Six Common Misconceptions About Cybersecurity

Interest in cybersecurity is escalating across the legal profession, reflecting the complex and potentially catastrophic threats that clients, particularly financial services firms, now face. Because these risks are deep and potentially disastrous, lawyers are increasingly tasked with counseling clients about how to contain them.

By Jed Davis | March 03, 2018

Interest in cybersecurity is escalating across the legal profession, reflecting the complex and potentially catastrophic threats that clients, particularly financial services firms, now face. The combined power, speed and baked-in vulnerabilities of information technology (IT) have given rise to previously unimaginable but now-endemic risks to organizations. Malicious actors can and do steal, lock or destroy confidential data, in bulk or in smaller but still-devastating caches, and then exploit the information's resale, extortion or spite value. Moreover, even accidental errors can cause confidential information to leak, with similarly costly regulatory, litigation and business fallout.

Because these risks are deep and potentially disastrous, lawyers are increasingly tasked with counseling clients about how to contain them. Frequently this requires dispelling clients' misconceptions about those risks and effective countermeasures. Below we explore each of six such misconceptions that often beset organizations. Avoiding these errors is essential to fulfilling the core functions of a cybersecurity program: (1) identifying cyber-risks, (2) protecting critical infrastructure using appropriate safeguards; (3) detecting incidents; and (4) responding and (5) recovering from them. National Institute of Standards, Framework for Improving Critical Infrastructure Cybersecurity (v. 1.0) (2014) at 7-8 (NIST Framework).

1. "We don't face the same risks as [Name of Fortune 500 Victim of Massive Credit Card Hack]."

Got data? Then you have cyber risk. Yet, many organizations remain in denial about cyber exposure. For example, a broker-dealer that serves only institutional clients may incorrectly infer from its minimal holding of personally identifiable information (PII) that it has little to worry about. That business may not require the fortress-like protections eventually adopted by large, well-known victims of identity theft (e.g., card processors or big box stores). Even a small leak of SSNs or other PII, however, can trigger breach notification and/or remedial obligations under one or more state laws. Moreover, organizations of any size are vulnerable to an expanding array of cybercrimes, any of which can interrupt or destroy a business, including ransomware attacks, impersonation schemes to effect wire transfer frauds, and theft of inside information. Leadership needs to appreciate the severity of this new and dangerous reality. Unless and until it does, an organization is ill-prepared to develop and fulfill the core functions set forth in the NIST Framework.

2. "We can't afford new technology."

Leadership may also recognize that an organization is at substantial risk, but mistakenly assume that lack of budget to replace existing IT means that safety cannot be improved. This assumption perpetuates a fallacy that has fostered the prevailing unsafe state of things. Over the last four decades, layers of IT were designed and rapidly rolled out to favor connection, volume and speed. From a security perspective, this makes IT fundamentally flawed. It also means that new IT is unlikely to fix the underlying flaws because that new technology is retrofitted onto the existing, perilous structure. In these circumstances, there are lower-cost people and process improvements, which management should emphasize. For example:

- Analyze sensitive data holdings—and cut access to them;
- Budget for security improvements, based on periodic penetration testing (a limited application of tech that is now affordable to most organizations);
- Mandate yearly security awareness training of all managers and staff.

3. **"Our IT director handles our cybersecurity."**

Over the last 40 years, it has also become commonplace to cabin IT management in a separate department or to outsource it to a vendor. As cyberattacks and accidents have surged, these arrangements put companies at increased peril. Cybersecurity is a multidisciplinary responsibility. As a threshold matter, technical expertise in IT and cybersecurity are not the same. IT personnel know which protocols and configurations are within expected parameters. By contrast, experts in cybersecurity know how to spot hidden intrusions and other abuse. Controlling cyber-risk can also require other expert assistance, including privileged advice from counsel, and (as most breaches occur due to human error) advice on corporate controls. Effective cybersecurity depends as well on an internal incident response team that complements IT professionals with a cross-section of troubleshooters from across the organization. That cross-section should include compliance, risk management and also have input from ordinary employees who understand (sometimes better than anyone else) the particular risky ways that users perform that organization's work. With insights honed in realistic drills, that multidisciplinary team can develop the shared knowledge and collaborative process with which to navigate:

- The spectrum of regulatory and litigation concerns that arise in an actual or suspected breach,
- The identification and retention of outside counsel and other experts,

- Cyberliability insurance, including negotiation of coverage and issuing timely claims notice,
- Internal crisis communications, including briefing board and senior management and obtaining their approval, and
- External communications, including addressing public or stakeholder concerns before and once a breach determination is made.

