Deloitte.

Cyber risk in retail

Protecting the retail business to secure tomorrow's growth

Table of contents

Foreword

Years 2013 and 2014 saw an unprecedented level of cyber assault on retailers. Several major breaches hit the headlines and retailers reported tens of millions of customer data and credit card records exposed. Despite widespread attention to payment card industry (PCI) compliance, cyber criminals have clearly taken retailers by surprise.

Regardless of whether an organization has been breached, there is an almost universal perception that such an event may be imminent, that companies are ill prepared, and that the problem needs to be addressed thoroughly. This has led to a decisive shift among retail organizations. There is a growing recognition that cybersecurity has an impact on a larger universe of business risk, and "security" programs are no longer the sole purview of Information Technology (IT) departments. Ownership for a more comprehensive approach to security has moved to business leaders themselves.

"If we focus on the particular threat, identify what we know about it, and go after the gaps [in our capabilities], we can be successful."

In response to both the general sense of alarm and the shifting cybersecurity landscape, Deloitte undertook two projects over the summer of 2014 to gather information and facilitate practical dialogue on how to move forward. The first of these was a 65-question survey on the current state of retailers' cyber risk and security programs, including investment and governance priorities. Forty organizations, representing a diverse range of large and mid-size retail companies, participated in the survey.

The second project was a first-of-its-kind Retail Cyber Risk Leadership Forum that brought together 85 Chief Executive Officers (CEOs), Chief Financial Officers (CFOs), Chief Information Officers (CIOs), Loss Prevention, General Counsel, and Chief Information and Security Officers (CISOs) from more than 45 retail and distribution organizations, along with leaders from government, law enforcement, and supporting service organizations, for two days of practical discussion and collaboration. As Alison Kenney Paul, Vice Chairman and US Retail & Distribution Leader of Deloitte LLP, noted in her opening remarks, "Despite heightened attention and unprecedented levels of security investment, the number of cyber incidents and their associated costs continue to go up. No retail or distribution organization is immune."

Yet, according to Robert Mueller III, former director of the Federal Bureau of Investigation (FBI), there are reasons to be optimistic: "I'm not one of the naysayers who says that [the cyber attackers] are so far ahead of us that we can't catch up," he said. "If we focus on the particular threat, identify what we know about it, and go after the gaps [in our capabilities], we can be successful."

This report summarizes four key themes that emerged from the two initiatives. It also outlines actions that retail organizations can take near term to mitigate cybersecurity risk, and concludes with a set of issues that call for future research, dialogue, and collaboration.

Four issues come to the fore

Recent cyber attacks indicate that retailers have become a coveted target for cyber criminals, hackers, and others. These small, highly skilled groups of actors are exacting disproportionate damage by exploiting weaknesses that are byproducts of business growth and technology innovation. While organizations have begun to focus attention and resources on combatting cyber risk, the issue is not going away. In fact, all evidence points to a problem that is growing ever-more challenging, as it shape-shifts to elude those that attempt to address it.

According to Ed Powers, principal and National Cyber Risk Services leader at Deloitte & Touche LLP, there are several important reasons that conspire to make the problem of cyber risk especially thorny. The first is that public networks were designed to share information, not protect it. Additionally, a significant amount of organizational risk derives from human factors—employees and third parties. Also, cyber risk and business performance are closely related. The very things organizations undertake to grow tend to exacerbate cyber risk.

Art Coviello, Executive Vice President, EMC Corporation and Executive Chairman of RSA who presided over RSA's response to the theft of their intellectual property in 2013, acknowledged the difficulty of addressing cybersecurity in the retail sector, noting "You are in one of the toughest industries in the world—high volumes, razor thin margins, competitive advantages derived through marketing and technology." He went on to say "I don't think it's a stretch to suggest that there is a pandemic with respect to retail industry cyber attacks."

Nevertheless, digital integration and innovation are critical to the future of retail. In fact, e-commerce is where most of the growth is today. Retailers need to think about their digital assets as more than just ways to increase online shopping, and design them to support shoppers' in-store experiences as well. Addressing the issue of cyber risk is integral to that process, because as digital becomes more and more pervasive, risks will only skyrocket.

