A Culture of Cybersecurity: The Only Way Forward

A Logical Operations Whitepaper

Logical Operations

Is the Russian government actively trying to influence the U.S. Presidential election? Is the House Oversight and Government Reform Committee's assertion that we must treat federal employees the same as outside threats in order to prevent data breaches correct? Are American businesses truly losing the battle against hackers? Recent media headlines suggest the American public is hungry for news about cybersecurity incidents. Given that media outlets stay in business by getting eyes on the screen, it seems a safe bet to say they're right. And, with good reason.

Attacks are hitting users and systems in frightening numbers. According to the Kaspersky Security Bulletin for 2015, more than one in three user computers (34.2%) experienced an attack while the owners were online last year. Given the number of computer users worldwide, that's a staggering figure. Security breaches, identify theft, and malicious attacks on critical infrastructure, quite simply, have people scared. And when people are scared, they want information. And these days, there's no shortage of it.

However, outside of general public-awareness campaigns and media attention, the only exposure to cybersecurity training most people receive is through programs delivered to them, as either employees or contractors, through companies and other organizations. Unfortunately, this type of training typically comes in one of two forms: buried within other onboarding paperwork as part of Human Resources processing, or through self-paced learning modules that employees begrudgingly complete on a second computer monitor while attending to "more important" matters.

In addition to the relatively low standards of the security training programs offered by many organizations, these programs often also overlook a critical component of knowledge retention: engagement. Many security awareness programs simply don't answer the questions "why should I care?" and "how does this impact me?" The general public still has this pervasive sense of cybersecurity being an "IT issue," despite the mountain of information publicly available indicating that end users represent the single greatest risk to information and system security. Consider these two additional facts from the latest Kaspersky Security Bulletin:

- More than 75% of all web-based attacks last year came in the form of malicious URLs (how many end users in any large organization could have clicked just one of them?).
- The United States accounted for nearly a quarter (24.18%) of all cases of infected online resources (as measured by antivirus systems blocking known exploits).

Until organizations, their end users, and the population as a whole adopt a culture of cybersecurity, all of the awareness training, system hardening, and resource allocation could be for naught.

But, there are signs of progress. As cybersecurity threats have increased, both in frequency of occurrence and media attention, some organizations are formalizing their training and awareness efforts as a way to protect the massive amount of data they generate, especially as data has become an increasingly valuable asset. Instead of simply providing their employees and customers with policy updates or basic instructions on how to identify and report potential threats, organizations are beginning to understand that systems threats have taken on many new forms, and that training must be delivered by an expert facilitator in order to convey the true importance of this issue.

Recognizing the need this new understanding is creating, Logical Operations released its "CyberSAFE: Securing Assets For End-users" education program to commercial training providers, corporations, and consumers in 2015. The program was designed from the ground up to be delivered by an expert facilitator (in either live, virtual, or blended environments), which helps to ensure the transfer of knowledge and skills—along with the critical importance of them—to learners who might otherwise gloss over the material on their own. The result? Organizations with staff and customers who have a much greater sense of the dangers of the virtual world and how to mitigate against them, and consumers with a heightened demand for cybersecurity protection from the vendors they trust with their digital information.

While practical, engaging training programs are beginning to have a positive impact on end users and how they interact with technology, the most promising approaches for addressing cybersecurity training needs into the future will feature a way for people to validate their new-found knowledge and skills. Well-designed and implemented training programs are unquestionably effective. But, it's critically important to be able to measure or verify that effectiveness. As a student, it's common to attend a training program (whether self-paced or instructor-led) and come out on the other side feeling as if he or she retained all of the important information. As someone responsible for implementing a training program, it would be easy to review a program's content, verify that it is sound, observe live training sessions, and assume that attendees achieved the desired result. The problem, though, is that it's still an assumption.

Neither of these scenarios actually demonstrates that students retained knowledge. And without proof that the desired outcomes have been achieved, what was the point of putting the training program into place to begin with? Cybersecurity is simply a topic that can no longer be given only passive attention. The addition of a knowledge-verification process, such as a credential or certification program, provides the mechanism necessary to, if not guarantee, at least verify training effectiveness.

