UNITEDLEX

Sep/Oct 2014 ■ Volume 17 ■ Issue 5

FINTECH LAW REPORT

E-Banking, Payments & Commerce in the Mobile World

Whatever You're Doing Isn't Good Enough: Paradigm Shift in Approach to Cybersecurity Needed to Minimize Exposure, Liability and Loss

BY R. JASON STRAIGHT

R. Jason Straight is a Senior Vice President and Chief Privacy Officer at UnitedLex. Mr. Straight has more than a decade of experience assisting clients in managing information security risks, data breach incidents, data privacy obligations and complex electronic discovery challenges. He is also a member of the Editorial Advisory Board of FinTech Law Report. Contact: jason.straight@unitedlex.com.

Details are still emerging about the recent attack on Home Depot's computer network, which investigators now believe could affect more than 60 million customers, making it the largest known data breach ever among retail companies, according to the *New York Times*.[1] Just days before the Home Depot story emerged, a *Bloomberg* report revealed that hackers, most likely professional cybercriminals operating out of Eastern Europe, had conducted a "coordinated attack" on JPMorgan Chase and at least four other banks in August 2014, stealing customer data that could be used to drain customer accounts.[2]

As these and numerous other major data breaches in recent months indicate, the current wave of cyberattacks on corporate information systems continues unabated, in spite of unprecedented investments in defensive measures incorporating advanced technologies and expertise of which one could only dream just a few years ago. A recent letter to shareholders from JPMorgan Chase Chairman and CEO Jamie Dimon indicated the company would spend $250 million on cybersecurity in 2014, with

R. JASON STRAIGHT

THOMSON REUTERS

approximately 1,000 individuals focused on that effort—and those efforts are expected, in Dimon's words, to "grow exponentially" in coming years.[3] And yet, as the number and scope of attacks continue to increase, we can no longer ignore the perverse logic that governs this scenario: the more money we spend, the more intractable the problem seems to become. In order to come to grips with this apparent incongruity, one must understand the complex dynamics of the cyberthreat landscape.

To begin with, the attackers will always have more compelling incentives to get into your network than you have to keep them out, and their likelihood of success is inevitably higher. After all, a skilled attacker is almost guaranteed of finding a soft spot in a company's defenses given the incredibly vast and complex attack surface,[4] while the defender is largely unable to assess the true risk posed by a given threat at any given point in time and focus defenses where they are needed most urgently. Moreover, the attacker need only be right once in finding a single exploitable vulnerability, while a defender must be right 100% of the time to prevent an attack. The bottom line is that a sophisticated and sufficiently determined attacker will *always* get in. Our focus must then shift to the next line of defense—minimizing the damage that can be done.

Limitations of the Military Analogy

Despite the fact that—mercifully—no lives are at stake in a cyber "war," it is easy to slip into using military analogies when discussing the cybersecurity landscape. Unfortunately, this tendency contributes to the perpetuation of a security model that is essentially outmoded: that of the defender of a castle working the ramparts in an effort to keep the barbarian hordes outside the walls.[5] If one must draw a military parallel to today's cybersecurity reality, it is more accurate to view the battle as asymmetric or guerilla warfare. Consider the following:

- The attackers are often loosely confederated groups of anonymous individuals who are exceedingly difficult to identify before, during or after an attack.
- The attackers' strategy is heavily reliant on advance reconnaissance that allows them to identify a target's vulnerabilities.
- Although they do occasionally bring sophisticated weaponry to bear, the attackers rely mostly on primitive and unsophisticated tactics to inflict damage on their target where and when the defender is most vulnerable.
- "Conventional" methods of defense are ineffective, and offensive measures—*e.g.*, taking down a hacking ring—are difficult, resource-intensive and time-consuming, and have a low success rate.
- If one cybercrime ring is taken down, another quickly fills the gap.
- Successful breaches embolden other hackers to attempt similar breaches.
- There is no "winner" of the war, only a series of battles where either the defender is successful in repelling an attack or the attacker accomplishes its objectives.
- The "war" is unlikely to end at any time in the foreseeable future, due to the fertile target landscape.

Unfortunately, few of the tools and techniques available to defenders are effective in the sorts of close-quarters skirmishes that we see today. Even the largest security vendors, who have done their best to squeeze every last dollar from an obsolete—but exceptionally profitable—paradigm based on perimeter defenses and signature-based threat detection, now widely acknowledge that defensive tactics like antivirus are essentially dead.[6] The problem is that few technology alternatives have emerged that have proven effective against the kinds of attack vectors that are becoming increasingly common. Too often a security strategy is developed around already-available tools and technologies, which typically are easily defeated or bypassed by fraudsters, rather than an understanding of the true business risks posed by today's cyberthreats.

