INSIDE THE MINDS

Understanding Developments in Cyberspace Law

Leading Lawyers on Analyzing Recent Trends, Case Laws, and Legal Strategies Affecting the Internet Landscape

2015 EDITION

ASPATORE

Material in this book is for educational purposes only. This book is sold with the understanding that neither any of the authors nor the publisher is engaged in rendering legal, accounting, investment, or any other professional service. Neither the publisher nor the authors assume any liability for any errors or omissions or for how this book or its contents are used or interpreted or for any consequences resulting directly or indirectly from the use of this book. For legal advice or any other, please consult your personal lawyer or the appropriate professional.

The views expressed by the individuals in this book (or the individuals on the cover) do not necessarily reflect the views shared by the companies they are employed by (or the companies mentioned in this book). The employment status and affiliations of authors with the companies referenced are subject to change.

For customer service inquiries, please e-mail West.customer.service@thomson.com.

If you are interested in purchasing the book this chapter was originally included in, please visit www.legalsolutions.thomsonreuters.com

The Cybersecurity Playbook: Building Effective Attack and Breach Preparedness[1]

Mark Mermelstein
Partner

Antony Kim
Partner

Aravind Swaminathan
Partner
Orrick, Herrington & Sutcliffe LLP

ASPATORE

[1] Mark Mermelstein, Antony Kim, and Aravind Swaminathan, resident in Los Angeles, Washington, D.C., and Seattle respectively, are partners at Orrick, Herrington & Sutcliffe LLP and co-chair its Cybersecurity and Data Privacy Group. The authors would like to thank Mary Kelly Persyn for her invaluable assistance and research.

"Data security issues are no longer just an IT Department concern. Indeed, they have become a matter of corporate survival…"[2]

Introduction

With the most significant of cyberattacks resulting in millions of dollars in harm, irreparable damage to a company's brand, and key executives getting fired, organizations must begin to prepare for what most experts think is the inevitable breach. And yet, when it comes to cybersecurity, many still think of it like physical security: a matter for professionals to handle by fencing in a campus perimeter, putting the most important entry points under lock and key, and assigning someone to monitor the video surveillance.

But cybersecurity does not work like physical security. You might be able to station someone at every door and hallway in a building and manage the traffic of all persons and materials, like the arena security guards at a professional basketball game. Unlike a sports arena, however, *every single one of us* and *every single one of our devices* (desktops, laptops, phones, and tablets) is a viable entry point for even a novice attacker. The arena security team can deploy more guards and pay closer attention, immediately reaping the benefits of enhanced protection. In the cyber space, companies certainly now spend more on "guards,"[3] churning out more detailed incident

[2] Paul Ferillo, *Cyber Security, Cyber Governance, and Cyber Insurance*, HARVARD LAW SCHOOL FORUM ON CORPORATE GOVERNANCE AND FINANCIAL REGULATION (Nov. 13, 2014), http://corpgov.law.harvard.edu/2014/11/13/cyber-security-cyber-governance-and-cyber-insurance/.

[3] According to *Venture Beat*, the global security market was worth about $87 billion in 2014, likely increasing to around $120 billion by 2017. Bob Ackerman, *Three white-hot areas for cybersecurity investors in 2015*, VENTURE BEAT (Dec. 22, 2014), http://venturebeat.com/2014/12/22/three-white-hot-areas-for-cybersecurity-investors-in-2015/.

Venture investment in cybersecurity startups is concomitantly high; *MIT Technology Review* reports that 2014 set a record at $2.3 billion. Mike Orcutt, *Why Venture Capitalists Love Security Firms Right Now*, MIT TECH. REV. (March 17, 2015), *at* http://www.technologyreview.com/news/535851/why-venture-capitalists-love-security-firms-right-now/. Liana B. Baker, Olivia Oran, and Jim Finkle, *Exclusive: Cyber IPO pipeline grows as data breaches boost security spending*, Reuters (March 20, 2015), *at* http://www.reuters.com/article/2015/03/20/us-cybersecurity-ipo-exclusiveidUSKBN0MG2ET20150320 As breach frequency continues to escalate, more cybersecurity companies are going IPO, according to Reuters, including Rapid7, LogRhythm and MimeCast. Liana B. Baker, Olivia Oran, and Jim Finkle, *Exclusive: Cyber IPO pipeline grows as data breaches boost security spending*, REUTERS (March 20, 2015), http://www.reuters.com/article/2015/03/20/us-cybersecurity-response plans, and paying more attention to the rank-and-file and the board. The result as of 2015: somewhere in the vicinity of a 66 percent annual *growth* rate in cyberattacks by some accounts[4] and, over the past eighteen months, the largest reported breaches in history,[5] novel plaintiffs and plaintiff theories,[6] unprecedented actions by regulators,[7] and an apparently successful phishing attack on the White House.[8] The average cost of dealing with breaches has hit an all-time high, with the number of

ipo-exclusive-idUSKBN0MG2ET20150320. Network security provider FireEye, which went IPO at $304 million in 2013, now has a market cap of about $4.6 billion. PwC, *Managing cyber risks in an interconnected world: Key Findings from The Global State of Information Security Survey 2015 (September 30, 2014), at* http://www.dol.gov/ebsa/pdf/erisa/Advisory council2015security3.pdf ("PwC Report").

[4] PwC Report at 7.