As part of Logical Operations' CyberSAFE program, all students are provided the opportunity to earn their own CyberSAFE credentials, which demonstrate competence in key areas of cybersecurity awareness. And, Logical Operations' approach to the credentialing process avoids some of the pitfalls of other similar programs. Perhaps the most appealing part of this approach is the fact that CyberSAFE credential candidates are not forced to schedule and take an exam at a remote testing center. This is a huge convenience for students and it allows their organizations to save the time and money that they'd otherwise naturally expend if they had to rely on third-party facilities. CyberSAFE candidates can access the credentialing process through Logical Operations' CHOICE LMS platform, providing them with anytime, anywhere access (via nearly any device) to complete the credentialing process in a way that makes the most sense for them.

In addition to the convenience this approach provides, it also helps students avoid feeling trapped by the constraints they might otherwise be faced with. Formal, high-pressure situations that tether candidates to a specific place at a particular time leave them feeling stuck, rather than empowered. This fosters a sense that cybersecurity is something with which they must comply, rather than a problem they can actively help to solve. Providing a positive experience simply makes the process seem more realistic and achievable.

Another key differentiator of Logical Operations' approach to the credentialing process is what happens to candidates who don't pass the exam on the first attempt. To expand on the idea of being trapped, candidates who know they have one chance to pass an exam might either cram for it, or try to cheat in order to get by on the first try. The downside of failing, which is having no ability or encouragement to earn the credential without significant cost or effort, actually works against the goal of having more people be able to demonstrate a comprehensive understanding of key security principles and practices. This is precisely why candidates have ready, ongoing access to CyberSAFE course materials through the CHOICE LMS and can retake the assessment at their convenience.

Another positive aspect of Logical Operations' approach is that it provides successful candidates the ability to broadcast their understanding of cybersecurity awareness principles to their colleagues and peers. The traditional method of sending an email announcement or mailing a certificate is static and old; it isn't inspiring for the certificants, and it doesn't allow them to serve as advocates for more participation in the process. Instead, Logical Operations issues successful candidates an electronic badge that can easily be shared via social media platforms, such as LinkedIn, and in email signatures. Enabling people to broadcast their achievements not only provides them a platform for demonstrating their understanding of this critical issue, it also helps raise the general awareness level of cybersecurity concerns among their peers.

So, what can we do collectively in the coming years to better address the challenge? Launching an effort to promote engagement, whether for employees within an organization or the public at large, is critical, and we should capitalize on the mechanisms for doing so that are already in place for a number of other efforts. Think about how an organization drums up support for an effort such as a blood drive or a charitable-giving campaign. People put cards and table tents out in common areas, they hang signs in hallways, they give out coffee mugs and t-shirts, members of the management team engage with their direct reports, the marketing team produces and shares awareness videos, and so forth. The same approach would absolutely work when promoting security awareness. Businesses should look beyond the tired, and often ignored, email from the IT department when trying to engage with staff, and public service organizations need to be using all of the tools they have at their disposal to get the message out.

All of this should be pointing all of us in a single direction: fostering a culture of cybersecurity in which everyone has a stake and can play an active role in keeping critical data safe. Ongoing internal marketing efforts and public awareness campaigns can engage people throughout the training and certification process—and beyond. This is a far more effective approach than simply reaching out to people once every three years when it's time to recertify. In the rush of daily life and the complex operations of large organizations, it's easy for people (who are the weakest link in the security chain) to simply forget, even if just momentarily, their roles and responsibilities when it comes to keeping systems safe. A single click on a malicious link can lead to a major security breach costing millions of dollars—the latest global analysis from the Ponemon Institute puts the figure at an average of $4 million per breach. We simply cannot go on thinking cybersecurity is somebody else's job.

