Cybersecurity challenges in an interconnected world

Key findings from The Global State of Information Security® Survey 2015

Introduction

Over the past year, the phrase “data breach” has become closely associated with the word “retailer” as attacks reached epic levels.

The most notable “mega-breaches” occurred in the US, where cyber compromises resulted in the loss of information for more than 100 million payment cards. The trend is not limited to America, however. In the UK, payroll and bank account numbers of 100,000 employees of a supermarket chain were stolen. And hackers employed a new version of the point-of-sale (POS) malware known as ChewBacca to pluck payment card data from numerous retailers in 11 nations, including Russia, Canada, and Australia.

Our research shows that retail and consumer goods companies are most likely to report cybercrime incidents than businesses from any other industry except financial services. These breaches have resulted in global negative publicity, loss of shareholder value, reduced profits, and millions of dollars in breach-mitigation expenses. They also may have eroded customer trust, which is indispensable to any retailer and brand. Our research shows, for instance, that concerns about the security of personal and payment data are top reasons why some consumers still do not shop online. These breaches have very likely increased shopper concerns about in-store security as well.

“Threats to retail and consumer goods companies continue to become more persistent and dynamic, and by all indicators these threats will only increase,” says G. Christopher Hall, an Advisory principal focused on cybersecurity and privacy. “Companies must step up their efforts to invest in security personnel, processes, and technologies that address holistic information security strategies and go beyond any industry-specific mandates.”

Labeling 2013 as “the year of the retailer breach,” Verizon counted 467 retailer compromises around the world in its annual Data Breach Investigations Report, noting that payment card data was the primary target in 95% of incidents within the retail industry.

1 Networkworld, Morrisons supermarket suffers major pay-roll data breach after insider attack, March 14, 2014.
2 Networkworld, Tor-enabled malware stole credit card data from PoS systems at dozens of retailers, January 30, 2014
5 PwC, Global Total Retail Survey 2014, February 2014
If there is an upside, it’s that the compromises have spurred stakeholders in the US payment card industry to move from the existing magnetic-stripe technology to EMV (short for Europay, MasterCard, and Visa), a more secure microprocessor-based standard that is less vulnerable to compromise.

The breaches have also increased awareness of cyber risks across industries and elevated the cybersecurity discussion to top executives and Boards of Directors.

While it’s no longer possible to protect all data, networks, and applications at the highest level, a proactive cybersecurity program will enable retail and consumer goods manufacturers to prioritize protection and more quickly react to incidents that are all but inevitable.
If there is an upside, it’s that the compromises have spurred stakeholders in the US payment card industry to move from the existing magnetic-stripe technology to EMV (short for Europay, MasterCard, and Visa), a more secure microprocessor-based standard that is less vulnerable to compromise.

The breaches have also increased awareness of cyber risks across industries and elevated the cybersecurity discussion to top executives and Boards of Directors.

While it’s no longer possible to protect all data, networks, and applications at the highest level, a proactive cybersecurity program will enable retail and consumer goods manufacturers to prioritize protection and more quickly react to incidents that are all but inevitable.
If there is an upside, it’s that the compromises have spurred stakeholders in the US payment card industry to move from the existing magnetic-stripe technology to EMV (short for Europay, MasterCard, and Visa), a more secure microprocessor-based standard that is less vulnerable to compromise.

The breaches have also increased awareness of cyber risks across industries and elevated the cybersecurity discussion to top executives and Boards of Directors.

While it’s no longer possible to protect all data, networks, and applications at the highest level, a proactive cybersecurity program will enable retail and consumer goods manufacturers to prioritize protection and more quickly react to incidents that are all but inevitable.
Incidents rise, while budgets fall

The number of detected incidents may be rising because many organizations have deployed network monitoring and logging technologies in recent years.

The Global State of Information Security® Survey (GSISS) shows that, among 836 worldwide retail and consumer goods respondents, the number of detected incidents in 2014 increased 19% over 2013. (We define a security incident as any adverse incident that threatens some aspect of computer security.)

