ICIT | Institute for Critical Infrastructure Technology

The Cybersecurity Think Tank

The Cybersecurity Show Must Go On

Surpassing Security Theatre and Minimal Compliance Regulations

January 2017

Authors

James Scott (Senior Fellow – Institute for Critical Infrastructure Technology)

Drew Spaniel (Researcher – Institute for Critical Infrastructure Technology)

`

Underwritten by:

Centrify®

The Cybersecurity Show Must Go On: Surpassing Security Theatre and Minimal Compliance Regulations

January 2017

Authors
James Scott, Sr. Fellow, ICIT
Drew Spaniel, Research, ICIT

Upcoming Event

Learn more about moving past security theatre and developing robust, holistic security strategies at the 2017 ICIT Winter Summit.

THE 2017 ICIT WINTER SUMMIT

Protecting the Cyber Frontlines

CO-CHAIRED BY CENTRIFY AND ICIT

January 23, 2017 • Ritz Carlton-Pentagon City

Registration is Now Open – www.ICITWinterSummit.org

Visit the ICIT Library to view additional research and publications

https://www.amazon.com/James-Scott/e/B01IPLQKSQ/ref=dp_byline_cont_pop_ebooks_1

The Curtain Falls on Security Theater

The United States Cybersecurity culture is heavily rooted in practices of Security Theater, where an organization that suffers a data breach or that wishes to forestall regulation can invest in countermeasures that provide a feeling or sense of security without actually improving the cybersecurity threat posture of the organization. These practices are a form of perception management intended to divert critical attention away from the organization and its reputation, and in many cases are gestures of Security Theater, used to shift the risk or impact of a breach onto consumers or the public at large. The public is defended from Security Theater by auditing, regulatory, and accountability efforts that institute mandatory minimum requirements and that provide a basic level of oversight, governance, and, in some cases, assistance. However, these compliance driven initiatives are no longer adequate to deter modern threats, and adherence to minimal compulsory requirements is now just another form of Security Theater.

At the advent of the age of the Internet, Security Theater was a cost-effective solution to protect an organization's profit margin, through calculated investments that minimally secured critical assets and minimally deterred threat actors. At the time, cyber-attackers were less sophisticated, were less numerous, and were more willing to target organizations with no cybersecurity than organizations with the absolute minimal cyber-perimeter defenses. Now, attackers that range in sophistication from script kiddies to nation-state Advanced Persistent Threats (APTs) have access to easy-to-use powerful exploit kits and malware, capable of compromising even well-resourced organizations that adhere to cybersecurity regulations and guidelines. Due to the time necessary to formulate, draft, pass, and update minimal compliance regulations, the controls are rarely and only-transitorily reflective of the hyper-evolving cyber-threat landscape. By the time organizations invest in the mandated controls, the solutions are often outdated or ineffective against the current threats. This is particularly the case for U.S. Federal agencies who received mandates from numerous entities including Congress and the Office of Management and Budget (OMB).

Minimal Requirements Equate to Minimal Security

Security Theater derives from the complex dynamic between the public, private entities, and government leaders. When the public is scared by a breach or the threat of imminent harm, the private sector and government officials seek short-term solutions to stymie panic and disenfranchisement. For a time, Security Theater served as the placebo to calm public outcry enough for incident responders and authorities to forensically investigate an incident or at least to develop impact mitigation strategies. Unlike the complex attack vectors (tools, techniques, and procedures [TTPs]) and malware used by cyber-adversaries, meaningful incident response has not rapidly evolved over the past decade. In order to avoid investment in cybersecurity infrastructure, solutions, and tools, many organizations have clung to Security Theater strategies that respond to breaches by retroactively implementing obsolete or irrelevant controls, offer meaningless credit monitoring services, or shift the burden of impact onto consumers. These strategies persist because C-level management at many organizations believe that it is still cost-effective to suffer a breach and either absorb the impact or shift the burden onto consumers.

These decision makers fail to realize the full harm an incident inflicts on organizational reputation, the consumer base, the national economy, and on numerous other scales and factors.

As a counter-balance to the economic disincentive to invest in layered security-by-design cybersecurity and cyber-hygiene solutions, government entities issue regulations and minimal cybersecurity requirements. Minimal security requirements, often known as compliance checks or check-box requirements, began as a means to compel organizations to act in favor of the public and the cybersecurity of the community, when deciding whether or not to invest in cybersecurity solutions. One of the most significant problems with this approach is that the requirements cannot be tailored to the needs of the organization or the data that it protects. Instead, cybersecurity controls that protect the confidentiality, availability, and integrity of data at rest, in transit, and in processing, must be simplified and limited to the lowest common denominator so that the majority of organizations in the target sector can conceivably meet the requirements. As a result, many organizations either struggle to meet portions of the compulsory requirements or fully adhere to the check-box list (and thus discharge most legal liability) and are still compromised by cyber-adversaries.