What's needed is a complete change in philosophy toward cybersecurity. First and foremost, companies must give more than lip service to the idea that preventing a breach is impossible. While virtually any serious security expert would readily concede this point, few security programs are built around the central idea that no matter how much you spend and how sophisticated your defensive tools are, a determined attacker will eventually find an exploitable vulnerability that will allow a compromise. If security programs were to take this idea seriously, their primary emphasis would be on building, maintaining and testing a robust and comprehensive incident response capability. Not only is incident response rarely the centerpiece of a security program, but many otherwise exemplary programs fail to include *any* serious attempt to incorporate a holistic incident response function. What is the explanation for this?

For one thing, incident response is inherently chaotic. It requires close collaboration, open communication, total transparency and accountability among stakeholders from a variety of business functions—including IT, legal and compliance professionals as well as C-level executives—that typically are not accustomed to interacting together at a strategic level. Traditionally, such functions operate in silos, because it's easier for corporations to assign tasks, allocate budgets and resources, calculate profit and loss, and ascertain the performance of a single business unit, as opposed to a "layer" that floats above multiple business units. In a corporate setting, these units are inherently competitive for budget and other resources, and are also highly protective of their unit's actual or perceived performance, which typically is the yardstick for measuring and disbursing professional bonuses or other perks. In short, few are willing to share resources or stick their neck out without some guarantee of success. In order to change this, the organization must undergo a profound cultural shift, driven from the top, in which collaboration is encouraged and expected, and budgets, personnel and other resources are allocated specifically for incident response.

Secondly, despite the fact that the global cybersecurity market is growing rapidly, with a value estimated at a robust $77 billion in 2014,[7] the industry still has very few good solutions that support incident response and is, in fact, heavily incentivized to perpetuate the broken status quo of perimeter defense. Focusing on perimeter defense over incident response appeals to our natural human instincts as well. To briefly return to our castle analogy, it is much easier to generate support for building higher walls or digging deeper moats than for a program that imposes increased internal surveillance, disruptive policies or general inconvenience on the people we're purportedly trying to protect.

Whatever You're Doing Isn't Good Enough

If the problem is left to IT to solve, they will look almost exclusively at technology fixes. That's not a criticism; it is a fact that reflects the training and mindset of IT as well as the realities of IT's limited scope of influence in an organization. But many problems and vulnerabilities are more likely to be rooted in the policies and procedures that operate at the human level and cannot be addressed by IT alone. While a close look at many significant data breaches of recent years will confirm this important principle, details emerging from the Target incident in late 2013 are especially instructive in demonstrating how a defensive posture that relies heavily on technology can engender complacency and make it nearly impossible to respond to an intrusion effectively. When it comes to addressing today's cybersecurity challenges, the focus on perimeter defense is simply too narrow to encompass the severity of the problem and the scope of financial and legal risks that a large-scale cyberattack represents.

To be sure, technology must play a central role in any information security program. In particular, advanced data analytics and security event correlation tools can enable a company to preempt an attack before it has an impact. But even the most sophisticated technology is rendered ineffective if you don't have the right people managing its implementation and use. Skilled security analysts are in high demand and low supply.

Even those companies fortunate enough to have quality security personnel cannot sustain staffing levels sufficient to monitor and manage what has become the weak link in most security programs and, accordingly, is on page one of many hacker playbooks: the human layer. Whether focusing on insiders or trusted third parties, attackers are investing more time developing social engineering and other exploits with which to launch sophisticated attacks. Most companies are doing little beyond perfunctory, compliance-driven awareness trainings to address the threats posed by spear phishing, weak passwords and misuse of corporate IT assets by trusted users.

One solution to reducing risks associated with "the human element" is better education, awareness and training, which is a function generally handled by human resources. However, most HR departments have limited resources available for training and only a cursory understanding of IT security protocols—limited to, typically, whatever is printed in the employee handbook. Even if formal security training is conducted, many corporate HR departments default to canned, do-it-yourself security training programs that are rarely reinforced during the employee's tenure, and provide only a general overview of security red flags and procedures. In the words of Heidi Shey, a Gartner analyst who studies data security and privacy, "Security awareness and training is underappreciated and undervalued in many organizations—and it shows. The goal of an awareness and training effort should not be distribution of information, but driving behavioral change."[8]

If employees are the main entry point for most cyberattacks[9], they must first be educated about the internal and external threats they face, and then empowered to act as their organization's first line of defense. This can only occur through a close collaboration between the IT/security and HR functions via a comprehensive, customized training program that focuses on identifying and protecting the organization's vulnerabilities, and consistently reinforced through recertification, mock drills and performance benchmarking.

