SANS SECURITY AWARENESS

Whitepaper

What Short-Format Technical Training Means for IT Professionals

With misconfigurations by IT staff being a leading cause of data breaches, computer-based security training isn't just for end users anymore.

April 2023

The concept of human risk within an organization and the security awareness techniques to manage that risk have matured to a point where the question is no longer **if** a program is necessary but more about **how** to deliver a program with the greatest effect on your organization's overall security posture.

While role-based training has emerged as a popular way for awareness teams to reinforce secure behaviors across a multitude of roles and responsibilities across a given enterprise, a very specific training gap is surfacing; and threat actors are taking notice.

Recent years have seen the IT Administrator, and the systems and networks they manage as a primary attack vector for bad actors. This begs the question: Are System and Network Administrators receiving regular security training?

Of course they are.

A better question to ask is: Are System and Network Administrators receiving the **correct** security training.

Absolutely not.

Training System and Network Administrators on security—network and system security, not just passwords and phishing—is more important today than ever before.

For System and Network Administrators, receiving security training is imperative. However, it's crucial to note that training that does not go above and beyond the same training that is given to non-technical staff will prove ineffective. It is crucial to provide highly technical IT professionals with security training that has been specifically crafted to suit their needs. This paper will examine the necessity of technical security training and offer solutions to deploy technical training to better secure your systems.

The rapidly expanding complexity of the IT world makes proper configuration more difficult than it has ever been. That is part of the reason misconfiguration errors are becoming the leading cause of security breaches according to reports from Gartner, Symantec, Verizon, among others. Training System and Network Administrators on security—**network and system security, not just passwords and phishing**—is more important today than ever before.

The Misconfiguration Problem

The Target Corp. data breach of 2013[1] affected 70 million customer credit cards and racked up damages of around $292 million. While the initial breach used stolen end-user credentials, hackers were able to roam the company's systems virtually unchallenged for weeks thanks to poorly configured permissions; offering an important lesson to the company's IT staff about limiting user permissions and third-party access.

Although the Target incident occurred nearly a decade ago, misconfigurations of IT systems are now a more significant security issue for organizations than ever before.

Notpetya (June 2017) was a worm took advantage of the "EternalBlue" vulnerability. While Microsoft had patched this months earlier, organizations did not implement the patch promptly and completely across all servers were left at risk. If notpetya gained access to as little as one unpatched server it had the ability to infect any server on the network.

[1] www.computerworld.com/article/2487425/target-breach-happened-because-of-a-basic-network-segmentation-error.html

The Equifax breach of 2017—which cost the company $1.4 billion (the most expensive breach in history)—was due to unpatched and misconfigured systems, for example. The Marriott breach (2018), the Capital One breach (2019), and the breach at Colonial Pipeline (2021) were due to similar issues, from password leaks to other types of unauthorized access.

Indeed, according to Verizon's most recent Data Breach Investigations Report (DBIR),[2] IT misconfigurations for the first time have eclipsed end users as a leading underlying cause of data breaches in 2021.

Even as recently as September of 2022, the Fastcompany news agency had a breach in which their website was defaced and their Apple News API Key was stolen.[3] This allowed the attackers to post inappropriate messages to Apple News coming from Fastcompany. The primary problem was that "dozens of accounts including administrator accounts" used the password "pizza123."

Security Awareness professionals have known for years that security is everyone's responsibility. This paper will explore how this recent shift in responsibility has created new opportunities for awareness teams to expand their training beyond the end user.

While most patterns have changed over the years, one constant has been people making mistakes. While this pattern is by definition made up of either Internal or Partner actors, this year's data shows it is all about your employees. Misdelivery and Misconfiguration are the top two varieties.

Human Error Isn't Always End User Error

End users have been flagged countless times over the years as the major—and often unwittingly—cause of cybersecurity incidents and data breaches.

But according to the most recent DBIR, misconfigurations by IT professionals are now one of the leading causes of human-error data breaches.

The report details how the misconfiguration problem began in earnest around 2018, driven mainly by cloud data stores set up without the right access controls.[4] And although public cloud providers have tweaked their default configurations to be more secure, Additional training in system administration best-practices is often necessary to stay one step ahead of bad actors waiting for IT teams to blink.

Indeed, a recent cloud security report[5] by Sonatype and Fugue indicates that more than 80 percent of cloud engineering and security professionals feel their organization is at risk of a data breach due to improperly configured networks and systems. And a recent Gartner report[6] predicts that by 2025 nearly all cloud-related security breaches will largely be driven by client errors such as system misconfigurations.