A synthesis of dialogue at the Forum and data from the survey revealed the following four key themes that characterize the state of cyber risk programs and the cyber risk issues facing the retail and distribution sector.

- Compliance does not always equal risk management
- Breach response readiness is top of mind as companies scramble to shore up detection
- External intelligence will play a crucial role in the war against cyber threats
- Cyber risk is a business issue

"The threats are obviously becoming more sophisticated. Because of the innovation [retailers] deliver to reach customers—omnichannel approaches, social media, efficiency efforts—the way we work is very different than other industries, and the way we worked a decade ago. While that presents great opportunities, it also raises the stakes of the game. That's why we need to work together."

—Alison Kenney Paul, Vice Chairman and US Retail and Distribution Leader, Deloitte LLP

I. Compliance does not always equal risk management

Regulations have been essential in ensuring at least a foundational security capability—prompting security investments that may not have been made without a mandate. While they provide a starting point for protection of information and breach preparedness, an exclusive focus on compliance may result in a sense of complacency that can blind executives to serious cyber risk gaps.

As Ed Powers summed up during his presentation at the Forum, "When we focus on security alone, we naturally tend toward a compliance-oriented approach, a checklist approach. But that doesn't equate to risk management. And it doesn't address the fundamental risks that we're talking about."

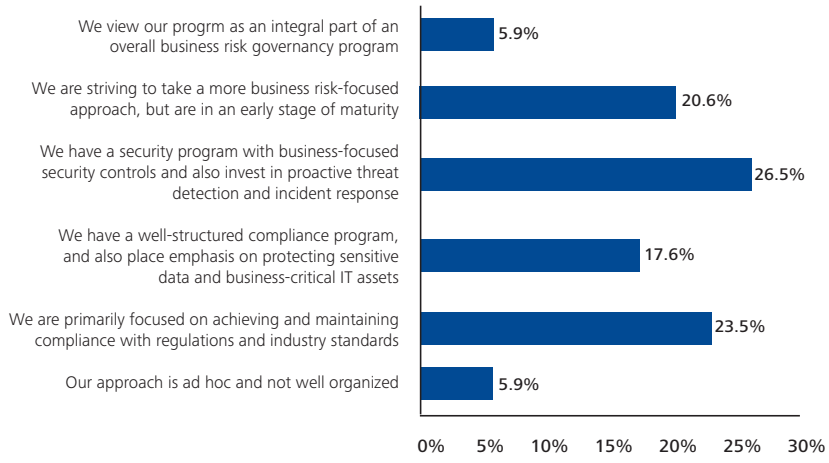
There is a growing awareness that compliance is the bare minimum for combatting cyber threats, and that retailers need a more proactive approach, geared toward the industry's changing risk posture. The Deloitte & Touche LLP Cyber Risk survey corroborates this: Most leaders feel that regulatory and standards requirements are only "somewhat effective" in reducing security breach exposure (71%) and improving cyber risk posture (80%).

Nevertheless, achieving compliance is no small feat, given profitability pressures, talent shortages, and other challenges. While more than 90% of survey respondents feel they have senior executive support to effectively address regulatory or legal compliance requirements, more than half indicate that additional funding would help to improve their current programs.

Requirements continue to become more stringent and, as organizations diversify and extend their reach, the regulatory environment becomes increasingly complex. The perpetual acceleration of regulatory pressures may be what motivates 86% of survey respondents to review their security policies against laws and regulations at least annually. Despite the maze of compliance challenges, there are several indicators that program drivers for retailers may be shifting more toward a business risk-focused approach.

Retailers seem to be setting their objectives higher.
More than 55% of respondents describe their mission as achieving business-aligned or risk-aligned programs, signifying that companies are recognizing that a compliance-based approach may no longer be adequate. A middle set of companies are working toward a greater business-critical asset focus. Less than 25% say they are focused narrowly on compliance.