[5] Last year saw "huge" breaches strike Home Depot (cyberthieves stole as many as 60 million credit card numbers); Target (breached during the holiday season, the retailer continued to feel repercussions into 2014, ultimately ballparking costs at $148 million); Apple (several celebrity users suffered a hack of their personal and intimate photos); Neiman Marcus (a February breach resulted in the loss of about 350,000 card numbers); and Anthem and Premera (as many as 1 in 3 Americans were affected by these two breaches). Benjamin Snyder, *5 huge cybersecurity breaches at companies you know*, FORTUNE (October 3, 2014), *at* http://fortune.com/2014/10/03/5-huge-cybersecurity-breaches-at-big-companies/; Jeremy Kirk, *Anthem now says 78.8M were affected by breach*, COMPUTERWORLD (February 24, 2015), at http://www.computerworld.com/article/2888267/anthems-now-says-788m-were-affected-by-breach.html; Brian Krebs, *Premera Blue Cross Breach Exposes Financial, Medical Records*, KREBS ON SECURITY (March 17, 2015), *at* http://krebsonsecurity.com/2015/03/premera-blue-cross-breach-exposes-financial-medical-records/.

[6] In a novel development, a federal judge has ruled that both banks and consumers can sue Target for losses suffered due to the breach. The consumer suit has since settled for $10 million. Megan Geuss, *Judge rules that banks can sue Target for 2013 credit card hack*, ARSTECHNICA (December 4, 2014), *at* http://arstechnica.com/tech-policy/2014/12/04/judge-rules-that-banks-can-sue-target-for-2013-credit-card-hack/; Peter Cooney and Supriya Kurane, *Target agrees to pay $10 million to settle lawsuit from data breach,* REUTERS (March 19, 2015) *at* http://www.reuters.com/article/2015/03/19/us-target-settlement-idUSKBN0MF04K20150319.

[7] The FCC has become more aggressive in its data breach enforcement stance, fining two telecommunications companies, Terracom, Inc. and YourTel America, Inc. $10 million, and more recently levying an astounding $25 million fine against See FCC 14-173, *Notice of Apparent Liability for Forfeiture [In the Matter of TerraCom, Inc. and YourTel America, Inc.]* (October 24, 2014), *at* https://apps.fcc.gov/edocs_public/attachmatch/FCC-14-173A1.pdf; See FCC DA 15-399, *Order* (April 8, 2015), *at* https://apps.fcc.gov/edocs_public/attachmatch/DA-15-399A1.pdf FCC, *AT&T to pay $25 million to settle consumer privacy investigation* (April 8, 2015), at https://www.fcc.gov/document/att-pay-25m-settle-investigation-three-data-breaches-0.

[8] Armin Rosen, *REPORT: Russia hacked the White House*, BUS. INSIDER (April 7, 2015), *at* http://www.businessinsider.com/report-russia-hacked-the-white-house-2015-4.

companies reporting losses over $20 million growing by 92 percent.[9] And all agree that cyberattacks will only accelerate in the years to come—not only in frequency, but in volume and sophistication.

But even in the face of escalating threats and their attendant costs—both financial and reputational[10]—global corporate spend on cybersecurity, by some reports, actually *decreased* 4 percent in 2014.[11] And many corporate structures still "bury" cybersecurity issues—and budget—in IT departments, delegating management of chief information security officers to IT rather than requiring CISOs to report directly to top management.[12] The reality is that effective threat mitigation and incident response long ago outgrew the four walls of "IT," and now demand the full vigilance of every company employee from the C-suite down. Companies simply must do better.

The saying, "an ounce of prevention is worth a pound of cure" may be a cliché, but when it comes to developing a robust cybersecurity program, it has never been truer. In this chapter we offer some key elements of cyber preparedness that fit the current threat landscape and, frankly, reflect the *minimum* that companies should implement.

The Tri-Part Approach To Cybersecurity Preparedness

Dealing with today's cyberattacks is not a simple process of building a better wall or even the moat around your wall. The reality is that no cybersecurity defense program is bulletproof. The technology simply has not evolved to address all possible threats. Moreover, the human element in enabling cyberattacks and enterprise damage is omnipresent. As a result, cybersecurity preparedness must evolve into an exercise in risk mitigation, management, and displacement—not perfection.

[9] PwC Report at 10.

[10] *See* Ferillo, *Cyber Security, supra* at n. 2; *see also* Elise Vlebeck, *Companies see personal data breach as biggest threat,* THE HILL (April 10, 2015), at http://thehill.com/policy/cybersecurity/238463-companies-see-personal-data-breach-as-biggest-threat; Tim Luckett, *Data & Reputational Risk,* Hill + Knowlton (December 9, 2014), at http://www.hkstrategies.com/blogs/crisis/data-reputational-risk (Global security advisor Hill + Knowlton recently opined that "[n]o matter which sector or which part of the world we are in—this is now where reputations are won or lost.").

[11] PwC Report at 19.

[12] PwC Report at 19.

The proactive (pre-breach) playbook must focus on the twin goals of minimizing the likelihood of a successful attack and mitigating the effects of a breach. The two are different. Minimizing the likelihood of a breach is a multi-step process that requires an organization to develop awareness of its assets and their relative values to each other, develop threat and attacker profiles relevant to the organization's specific business and operations, conduct security assessments indexed to the threat landscape and the assets to be protected, formulate and deploy remediation measures based on the conducted assessments (e.g., employee training, procurement of new technical defense measures, and destruction of data that serves no ongoing business purpose), and establishment of audit (and improvement) processes to ensure the ongoing effectiveness of cybersecurity policies and procedures.

