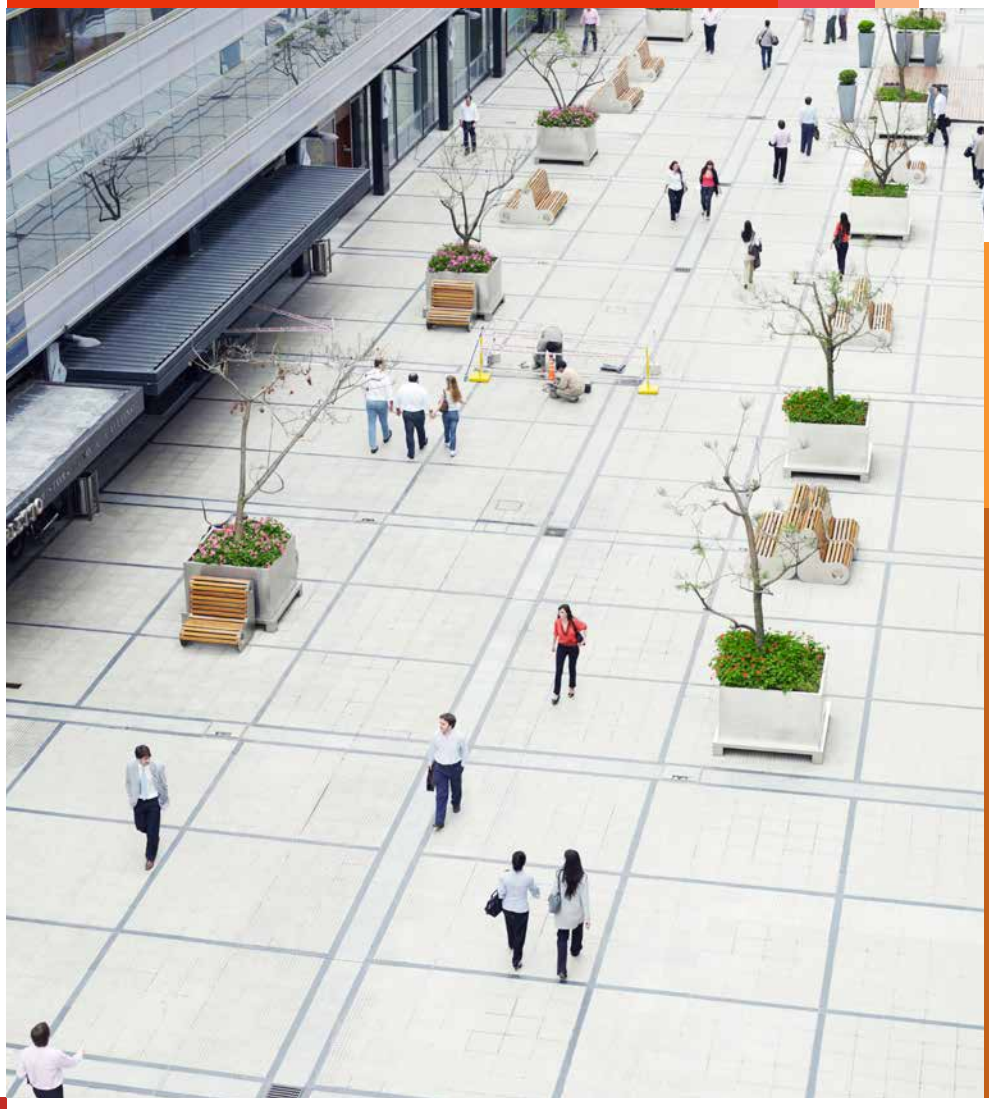
Answering your cybersecurity questions

The need for continued action

January 2014



pwc

Boards and executives keeping a sustained focus on cybersecurity do more than protect the business: they reap bottom-line benefits.

Significant cybersecurity challenges reinforce the need for continued action

There continues to be systematic security issues with retailers in the United States. A number of recent high-profile data breaches demonstrate that cyberattacks on retail and consumer organizations are increasing in number. Incidents during December of 2013 underscore the growing threat and evolving sophistication of these attacks.

Stolen customer payment card data translates into huge dollars for cyber criminals. As a result, retailers are prime targets for hackers looking to steal sensitive customer information. When retail companies suffer security breaches and customer information is stolen or lost, they run the risk of facing wide-spread negative publicity, lost business, expensive lawsuits and potentially large fines from the PCI Security Standards Council.