Taking Aim at Target: Financial Fallout, Legal Actions, Ongoing Crisis

Target's online and in-store data systems were compromised between November 27 and December 15, 2013. Financial and personal information of Target customers was stolen by hackers who installed malware on the company's computer network. The custom-designed malware embedded itself in Target's point-of-sale systems and captured payment card data as it flowed from Target's checkout lines. The attackers initially gained access through a third-party vendor, a small Pennsylvania HVAC company that reportedly "did not appear to follow broadly accepted information security practices."[10] Current estimates suggest hackers may have accessed debit and credit card accounts and PIN numbers of 40 million customers, and compromised the personal information of 70 million customers.[11]

One need look no farther than the Target incident to clearly see the scale of business-level impact a serious cyber-incident can have. Security analyst Brian Krebs calculates that hackers generated $53.7 million in income from selling stolen credit card information on the black market at a median price of $26.85 per card. As a direct result of the breach, banks and credit unions were forced to spend an estimated $200 million to reissue 21.8 million cards. By February 1, Target had already spent $61 million responding to the incident.[12] Meanwhile, fourth quarter 2013 profits at Target came in 46% lower compared to the same quarter in the previous year.[13] The CIO quickly resigned and Gregg Steinhafel, who was the company's CEO when the breach occurred, and who struggled to recover the trust of customers and investors in the months that followed, was forced to resign on May 5, 2014. Indeed, Steinhafel may be the first CEO of a major corporation to lose his job due to a cybersecurity incident, but he is unlikely to be the last.

Unlike the media storm that engulfed the incident and the immediate financial fallout, the legal fallout from the Target breach will take years to unravel. Over 100 lawsuits stemming from the incident have been filed across the country, including at least 45 in various Federal district courts.[14] A sampling of the causes of action that have been asserted against Target, along with a quick summary of the corresponding arguments, appears below.[15]

Common Law Causes of Action

- **Negligence:** By accepting customer information, Target owed a duty of reasonable care to protect that information, and disclose any breaches in a timely manner.
- **Negligence per se:** Target's failure to safeguard customer information violated several statutes and industry standards.
- **Negligent misrepresentation:** Target misrepresented that customer information was secure.
- **Breach of contract:** In exchange for payment, Target expressly and/or implicitly agreed to protect customer information.
- **Conversion:** Customers own/possess their information, and Target's conduct has interfered with this ownership/possession.
- **Unjust enrichment:** Part of the money paid to Target in the course of transactions was meant for the costs of data security, and Target shouldn't retain money it failed to spend on data security measures.
- **Bailment:** Customer information is personal property and upon its delivery to Target, the company owed a duty to use it only for the time necessary to complete the purchase, and then properly protect it.
- **Breach of fiduciary duty:** Target owed fiduciary duties to protect customer information by becoming "guardians" of that information.
- **Invasion of privacy:** Customers have a reasonable expectation their information will be kept confidential, and its disclosure is highly offensive.

Statutory Causes of Action

- **Federal Stored Communications Act:** Prohibits the knowing disclosure of the contents of an electronic communication. The stolen customer information was contained in an electronic communication, and Target knowingly disclosed this information by failing to take reasonable steps to protect it.
- **Consumer Fraud and Deceptive Business Practice acts (various states):** Accepting customer information and failing to take reasonable steps to prevent its disclosure is a deceptive business practice, as is representing that customer information will be kept secure. The harmful impact of the disclosures outweighs any justification for Target's acts.
- **Prompt Notification of Data Disclosure acts (various states):** Target was required to disclose the breach to any person whose personal information was acquired by an unauthorized person in the most expedient time possible without unreasonably delay. Target learned of the breach on December 15, but didn't publicly announce it until December 19, and didn't make individualized communication until December 20.
- **Statutory invasion of privacy:** Customers had a reasonable expectation in privacy of their personal information, and failing to protect it invaded this expectation.

Damage Theories and Assertions

The complaints against Target generally do not articulate exact dollar figures or damage estimates, but instead request damages in amounts to be determined at trial. The complaints, however, do assert a variety of ways in which customers have been—and will continue to be—damaged by the breach. Two common themes are that any damages were made worse because of Target's delay in notifying customers of the breach, and that the risk of harm will linger for years since the stolen information can be sold on the black market at any point. Below is a list of damage assertions that have been made.

