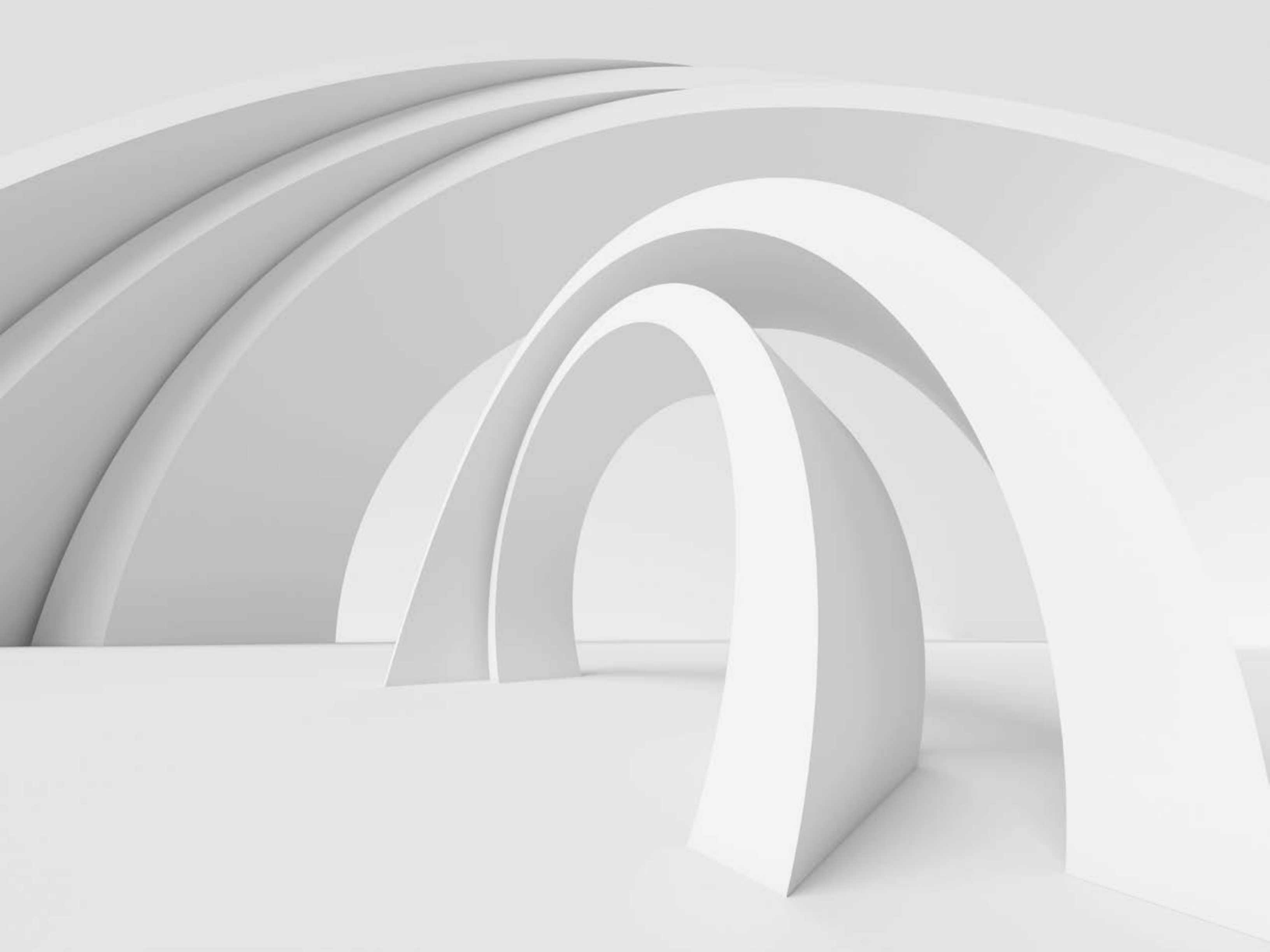
MANAGED TECHNOLOGY SERVICES

an HBR Consulting solution



How to Manage Evolving Data Security Threats

3 Keys to Continuous Realignment of Internal Controls

© 2017 Managed Technology Services LLC. All rights reserved.