"While most patterns have changed over the years, one constant has been people making mistakes," the DBIR report reads. "While this pattern is by definition made up of either Internal or Partner actors, this year's data shows it is all about your employees. Misdelivery and Misconfiguration are the top two varieties."

Unfortunately, the more complex an organization's cloud environment becomes, the chances of misconfiguration rise exponentially—especially if IT staff aren't aware of or don't appreciate that security is an essential part of their job.

---

[2] www.verizon.com/business/resources/reports/dbir

[3] https://restoreprivacy.com/fast-companys-hack-apple-news-profanity

[4] www.wired.com/story/billion-records-exposed-online

[5] www.itpro.co.uk/cloud/361113/the-rise-of-cloud-misconfiguration-threats-and-how-to-avoid-them

[6] https://venturebeat.com/business/takeaways-from-gartners-2021-hype-cycle-for-cloud-security-report

The Siloing of IT and Security

There is a correlation to be seen between the rise of misconfiguration the increasigly siloed roles IT practitioners and security teams occupy within an organization. While it may have been common 20 years ago for system and betwork administrators to be well versed in the security threats of the day, the increasingly conmplex nature of these roles has made it more difficult to keep security top of mind.

The role of a systems administrator, for example, in an organization is often multi-faceted and requires expertise in various aspects of information technology. They are often seen as the in-house computer wizards who are responsible for maintaining—first and foremost—the reliability and functionality of the computer systems that the organization depends on to carry out their daily operations.

This broad range of responsibilities also makes it challenging for systems administrators to prioritize security as part of their job function. Given the multitude of tasks under their purview, it can be easy for security-related issues to slip through the cracks. Furthermore, ensuring security often requires a significant investment of time and resources, which can be difficult to justify in the face of competing demands.

There exists an irony in the idea that system administrators, who possess the necessary skillset to become proficient cybersecurity practitioners, often struggle to stay up-to-date on those skills due to their heavy workload.

There exists an irony in the idea that system administrators, who possess the necessary skillset to become proficient cybersecurity practitioners, often struggle to stay up-to-date on those skills due to their heavy workload. While their expertise in IT is valuable for security, the demands of their primary job duties often make it challenging to prioritize. Furthermore, corporate leadership may not be fully aware of this divide and may overlook the ramifications. Among other things, this could lead to an inadequate security framework that may be vulnerable to cyber threats, putting the organization at significant risk.

How Security Training for IT Administrators Benefits Employees, Managers, and Their Organizations

Despite what some employees may want to believe, security is everyone's job—and security awareness training was developed to address this fact. The concept of short-form, computer-based video modules to teach and test end users—that is, employees whose primary job function is not cybersecurity or even IT—on security topics was developed decades ago.

Security training teaches employees that security is in fact part of their jobs, along with the best ways to mitigate potential threats as they relate to their daily tasks and interactions. Since then, many enterprises have invested in and benefited from cybersecurity awareness training for non-technical end users such as accountants, marketing teams, human resources, sales, and similar workers.

What has only recently become apparent, however, is that short-form, computer-based video training can deliver similar benefits to highly technical systems and network administrators.

Indeed, while training that prioritizes short videos and quizzes to help users reinforce what they've learned has proven extremely successful among end users, it until now hasn't been deployed to tech-savvy IT staff. This is a critical gap, because their exclusive knowledge and privileged access make IT administrators a prime target for cyberattacks.

Given the advanced level of knowledge of IT staff, however, successful security awareness training for these tech-savvy individuals must be delivered by expert course authors with a vast reservoir of knowledge and experience.

Short-form, computer-based security training delivered by expert course authors can provide many benefits for technical staff and their organizations, including:

- **Upskilling your technical team.** As cybersecurity becomes more critical, there has been an demand for cybersecurity professionals as companies strive to protect their information assets. However, the shortage of dedicated cybersecurity specialists has presented challenges for employers. As organizations look inward to fulfill their cybersecurity needs, it becomes natural to transition existing IT staff into these roles. Organizations that prioritize training and development opportunities for IT staff will be well served.
- **Improved rapport between IT and security staff.** Their specialized nature often means there's little understanding or rapport between IT and security groups at large organizations. Security awareness training helps improve the relationship between these two groups by providing baseline training and common ground while demonstrating the thinking behind various measures.
- **Scaling the security effectiveness of your team.** While many managers or leaders of technical groups may hole technical certifications such as CISSP, CISM, or any number of GIAC certifications through lengthy and rigorous training, it's not always realistic or necessary to expect of increasingly large IT teams. Organizations can use computer-based short-form technical training to upskill large IT teams without the budgetary or time constraints large-scale in-person training can represent.