- **Actual and compensatory damages.** Customers are seeking reimbursement for:
  - Fraudulent charges/purchases and unauthorized withdrawals
  - The inability to use credit cards and loss of access to credit
  - Time and money required to monitor accounts and credit scores
  - Lost wages from spending time on the phone or in-person with banks and credit agencies to reverse unauthorized charges, order new cards and clean up credit issues
  - Credit monitoring services and identity theft insurance
  - Damaged credit scores and impaired ability to obtain additional credit
  - General anxiety over financial well-being
  - Loss of rewards tied to debit and credit card usage
- Financial institutions[16] are seeking reimbursement for:
  - Customer losses
  - Reversing fraudulent charges
  - Closing compromised or suspected-to-be-compromised and cancelling corresponding cards and checks
  - Opening new accounts and issuing new debit cards, credit cards and checks
  - Increased monitoring of customer/member accounts to determine if transactions are legitimate or fraudulent
  - Notifying customers/members of potential credit problems
  - Lost interest and transaction fees
- **Injunctive relief.** Many complaints request the court order specific injunctive relief, including requiring Target to:
  - Stop its allegedly deceptive practices
  - Increase security and adequately safeguard personal information
  - Engage in a proper notice campaign in regards to the breach
  - Provide prompt notice for any future security breach
  - Provide customers with free identity theft insurance
  - Provide customers with free credit and fraud monitoring services
- **Identity theft.** The complaints allege that the stolen personal and financial information could be used to:
  - File fraudulent tax returns and obtain tax refunds
  - Commit immigration and medical service fraud
  - Take out loans
  - Obtain government benefits, driver's licenses, jobs or housing
  - Give false information during an arrest
- **General considerations.** The complaints also include the following standard requests:
  - Attorneys' fees, expenses and costs
  - Pre- and post-judgment interest
  - Statutory damages and statutory penalties
  - Punitive damages
  - Equitable relief in the form of restitution and disgorgement of revenues wrongfully obtained as a result of Target's alleged wrongful conduct

It remains to be seen how successful these claims against Target will be. Many of the liability and damage theories are untested and will require some creating lawyering to sustain. But regardless of the outcome of the suits, there is no doubt that Target will be forced to spend millions defending itself against this onslaught of litigation. This brief summary of the potential financial and legal—not to mention reputational—liabilities that Target faces in an incident for which it appeared: 1) clearly unprepared, 2) slow to recognize and understand as a serious incident, and 3) slow to remediate should give readers a better sense of the scope of the fallout that can result from a major cyberattack when information security planning falls short.

It is important to emphasize, however, that we cannot lay the blame for the incident and the widespread damage that Target is still experiencing today solely on its IT infrastructure, nor should we assume it was a lack of an appropriate level of investment in cybersecurity measures and tools that explains the company's vulnerabilities. After all, Target had an "advanced" malware intrusion detection system in place when its network was first infiltrated. Despite the fact that the system appeared to generate "urgent alerts" at the early onset of the attacker's activity, it should be noted that a prominent cybersecurity expert described the system as a "relatively crude" tool that, even in a full-featured version, could be purchased for a mere $2,300.[17] Reports conclude that the response to these alerts by Target's security team was insufficient,[18] indicating that it was a human, rather than a technological, failure that ultimately made the breach possible and prevented the company from containing the scope of the damage.

In addition, while the Target event is widely regarded as a malware intrusion, it's worth reminding readers that the original breach of security was traced back to an email phishing attack sent to employees of the Pennsylvania HVAC contractor, which allowed attackers to gain access to network credentials two months before attackers actually began stealing card information from the retailer.[19] In order for the attack to succeed, only a single employee with the HVAC contractor needed to open the malware-laced email and trigger its payload—which one of them did. This again suggests that human behavior is at least as culpable in the Target disaster as the failure of technological defenses.

Lessons from Recent Incidents

As the details of the Target incident fade into memory and are supplanted by even more megabreach reports, it is important to pause and consider what we all must learn from these incidents in order to avoid being the next victim, or, if that is unavoidable, that we at a minimum ensure we are better prepared to respond with confidence and skill when the inevitable incident does occur.

Lesson #1: Cybersecurity Is a Business Risk Issue—It Can't Be Addressed By IT Security Staff Alone

It's 2014—do you know where your critical data assets are? This seems like a relatively straightforward question. However, upon closer examination, it becomes clear that answering it requires input from a variety of sources, certainly beyond just the IT department. After all, IT's primary role is managing systems rather than data. Indeed, you will get a very different answer on what constitutes the company's crown jewels depending on whom you ask. The R&D and engineering teams will tell you it is the company's intellectual property. Investor Relations will tell you it is financial data and forecasts. HR will say it is personal information about employees. Unfortunately for those tasked with creating an inventory of critical data, all of these answers are correct.

