CORPORATE COUNSEL
An ALM Website
corpcounsel.com

Cybersecurity Madness: 3 Things that Really Matter and 3 That Don't

From the Experts

Diane D. Reynolds and Leonardo M. Tamburello

The volume and increased sophistication of threats to the security of corporate data and systems, combined with a tidal wave of well-intentioned experts—ranging from large management consulting firms to reformed hackers carrying a business card—have created a perfect storm of cybersecurity confusion and misinformation for companies of all sizes.

Corporate legal professionals seeking a rational and cost-effective means of managing risks related to data privacy and online security are required to decipher cybersecurity jargon and marketing hype, to make or influence high-stakes decisions based on that information, and to explain and defend those decisions in the corner office as well as the boardroom.

To address the current cybersecurity madness, and reflecting on our experience over the past decade, we offer the following road map for corporate legal counsel to help sort out what's important and what's not. Let's start with the important stuff.

What Really Matters

1. Elevate the Privacy/ Cybersecurity Function

Corporate boards should invest the necessary resources and assume oversight of senior management to ensure that appropriate steps are in place to address privacy and cybersecurity risks. The most effective way to accomplish this goal is the creation of a dedicated, board-level cybersecurity risk management committee.

To address the increased rate of data breaches at U.S. public companies, last December the Cybersecurity Disclosure Act of 2015 was introduced in the U.S. Senate. According to the press release, the bill seeks to "strengthen and prioritize cybersecurity at publicly traded companies by encouraging the disclosure of cybersecurity expertise, or lack thereof, on corporate boards at these companies."

If this legislation is enacted, public companies will be required to disclose whether they have a director who is a "cybersecurity expert," or alternatively, to explain what steps the company has taken to exempt them from having a cybersecurity expert on the board. The bill would also require the SEC and the National Institute of Standards and Technology (NIST) to provide companies with guidance on the qualifications necessary to be considered a cybersecurity expert.

Regardless of whether this well-intentioned legislation ever becomes law, delegating responsibility for cybersecurity risk to an individual board member is ill-advised for several reasons. Notably, cybersecurity is not a singular discipline. It encompasses many areas of expertise, drawing on specialized knowledge from technical, legal, operational, risk management, forensic and insurance professionals. Proper management of a company's cybersecurity risk demands a board-level committee whose members represent all of those skill sets.

A cybersecurity risk committee functions like other board committees, such as accounting or governance, and its mandate is twofold: first, to review and approve plans and to implement steps that address the company's specific risks and culture. Second, to ensure that those initiatives are benchmarked to industry standards and best practices, such as those described in the NIST Cybersecurity Framework.

Boards are protected by the business judgment rule, but this rule also obligates boards to complete appropriate due diligence to understand the risks faced by the company.

2. Make Privacy Issues the Top Priority

According to the sheer volume of complaints that are filed, data privacy should far outweigh data security, in terms of corporate priorities. Although a significant portion of data privacy complaints are related to telemarketing and the Telephone Consumer Protection Act, a substantial number arise from allegations of "unfair or deceptive" trade practices under Section 5 of the Federal Trade Commission Act.

Deceptive trade practices typically arise out of claims based on discrepancies between what a company promises it will do to safeguard the privacy or confidentiality of the information it collects from consumers in its privacy notice, and what the company actually does under its internal, operational privacy policies. A company's external-facing privacy notice (or "privacy policy") must be consistent with the privacy policies and practices that the company and its vendors apply. For example, a recent FTC enforcement action concluded that it was a deceptive trade practice for a company to state in its privacy policy that its advertising software would only track consumers' locations if they "opted in," but the company actually tracked consumers' locations even when the consumer specifically denied permission for tracking.

Unfair trade practices usually arise out of operational tactics or processes that cause harm. Section 5(n) of the FTC Act provides that an act or practice may be deemed unfair if it "causes or is likely to cause substantial injury to consumers," which is neither reasonably avoidable by consumers nor outweighed by countervailing benefits to consumers or competition.

However, there are inconsistencies in how "unfair acts or practices" are defined. State-level interpretations can differ from the FTC in this regard, and companies can find themselves in state court defending against the views of judges or juries who do not possess the requisite technical expertise and employ no technical experts to advise them. To address this risk, companies should assign targeted groups with managerial responsibility (and on-going training) to proactively and periodically monitor their privacy notices, policies and procedures so that they are not only effective, but accurate and congruent as well.

Effective enterprisewide risk management of data privacy is an essential element in building a privacy-oriented culture. Achievement of that goal is always rooted

in ongoing employee education, training and monitoring.

3. Leverage Attorney-Client Privilege

In the rush to become "compliant," many companies fail to consider the post-breach realities of litigation and the discovery process. For that reason, a company's risk assessments, incident response tabletop training exercises, security investigations and all other internal examinations covering privacy and security benchmarking tests should be conducted under the supervision of counsel, so that the results are covered within the attorney-client privilege.