Our understanding of systemic security issues—based on PwC's experience

The most common way in which cybercriminals gain access to customers' payment card data or " track data" (the electronically encoded data on the magnetic stripe on the back of a credit card) is by installing electronic software "skimmers" on retailers' point of sale (POS) terminals. The skimmers are designed to collect the track data on the card's magnetic stripe as customers swipe their card to complete a purchase transaction. Capture of track data enables cybercriminals to create counterfeit cards by encoding the track data onto a new card with a magnetic stripe.

There are three key forensic questions for this type of attack: How do thieves gain access to the POS terminals and install skimmers on such a large scale, how do they exfiltrate the skimmed data, and how can they accomplish this while avoiding detection by security monitoring controls. If the theft includes collaboration with an insider—an unreliable and unmonitored employee, contractor, or vendor with authorized access to the retailer's POS infrastructure—then the insider would use both access and knowledge of the system to install the skimmer, establish the collection and exfiltration process and software, and either disable, circumvent, or otherwise remain under the visibility of security controls. If the thief is an outsider without authorized access, it is likely that the external actor will undertake the following in a coordinated, sequenced manner (based on our firm's experience with data breaches):

1. Initial intrusion (gaining access to the infrastructure by finding and then exploiting vulnerability in a system or device that was connected to the Internet, or taking advantage of a human error that led to a system configured in an insecure manner);
2. Reconnaissance (using the access to the infrastructure to probe the environment as a means of both developing an understanding of the security controls and identifying applications or business processes to target);
3. Attack (focus on the point of sale terminals, install tools to the appropriate part of the process to enable the attacker to capture and record credit and debit card transactions that were not encrypted);
4. Exfiltration (removal of captured information without detection); and
5. Remaining undetected (all these activities have to be conducted without being caught by the security controls within the environment).

It is important to understand that the timeline for these activities can vary greatly depending on the sophistication of the attack and, in many instances, can take place over months or even years. Initial reconnaissance and intrusion can be performed months before an actual "attack," thereby providing a window of opportunity to maximize the volume of sensitive data collected.

Key breach or incident indicators, identified early on in an attack sequence, can be used to minimize or avoid the compromising of the point of sale terminals (or the compromising of the central repository of point of sale transaction information). This highlights how advanced actors take a "low and slow" approach to circumvent sophisticated security monitoring and detection mechanisms and methodically escalate access over days, months, and even years until they reach systems of high value. Executives and key business leaders should always be mindful that they may already be in a state of compromise, and that threat actors wait patiently for the most opportune time or scenario to extract valuable data assets.

What is covered by an integrated audit on financial statements and internal controls over financial reporting?

Integrated audit

Cyberattack is not likely within the scope of an integrated audit. Specifically, independent auditors are required to perform periodic assessments of the effectiveness of the design and operation of a company's disclosure controls and procedures pursuant to Rules 13a-15 and 15d-15 of the Securities Exchange Act of 1934. One aspect of the integrated audit on financial statements and internal controls over financial reporting (integrated audit) is to assess whether a company maintains, in all material respects, effective internal control over financial reporting as of a point in time based on criteria established in the internal control—integrated framework issued by the Committee of Sponsoring Organizations of the Treadway Commission (COSO).

Third parties/third-party payment processor

Many third parties will have an **SSAE No. 16** (Statement on Standards for Attestation Engagements No. 16) undertaken by a service auditor to report on controls at organizations that provide services to user entities when those controls are likely to be relevant to the user entities' internal control over financial reporting. However, as these are controls related to financial reporting, they would likely not be designed to detect a typical cyberattack.

Additional considerations

Payment card industry data security standard

Payment card industry security for merchants and payment card processors is the result of applying the information security best practices in the Payment Card Industry Data Security Standard (PCI DSS). The standard includes 12 requirements for any business that stores, processes or transmits payment cardholder data. These requirements specify the framework for a secure payments environment; for purposes of PCI compliance, their essence is three steps: assess, remediate, and report.[1]

It is worth noting that many breaches have occurred on PCI systems that met or exceeded its standard. This could be for many reasons, but in our experience is mainly based on the magnetic stripe card, which is easier to clone and harder to control than the integrated circuit, chip-enabled EMV[2] card standard used in Europe, Canada, and Latin America. Stolen account numbers and other data are less monetizable for EMV cards, and thus less attractive to thieves using the skimmer approach. Fines from the PCI Security Standards Council can be significant.