While this proliferation undoubtedly reflects the increased activity of cyber adversaries, the number of detected incidents also may be rising because many organizations have deployed network monitoring and logging technologies in recent years. Use of these technologies will result in discovery of more incidents.

It’s also worth noting that adversaries appear to be targeting retailers more frequently than consumer products manufacturers. Consumer products companies detected an average of 2,065 incidents, fewer than the 3,447 incidents detected by retailers, and a decline of 14% over 2013.

Current employees (34%) and former employees (30%) account for the most incidents, with a notable increase in retail and consumer goods respondents who point the finger at current employees. We also saw a 27% jump in incidents attributed to third-party service providers, contractors, suppliers, and business partners, which often have trusted access to the company’s network and data.

While the total number of survey respondents who link incidents to sophisticated threat actors like nation-states, hacktivists, and organized crime are comparatively low, they are among the fastest growing sources. Respondents who cited foreign nation-states as the cause of incidents increased 115% in 2014.

Customer and employee data are the target of most incidents—not surprising, considering that threat actors often set their sites on payment card information. Among consumer goods manufacturers, theft of intellectual property (IP) is a larger concern. That’s because manufacturers often produce products for other smaller businesses, and they often store these clients’ IP and research and development information.

This year, one in four consumer goods respondents say they lost “soft” IP (information such as processes and institutional knowledge), a 27% jump over last year.
Despite the rise in detected incidents, retail and consumer companies report that total financial losses resulting from security incidents declined 46% in 2014.

This finding seems counter-intuitive, given the upsurge in detected compromises.

In part, the discrepancy may be attributed to a 61% rise in security spending in 2013, which may have enabled organizations to more quickly detect and mitigate incidents. What’s more, as businesses implement monitoring and logging technologies they will detect more incidents that are benign, such as viruses that do not result in costly damage.

It is troubling, however, to find that information security budgets are down 15% over 2013. Retailers cut their security investments more sharply than consumer goods companies.

The decline in security spending initially seems puzzling, given the recent high-profile breaches. It’s likely that organizations had finalized their 2014 budgets before December 2013, when the first mega-breach was announced. Afterward, some businesses we know revisited their budgets and reallocated more funds for cybersecurity. We expect to see a spike in security spending in the coming year.

### The fastest-growing sources of security incidents

<table>
<thead>
<tr>
<th>Source</th>
<th>Increase over 2013</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information brokers</td>
<td>54%</td>
</tr>
<tr>
<td>Organized crime</td>
<td>54%</td>
</tr>
<tr>
<td>Foreign entities and organizations</td>
<td>66%</td>
</tr>
<tr>
<td>Activists/hacktivists</td>
<td>67%</td>
</tr>
<tr>
<td>Foreign nation-states</td>
<td>115%</td>
</tr>
</tbody>
</table>
Data governance is lacking

Many businesses emphasize regulatory compliance at the expense of a framework that governs information.

Retailers, in particular, often take a compliance-checklist approach to information security, focusing on Payment Card Industry Data Security Standard (PCI DSS) requirements while disregarding implementation of adequate data governance to protect valuable information assets.

Good data governance will require that businesses develop a framework and policies for the creation, use, storage, and deletion of information. It will also demand that retail and consumer companies know where their data is stored, manage access to sensitive information, and govern the use and security of valuable data by third-party partners.

Attrition in data governance safeguards
A basic foundation of data governance is centralized data storage, which enables organizations to consolidate, manage, and secure their information.

This is becoming increasingly essential as the use of smartphones and social media accelerate the creation and sharing of data. Yet organizations seem to be falling short of fundamentals: Just 55% of respondents say they have centralized user data storage, down from 63% in 2013.

Other security basics include safeguards to limit access to data and systems, and monitoring for anomalous network activity.