Moreover, all of the assessments and minutes of review meetings related to cybersecurity may be discoverable by a plaintiff's lawyer unless they are privileged. Having an outside law firm subcontract all other cybersecurity service providers is an effective defensive tactic that will help to ensure attorney-client privilege. It is also important to emphasize that if current outside legal counsel does not possess expertise in data privacy and cybersecurity, companies should also engage a firm that does, to ensure that these specific issues are managed effectively and that "compliance" oversight is conducted properly.

What Doesn't Matter

1. Reliance on Ad Hoc or Piecemeal Technology Solutions

There is growing recognition, based on failure rates, that antivirus software and other types of piecemeal cybersecurity solutions are not silver bullets, and that the modern threat environment requires integrated and automated capabilities, combined with companywide program adoption protocols.

Because networks have different profiles, priorities, capabilities and risk tolerances, "off the shelf" or "one-size-fits-all" solutions such as firewalls or antivirus and anti-malware applications may serve a role as components of an overall cyberdefense, but they are not effective as standalone solutions.

From a technical perspective, an integrated defense begins with perimeter/boundary protections such as deep packet inspection, malicious behavior prediction and web content filtering, along with email filtering and malicious link inspection. On the network level, behavior-based detections and malware neutralization/sandboxing along with additional malicious behavior prediction should be monitoring network activity for abnormal and suspicious activities. On the host level, behavior-based detections, malware containment, application whitelisting and continuous antivirus/anti-malware monitoring are required.

An integrated approach must also include corporate policies, procedures, training and updates that are understood by, and relevant to, every employee in the organization. Because so many cyberattacks within companies rely on tricking employees into giving up their credentials, or to activate a malicious link or payload, the importance of establishing this first line of defense cannot be overstated. Employee education, training, testing, feedback (both positive and negative) and retraining must be a permanent part of every company's culture.

2. Most Cybersecurity Insurance Policies

Many organizations purchase cyber insurance, but very often those policies either exclude or underinsure coverage of high probability events, so that the confidence the company exhibits is nothing more than a false sense of security.

As with any legal document, insurance policy details are important. Management should have a complete understanding of what is covered and excluded in a cyber policy before it is invoked. Although most cyber policies purport to cover direct loss, legal liability and consequential damages resulting from cybersecurity breaches, the scope of the risks that these policies actually cover is often narrowly defined.

In the rapidly evolving world of global cyberthreats, cyber policy language can quickly become outdated and irrelevant. These "stale" policies create unanticipated risks and vulnerabilities for an organization. Increasingly, courts have upheld denials of

coverage decisions by insurance companies when those claims are passed through third parties with which the insured has a separate contract involving assumption of liabilities.

For that reason, careful and ongoing attention must be paid to policy exclusions, which often include employee-generated losses. For example, this might involve a malware attack launched by a phishing email opened by an employee. It could exclude damages incurred as a result of an employee intentionally disclosing private information regarding a celebrity who is a customer or patient. Or it might exclude coverage if an employee sells information for their own benefit, or as part of an identity theft ring or other fraudulent enterprise.

Cyber policy exclusions can leave your organization extremely vulnerable, and even economically incapable of resolving post-breach litigation and damages with the affected parties.

3. 'CYA' Systems, Policies and Procedures

Cybersecurity-related risks are real and increasing, and enterprise systems, policies and procedures must be much more than "Wizard of Oz" window dressing to appease the board, or be left entirely in the hands of a company's IT department.

To provide the necessary level of rigor, a company's threat monitoring, detection, containment and eradication processes should be occurring at every level of infrastructure in an integrated and automated manner. Event classification and log filtering should be used to produce customized alerts for network administrators. This is a crucial step in preventing "alert fatigue" where low-level but persistent alarms desensitize an organization, causing actual threats to be disregarded or response time to be compromised.

In addition to being able to defend themselves, local networks should participate in regional or industry-level collaboration that provides over-the-horizon visibility and defense strategies. As the rapid spread of ransomware has demonstrated over the past year, once malicious actors discover a lucrative new attack tool, the practice spreads and is refined in various ways. For that reason, comprehensive protection also includes a global, cross-enterprise, cyber response capability to monitor large-scale threats and vulnerabilities.

The Bottom Line

Sorting through the current volume of cybersecurity noise can be a challenge, and it's a task that should not be managed in siloed fashion. Toward that end, the corporate legal, securityrisk management and IT functions must be aligned, sharing information and insights and working in partnership to address cyberthreats. IT and risk management/security groups should understand legal ramifications of network intrusions and data breaches. Additionally, legal professionals should collaborate with IT and security/risk management on issues such as regulatory requirements for preparedness and incident response, particularly in determining whether breach notification requirements apply to a particular incident.

In fact, the most significant cybersecurity threat is not external; instead, it is what happens, or fails to happen, inside the organization in advance of a breach.

Diane D. Reynolds *and* ***Leonardo M. Tamburello*** *head up the cybersecurity, data protection and privacy practice group at New Jersey-based McElroy, Deutsch, Mulvaney & Carpenter. They both hold advanced certifications as privacy professionals.*

Reprinted with permission from the November 14, 2016 edition of CORPORATE COUNSEL © 2016 ALM Media Properties, LLC. This article appears online only. All rights reserved. Further duplication without permission is prohibited. For information, contact 877-257-3382 or reprints@alm.com. # 016-11-16-04