There are hundreds of evolving data security threats in the battle against financial fraud schemes. The latest major breach was revealed when Equifax announced a cybersecurity incident potentially impacting 143 million American consumers. Adjusting for the number of minors in the U.S., this incident puts up to 56 percent of American adults at risk.[1] Unfortunately, incidents like these make it clear that it is impossible to stay ahead of all data security threats that are lurking online and to defeat all attempted cybersecurity attacks. “There is no such thing as ‘being secure’,” said Steven Maske, an information security expert. “There's just operating at an acceptable level of risk.”[2]

> **“There is no such thing as ‘being secure.’ There’s just operating at an acceptable level of risk.”**

Evolving Threats

According to the 2017 Thales Data Threat Report, issued in conjunction with analyst firm 451 Research, 68 percent of senior IT security executives at large enterprises around the world reported they have experienced a breach, with 26 percent experiencing a breach in the last year – both numbers that rose from the 2016 report.[3] Overall IT security spending was also higher, with 73 percent of organizations increasing IT security spending for 2017, up sharply from 58 percent in 2016.

Given the high-profile nature of data breaches and the massive amounts of resources that have been devoted to the battle in recent years, it is reasonable to wonder why vulnerability appears to be higher than ever. Indeed, data security is a priority virtually everywhere, regardless of industry or global location. Too often, though, organizations treat this as a “set it and forget it” operation: they obtain the right data security certifications, check the right boxes when it comes to IT controls, and then move on to the next item on their project list. Unfortunately, this is not an effective tactic, as threats change and evolve to adapt to the latest data security policies, procedures and defensive technologies. For example, despite the growing popularity of cloud computing is for its cost-efficiency and 24/7 secure data access, “new threats are evolving alongside the cloud”, according to John Howie, former COO of the Cloud Security Alliance.[4]

Going Beyond Compliance

"People are used to having a technology solution, [but] social engineering bypasses all technologies, including firewalls,” said Kevin Mitnick, the former cybercriminal who is now a successful information security consultant.[5] “Technology is critical, but we have to look at people and processes. Social engineering is a form of hacking that uses influence tactics.“ The earliest triggers for data security protocols were oriented around fighting off website hacks. IT teams drew up multi-layered network architecture and put in place all sorts of early warning systems that would alert them of an attack. As is always the case, their efforts were overrun by a complex web of government regulations that included ambiguous regulatory mandates (such as HIPPA’s requirement to “protect against all reasonably anticipated threats”[6]) and organizations worked hard to sort out the pieces.

But as Computerworld put it, “Compliance does not equal security.”[7] Many CSOs and CIOs have learned the hard way that technical compliance with regulatory standards may protect an organization from audits and fines, but it is no assurance that an organization is safe from an attack that can cause business disruption, reputational damage and big-ticket litigation. This is because compliance is not enough; rather, compliance should be viewed as the “table stakes” in data security, a baseline that establishes the minimum standard and a starting point for an overall data security program. To deal with evolving threats, organizations need an approach that goes beyond compliance and instead places a focus on continuous realignment of internal security controls that adapt to new risks.

3 Keys to Continuous Realignment of Internal Controls

The very nature of this challenge – to deploy a security posture that is in the mode of constant reassessment – is such that there is no magic list of best practices to follow. Data security threats evolve in real-time, so an organization’s security protocols must be flexible enough to adapt to the shifting landscape.

Based on our experience of providing data security support to law firms and corporate legal departments, here are three suggestions to consider.

Continuous monitoring. It is important to ask every week, “What’s new on the radar? Where are we vulnerable this week to the latest threats and scams that we know about in our industry? Are there changes internally that have taken place recently that have reduced our security posture? Do these threats and changes need to be remediated to help stay within our risk tolerance?”

Leverage your vendors’ continuous monitoring capabilities and work with external security firms to stay on top of recent threats and challenges. The goal is to make minor adjustments along the way and stay ahead of the curve. Although it may create more work up-front, these minor adjustments ultimately help organizations avoid major disruptions in the long run. Do not let changes or threats to infrastructure or systems get to the point where a major and potentially disruptive change is necessary to get back into compliance.