Furthermore, many companies seem to know very little about the sensitive data they hold or allow third parties to access. Consider, for instance, that the number of respondents who say they have an accurate inventory of where personal data for employees and customers are collected, transmitted, and stored dropped to 54% this year, down from 60% in 2013.

A sound data governance program also will limit the data that is stored to only what is needed. It’s a practice that many do not follow: Only 54% say they limit the collection, retention, and access of personal information to the minimum necessary to accomplish a legitimate business purpose.
Increasing third-party threats
Data breaches often start with the compromise of suppliers, contractors, and vendors.

In the past year, several retailers that have been hit by costly, high-impact breaches have had one thing in common: Criminals gained access to their networks and POS systems through attacks on third-party suppliers and contractors, resulting in the compromise of millions of payment card accounts.

These breaches resulted in heavy financial and reputational losses, but they also encouraged some retailers to more rapidly migrate to the EMV system.

Today, very small percentage of payment and debit cards in the US employ EMV technology, which is more resistant to compromise and counterfeit than magnetic-stripe cards. That's changing, however, as several major card networks have begun migration to the chip-based EMV system and have set an October 15, 2015 deadline for implementation of EMV technologies. (Gas station owners will have until October 1, 2017 to migrate to EMV.) Thereafter, fraud liability will shift to the party that is not EMV-compliant.6

While retail and consumer companies are adopting the EMV standard, many have not yet taken more basic precautions to protect themselves from breach via the systems of third parties. Consider, for instance, that only 54% of survey respondents say they have established security standards for external partners, suppliers, and vendors. And just 44% conduct risk assessments on third-party vendors, down from 55% last year.

Furthermore, we asked if organizations have implemented or plan to implement a program that monitors third-party partners and service providers to ensure they comply with security and data-protection policies.

The responses are not encouraging:

Only 29% say they have this type of monitoring program in place, and 37% say they plan to add one.

But one in five say they have no plans to implement a program to monitor third parties.

An effective vendor-management program will require more than individual policies and processes, however.

What’s also needed is a tiered framework that assesses, segments, and manages third-party partners based on the risks they present to the business. This is critical because large organizations may have thousands of vendors that have access to their systems and data; a tiered approach will help them focus on the most serious risks.

This tiered approach also will enable organizations to hold third parties to different levels of accountability. For instance, businesses that share sensitive information of customers with external marketing partners should ensure that those firms adhere to the very highest level of security, while those that have access to less sensitive information need not be held to the most rigorous standards.

6 PwC. Securing the card payments infrastructure: Where are we headed? July 2014
Retail and consumer

Cybersecurity challenges in an interconnected world // Key findings from The Global State of Information Security® Survey 2015

Key safeguards for third-party security and privacy are lacking

- Established security baselines/standards for external partners/customers/suppliers/vendors
- Require third parties to comply with privacy policies
- Have an inventory of all third parties that handle personal data of employees and customers
- Have incident response process to report and handle breaches to third parties that handle data
- Perform risk assessments on third-party vendors

Increasing third-party threats

2013
2014
2013
2014
2013
2014
2013
2014
2013
2014

60% 54% 59% 51% 52% 49% 55% 48% 55% 44%

Contacts

Introduction

Incidents rise while budgets fall

Data governance is lacking

New technologies and their risks

Toward a more strategic approach

Linking security and risk
New technologies and their risks

Retail and consumer goods companies are embracing new technologies to connect with customers, build operational efficiencies, and enable collaboration.

The trouble is, many businesses adopt these technologies before they effectively secure them.

Consider cloud computing, perhaps the decade’s most transformative technology trend.

More than half of respondents say they use some form of cloud computing for file storage and sharing, and hosting of databases, applications, e-mail, and websites.

Yet only 45% of respondents have a security strategy for cloud computing—an astonishing finding—and just 33% say they are “very prepared” to protect sensitive data in the cloud. Given that 29% of respondents say they use cloud services for e-commerce, that’s certainly disquieting.