Mitigation of the potential negative fallout post-breach is predicated on preparation, and thus, includes detailed preparation of a comprehensive, enterprise-wide security incident response plan, testing of that plan, and regular updates and fine-tuning based on new intelligence developed through experience and practice.

Proactive preparedness must be indexed to the most significant harms that befall organizations after a breach: harm and disruption to brand and litigation. Accordingly, organizations should orient their efforts around a narrative that demonstrates that the organization acted reasonably and diligently to protect valuable assets and customers.

Even though it is impossible to prevent every breach, organizations can take a wide variety of measures to safeguard data and network assets, especially where the causes involve human errors like phishing, weak passwords, and laptop/device loss. The key is to build a collaborative team approach that is predicated on a risk management model.

These principles remain just as true in cyberwarfare as they did in conventional warfare over two millennia ago:

> So it is said that if you know your enemies and know yourself, you can win a hundred battles without a single

> loss. If you only know yourself, but not your opponent, you may win or may lose. If you know neither yourself nor your enemy, you will always endanger yourself.[13]

Accordingly, the first two elements of cybersecurity preparedness strategy begin with these basic principles, and incorporate three additional elements:

1. Cyber threat and risk awareness;
2. Internal awareness of data/network assets and vulnerabilities via cybersecurity assessments, coupled with remediation efforts; and
3. Development and testing of an incident response plan.

And, just as there are several elements to comprehensive preparedness efforts, there are similarly multiple stakeholders and participants that must be included to develop an enterprise-wide approach.

Cyber Threat and Risk Awareness

Threat Actors and Threat Vectors

In the context of cybersecurity, organizations must first develop situational awareness of the cyber threat landscape and the risks that attackers pose to their networks and assets. How can you protect your enterprise and prepare to defend it against an attack when you have no particularized idea of what your adversary can and will do? This should come as no surprise. Indeed, the annual cybersecurity trend reviews issued by Ponemon, IBM, SANS, Verizon, PwC and others regularly begin with a survey of the types of threat actors, where the attackers are emanating from, what information they are after, and the motivations that drive their actions. Organizations should view the threat actors in relation to the threat vectors that those attackers are most likely to exploit to achieve their desired purpose—*i.e.*, how attackers get into corporate network environments, their favorite tools and techniques, how they obfuscate and disrupt, etc. This type of composite view that indexes the threat actors to the threat vectors allows for development of a more informative matrix that can be used to build a cybersecurity strategy that makes efficient use of limited resources to target the most significant risks.

[13] Sun Tzu, THE ART OF WAR.

The threat actors traditionally can be categorized as follows:

- Nation States are typically motivated by economic, political, and military advantage. They tend to target trade secrets, sensitive business information, emerging technologies, and critical infrastructure. Attacks can result in loss of competitive advantage and disruption of critical infrastructure.
- Organized Crime typically seeks immediate and future financial gain. Cybercriminals typically target financial payment systems, personally identifiable information, payment card information, and protected health information of both customers and employees. Criminal attacks can lead to regulatory inquiries and penalties, consumer and shareholder lawsuits, and the loss of consumer trust.
- Hacktivists typically seek to create political change or to pressure businesses and industries to change their practices. They target corporate secrets, sensitive business information, and information related to key business executives, employees, customers, and business associates. Often the attack is aimed at simply disrupting business, by causing harm to the organization's reputation or brand and destroying consumer confidence.
- Malicious Insiders are an entirely distinct and quite significant type of attacker motivated by personal and financial gain, professional revenge, and/or patriotism. They take information concerning sales, deals, market strategies, corporate secrets, intellectual property, business operations, and specific persons. Impacts can include trade secret disclosure, operational disruption, brand and reputation damage, and harm to national security (the Snowden effect).

Although these classes of threat actors may appear distinct, there are a number of hybrids emerging. Nation states and terrorists are launching the financially motivated kinds of attacks normally associated with organized criminals, to fund their operations. Malicious insiders are increasingly affiliated with nation states, in an effort to obtain information that could be used to gain competitive advantages in the market. That said, while the general categories of threat actors remain relatively stable, the threat vectors do not. According to Verizon's 2015 Data Breach Investigations Report, some of the most prevalent recent cyberattacks fall into the following categories:

1. Point-of-Sale Intrusions[14]
2. Payment Card Skimmers[15]
3. Crimeware[16]
4. Web App Attacks[17]
5. Denial-of-Service Attacks[18]
6. Physical Theft/Loss
7. Insider Misuse
8. Miscellaneous Errors
9. Cyber-Espionage

It is critical to note, however, that the type of threat vectors and methodologies used by attackers can vary across industries, and they are *constantly* changing. Accordingly, each organization should construct a personalized threat profile, while still being mindful of the most common types of industry threats being reported by third party researchers and government sources.

Organizations should also be sensitive to a population of individuals who straddle the line between threat actors and threat vectors. Benevolent insiders (i.e., employees with good intentions) can cause accidental loss in

[14] "Point-Of-Sale (POS) Intrusions" attack POS systems, which businesses (especially in retail and hospitality) use to accept payment and execute other business operations like accounting, sales tracking, and inventory management. Hackers intrude into a POS system—which is often networked with others in the same enterprise—and install software that steals financial information. POS systems are popular hacker targets because they process financial transactions. Trend Micro, *Point-Of-Sale System Breaches,* http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-pos-system-breaches.pdf.

[15] "Payment Card Skimmers" are devices made to be affixed to a payment system and secretly swipe credit and debit card information when customers use their cards. Brian Krebs, *All About Skimmers*, KREBS ON SECURITY *at* http://krebsonsecurity.com/all-about-skimmers/(accessed August 7, 2015)(includes illustrations of typical skimmers).