Assess exposures to third-party vendors. It is not enough to tighten your own ship. Organizations must look outside and consider possible vulnerabilities among its third-party vendors and service providers.

There has always been speculation regarding criminals potentially targeting law firms to access data that their clients entrust to them, but over the years, hacking a third party has proven to be easier than the target itself.[8] Over half of massive data breaches in recent years can be traced to vulnerabilities with third-party vendors. Security is no longer just an inside problem; it is a tangled web of third, fourth and fifth parties along with an organization’s own clients.

Regularly scheduled data security assessment. In addition to a weekly self-evaluation for gaps in the organization’s data security armor, it is also important to pause periodically and conduct an enterprise-wide assessment of all systems, policies and procedures. The results of this assessment should yield important insights regarding changes that should be made to internal controls, modifications to policies, and alignment of risk within the organization. Sometimes, these assessments are regulation-driven to help performance, but it can also be worthwhile to take an outside look in to help focus on strategy and enable the organization. Using third parties to conduct gap assessments and technical testing helps identify and remediate blind spots. Organizations should also use this time to align on where the business is going and how it can be taking “smarter” risks with technology.

Looking Forward

Compliance with data security standards is never a “steady state” function of any organization, where covering every item on the checklist means that the company is in the clear. In fact, doing so tends to create a culture that is focused in the wrong direction. Checkbox compliance creates complacency and is the proverbial “cart driving the horse,” which is a dangerous road to travel. Threats to the enterprise from cybercriminals are in constant evolution, so a well-defended organization must be adapting its security protocols to keep pace with these changing threats. Stay focused on the challenge at hand by looking at security and risk alignment first, and then validate using compliance checklists. As all security practitioners know, compliance does not equal security, but when you do good security, compliance is easily achieved.

Connect With An Expert

Jeff Norris, Senior Director of Information Security
937.247.1506 | Jeffrey.Norris@hbrmts.com

© 2017 Managed Technology Services LLC. All rights reserved.

Sources

[1] "More than credit scores: Why Equifax for Business matters," Forrester Research. September 8, 2017. http://www.zdnet.com/article/equifax-does-more-than-credit-scores/

[2] Maske, Steven. August 31, 2017. https://twitter.com/ITSecurity/status/903256164594573317

[3] "2017 Thales Data Threat Report: Security Spending Decisions Leave Sensitive Data Vulnerable," https://dtr.thalesesecurity.com

[4] "Expert: Threats To Secure Cloud Operations Are Evolving," Babcock, Charles. January 30, 2017. https://www.informationweek.com/cloud/infrastructure-as-a-service/expert-threats-to-secure-cloud-operations-are-evolving/d/d-id/1327998

[5] "World-famous hacker Kevin Mitnick and KnowBe4 fight phishing with training," Kassner, Michael. June 22, 2015. http://www.techrepublic.com/article/world-famous-hacker-kevin-mitnick-and-knowbe4-fight-phishing-with-training/

[6] "6 Basics of Risk Analysis and Risk Management," Centers for Medicare & Medicaid Services, HIPPA Security Series, Volume 2, Paper 6. March 2007. https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/riskassessment.pdf