Mobility continues to transform how companies and their employees operate. The use of mobile devices also introduces new risks, including data loss, device theft, and accidental leakage. In fact, 23% of respondents say mobile devices were exploited this year. While many retail and consumer companies have made progress in strengthening their mobile security practices, there remains considerable room for improvement. For instance, only 51% say they have a mobile security strategy, and fewer (43%) use mobile device management software to safeguard their fleet of mobile devices.

Another risk lies in the rise in employee use of personal devices in the workplace, a trend known as bring your own devices or BYOD. This year, 69% of respondents either plan to allow or already do allow use of employee-owned devices to access the corporate network, yet most organizations are ill-prepared to secure their assets. The number that have a security strategy for BYOD dropped to 49% this year, down considerably from 2013.
As workers become increasingly more mobile, employees access the network, data, and applications remotely via laptops, smartphones, and tablets. So it was worrisome to find that the number of respondents who have secure remote access software like virtual private networks is low and shrinking: Only 56% have this essential technology, down from 69% in 2013.

Another technological juggernaut is social networking, which enables retail and consumer companies to attract and engage customers, improve the customer experience, and manage brand images. The benefits are many, but so are the risks.

Employees can inadvertently disclose sensitive data via social networking sites, and cyber criminals can mine accounts to obtain valuable information that can be used in targeted phishing attacks. Despite these very real risks, only 45% of respondents have a security strategy for social media, a number that decreased considerably over last year.

Finally, this year’s game-changing technology may be mobile payment systems or “digital wallets.” The capability to make payments from smartphones is not new, but it is gaining momentum as more devices support payment systems like Apple Pay, the Merchant Customer Exchange (MCX) CurrentC, and Google Wallet. And given the recent rash of retailer breaches, consumers may prefer to whip out their smartphones and leave their payment cards in their wallets.

It’s worth noting, however, that no payment system will be 100% secure. Determined threat actors will very likely find ways to circumvent technologies that underpin digital payment systems. In fact, compromises already have been reported.

The success of mobile payments will require a wide constellation of retailers that are capable of accepting these digital payments, of course, and that’s not yet a given. One-quarter (25%) of retail and consumer respondents say they have implemented systems for digital wallets, and an additional 36% say they plan to implement them in the future.
Toward a more strategic approach

Our survey results show that many retail and consumer companies need to take a more strategic approach to help identify, manage, and respond to privacy and security threats.

In many cases, commitment to strategic security safeguards seems to be diminishing.

It all starts with an information security strategy that is aligned with the specific needs of the business. This year, 59% of respondents say they have united their security strategy and business goals. An effective security program also should apportion spending to the data assets that have the highest business value. Respondents show a more solid, if incomplete, commitment in this area: 67% say their security investments are allocated to the organization’s most profitable lines of business.

Before resources can be allocated, however, it will be necessary to first identify the organization’s most valuable assets and determine who owns responsibility for them. This is an area in which we found significant potential for improvement: Only 52% of respondents have a program to identify sensitive assets.

Strategic processes are often lacking

A senior executive communicates importance of security to entire enterprise

Information security strategy is aligned with specific business needs

Program to identify sensitive assets

Collaborate with others to improve security

Have cyber insurance

Have employee security training and awareness program
An effective security program will require top-down commitment and communication of information security fundamentals and priorities.

Organizations have made some progress in this measure: 61% of respondents have a senior executive who communicates the importance of information security to the entire enterprise.

Information security communications also must cascade upward to the Board of Directors to ensure that members have the information they need to manage risks and protect the company from cyber adversaries. Boards are increasingly concerned about having the right risk intelligence, and they may also be worried that their personal reputations could be tarnished by a high-profile compromise. Earlier this year, several directors of a prominent retailer came under public scrutiny after the company suffered a very public data breach that also resulted in the resignations of several C-suite executives.