[16] "Crimeware" means computer programs that are designed to execute malicious and illegal activities online. Crimeware automates the theft of information. techopedia, *Crimeware*, http://www.techopedia.com/definition/4258/crimeware.

[17] "Web App Attacks" occur when malicious actors inject code into web applications. Common attacks include cross-site scripting (XSS) and SQL injection attacks, which often take advantage of flawed coding. Phishing is another common threat. *See* DBIR at 41.

[18] "Denial-Of-Service Attacks" attempt to make websites inaccessible by flooding them with traffic from multiple sources. United States Computer Emergency Readiness Team, *Understanding Denial-of-Service Attacks,* U.S. Department of Homeland Security (February 6, 2013), *at* https://www.us-cert.gov/ncas/tips/ST04-015.

a number of ways, from falling victim to phishing scams to using weak passwords to losing laptops or other devices. Insider accidents are a major cause of data loss, and they are among the most preventable sources of data breaches.

In 2014, some 90 percent of all security incidents had an insider component, whether it was inadvertent (e.g., falling for a phishing exploit) or intentional (e.g., misuse of access rights to gain authorized access to data/systems).[19] Approximately 50 percent of security incidents resulted from unintentional employee actions. The other half of the time the insider threat is malicious, whether it comes from a disgruntled employee seeking revenge, a departing employee taking trade secrets, or some other cause.[20] When confronted with this type of overwhelming data focused on employees, companies must act specifically to address it.

Gathering Threat Intelligence

Threat intelligence gathering adds a third dimension to the awareness phase of cyber preparedness. Threat intelligence information generally consists of incident reports, indicators of compromise, and threat signatures, and its value cannot be overstated. Integrated into intrusion detection and protection systems, firewalls, and other cyber defense strategies, threat intelligence offers an opportunity to stop (or slow down) an attack before it happens.

Threat intelligence information can be gathered in a number of different ways. There are, of course, managed security service providers (MSSP) that can gather intelligence directly from attacks on your network. These relationships can also be leveraged to get the benefit of threat intelligence data they gather across their clients. That intelligence, while valuable, is not necessarily industry-specific.

Over the past eighteen months, state and federal regulators have placed increasing importance on sharing such information.[21] Information Sharing

[19] DBIR at 31 Fig. 24, 32.

[20] NetDiligence, 2014 CYBER INSURANCE CLAIMS STUDY, *at* http://www.netdiligence.com /NetDiligence_2014CyberClaimsStudy.pdf.

[21] *E.g., Sharing Cyber Threat Information Can Help Secure Nation's Networks and Improve Efficiency; Properly Designed Sharing Not Likely to Raise Antitrust Concerns,*

and Analysis Centers—industry forums for collaboration on critical security threats—have long been a hub for threat intelligence sharing. Organizations with access to formally organized ISACs or functional equivalents should strongly consider participation. With the DOJ and FTC recently issuing guidance that such threat intelligence sharing likely raises few antitrust concerns (as long as the shared information does not include pricing or business information), the legal roadblocks to industry-wide threat intelligence sharing have largely been mitigated.[22] Indeed, regulators and government agencies are increasingly advocating for threat intelligence sharing, and legislators (both federal and state) continue to offer cyber threat intelligence sharing legislation that would offer organizations some liability limitations for engaging in defined sharing activities.[23]

As important as external threat intelligence may be, organizations should continue to focus on internal threats. Although internal threat intelligence is generally more difficult to accurately obtain (it depends on a number of factors specific to your organization), simply knowing the magnitude of the insider threat problem is critical to orienting defense strategies. For example, the unintentional insider threat may merit strong internal policies and training as a prophylactic measure to prevent breach, while malicious insiders might be combated via employer review of email accounts and tracking of employee activity in data collections not directly relevant to the employee's duties.[24]

FTC, DOJ Press Release (April 10, 2014), at https://www.ftc.gov/news-events/press-releases/2014/04/ftc-doj-issue-antitrust-policy-statement-sharing-cybersecurity.

[22] *Sharing Cyber Threat Information Can Help Secure Nation's Networks and Improve Efficiency; Properly Designed Sharing Not Likely to Raise Antitrust Concerns*, FTC, DOJ Press Release (April 10, 2014), *at* https://www.ftc.gov/news-events/press-releases/2014/04/ftc-doj-issue-antitrust-policy-statement-sharing-cybersecurity.

[23] *See, e.g.*, *Promoting Private Sector Cybersecurity Information Sharing*, Exec. Order No. 13691 (February 13, 2015), *at* https://www.whitehouse.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari; FINRA, *Report on Cybersecurity Practices* (February 2015), *at* https://www.finra.org/sites/default/files/p602363%20Report%20on%20Cybersecurity%20Practices_0.pdf; SEC National Exam Program Risk Alert, *Cybersecurity Examination Sweep Summary* (February 3, 2015), *at* https://www.sec.gov/about/offices/ocie/cybersecurity-examination-sweep-summary.pdf.

[24] Note that companies with employees in the EU should pay special attention to employer-employee issues.

Asset and Cybersecurity Posture Awareness and Remediation

Data and Network Asset Mapping

You cannot protect what you do not know that you have. The corollary is similarly true: you cannot design a defense strategy if you do not know what you need to protect. Accordingly, in addition to external threat awareness, organizations must develop internal awareness as well, principally on (a) data and network assets, and (b) cybersecurity posture (strengths and weaknesses). The answer lies in some form of data and/or network asset mapping.

