How IT and Audit Can Work Together to Strengthen Cybersecurity

Best Practices and Solutions

SOXhUB

The New Standard in SOX Management

Table of Contents

Introduction

Affecting over 200,000 machines in more than 150 countries, the ransomware known as Wanna Decryptor, or "WannaCry," became the largest cybersecurity attack in history in May 2017. The malicious software locked out users from critical data, and demanded a ransom payment to unlock the contents. Governments, hospitals, and corporations scrambled to address the attack and prevent the infection from spreading. Ironically, the virus' execution method was simple: it exploited a vulnerable Windows SMB protocol to spread – an exploit Microsoft had addressed two months prior to the attack with the release of a patch.

Cybersecurity is all too often discussed in a reactionary context, focusing on the aftermath of a breach, rather than proactively assessing the risk landscape.

Costs resulting from ransomware damages are predicted to exceed **$5 billion globally** in 2017, up from $325 million in 2015.[1] The cost of cybersecurity improvement, once thought of as ambiguous and hard to quantify, is now more tangible than ever. It is imperative that Internal Audit collaborates with IT to actively identify, prevent, and mitigate cyber risks by leveraging solutions through technology, personnel, and shared knowledge.

This whitepaper will address several steps to improving your cybersecurity defense, as well as how to bridge the communication gap between Internal Audit and IT to create a strong environment to prevent successful cybersecurity attacks.

[1] Morgan, S. (2017, May 19). Ransomware Damage Costs $5 Billion in 2017, Up From $350 Million in 2015. Retrieved from http://cybersecurityventures.com/ransomware-damage-report-2017-5-billion/

System Based Solutions

PATCH IT SYSTEMS

The most obvious and often overlooked method to prevent successful cyber attacks is to patch IT systems. Cybersecurity attacks will most frequently target basic exploits which can be easily fixed, many of which have had patches available for months or years. This is the number one reason organizations and individuals alike are susceptible to cyber attacks.

VULNERABILITY SCANS

While actively patching systems is the best preventative measure toward a strong cybersecurity foundation, detective measures need to be implemented as well. Regularly performing vulnerability scans (both on internal and publicly facing networks) is an essential action to identify Common Vulnerabilities and Exposures (CVEs) on systems within the network. CVEs are documented through a public list maintained by the National Cybersecurity FFRDC (NCF). Vulnerability scanning tools can quickly identify which of these CVEs exist on systems within a network, providing a comprehensive listing of assets requiring emergency patches.

ENFORCING REMEDIATION

Equally important to routinely performing vulnerability scans is enforcing the remediation of noted vulnerabilities and exposures identified through the scans. Application and solution owners should be trained on the organization-wide incident response program to ensure timely remediation of vulnerability scan results.

ACTIVITY AND APPLICATION LOGGING

Activity and application logging and monitoring is crucial to identifying malicious behavior within an IT environment. Tools should be implemented to aggregate logs and identify signature patterns of attacks.

CONFIGURING ENCRYPTION

Additional cybersecurity preventative measures include configuring encryption for all sensitive data in transit. At minimum, all communications transmitted over public or outside networks should be protected, with secure encryption and/or encapsulation techniques.

Finally, an often-overlooked aspect of cybersecurity is physical security. All areas containing information security assets, or access to internal assets (e.g., wired network ports), should be restricted and monitored through periodic user access reviews.

Solutions Through People

While system based solutions are essential to maintaining a secure environment, it is critical to remember the impact made by internal users. IBM found in its 2017 Cyber Security Intelligence Index that 58 percent of all attackers are "insiders," or attacks originating from within an organization.[2] While most internal attacks were likely not initiated with malicious intent, the threat of "inadvertent actors," or employees unknowingly carrying out or falling victim to cyber attacks on their machines, is prominent.

The clear initial step toward preventing internal threats is to ensure access to physical, system, and network assets is segregated, restricted, and only provisioned on a need-to-have basis. Access should be periodically reviewed for appropriateness.

[2] IBM X-Force Research. (2017, March 29). IBM X-Force Threat Intelligence Index 2017. Retrieved from https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=WGL03140USEN&.