4. **"We already have a detailed manual."**

In response to frequent headlines about data breaches, some financial service companies and other similarly-situated businesses transpose earlier solutions to longstanding compliance regulations (e.g., the FCPA, AML laws, SEC and FINRA rules): they adopt cybersecurity manuals. While something is usually better than nothing, manuals can foster a false sense of security if they come directly and untailored from stock templates, whether supplied by counsel a company's outside IT provider or worse still, pulled straight off the Internet. Unless the organization thereafter applies findings about its specific risks to customize the manual, it is ill-suited to contain those risks. Moreover, in the midst of a suspected and actual breach, any manual (even a truly risk-based one) is, for reasons discussed above, cold comfort, unless complemented with rigorous drills to test and refine the company's incident response plan.

5. "We'll need to change our approach if the SEC tightens cybersecurity rules."

Such a change is already an imperative. The SEC has for several years been tightening requirements and appears likely to tighten up still more. Most recently, on March 21, 2018, the SEC issued its (unanimous) "Commission Statement and Guidance On Public Company Cybersecurity Disclosures." Though cast as "reinforcing and expanding" a

2011 staff advisory, the new Guidance marks a new and demanding era, aimed at avoiding a recurrence of recent debacles at Yahoo, Equifax and elsewhere. Henceforth, public companies will need to file much more detailed public disclosures before, during and after actual and suspected security breaches and concomitantly, to devote more resources to efforts to such risks from ever unfolding. For example, the new Guidance emphasizes that companies must in periodic filings "provide timely and ongoing information" about "material cybersecurity risks and incidents," may need revise prior disclosures in light of new findings and need continually to evaluate whether their controls suffice timely to warn leadership. Moreover, even before the Commission's recent raising of standards for public companies, the SEC staff increased its oversight of registered broker/dealers and investment advisers (BDs & IAs). Increasingly since 2014, the staff has leveraged the business continuity provisions of Regulation S-P (adopted 2004), the 'red-flag" identity theft requirements of Regulation S-ID (adopted 2013) and the agency's plenary examination powers to import the criteria of the NIST Framework as prod cybersecurity upgrades at BDs & IAs. As stated and applied by the Office of Compliance Inspections and Examinations (OCIE) in Risk Alerts, "sweep" testing and in document requests and deficiency letters, the criteria used by the staff are often lifted verbatim from that Framework. As such, the SEC now contemplates that regulated entities will engage in periodic and detailed risk assessments, document existing controls and incidents, and prepare written plans for improvement. For larger BDs & IAs, these requirements are already standard and therefore no surprise. For small and mid-sized firms, however, the increased requirements are sometimes a slow-moving shock, revealed when OCIE makes its next examination visit.

6. "We're not regulated by NYDFS, so its cyber regulations don't matter."

Last year, the New York State Department of Financial Services (NYDFS) promulgated the most sweeping cybersecurity regulations ever issued in the United States. Over a two-year phase-in ending March 2019, entities licensed by NYDFS are required to conduct an intensive risk assessment, implement a cybersecurity program and policies and specified mandatory security approaches, such as vulnerability and penetration testing and encryption. Moreover, NYDFS set an unprecedented 72-hour deadline for notifying the agency of cybersecurity events (currently, no other state specifies fewer than 30 days' notice). While it is possible that other jurisdictions will refrain from reaching as far as New York has, future restraint should not be assumed. Dismay over the Equifax data breach recently prompted NYDFS to propose to expand its cybersecurity regulations to govern the major credit bureaus. The public's continuing deep concern over data breaches nationally could well result in other states mandating compliance with the NIST Framework, if not necessarily in as much granular detail as NYDFS has in New York.

Jed Davis is a partner in the New York Office of Day Pitney and the co-head of its cybersecurity practice. He is a formerly federal cybercrimes prosecutor and also previously worked as a managing director at a global investigations firm.