Even though many companies are giving lip service to the idea that cybersecurity is more than an IT issue, most still manage it as a technical problem. New technologies can provide organizations with powerful tools to defend against cyberattacks, but those tools can be prohibitively expensive or difficult to use, facts that contribute to a widespread perception that there is a necessary "trade-off" between security and efficiency. While this perception remains pervasive across a broad range of industries and organizations, we believe it is obsolete and reliant on a narrow conception of enterprise security.

As the fallout from countless large-scale breaches we have seen in recent years has made abundantly clear, it is no longer appropriate to regard cybersecurity concerns in terms of IT operational risk. On the contrary, threats to information security now represent a significant business risk that extends across the entire enterprise. It follows that an effective information security management program requires active involvement—and close collaboration—among a range of business stakeholders, including IT and security staff, certainly, but also legal, compliance, executive-level management, HR and even board members. Information security can no longer be accomplished with tools and tactics alone; it is a strategic concern at the heart of your business, and it requires a strategic mindset.

The good news is that this challenge is eminently addressable. Regular collaboration among these stakeholders in assessing risks can quickly put enterprises on firmer ground when they consider major business initiatives, whether that means opening up a new line of business, entering a new geographical market, acquiring another company or entering into a strategic partnership. Far from being a mere cost center that has the potential to inhibit competitiveness, collaborative cybersecurity risk management planning can actually help companies move forward with initiatives and take advantage of business opportunities more quickly and confidently, and with better and more complete information, while remaining within acceptable risk parameters.

A great example of how a multi-stakeholder, business risk approach can pay dividends comes in looking at the first step a company should take once it has identified its critical data assets. An IT or security-centric approach might dictate that the company immediately set about restricting access to those sensitive data stores and focus monitoring efforts where they are needed most. While these tasks are certainly part of the solution, we would submit that there is a more fundamental non-technical question that should be asked first: "How much of the critical data we identified do we actually need to hold on to?" Nearly every company holds on to far more data for much longer than it is useful or necessary to keep. It is a simple fact that data you don't have cannot be compromised. This is not a question that IT can answer on its own. Input from legal, compliance, HR, finance, operations and other business-line leaders is critical to determining what the company must keep (and protect) and what it may destroy as a risk-mitigation technique. This is not an easy process but companies that commit to investing the time will recognize considerable dividends.

Lesson #2: The Attackers Will Get In; You Need to Be Ready

You need to assume that your defenses will fail and focus on establishing a second line of defense that will help safeguard critical data assets from intruders that do get inside your perimeter. Having measures in place to identify suspicious or anomalous behavior that may indicate the presence of an intruder is a critical piece of any modern cyber defense system. Advanced data analytics present in newer Data Loss Prevention tools and Security Incident and Event Management platforms have shown considerable promise as a means of allowing organizations to automatically identify anomalous behavior that would not be recognizable by signature- or indicator-based technology. "Big data" analytics can provide security-conscious enterprises with a number of advantages, including the ability to:

- Reduce false alerts produced by existing systems by checking them against contextual data
- Correlate resulting high-priority alerts across multiple monitoring systems to detect patterns of abuse and fraud
- Pool data from both internal and external sources in a single logical location, and comb that data for patterns of fraud or potential attack
- Look for anomalous transactions within user or other account "profiles"[20]

Data analytics also positions enterprises to respond much faster to suspicious activity and either resolve it as benign or suppress it if were malicious.

Unfortunately, it appears that the technology of data analytics is still beyond the ability of many organizations' ability to adopt and use effectively.[21] For example, operational issues—such as the need to utilize APIs, or requirements for custom development to incorporate alerts from previously siloed applications, or to create a common dashboard—can easily inhibit an organization's efforts to integrate the technology successfully.[22] The biggest challenge for many companies in trying to take advantage of modern security tools is recruiting and retaining sufficiently qualified analysts to operate the tools. Without these specially trained experts, the tools are largely ineffective. Despite these challenges, the bottom line is that companies must alter the focus of security spending to emphasize mechanisms that will detect and suppress advanced threats that manage to penetrate external defenses.

Most importantly, companies must realize that incident response capabilities must be the centerpiece of an information security program. Companies must recommit themselves to developing and maintaining an effective and collaborative incident response plan rooted in the reality that it is not possible to prevent all cyber-attacks. Investments in tools and expertise that empower incident response, preemption and suppression are every bit as important as investments in prevention. In addition, the incident response plan should fully define roles and responsibilities in the event of an incident and provide clear guidance on when to engage outside experts such as attorneys and forensic investigators. A good incident response plan is constantly evolving to fit the changing threat environment. This is not an easy process, but there simply is no short-cut for the manual process of building, maintaining and testing an effective response plan.