Minimal Compliance is as Ineffective as Security Theater

Small and medium businesses suffer most under compliance requirements because they often lack the resources to invest in the expensive enterprise solutions needed to secure larger entities. For instance, The Department of Health and Human Services estimates that adherence to the compliance requirements set by the HIPAA Security rule should annually cost an organization approximately $1,040; however, a Security Metrics study of HIPAA compliance costs, estimates annual costs of $4,000-$12,000 for small entities and more than $50,000 for medium and large entities [1]. Compliance rates for policies such as HIPAA are also low due to their complexity. For instance, the Security Rule consists of 75 requirements and 254 technical validation points. Organizations without information security teams lack the capability to comply with every requirement or validation point. According to HHS' estimated compliance budget, which allocates $113 to the Security Rule, this leaves roughly $4 per requirement [2]. Technical controls that address the requirements and validation points are typically far more expensive than $4. Further, terms change according to the categorization of the organization [1]. For example, if an organization sees itself as a healthcare data handler, but an auditor assesses the organization as a healthcare clearinghouse, then the organization must meet the latter set of requirements, even if those security controls do not accurately support their security posture. Consumers and small and medium businesses would be better protected if organizations made responsible investments in cybersecurity and cyber-hygiene solutions that fulfill the needs of their organization, protect their critical assets, and mitigate current threats from the hyper-evolving threat landscape.

Well-resourced collections of organizations forestall the establishment of regulation and mandatory requirements through coalitions and sectoral standards that often promote the business continuity over the cybersecurity of the sector. Some argue that the 2006 Payment Card Industry Data Security Standard (PCI DSS) was designed and implemented with the dual purpose of mitigating massive financial losses due to cyber-incidents and of avoiding

Congressional oversight or regulation of the sector [3]. While PCI is arguably effective at regulating the financial sector, it does not promote cybersecurity for the sake of the consumer and it, to a degree, enables organizations to suffer or handle cyber incidents without public transparency and accountability. The government and regulatory bodies could push for stricter controls that better protect the public; however, the efforts would be ineffective because they would not be tailored solutions; would be delayed by bureaucracy and opposition efforts; and would lack the innovation and momentum necessary to respond to emerging threats. Cooperative solutions between responsible organizations, informed public officials, and trusted vendors may be the best future strategy.

Minimal Compliance Requirements Breed Lethargy and Stagnation

Designing a “cookie-cutter” checklist of cybersecurity minimal requirements is alluring to key decision makers because it is a short-term solution (in terms of effectiveness) that can be used to argue that an organization did its “due diligence” or “as much as can be expected,” when in reality both the organization and the public would be better served by more complex, long-term meaningful investments in reliable cybersecurity and cyber-hygienic solutions. Minimal compliance solutions are thereby the newest form of Security Theater. Once compliance controls are set, regulators focus on measuring compliance, many organizations focus on dedicating the least resources possible to meet minimal compliance, the public is dissuaded from recognizing that consumers receive the least protection possible, and the cybersecurity of the sector, which remains anchored around the absolute minimum requirements, stagnates. Meanwhile, adversaries continue to evolve, develop more powerful tools, and increase in sophistication and ease of access. Overall, the threat landscape becomes more asymmetrical as antiquated defense solutions, affixed around minimalistic requirements and Security Theater, become wholly insufficient to emerging attack vectors, novel exploits, and more overwhelming adversaries.

Conclusion

Compliance is not security; rather, compliance is a snapshot of how a security program meets a specific set of security requirements at a given moment in time with respect to the current threat landscape [4]. Standards and regulations are important first steps towards developing a layered cybersecurity defense; however, organizations will not remain secure if the security strategy does not exceed the minimal requirements to the greatest extent of the organization’s capabilities. Comprehensive cybersecurity and cyber-hygiene can only be achieved when organizations transition from cybersecurity compliance to cybersecurity competency. So long as the United States Cybersecurity culture remains rooted in Security Theater and its derivative, minimal compulsory requirements, incident response cannot surpass or preempt adversarial tactics. Systems and networks will forever lack the resiliency to self-mitigate attacks. As a result, organizations will be forced to be repeatedly victimized and perpetually under siege. Instead, organizations should conduct comprehensive risk assessments of their systems and recognize that long-term investment in cybersecurity solutions that reduce the threat landscape and better protect employees, data and consumers, are more cost-effective and worthwhile than pretending at Security Theater.

<u>Sources</u>

[1] SBN Staff, "Know your rights and obligations under the HIPAA privacy rule - smart business magazine," in *Smart Business Magazine*, Smart Business Magazine, 2016. [Online]. Available: http://www.sbnonline.com/article/hipaa-privacy-rule/. Accessed: Dec. 3, 2016.

[2] T. Ferran, "How much does HIPAA compliance cost?," in *Security Metrics Blog*, 2015. [Online]. Available: http://blog.securitymetrics.com/2015/04/how-much-does-hipaa-cost.html. Accessed: Dec. 3, 2016.

[3] D. Rice, *Geekonomics: The real cost of insecure software*, Second ed. United States: Addison-Wesley Educational Publishers, 2007.

[4] K. Hagerman, "Security vs. Compliance: Navigating Three Common Misconceptions," in *Armor*, Armor Resources, 2016. [Online]. Available: https://www.armor.com/resources/security-vs-compliance/#. Accessed: Dec. 3, 2016.