Despite the discussion following recent retailer breaches, many companies have not yet elevated security to a Board-level discussion. Consider, for instance, that only 39% of respondents say their Board participates in the overall security strategy, and 35% say the Board participates in the security budget. Fewer (22%) say their Board is involved in reviews of current security and privacy risks—a crucial component of any effective security program.

Many organizations are finding that cyber insurance can be an effective way to help manage risks and mitigate financial losses of cyber attacks. It has been widely reported, in fact, that several retailers breached over the past year recovered tens of millions of dollars in mitigation costs through insurance coverage.

This year, 50% of respondents say they have purchased cybersecurity insurance, up from 40% last year.

Perhaps more significant is the finding that some companies are leveraging cyber insurance as a way to improve their security program. Almost one-third say they have taken steps to enhance their security posture in order to lower insurance premiums.

Finally, sharing information about security—internally and externally—is essential to the success of security programs as cyber threats, technologies, and vulnerabilities evolve at lightning speed. Employee training and awareness is particularly important because the weakest link in the security chain is often human. So it was a bit worrisome to find that the number of respondents who have an employee training program in place dropped to 49%, from 59% in 2013.

Externally, sharing information among public and private entities has enabled businesses to gain better intelligence on threats and response tactics. To this end, US retailers recently formed the Retail Cyber Intelligence Sharing Center (R-CISC) to serve as an Information Sharing and Analysis Center (ISAC) as well as a forum for education, and training and research on future threats. Among our survey respondents, more than half (52%) say they share security intelligence and tactics. That’s an improvement over last year. Consumer packaged goods companies may not have a dedicated ISAC, but they tend to share information more readily. Among consumer products respondents, 65% say they collaborate with others to improve security.

More than ever, senior executives should proactively ensure that the Board understands how the organization will detect, defend against, and respond to cyber threats.
Linking security and risk

As incidents continue to proliferate, it’s becoming clear that cyber risks can never be completely eliminated.

Protective measures remain important, but they may not stop determined and highly skilled adversaries.

Case in point: Most of the retailers impacted in recent data breaches were compliant with PCI regulations.

In addition to regulatory compliance, effective cybersecurity will require up-to-date processes, trained personnel, and tools to detect, analyze, and respond to incidents.

To make this adjustment, retail and consumer companies should reposition their security strategy by more closely linking technologies, processes, and tools with the firm’s broader risk-management activities. Doing so will result in a cyber-resilient program that can effectively manage risks based on the business’s individual tolerance for risk.
Contacts
To have a deeper conversation about cybersecurity, please contact:

United States

- **Alexander Coassin**
  Principal
  415 498 5292
  alexander.t.coassin@us.pwc.com

- **G. Christopher Hall**
  Principal
  412 355 6183
  g.christopher.hall@us.pwc.com

- **Ron Kinghorn**
  Principal
  617 530 5938
  ron.kinghorn@us.pwc.com

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

- **Bryan Oberlander**
  Principal
  617 530 4125
  bryan.a.oberlander@us.pwc.com

- **Paul Ritters**
  Director
  612 596 6356
  paul.j.ritters@us.pwc.com

www.pwc.com/gsiss2015 // www.pwc.com/cybersecurity

PwC helps organisations and individuals create the value they’re looking for. We’re a network of firms in 157 countries with more than 195,000 people who are committed to delivering quality in assurance, tax and advisory services. Tell us what matters to you and find out more by visiting us at www.pwc.com.

PricewaterhouseCoopers has exercised reasonable care in the collecting, processing, and reporting of this information but has not independently verified, validated, or audited the data to verify the accuracy or completeness of the information. PricewaterhouseCoopers gives no express or implied warranties, including but not limited to any warranties of merchantability or fitness for a particular purpose or use and shall not be liable to any entity or person using this document, or have any liability with respect to this document.

© 2015 PwC. All rights reserved. PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity. Please see www.pwc.com/structure for further details.

The Global State of Information Security® is a registered trademark of International Data Group, Inc.