Network mapping is the process of determining what devices are on your network and their connectivity. Through these exercises, organizations can develop awareness of how many endpoints and mobile devices have access to the network, create a catalog of those devices (critical in the event that one is lost or stolen), and gain a better understanding of how the network is generally organized.

Data mapping, on the other hand, is the process for determining what data and other intangible assets the organization possesses, and where on the network (including endpoints) that data is stored. Organizations with mature information governance programs should leverage them to develop a data map efficiently. Data mapping can also offer visibility into data retention policies and practices. These should be reviewed (regularly) to determine whether there is data that no longer has a business purpose, and can thus be disposed of, obviating the need to expend resources to protect it. This is a particularly important consideration for companies that collect information about data subjects in the EU.

Finally, data mapping also offers an opportunity to classify data based on its importance and value, including identification of the organization's so-called "crown jewels." This empowers organizations to make informed decisions about how and to what extent each classification of data should be protected, which decisions are indexed, among other things, to the legal obligations to protect the information and the operational workflow changes that accompany increased security measures. For example, encrypting data protects the information, but requires additional processing time each time the organization needs to access and process the data. Accordingly, organizations must make informed decisions as to whether trade-offs between speed and security are appropriate. They can also use the information to prioritize remediation efforts if/when weaknesses in that security are identified.

Determine Current Cybersecurity Posture through Cybersecurity Risk Assessments

Using an understanding of data and network assets that need to be protected, organizations can begin conducting cybersecurity assessments to determine their current posture and identify weaknesses/vulnerabilities that require mediation. Information security teams have conducted these types of assessments internally for years, knowing that they are critical in preparing defense strategies and ensuring that they are effective. Today, organizations should consider involving outside cybersecurity firms to complement internal efforts, as they bring specialized expertise and real-time awareness of the evolving threat landscape that can improve the quality of assessments.

Organizations are also well advised to give legal counsel a co-leadership role in partnership with the information security team, and to involve other risk management functional groups, particularly those that are involved in procuring insurance, in the process of cybersecurity assessment. There are two basic reasons to include Legal, both of which are shaped by the significant rise in data breach-related litigation and enforcement proceedings. First, Legal can help scope cybersecurity assessments. Because organizations do not have unlimited resources to conduct testing, those resources should be allocated relative to legal risks and obligations that may arise in the event of a breach. For example, publicly available data, or data that is not identifiable to a natural person, may not require the same level of protection as Social Security numbers or intellectual property. And thus, the security of systems that contain and protect such "non-sensitive" data need not be tested to the same degree as those systems that contain more sensitive information.

Second, these types of assessments typically identify a variety of weaknesses and vulnerabilities that can and should be remediated through techniques such as "pen testing" and others that identify possible holes in security tool or patch management.[25] Again, resource limitations require that remediation efforts be staged on a timeline that is indexed to the risks associated with a breach of that information. For example, remediation of vulnerabilities in systems protecting intellectual property and Social Security numbers should be prioritized over other vulnerabilities, and resources (money and time) allocated appropriately.

Scoping assessments and planning remediation require judgments about legal risk, and thus should be directed by counsel, at least in part so that organizations gather the information necessary to make these types of legal judgments and analyses.

The inclusion of Legal offers an additional crucial advantage. If the assessments are directed by Legal for the purposes described above, the resulting communications and work product are subject to the attorney-client privilege and work product doctrines. In a recent Middle District of Tennessee ruling in data breach-related litigation, the plaintiff sought to obtain communications and work product of cybersecurity firms that had been retained to conduct assessments of the organization's security. The court denied the plaintiff access to communications and work product generated by the breached entity because legal counsel had retained the firms to provide counsel with technical assistance to enable it to render legal advice to a client. The court, applying principles similar to those traditionally extended to forensic accountants, explained that "attorneys' factual investigations fall comfortably within the protection of the attorney-client privilege," and "[t]his privilege extends to [a cybersecurity] firm that assisted counsel in its investigation." Similarly, the court held that the forensic reports constituted protected attorney work product because "work product privilege also attaches to an agent's work under counsel's direction." This is because "attorneys must often rely on the assistance of investigators and other agents in the compilation of materials in preparation for trial." This decision underscores legal counsel's critical role in cybersecurity risk assessment, mitigation, and incident response strategies. Covering these activities under legal privilege offers a "safe place" for

[25] And certain types of assets may be subject to specified testing, for example in the credit card context, the Payment Card Industry (PCI) promulgates specific data security standards that must be complied with via testing and certifications.

clients to request and receive legal advice, and therein, to deliberate over issues such as the remedial efforts that will—and, more importantly, will not—be undertaken in response to a cyberattack or identification of a vulnerability. Moreover, the "safe place" created by thoughtful, appropriate use of the attorney-client privilege and work product doctrines can be leveraged to ensure that your organization is gathering the best and most accurate information about its cybersecurity posture (regardless of whether it is good or bad) when implementing a stronger risk mitigation strategy.

These are meaningful protections. Organizations that have experienced a breach should expect that plaintiffs and government regulators will prioritize requests for information regarding the organization's most recent cybersecurity assessment and mitigation plan. The legal privilege, however, shields this information from discovery, and cannot easily be pierced by such lawful legal process (including a grand jury subpoena or search warrant), unlike non-disclosure agreements or contract-based confidentiality arrangements.