Solutions Through People *Continued*

A comprehensive cybersecurity training program is the most effective long-term solution to converting employees from potential threats to cybersecurity champions. An organization's security is a shared responsibility, and educating users on their portion of that responsibility is crucial to fostering a cyber-aware environment. Training should emphasize the ownership everyone maintains within the organization, and focus on common attacks which affect users, such as phishing.

Training results can be magnified by incorporating rewards and gamification. For instance, routinely sending "phishing" emails to users, and rewarding those who report these messages to Information Security with points or prizes, can encourage education and participation with a much higher engagement level than traditional methods. Users should be educated to not only identify common attacks, such as malicious email attachments and phishing efforts, but also to report attacks or suspicious activity.

In other words: See Something, Say Something.

IT and Internal Audit Collaboration

THE CHALLENGE

Traditionally, Information Security and Internal Audit teams have held common end goals but have encountered difficulties in creating effective collaboration. Both teams seek to help the enterprise prevent and mitigate risk and remain secure. However, the differences in the day-to-day operations of each team can induce challenges in tying the collective goals and objectives together.

While Internal Audit teams know what they need to accomplish to mitigate risk, information gaps reside in the technicalities of how to do so. On the other hand, IT teams are well-versed in the technical specifications and how to configure a system to fight different cyber attacks, but they may not completely understand the compliance or regulatory goals that Internal Audit measures effectiveness upon. Thus, among the biggest challenges companies face in creating an effective defense against cybersecurity attacks is ensuring communication between Internal Audit and IT.

THE SOLUTION

1. Internal Audit teams should strive to create strong and transparent partnerships with Information Security groups through open communication and collaborative planning. Rather than announcing audits sporadically, Internal Audit should work closely with Information Security during annual risk assessments and the audit plan development phase to identify the most effective audit areas to target - inclusive of the risks addressed by Information Security.

   By leveraging the ERM tool within SOXHUB, auditors can send personalized risk collection surveys to Information Security process owners, streamlining the flow of information between teams.

2. Internal Audit can provide Information Security with helpful information to target risk and compliance considerations, such as internal policies, best practices, and pending compliance or regulatory requirements. By actively sharing relevant information with IT teams rather than withholding it until an audit is conducted, Internal Audit can become an effective yet independent partner to Information Security.

   Through SOXHUB's industry-leading licensing model, organizations are allowed unlimited users to have access to their Information Security program. Critical information is no longer limited to Information Security and Internal Audit teams - the entire organization will have access to policies to promote a cyber-aware culture.

3. Reciprocally, Information Security teams can assist the completion of the audit plan, and visibility into risk mitigation, by providing Internal Audit with up-to-date metrics and transparent data. By fulfilling standardized risk assessment surveys and data requests through a centralized solution such as SOXHUB, Information Security teams can assist in driving the most effective audit observations.

   Process and control owners are likely already aware of areas in which gaps may exist. SOXHUB can provide transparent, real-time insight into Information Security projects and processes to support an environment of collaboration and risk coverage.

Conclusion

Cybersecurity threats such as ransomware, phishing attacks, and vulnerability exploits continue to grow and evolve in complexity. As such, it is important to consider the impact a cybersecurity attack can mean for your bottom line. While people tend to consider compliance as a cost, recent large-scale attacks such as WannaCry illuminate how compliance is realistically a valuable measure in protecting your bottom line. With the increasing magnitude of malicious attacks, teams must work together and collaborate to effectively address current cyber risks.

With an all-inclusive and unlimited user licensing model, SOXHUB allows multiple teams throughout an organization to collaborate effectively to address audit and compliance risks. By leveraging SOXHUB's Workstream module for maintaining PBC (Prepared by Client) requests in a centralized workflow, Internal Audit can make it easier than ever for Information Security and IT teams to coordinate and distribute information without difficulty.

SOXHUB is the leading solution empowering Internal Audit departments to work more efficiently and effectively to meet evolving audit requirements. To learn how SOXHUB can change the way your Internal Audit team works, contact us here.

About the Author

Aaron Wright

Aaron Wright is a Manager of Product Solutions at SOXHUB. Before joining SOXHUB, Aaron was an Internal Audit Advisor at Cardinal Health, a Fortune 15 healthcare distribution company. Aaron has a background in IT systems administration and security. Aaron's primary goal at SOXHUB is to work with Internal Audit teams to provide the best product solutions.