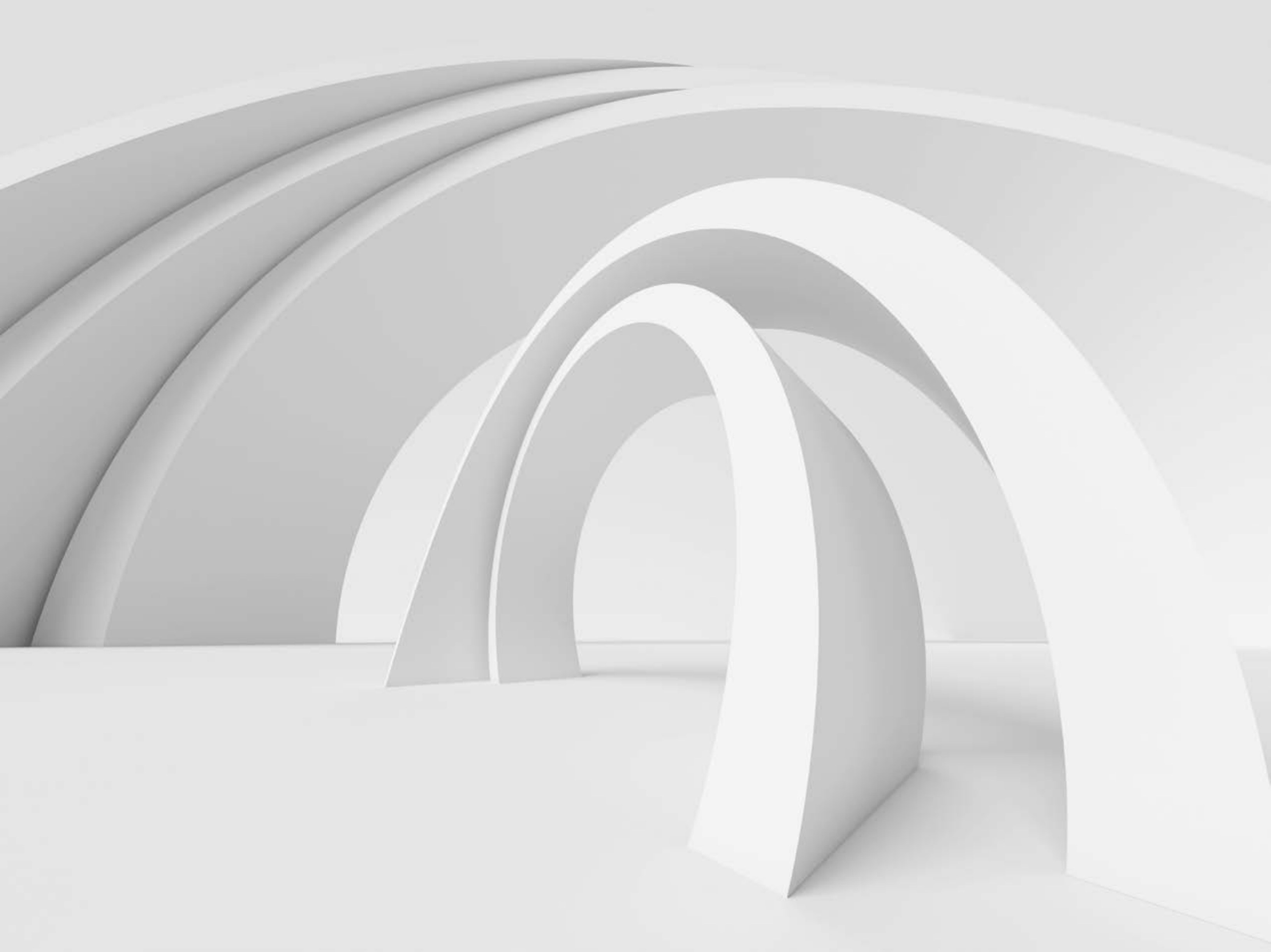
[7] "Compliance does not equal security," Thurman, Mathias. January 12, 2016. https://www.computerworld.com/article/3021787/security/compliance-does-not-equal-security.html

[8] "Law Firm Website Breaches: What to Do Next?," Managed Technology Services LLC. http://www.hbrlegalmts.com/insights/law-firm-website-breaches-what-to-do-next/

© 2017 Managed Technology Services LLC. All rights reserved.

MANAGED TECHNOLOGY SERVICES

an HBR Consulting solution



Managed Technology Services LLC (MTS) is a trusted data-hosting service provider to the legal industry. A leader in infrastructure and cloud hosting services, we maintain data and applications with the highest level of security standards. For over a decade, our team of MTS experts have collaborated with clients – including 25 percent of the Am Law 100 – to manage infrastructure, systems performance, cost and risk.

© 2017 Managed Technology Services LLC. All rights reserved.