/

Re-Gifting Digital Gadgets Can Lead to Identity Theft Woes
http://securitywatch.pcmag.com/security/330704-re-gifting-digital-gadgets-can-lead-to-identity-theft-woes

Sony says PlayStation Network is back online now, really
http://www.computerworld.com/article/2863446/sony-says-playstation-network-is-back-online-now-really.html

The 5 Most Dangerous Software Bugs of 2014
http://www.wired.com/2014/12/most-dangerous-software-bugs-2014/

Cyber attack on Angela Merkel aide: Report
http://www.dw.de/cyber-attack-on-angela-merkel-aide-report/a-18155195

Secret Service Withheld Monitoring Data from DHS
http://www.govinfosecurity.com/secret-service-withheld-monitoring-data-from-dhs-a-7720

Why It's Time For A Board-Level Cybersecurity Committee
http://www.forbes.com/sites/frontline/2014/12/27/why-its-time-for-a-board-level-cybersecurity-committee/




**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

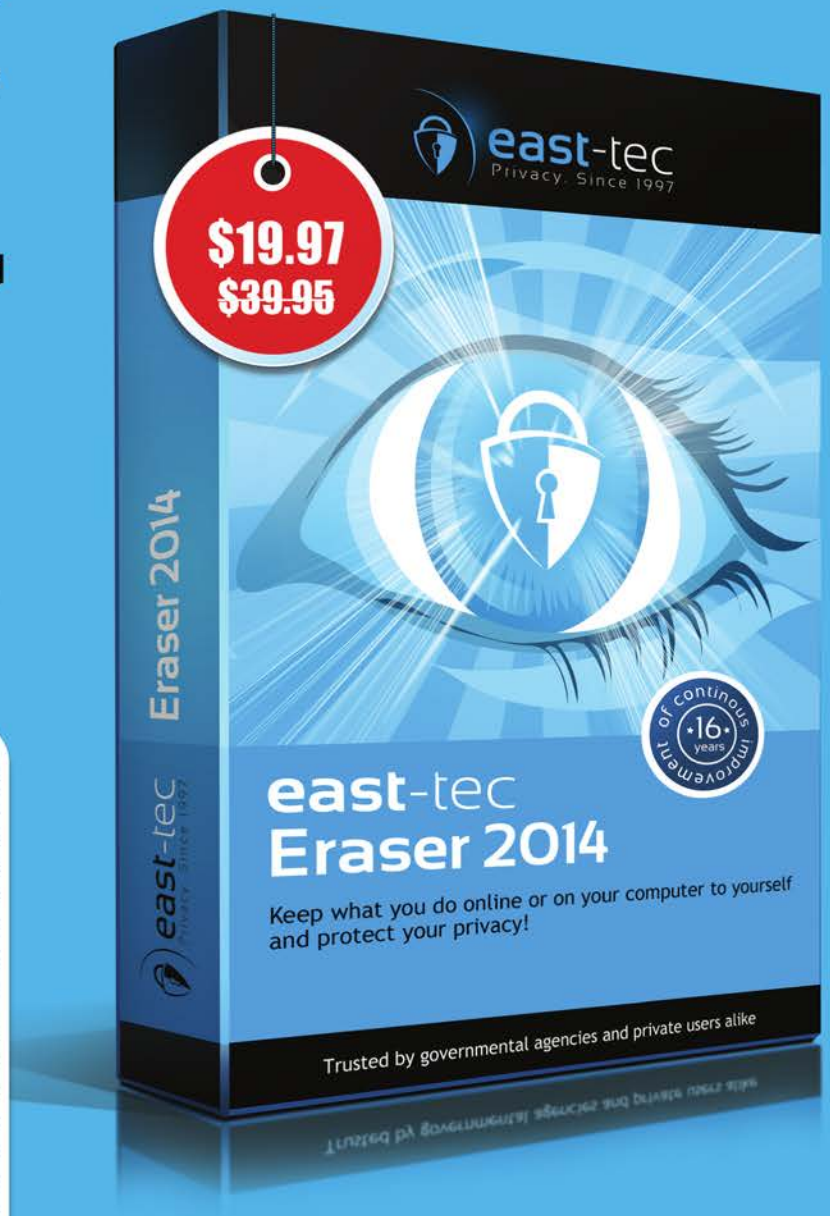
Cyber Defense Magazine - Cyber Warnings rev. date: 12/29/2014

east-tec
Privacy. Since 1997

www.east-tec.com

# east-tec Eraser 2014

Protect your data and privacy by removing all evidence of your online and offline activity with **East**-Tec **Eraser 2014**.
Securely erase your Internet and computer activities and traces, improve your PC performance, keep it clean and secure!




Exclusive offer for Cyber Defense magazine readers

**Save 50%**

on ALL East-Tec products
www.east-tec.com

**Coupon Code:**

CYBERMAG2014

private evidence protection traces from 250 + apps history pages online privacy secure search pictures cookies security emails