Given the advanced level of knowledge of IT staff, however, successful security awareness training for these tech-savvy individuals must be delivered by expert course authors with a vast reservoir of knowledge and experience.

Video-based training isn't just for end users in marketing or sales. Technical users such as IT admins, software developers, and industrial control engineers also need reinforcement, and computer-based video training can get them there without disrupting their schedules or your budget.

The Solution: Computer-Based Technical Training for IT Administrators

Role-based security awareness training done right has a history of bridging the gap between highly technical business leaders who typically upskill via long-form technical classes, and delivering computer-based training for their many employees.

The current climate of misconfiguration-fueled data breaches has led to a pressing need within the world of security awareness training—short-form, computer-based training to keep security top of mind for all IT staff (not just those with security in their job title).

Such self-paced courses should feature task-specific training and short-form, easily digestible content to help IT systems or network administrators advance their security knowledge and prepare for more advanced learning. These courses must also offer a progressive learning path with real-world use cases around a wide range of IT administrative roles.

To ensure the utmost relevance for highly technical IT staff, such training for technical individuals should include training on topics that include:

- Security maintenance (security hygiene and configuration management);
- Authentication and authorization (the use of passphrases, passwords, and multi-factor authentication);
- Security program management (how threats, vulnerabilities, countermeasures, laws, and compliance can inform risk management); and
- Attack mitigation technologies (how to deploy mitigation technologies to return to normal and repair root causes) among others.

Computer-based training has proven tremendously effective at upskilling adult learners in professional roles – and IT admins (and their organizations) now have a unique opportunity to benefit from a similar approach.

Wherever possible, real-world examples have the ability to drive home important learnings, such as sample attacks (spear phishing, social engineering, etc); and attack scenarios (including the evolution of detection methods and responses).

It all adds up to an increasingly complex training path catered to an individual's needs and the demands of their current role. Even among highly trained individuals, short-form reinforcement can prove beneficial as an effective way to maintain skills while keeping current on modern threats.

Computer-based training has proven tremendously effective at upskilling adult learners in professional roles—and IT admins (and their organizations) now have a unique opportunity to benefit from a similar approach.

SANS Institute: A Global Leader in Cybersecurity Training

SANS Institute, a global thought leader in information security training and certifications since its founding in 1989, has decades of experience delivering IT security training content to technical users, end users, and business leaders.

The organization recently launched a series of 12 computer-based training videos to cater to the cadre of IT professionals without a security background, but who spend much of their time working on implementations with far-reaching cybersecurity implications such as setting permissions and password policies.

Security Essentials for IT Administrators series targets IT systems and network administrators who contribute to an organization's overall security and provides increased awareness and reinforcement of critical issues for a wide range of IT roles through a range of relevant topics that include:

- The Principle of Least Privilege and how important it is to security
- The real source of breaches
- Shortening long dwell times (the time between breach and discovery)
- What mitigating risk truly means
- Using Confidentiality, Integrity, and Availability (CIA) for prioritizing budget and people
- Putting security into the Holistic System Design Lifecycle
- The importance of proper computer hygiene in preventing vulnerability
- The criticality of Two-Factor authentication
- How to help users (and themselves) develop better authentication practices
- Zero-Trust environments and how they enhance security
- Zero-Knowledge implementations and its impact on secure cloud storage
- Understanding what cryptography can – and cannot – do for us
- How poor cryptography practices can be devastating
- An understanding of common attacks
- Reviewing attacker tactics via an attack scenario
- Common Web attacks and their mitigation
- Cloud security—both the good, and the bad—and where to find guidance
- And two case studies to understand the highly complex and potentially disastrous world of supply chain attacks

With the increasing frequency and sophistication of cyber threats, it is critical that network and system administrators stay current on the necessary knowledge and skills to protect against these threats. Short-format computer-based technical training provides a convenient and effective way for administrators to maintain security best practices. By investing in this type of training, organizations can enhance their overall security posture to ensure that they are equipped to handle the every security challenge they face.

For more information and to learn more, please contact SANS today or join the SANS.org community for up-to-date cyber security news, training, and tools.