Organizations have also looked to creative ways of gathering additional information about possible vulnerabilities through non-traditional types of assessments. In particular, there has been a significant rise in the use of so-called "white-hat hackers"[26] to conduct network security assessments; they essentially perform crowd-sourced security assessments. These engagements (often through an intermediary third party platform) can be extraordinarily valuable because they simulate the Tactics, Techniques and Protocols (TTPs) that sophisticated hackers would deploy in attempting to penetrate your network environment. These exercises, however, should be carefully considered, and may not be appropriate for every organization. First, because these individuals are not directed by counsel, their work product and communications are not likely to be covered by the confidentiality protections of the attorney-client privilege or the work product doctrine. Rather, confidentiality is merely limited by contractual terms, which may be difficult to enforce, given that most white-hat hackers reside outside the United States (e.g., Egypt, India, Vietnam, etc.).

[26] *White hats to the rescue,* THE ECONOMIST (February 22, 2014), *available at* http://www.economist.com/news/business/21596984-law-abiding-hackers-are-helping-businesses-fight-bad-guys-white-hats-rescue.

Second, organizations should be cognizant of recent developments empowering the US Treasury Department to impose sanctions on persons who are identified as being connected to certain "cyber-enabled activities" that threaten or could threaten US national security, foreign policy or economic interests.[27] While most white-hat hackers do not engage in these activities, there is an indeterminate risk that they do. Organizations thus must consider whether that possibility implicates additional compliance considerations that the organization may not be currently equipped to handle. Although this may not present any additional legal obligations on organizations that already comply with the existing US sanctions regime, some organizations will need to develop compliance programs. Organizations that choose to outsource that compliance function (for example, by putting the burden on the intermediary platform through which the hackers are engaged) must still conduct diligence to ensure that the outsourced compliance process is effective and limits the organization's exposure.

Implementing Mitigation Measures

As discussed above, once an organization has identified the potential vulnerabilities and weaknesses in its cyber defense strategy, mitigation measures should be identified, prioritized based on asset sensitivity and legal risk and obligations. To gain the confidentiality protections of the attorney-client privilege and work product doctrine, these activities too should be directed by Legal in partnership with information security teams. While there are a host of potential mitigation strategies, two bear significant discussion:

Training

Employee training should be the keystone for cybersecurity preparedness and risk mitigation. As we noted, part of the "insider threat" that organizations face emanates from loyal employees who inadvertently misuse or lose data in all kinds of ways, whether they are falling victim to phishing

[27] *Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities,* Exec. Order No. (April 1, 2015), *at* https://www.whitehouse.gov/the-press-office/2015/04/01/executive-order-blocking-property-certain-persons-engaging-significant-m.

schemes or leaving laptops exposed to theft. Building a culture of cybersecurity compliance thus must form a key component of minimizing these types of preventable losses. Establishing policies and procedures is simply not enough without relevant training. This is especially important because many human vulnerabilities cannot be addressed by IT, Legal, Compliance, or any other department acting alone. They must be remedied by creating a unified message and delivering it effectively to employees.

Accordingly, the first step is to create security awareness for all employees. This is—especially for some—a profound cultural shift. Rather than assuming that software is always updated or that company systems are invulnerable because there is an IT department, employees must perceive *themselves* as key players in the organization's cybersecurity, instead of as the target of persistent reminders to change their passwords every few months. Security awareness should cover issues like unique passwords, phishing and other malware scams, company policies on the handling and protection of confidential data, and company policies on the handling and protection of laptops and other mobile electronic devices. In addition to the generalized security instruction delivered to all employees, they should also receive security training that is specific to the particular business needs of their respective units.

The good news is that training can have a real impact in preventing cyber loss. Research shows, for example, that one in ten phishing emails results in a click that lets the intruder in, so minimizing the likelihood that an employee will click on links in such emails is critical to defensive cybersecurity.

Mobile Work and BYOD

Employees working offsite, whether at home or while traveling, create further security issues. Organizations should develop policies and procedures that minimize the risk that employees working remotely or from home will open up opportunities for threat actors to gain a foothold in the organization's network. Employees who use mobile devices with access to confidential business information need to be especially vigilant, and understand the importance of immediately reporting the loss or theft of any computer or mobile device that has been connected or granted access to the organization's network. Reporting the loss or theft enables IT to monitor the use of the machine and cut off network access as necessary.

Preparing for a Breach

The principal challenge and frustration is that there is no bulletproof shield. The reality is that organizations will be breached, and valuable information will be compromised. Given that reality, organizations must prepare for the inevitable. Crisis management is about crisis planning and preparation. Accordingly, a key element of cybersecurity preparedness is the development of an incident response plan, and regular practice on executing that plan.

Developing and testing an incident response plan has another advantage. In the event of a breach, inevitably regulators, plaintiffs and the public will ask whether you had a plan. Accordingly, crafting a plan, routinely testing it, and refining it is key to answering those questions. In practical terms, this means that the organization should be in a position to say that its breach prevention was reasonable and that it had a well-thought-out and practiced incident response plan.

The Incident Response Plan

Each organization's breach incident response plan is different, and must be tailored to meet the particular requirements of the organization, including regulatory requirements. Accordingly, there is no one-size-fits-all solution. There are, however, certain indispensable elements to every breach incident response plan.

Building an Incident Response Team

Perhaps the most important element to any plan is the composition of people who will execute the plan. Incident response teams need not only have trust in team members, but also need to be comfortable working with one another. Assembling a team in the midst of a crisis is an unnecessary extra step that absorbs valuable time and resources. For that reason, among others, the first step in building an incident response plan is identifying the team.