Moving ahead over the next decade, organizations need to execute a plan for routinely verifying the comprehension of key cybersecurity knowledge while promoting the idea of security as everyone's responsibility. The pace at which new types of cybersecurity threats emerge is, as an understatement, rapid. A training session from last year is rarely reflective of the current security threats that could impact to the average data consumer or employee. The same holds true for a certificate or certification program associated with the topic of security awareness. Organizations need to routinely assess both their customers and their employees in order to identify weak spots that expose their data to cyber threats. And, we as consumers need to do the same in terms of our daily habits. We need to identify the specific areas of cybersecurity we are unfamiliar with, and then educate ourselves on them, in order to adequately protect our personal data.

Along the same line, organizations absolutely must start adopting a prevention-first mindset. Though the importance of cybersecurity is unquestionable and the resulting damages from attacks are daily fodder for news outlets, many organizations still feel it is more cost effective to wait until they experience a breach and then react to it, rather than invest the necessary time and resources into hardening their systems and training their people ahead of time. It is this type of shift in paradigm that is desperately needed in the coming decade and beyond to ensure data consumers and employees alike are vigilant against cyber attacks. Given the number of people who experience identity-theft issues, the incredible amount of compromised personal data, and the hugely expensive organizational attacks that have become all too common, it's astonishing that people and organizations are still slow to react.

While end-user training and certification are critical to helping solve the current information gap, it is important that organizations of all sizes continue to invest in training and certification for the people specifically charged with designing and maintaining a secure network. All too often, organizations that do send their IT staff for training are sending that staff to classes built around certifications that were cutting edge a year, or substantially longer, ago. A lot has changed, and continues to change, in the realm of IT. Gone are the days of an organization using purely Microsoft software or Cisco hardware solutions. Organizations today are vendor agnostic; they use the most appropriate vendor technology and solutions for the tasks at hand. And potentially more disruptive yet, these solutions are increasingly shifting to the cloud.

To prepare for these challenges, Logical Operations has launched additional training and certification programs within the market that are geared toward the IT professional within a typical organization. These programs take a fresh look at training, and ensure applicability against both the latest and the emerging trends in IT.

“CyberSec First Responder” (CFR) is an IT security program designed to prepare candidates for the key job tasks of actively analyzing a network for security threats, and then responding to incidents. While many IT security programs focus on core IT security principles and prevention measures, the CFR program takes a different approach, placing the emphasis on disrupting a live attack and then working to mitigate its negative effects from not only a data perspective, but also the perspective of employees and an organization’s customers.

Although the program demonstrates a more specialized skill set than those presented in common fundamentals programs available on the market today, CFR also addresses the roles played by nearly all members of an IT team during a breach. When a breach does occur, it’s all hands on deck…period! And, it’s critically important for those hands to be specifically prepared to respond to an IT security incident. The CFR exam, administered at Pearson VUE testing centers worldwide, is maintained continuously by Logical Operations’ various training content and certification development subject matter experts and practitioners. The content and the exam are updated multiple times each year to ensure the program is keeping pace with the latest security threats. And, a key part of the program is focusing on the responsibility security practitioners have to research and keep up with those emerging threats. Similar to other Logical Operations offerings, CFR is also vendor-agnostic. A quick review of basic CFR information, such as the course outline or the exam objectives, demonstrates broad coverage of various technology environments and security tools that reflect the realities of working as a security professional in a variety of organizations.

Cybersecurity has emerged as one of the critical issues of the current era; no one is disputing this. What continues to challenge organizations and society as a whole as we combat this issue is a combination of poor prioritizing, a cultural misunderstanding of our own responsibilities, and the challenge of attacking an extremely fast-moving and rapidly-evolving problem with constructs and institutions that were put in place long before cyber threats could have even been imagined. However, like with so many past issues that seemed too big to grapple with, a change in mindset, proper education, and innovative thinking can help all of us make consuming data and storing critically valuable digital assets on network systems safer while still allowing us to embrace the incredible benefits offered by the digital landscape. But, we have start thinking differently…now.