Lesson #3: Don't Forget about the Trusted Insiders—Hidden Vendor and Employee Risks Are Looming Larger

The attack on Target via a small third-party vendor is hardly an outlier. According to a 2013 Forrester report on data security and privacy, insiders caused nearly half of incidents in that year, and approximately 36% of breaches in the same year originated with "inadvertent misuse of data by insiders…the top cause of breaches seen during the past 12 months."[23]

Notwithstanding their good intentions, insiders are actually contributing to a problem they would like very much to prevent. How can this be? In many cases, they haven't received any security awareness training, a key factor in driving behavioral change. In fact, Forrester found that only 42% of the end users and vendors it surveyed had received security training. And although the Forrester survey did not attempt to measure the success of training programs, the effectiveness of most canned, online awareness training modules is very limited.[24] The result is that many trusted insiders are granted access to an organization's most sensitive data without a basic understanding of data-use policies, let alone the ability to spot potentially malicious attacks in progress. Also, it is not unusual for the organizations themselves to have a poor understanding of the data they possess, to classify it in overly complex ways (or not at all) and consequently to have data-use policies that are hard to follow and ineffective. Finally, employees and vendors are typically using multiple devices (desktops, laptops, tablets, smartphones) to store and access files; according to the Forrester survey, 66% use a USB flash drive or CD/DVD in transferring data from one storage device to another.[25] These devices can be easily lost, stolen or compromised, thus putting the data, the network and the organization at risk for the sake of increased productivity and employee convenience.

Savvy organizations will respond to these dynamics by transforming employees and contractors from their biggest vulnerability to a valuable asset in their information security program. With regard to employees, that means developing clear policies and procedures related to information security, providing regular training to individuals to make sure they understand those protocols and constantly monitoring activity to identify potential threats, weaknesses and risky behavior. For instance, an effective security awareness training program will do more than tell users what they are allowed and not allowed to do; it will also:

- Describe specific attack vectors known to threaten their industry ;
- Provide specific examples of attempted or successful attacks on their own company ;
- Illustrate for employees the severe consequences of a successful breach;
- Train employees to recognize and report suspicious emails or other behavior immediately; and
- Provide practical solutions that will allow employees to perform their job functions efficiently and safely, effectively reducing the cost of the tradeoff between security and convenience.

With regard to third-party vendors, organizations need to adopt a vendor risk assessment program that is more than a "check the box" compliance exercise. While standard questionnaires based on industry standard risk assessment frameworks such as NIST or ISO 27001 may provide a helpful starting point, getting an accurate picture of vendor risk requires a more nuanced approach. Companies should identify vendors and contractors that have access to the most sensitive corporate data and systems and develop a more in-depth risk assessment approach for those vendors. These "high-risk" vendors should be subjected to an on-site visit that includes interviews of key business stakeholders as well as the IT security team. Companies should apply a "trust but verify" approach and insist on seeing evidence that security measures are properly implemented. In addition, companies should focus on the aspects of vendor risk management they can directly control within their own environment. For instance, companies should narrowly restrict the data to which a given vendor has access and limit them to only what they need in order to perform their business function. Vendor activity on the company's corporate network should also be carefully tracked and logged to maximize accountability in the event of an incident.

Lesson #4: Reducing Incident Detection and Suppression Time Reduces Costs

As we noted earlier in the Target example, the retailer's failure to respond and suppress the network intrusion in a timely and effective manner is now a prominent theme in the raft of legal actions currently being brought against it. Target was late in detecting the incident, and failed to respond to a variety of automated warnings that indicated an intrusion was in progress. With every day the compromise was active, the attacker was able to capture more payment card information, thus compounding the exposure and damage to Target's business and brand. Moreover, even after Target confirmed the occurrence of the intrusion, the company was perceived as slow in notifying affected consumers, further eroding trust and raising alarm regarding the scope and scale of the breach.

The failure to detect and understand an incident before it becomes a catastrophe is hardly unusual, and the imperative of timely response is becoming more difficult to achieve, in part because attackers are faster than they used to be. According to the most recent data from Verizon's annual *2014 Data Breach Investigations Report*, attackers are rapidly improving their effectiveness in quickly compromising assets and achieving their objectives following an intrusion. At the same time, defenders are losing ground in their efforts to discover intrusions more quickly. The gap between offense and defense is growing: Research "plainly show[s] that attackers are getting better/faster at what they do at a higher rate than defenders are improving their trade".[26] Every day that a breach continues undetected costs organizations more—not just in money, but also in reputational and legal risk.