Team members should be identified up front, and should be familiar with their roles and responsibilities. Principally among them, Legal and the designated incident response team lead (if different) should lead the effort to establish clear leadership lines and cover the response efforts under the attorney-client privilege and work product doctrine. Standard components of a breach incident response team include:

- Team Leader: Manages and coordinates the incident response plan execution, coordinating with Legal to ensure that privilege and work product protections apply
- Legal: Convenes the incident response team and works with the team leader to determine what procedures to deploy; implements protocols to protect the confidentiality of the response efforts and investigation under the attorney-client privilege and work product doctrine; retains all outside firms, including outside counsel, forensics, PR, and other vendors as appropriate; advises the board regarding corporate governance issues
- IT Security: Coordinates the forensic investigation, perhaps in partnership with an outside firm; preserves relevant digital evidence and systems; leads remediation efforts; documents triage, containment, and remediation plans
- Corporate Communications: Creates, maintains, and manages internal and external communications in cooperation with Legal; coordinates with external PR firm (as needed, and retained by legal counsel)
- Security Loss Prevention: Leads or assists in physical security investigations; preserves physical evidence; engages law enforcement at direction of Legal or team leader
- Human Resources: Manages communications to, and inquiries from, workforce; coordinates disciplinary action if needed; assists team leader and Legal in identifying, securing, and distributing remedy/compensation for employees, as applicable
- Customer Service: Manages inquiries directed to the customer service center; prepares FAQs and talking points for and trains call-in facility personnel (with PR, Communications, and Legal); assists team leader and Legal in identifying, securing, and distributing remedies or compensation to customers, as applicable

Although an incident response team is identified before a breach, organizations must plan for the possibility that certain team members may need to be quarantined off from certain portions of the response effort. To understand why, it is necessary to first reflect that one of the primary tasks in a response effort is to determine what happened; specifically, what was the source of the compromise, what information was leaked, and who did it. These and other questions must be answered to determine the company's legal obligations. Accordingly, strong consideration should be given to ensuring that the investigation portion of the response effort is conducted as independently as possible, free from real *or perceived* conflicts of interest. This is crucial, so that the findings and conclusions of the investigation can not only be used reliably to determine legal obligations, but also to ensure that the investigation is defensible. Indeed, in most breaches, some elements of the incident response team (typically from IT or information security) may be perceived to have a vested interest in the outcome of the investigation. This is common, and should be socialized early in the breach preparation process. Addressing potential conflicts in the midst of the breach response can be complicated, not only politically but because there is no pre-identified individual who can step in to assume the responsibilities of the quarantined employee.

As indicated above, typically the incident response team will be augmented with external resources, including counsel, forensic experts, and communications teams. These specialists should be retained by legal counsel to protect their activities and communications under the privilege, and consist of experienced players who have been though a breach response. Outside counsel will typically work with the team leader to execute the incident response plan. Forensic investigators will help with the technical aspects of incident response, and help threat awareness. Having a clear and well-rehearsed incident response strategy does not just protect the investigation and promote the flow of information—it has also been shown to reduce costs.

Another critical but often-overlooked factor is *pre-breach* retention of third party team members. Without contracts put in place in advance, response efforts typically stall out until third parties are selected and engaged, absorbing valuable time from the response and putting unnecessary pressure on the incident response team, which could lead to mistakes and issues. Organizations that are best equipped to act promptly have not only identified the internal incident response team, but have retained critical external resources prior to an event.

Other Important Elements of an Incident Response Plan

Organizations should also consider proactively establishing relationships with regulators and law enforcement in advance of an incident. Establishing law enforcement relationships will not only facilitate reporting of an incident, but also create opportunities to take advantage of statutory notification delays available if requested by law enforcement. Substantial law enforcement relationships can also be leveraged to obtain information (such as threat signatures, indicators of compromise, and remediation strategies) that could be valuable in conducting the breach response investigation. Organizations should also establish relationships with regulators prior to an incident. As a practical matter, this type of relationship building can also facilitate reporting, and tamp down the likelihood of adversarial investigations or enforcement proceedings.

Incident response plans must be operational and easily accessible to incident response team members. Accordingly, they should be short and easy to use, supported by appendices, such as checklists, frameworks, decision trees, or workflow charts that offer team members direct and clear instructions. They should also include references that are key to any breach response effort, such as a current map of the network and log of endpoints; a matrix for determining the severity of an incident; template communications statements that can be quickly adjusted and then communicated; and contact information for key players on the incident response team. Moreover, organizations should assume that the incident response plan is discoverable in ensuing litigation or enforcement actions, and it should be drafted clearly and concisely so as to minimize any possible misconstruction by adverse parties.

Tabletop Exercises

Having a plan alone is not enough. Preparation requires practice, practice, and more practice. Notwithstanding, organizations that have an incident response plan often report that the single biggest impediment they face in making their incident response plan effective is the failure/inability to review and practice the plan's procedures. Rehearsing what happens in an incident leads to dialogue and identification of areas for improvement.

In a tabletop exercise, the incident response team works together to react to and mitigate a hypothetical data breach. Mature tabletop exercises include injection of new facts and discoveries that must be addressed (injections), and include time pressures that simulate real-life constraints. They also incorporate anticipated adversaries and attack vectors developed through threat intelligence gathering and sharing.

Following a tabletop, incident response teams should debrief with experts, such as outside legal, forensic and communications firms to identify areas for improvement.