1 https://www.pcisecuritystandards.org/security_standards/getting_started.php

2 Europay, MasterCard and Visa, a global standard for inter-operation of integrated circuit cards.

SEC October 13, 2011 Cybersecurity Disclosure Guidance and other disclosures
On October 13, 2011, the SEC issued Cybersecurity Disclosure Guidance, which calls for disclosure related to cybersecurity incidents in Management's Discussion and Analysis of Financial Condition and Results of Operations, as well as filings on Form 6-K or Form 8-K to disclose the costs and other consequences of material cyberincidents.[3]

Management, risk management, and internal audit—Constructing three lines of defense
To combat the ever-increasing attacks on companies' data, we recommend that companies institute and continually shore up three lines of defense:

1. *Management.* Companies that are good at managing information security risks typically assign responsibility for their security regimes at the highest levels of the organization. Management has ownership, responsibility, and accountability for assessing, controlling, and mitigating risks.
2. *Risk management and compliance functions.* Risk management functions facilitate and monitor the implementation of effective risk management practices by management, and help risk owners in reporting adequate risk-related information up and down the firm.
3. *Internal audit.* The internal audit function provides objective input (under consulting standards) to inform the board and executive management about how effectively the organization assesses and manages its risks, including the manner in which the first and second lines of defense operate. It is imperative that this third line of defense be at least as strong as the first two for critical risk areas: without a function that provides competent and objective input, a company faces the real risk of its information privacy practices becoming inadequate or even obsolete. This is a role that internal audit is uniquely positioned to fill. But to do so, it must have the mandate and the resources to match.

These three lines of defense are not unique to data privacy and security, but they should be in place and operating at a robust level to deal with any critical risk to the business. For most companies, information security and privacy is one of these critical risks because of its potential to cause financial and reputational damage and also because it is so difficult to mitigate.

3 http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm, Footnote 2.

What should boards and executives do in response to an event?

Boards and executives may go beyond the independent integrated audit process as a means of gaining comfort related to the quality and capability of the information security program within the respective company. Boards and executives may consider engaging in a process to understand what the external audits, third-party audits, internal audits, and governance, risk, and compliance reviews by management include, and what they do not include. The board may consider having a deep-dive risk assessment performed that would cover the broad IT risks, including—but not limited to—security, privacy, and IT risk.

Boards should also consider working closely with management to better understand what management is doing to understand and manage cybersecurity-related risks and opportunities. The board may also discuss with management to consider the use of cyberinsurance to offset a portion of the risk associated with cybersecurity. Finally, it is critical that management develop an integrated corporate breach response capability that is a ready-to-operate and repeatable business process, one that is cross-organizational in nature (given the potential impact on brand, reputation, and business relationships) and focuses on both internal response and external communications (to the media, clients, employees, business partners or other stakeholders).

Regulators often get involved in these types of events—what should executives know & how should they be prepared?

In the United States, numerous regulators watch for breaches and then investigate the victimized organizations. For example, State Attorneys General, the Federal Trade Commission (FTC), and the Office for Civil Rights often become active when cybercriminals attack. In one recent example, the FTC was watching closely and published articles immediately containing advice on how consumers should react and best protect themselves.

Because the FTC's mission is to "prevent business practices that are anticompetitive or deceptive or unfair to consumers…"[4] and because one of the FTC's strategic goals is to "prevent fraud, deception, and unfair business practices in the marketplace,"[5] the FTC often investigates companies that experience breaches and in some cases, enter into consent decrees with those companies, requiring them to design, implement, and maintain comprehensive information security and/or privacy programs, and have the effectiveness of those programs assessed by an independent third party for many (often 20) years. The FTC and other regulators often impose fines upon the breached organizations as well. Executives can better position themselves for such investigations by designing comprehensive information security and privacy programs before breaches occur, thereby enabling them to demonstrate good faith effort to the regulators.