Once a breach is detected and understood, efficient and timely remediation can help organizations reduce costs on every front.

Lesson #5: Legal MUST Have a Seat at the Table in Planning for and Managing Cyber-Risks

Any credible information security management program should be based on a "converged" incident response model, where IT and legal have agreed upon a unified response to incidents before they occur. Why is this important? Even well-trained IT staff and consultants who have a basic understanding of incident response may not understand the full implications of a breach and act with sufficient urgency. They may not, for example, comprehend the importance of establishing a clear, comprehensive, defensible record of all response activities so that counsel has the documentation it needs to mount an adequate defense against subsequent legal and compliance actions, like those now emerging from the Target incident. Having legal involved at the very beginning of an event may also minimize delays in notifying authorities and the public after a breach is detected, which can go a long way toward countering claims that a slow response made things worse and merits higher damages.

As we've seen with the Target breach, Congress is increasingly interested in holding companies accountable for failing to adequately protect consumer information.[27] In addition, in the past year and a half alone we've seen the SEC and CFTC issue new cybersecurity guidance and HIPAA was revised to impose direct liability for exposing patient information upon both health care providers and any third parties that come into possession of protected health information. The Obama administration issued a cybersecurity Executive Order last year that provided new guidance for critical infrastructure companies (which includes financial services). We've also seen the Federal Trade Commission use its Section 5 authority to bring more actions against companies for failure to adequately protect personal information[28]. And finally, as we have most clearly seen with both the Target and Home Depot incidents, private litigations including class-action and shareholder derivative suits are increasingly being brought in the wake of these incidents.

This adds up to an increasing need for corporate executives to be ready to explain in exacting detail just how sensitive data managed to get compromised on their watch. Some of the questions that executives may be asked in a deposition or other testimony include:

- How did the attackers get in?
- Why weren't you able to stop them?
- What measures were in place to detect and prevent such an attack?
- How recently had you assessed the efficacy of such measures? By what means?
- What could you or should you have done differently to prevent this attack and/or the loss of data, exposure of customer information, etc.?

If these questions make you squirm in your seat when you think about answering them yourself, you've likely got some work to do to get ready.

Input from Legal is also critical in assessing risk transfer options such as cyber-liability insurance, indemnification language in corporate contracts and other mechanisms to defer some of the costs of a breach incident. Expenses arising from litigation and regulatory inquiries in the wake of a breach have become a major component of data breach costs. In order to factor these costs into risk management decisions, it is critical for legal to have a voice in the risk assessment process.

Conclusion

The old security paradigm is broken. It is critical to understand how attackers think—not just recognize the tools they use. We can no longer rely on the "antivirus" approach, which is 100% dependent on being able to recognize a known and well-defined threat. It's time for a new, business-centric approach to cyber risk management that takes into account human behavior and fosters a deep understanding of the organization's vulnerable assets and where they are located, and identifies potential points of entry and countermeasures that could be applied to defeat a broad range of threats.

We must accept that it is not possible to keep the attackers out. Instead of repeatedly focusing on an impossible goal, the key is to identify and lock down your critical data assets so that even when the attackers get in, they will be detected quickly and have a difficult time getting anything of value out. Moreover, defensive mechanisms must be designed not just to prevent attacks but to preempt them by quickly recognizing subtle clues and signals that an attack is imminent or even underway. Although the work ahead may seem daunting, companies should be encouraged that much progress can be made once we have changed our approach and our mindset.

NOTES

[1] Nicole Perlroth. "Home Depot Data Breach Could Be the Largest Yet." *New York Times*, September 8, 2014, *available at* http://bits.blogs.nytimes.com/2014/09/08/home-depot-confirms-that-it-was-hacked/. Accessed September 2014.

[2] Jordan Robertson and Michael Riley. "JPMorgan, Four Other Banks Hit by Hackers: U.S. Official." *Bloomberg.com*, Aug. 27, 2014, http://www.bloomberg.com/news/2014-08-27/

customer-data-said-at-risk-for-jpmorgan-and-4-more-banks.html. Accessed September 2014.