One final note is to document all of these efforts. While documenting efforts to prevent intrusion, for example, may not actually help prevent the intrusion, it will be helpful in being able to demonstrate to a regulator the nature and extent of the pre-breach work that was done to bolster the entity's cybersecurity. If those efforts are continually documented, that documentation can be very useful when demonstrating the steps taken on the front end to bolster a company's cybersecurity.

Conclusion

Breaches hit the headlines every day. More and more often, the threat they bear with them is existential. But given diligent preparation, awareness, and collaboration, enterprises are far from helpless. The key is to establish cybersecurity preparedness as a dynamic, proactive program that evolves with the threat landscape. Understanding the threat landscape for your industry, knowing where your data and devices are, training your employees, and assembling a well-rehearsed incident-response plan and team bolster your defensible cybersecurity posture and put your enterprise in the best position to fight back should a breach eventually strike. Sun Tzu was right: know your enemies, know yourself, and prosper.

Key Takeaways

- Cybersecurity preparedness must be seen as an exercise in risk mitigation, management, and displacement—not perfection. Focus on two goals: minimizing the likelihood of a successful attack and mitigating the effects of a breach. Document these efforts so your client can rely on them later to demonstrate diligence in protecting valuable assets and customers.
- The cyber threat landscape is not the same for every industry and every enterprise. Develop situational awareness of the cyber threat landscape and the risks that attackers pose to your clients' networks and assets to build a cybersecurity strategy that makes efficient use of limited resources to target the most significant risks.
- Be on the alert for threats and weaknesses coming from insiders, whether benevolent or malicious. Employees may fall victim to phishing scams, use weak passwords, and lose laptops or other devices—all preventable breaches. Counsel clients to be aware of malicious insiders as well, whether in the form of a disgruntled employee seeking revenge or a departing employee taking trade secrets.
- The first step in protection is awareness of what data your client collects and maintains and where it is located. This requires data and/or network asset mapping, including identification of devices connected to your client's network and their level of access. Data retention policies and strategies need to be cataloged and understood. Classify data based on its importance and value, to enable informed decisions on how and how much effort should be devoted to protecting each classification of data.

Mark Mermelstein is the Co-chair of the Cybersecurity & Data Privacy Group at Orrick, Herrington & Sutcliffe LLP. He has spent almost 20 years as a white collar criminal defense lawyer with more than 20 first-chair trials. This experience is crucial in a) running an attorney-client privileged internal investigation to determine the facts of the breach, b) leveraging law enforcement resources to help data breach victims, and c) defending data breach victims in regulatory investigations, which are very similar to white collar criminal investigations where the company is the target.

Mark has written many articles and spoken extensively on many aspects of his practice. A frequent commentator on matters related to cybersecurity, he was recently named to "The National Trial Lawyers: Top 100," and is recommended by Legal 500 for his cybersecurity work. Mark was also honored by the Southern California Super Lawyers Magazine as a Southern California Rising Star each year from 2004 through 2012.

Antony (Tony) Kim, is the Co-chair of the firm's Cybersecurity & Data Privacy Group at Orrick, Herrington & Sutcliffe LLP. Tony represents clients in investigations before federal and state regulators, and in private actions and counseling engagements across a broad array of antitrust and competition matters, and consumer-facing matters focused on data privacy, data security and breach response, and sales and marketing. His clients are engaged in diverse industries, such as chemicals, transportation, medical devices, media and newspapers, clothing and fashion, financial services, software and hardware, and a variety of online and mobile platforms.

In 2014, the International Law Office (ILO) and Lexology awarded Tony the exclusive Client Choice award in Competition for the District of Columbia and United States region based on a survey of more than 2,000 senior in-house counsel. The National Law Journal named Tony to its 2014 list of D.C. Rising Stars, a 40-under-40 group of "game changing" private, government and public interest attorneys who practice in our nation's capital.

Aravind Swaminathan, the Co-chair of the firm's Cybersecurity & Data Privacy Group at Orrick, Herrington & Sutcliffe LLP, is an accomplished trial lawyer, litigator, and former federal prosecutor, with extensive experience in cybersecurity and data breaches, government and internal investigations, and privacy-related matters. He advises clients in proactive assessment and management of internal and external cybersecurity risks, breach incident response planning, and corporate governance responsibilities related to cybersecurity. Aravind has directed dozens of internal data breach investigations and cybersecurity incident response efforts, including incidents with national security implications. Aravind also represents companies and organizations facing cybersecurity and privacy-oriented class action litigation that can often follow a breach.

Until 2013, Aravind was an Assistant United States Attorney for the Western District of Washington, where he served as one of the district's Computer Hacking and Intellectual Property Section attorneys. He led the United States Attorney's Office cybercrime outreach program for the Western District of Washington, where he worked with members of the Department of Justice, regulators, law enforcement and other organizations on cybersecurity and related privacy issues.

ASPATORE

Aspatore Books, a Thomson Reuters business, exclusively publishes C-Level executives and partners from the world's most respected companies and law firms. Each publication provides professionals of all levels with proven business and legal intelligence from industry insiders—direct and unfiltered insight from those who know it best. Aspatore Books is committed to publishing an innovative line of business and legal titles that lay forth principles and offer insights that can have a direct financial impact on the reader's business objectives.

Each chapter in the *Inside the Minds* series offers thought leadership and expert analysis on an industry, profession, or topic, providing a future-oriented perspective and proven strategies for success. Each author has been selected based on their experience and C-Level standing within the business and legal communities. *Inside the Minds* was conceived to give a first-hand look into the leading minds of top business executives and lawyers worldwide, presenting an unprecedented collection of views on various industries and professions.

ASPATORE