4 http://www.ftc.gov/about-ftc

5 Ibid.

The risks discussed thus far relate to operations and compliance, but other enterprise risks must also be seriously considered. Many of the more sophisticated nation-state actors (see Figure 1 for a summary of actor types) target highly sensitive intellectual property, sensitive communications, or other strategic assets and information. Assurance and compliance standards also rarely address insider risks. These enterprise risks are not within the scope of the independent integrated audit, and, if compromised, there is no specific requirement to disclose to the investing public. However, if compromised, the risk could be significant to a business unit, product, or service.

Cybercriminal types—the president's executive order, and questions to consider

Last February, President Obama signed an executive order calling for a set of voluntary standards for cybersecurity that focused on critical infrastructure, including in banking and finance. In February 2014, the Department of Homeland Security (DHS) will release this set of standards, termed the Cybersecurity Framework. However, even its authors state that this comprehensive set of standards may not protect against sophisticated threats, such as those from nation-states and organized crime. This is the difference between compliance and security, and closing this gap requires action by boards and executives.

Figure 1: Profiles of threat actors

Malicious actors	Motives	Targets	Impact
Nation state	• Economic, political, and/or military advantage	• Trade secrets • Sensitive business information • Emerging technologies • Critical infrastructure	• Loss of competitive advantage • Disruption to critical infrastructure
Organized crime	• Immediate financial gain • Collect information for future financial gains	• Financial/Payment systems • Personally Identifiable Information • Payment Card Information • Protected Health Information	• Costly regulatory inquiries and penalties • Consumer and shareholder lawsuits • Loss of consumer confidence
Hacktivists	• Influence political and/or social change • Pressure business to change their practices	• Corporate secrets • Sensitive business information • Information related to key executives, employees, customers and business partners	• Disruption of business activities • Brand and reputation • Loss of consumer confidence
Insiders	• Personal advantage, monetary gain • Professional revenge • Patriotism	• Sales, deals, market strategies • Corporate secrets, IP, R&D • Business operations • Personnel information	• Trade secret disclosure • Operational disruption • Brand and reputation • National security impact

Boards and executives keeping a sustained focus on cybersecurity do more than protect the business: they reap bottom-line benefits. There are at least three areas an organization should initially consider when assessing their cybersecurity posture, posing questions that can be answered only at the executive level and above:

1. *Enhancing the cybersecurity strategy and capability.* Is an integrated cybersecurity strategy a pivotal part of the organization's business model? Does the strategy consider the full scope of security: technical, physical, process, and human capital? Has the organization applied the required resources and investments? Does the organization have the security capability to advise internal business leaders on critical threats, emerging technologies, and strategic initiatives? Can the organization explain its cybersecurity strategy to stakeholders, investors, regulators, and ecosystem partners?
2. *Understanding and adapting to changes in the security risk environment.* Does the organization know what information is most valuable to the business, as a function of its most important value drivers? Has the organization prioritized security to protect those assets accordingly? Has the organization quantified the business impact if the assets were impaired? Does the organization understand the significant changes in the threats facing its business? Who are the organization's adversaries? What would they target? What techniques might they use? What controls does the organization have in place related to the insider threat? Is the organization actively acquiring and adapting to internal and external sources of intelligence? Has the organization already been breached, and how would the organization know? How are the organization's controls and countermeasures responsive to events and activities? Is the organization actively involved in relevant public-private partnerships to gain further knowledge and understanding of the threats facing their industry? Does the organization routinely assess the state of its security controls? And finally, does the organization have a plan for addressing a security incident, and does it practice that plan?
3. *Advancing the security posture through a shared vision and culture.* Do the organization's employees understand their role in protecting information assets, and have they been provided the necessary tools and training? What assurances does the organization require from suppliers and service providers? Does the organization actively monitor, audit, and remediate its risk portfolio? Does the organization have standards in place to protect its assets throughout the ecosystem?

Recent events and the evolving threat landscape will undoubtedly put a renewed focus on point of sale and payment systems. However, executives should consider the above questions in the context of the entire retail value chain and the associated underlying IT systems. Specific attention on enhanced security safeguards has been placed on POS and payment system infrastructure for years due to industry operating standards, and these POS and payment systems are generally considered to be the most protected environments in a retail technology footprint; in fact, few, if any, other systems are treated with as much care from a data protection perspective. Many companies should be discussing the susceptibility of the rest of the technology ecosystem if the ultra-secure environment is capable of being compromised.