3. Jamie Dimon. *Dear Fellow Shareholders*, 22 (2014), http://files.shareholder.com/downloads/ONE/3430314926x0x742267/e2efaf60-814f-430e-869e-6889ba3ec0ec/2013AR_Chairman-CEO_letter.pdf. Accessed September 2014.
4. A recent analysis of data from ThreatSim concluded that a phishing campaign of only 10 messages has a better than 90% of getting a click. See Verizon. *2014 Data Breach Investigations Report* [hereafter *Verizon DBIR*], at p. 47.
5. Anthony Caruana. "Today's Approach to Security Is Broken." *CSO*, April 17, 2014, *available at* http://www.cso.com.au/article/543144/today_approach_security_broken/. Accessed September 2014.
6. See, for example, Danny Yardon. "Symantec Develops New Attack on Cyberhacking: Declaring Antivirus Software Dead, Firm Turns to Minimizing Damage from Breaches." *Wall Street Journal*, May 4, 2014.
7. "*Global Cyber Security Market to be Worth $76.68bn in 2014.*" *ASDNews*, February 19, 2014, http://www.asdnews.com/news-53610/Global_Cyber_Security_Market_to_be_Worth_$76.68bn_in_2014.htm, accessed September 2014.
8. See Heidi Shey. "Understand the State of Data Security and Privacy: 2013 to 2014." *Forester.com*, October 1, 2013, at p. 2.
9. Grant Hatchimonji. "Report indicates insider threats leading cause of data breaches in last 12 months." *CSOOnline.com*, October 8, 2013. Available at http://www.csoonline.com/article/2134056/network-security/report-indicates-insider-threats-leading-cause-of-data-breaches-in-last-12-months.html.
10. U.S. Senate Committee on Commerce, Science, and Transportation. "A 'Kill Chain' Analysis of the 2013 Target Data Breach." March 26, 2014. http://docs.ismgcorp.com/files/external/Target_Kill_Chain_Analysis_FINAL.pdf. Accessed September 2014 [here after U.S. Senate Committee].
11. Anthony Wing Kosner. "Actually Two Attacks in One, Target Breach Affected 70 to 110 Million Customers." *Forbes*, January 17, 2014. http://www.forbes.com/sites/anthonykosner/2014/01/17/actually-two-attacks-in-one-target-breach-affected-70-to-110-million-customers/. Accessed September 2014.
12. Michael Riley, Ben Elgin, Dune Lawrence and Carol Matlack. "Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It." *Bloomberg Businessweek*, March 13, 2014. http://www.businessweek.com/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data. Accessed September 2014.
13. Brian Krebs. "The Target Breach, By the Numbers." *Krebs on Security*, May 14, 2014. http://krebsonsecurity.com/2014/05/the-target-breach-by-the-numbers/. Accessed September 2014.
14. Many complaints are seeking class action status, and the cases will likely be combined as a part of a "multidistrict litigation," which consolidates similar cases before one court and is meant to speed up litigation.
15. The strength or likelihood of success of these arguments is not addressed.
16. Several smaller financial institutions have filed complaints against Target, and are seeking class action status. Two examples are Jim Thorpe Neighborhood Bank (located in Pennsylvania) and the Alabama State Employees Credit Union.
17. Brian Krebs. "A First Look at the Target Intrusion, Malware." *Krebs on Security*, January 14, 2014. http://krebsonsecurity.com/2014/01/a-first-look-at-the-target-intrusion-malware/. Accessed September 2014.
18. U.S. Senate Committee, *supra* at 3.
19. Brian Krebs. "Email Attack on Vendor Set Up Breach at Target." *Krebs on Security*, February 14, 2014. http://krebsonsecurity.com/2014/02/email-attack-on-vendor-set-up-breach-at-target/. Accessed September 2014.
20. Avivah Litan. "Reality Check on Big Data Analytics for Cybersecurity and Fraud." *Gartner Report*, January 16, 2014, at 3.
21. Avivah Litan. "Reality Check*," supra* at 1.
22. Avivah Litan. "Reality Check*," supra* at 4.
23. Heidi Shey. "Understand the State of Data Security and Privacy," *supra* at p. 1.
24. Deanna D. Caputo, Shari Lawrence Pfleeger, Jesse D. Freeman and M. Eric Johnson. "*Going Spear Phishing: Exploring Embedded Training and Awareness.*" *IEEE Computer Society*, January/February 2014, http://www.computer.org/cms/Computer.org/ComputingNow/pdfs/IEEESecurityPrivacy-SpearPhishing-Jan-Feb2014.pdf. Accessed September 2014.
25. Heidi Shey. "Understand the State of Data Security and Privacy," *supra* at pp. 1-2.
26. *Verizon DBIR*, *supra* at p. 12.
27. Michael Riley, Ben Elgin, Dune Lawrence and Carol Matlack . "Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It." *supra* at 1.
28. Paul R. Gupta, Thomas Lahiff and Aravind Swaminathan. "FTC v. Wyndham: an Update." *FinTech Law Report* March/April 2014.