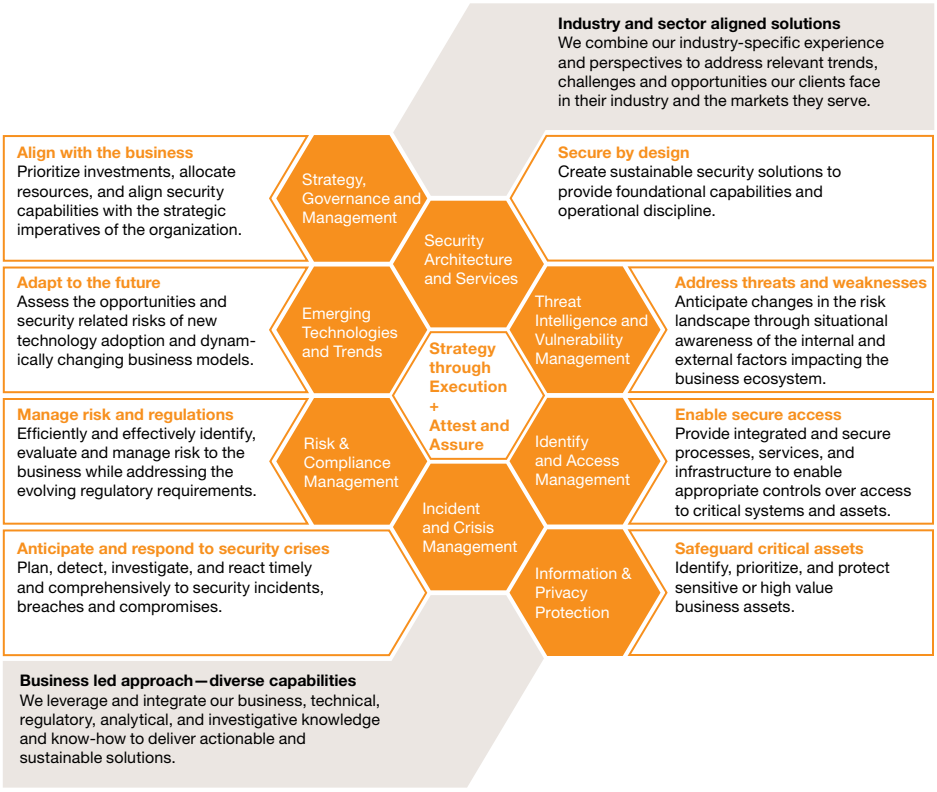
PwC's capabilities

PwC helps organizations understand dynamic cyber-challenges and breach/incident indicators to stay one step ahead of the threat actors, adapt and respond to risks inherent in their business ecosystem, and prioritize and protect the most valuable assets fundamental to their business strategy.

PwC's Cybersecurity Consulting Services is part of a practice that is consistently recognized as a market leader. By delivering innovative solutions today that help identify and protect against future threats, we enable organizations to adapt and respond to the dynamic cyber-risks inherent in doing business in a globally interconnected ecosystem.

A key issue moving forward, for corporate boards and executives as well as the president's cybersecurity initiative, is how to measure security: What standards can be measured and audited, and how can we link the results to actual security? Equally important is this question: How do we provide our corporate executives, board, and shareholders with transparency and visibility into enterprise cyber-risks, as well as other corporate risk?

Figure 2: PwC's Cybersecurity Consulting Services solutions*



*The range of services that PwC can provide will vary depending on whether the client is a restricted entity. In all cases there are capabilities that PwC can offer to our clients.

For more information

Visit ***www.pwc.com/cybersecurity***
Review the cybersecurity team's publications in the *PwC 365 App*.

Contact our Cybersecurity leaders:

David Burg
Principal
(703) 918-1067
david.b.burg@us.pwc.com

Michael Compton
Principal
(313) 394-3535
michael.d.compton@us.pwc.com

Peter Harries
Principal
(213) 356-6760
peter.harries@us.pwc.com

John D Hunt
Principal
(703) 918-3767
john.d.hunt@us.pwc.com

Gary Loveland
Principal
(949) 437-5380
gary.loveland@us.pwc.com

Joseph Nocera
Principal
(312) 298-2745
joseph.nocera@us.pwc.com

David Roath
Partner
(646) 471-5876
david.roath@us.pwc.com

www.pwc.com/cybersecurity