Figure 1: Mission of your company's cybersecurity or cyber risk program

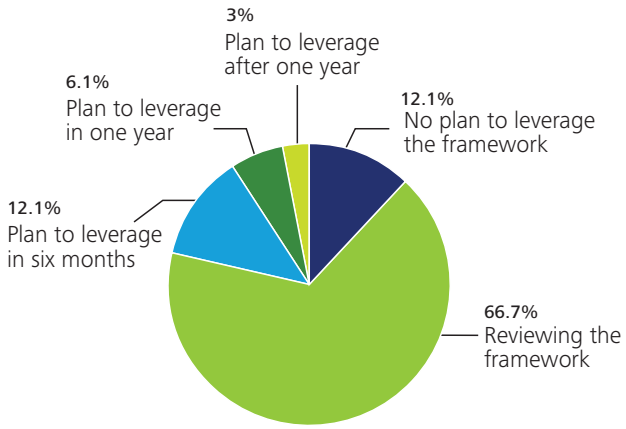


Source: Retail Cyber Risk Survey, Deloitte & Touche LLP, November 2014

When asked about the mission of their company's cyber security or cyber risk program, more than 70% of respondent organizations indicated they are striving for some degree of business alignment.

"Leading practices" standards are a significant frame of reference for the security or cyber risk program. While PCI is a universal guidepost for retailers, ISO27001/2, the System Administration, Networking, and Security Institute (SANS) Top 20, and Control Objectives for Information and Related Technology (COBIT) are commonly used (each by roughly one-quarter to one-third of respondents). Most notable is the broad interest in the National Institute of Standards (NIST) Framework for Improving Critical Infrastructure Security (CIS), released in February of 2014, which focuses on using business drivers to guide cybersecurity activities and which advocates addressing cybersecurity risks as part of the organization's risk management processes. More than 20% of respondents are already using the NIST Framework for CIS to guide their programs, and two-thirds are currently reviewing it.

Figure 2: Companies' plans to adopt the 2014 NIST Cybersecurity Framework



Source: Retail Cyber Risk Survey, Deloitte & Touche LLP, November 2014

Security/risk assessments and data protection initiatives outrank compliance as top program initiatives.
Other areas of focus for retailers include development of disaster recovery and business continuity programs, monitoring and security operations capabilities, and incident response—all areas that suggest greater focus on detection and response capabilities, than on preventive controls.

Figure 3: Identify your company's top five program initiatives for 2014

Source: Retail Cyber Risk Survey, Deloitte & Touche LLP, November 2014

II. Breach response readiness is top of mind as companies scramble to shore up detection

Regardless of the industry, the odds of preventing all cyber incidents are not good for complex organizations. Robert Mueller summed up the dilemma for retailers when he said: "We have to be right all the time; the bad guy only needs to get it right once." Historically, most retailers have focused their attention on traditional controls to secure assets. The focus now is on keeping an eye out for the bad guys (being vigilant) or preparing to respond and bounce back (being resilient) in the event of an actual breach.

What do retailers worry about most?

It is clear where the crown jewels are for retailers: 100% of survey respondents indicated that theft of customer data is their primary concern. Secondarily, respondents pointed to regulatory fines or breach-related costs, as well as financial fraud.

When asked about the three most worrisome sources of attacks, respondents cited organized criminals, disgruntled employees or former employees, and accidental misuse by authorized users as "somewhat high" or "very high" threats.

According to Forum presenter Adnan Amjad, partner at Deloitte & Touche LLP, insider threats (threats caused by disgruntled employees) can sometimes be more damaging than external threats, because those who carry them out are frequently malicious or hold a grudge. Amjad cautioned that while there are internal threat detection tools available, they do not constitute programs: "Insider threat detection is about people, not about technology."

Top considerations for breach response

- Appoint someone to lead incident response—a "breach czar" who can live and breathe the details, a team player with the political capital to push for tough decisions.
- Establish external support relationships—with law enforcement, legal and PR firms, and incident response service providers.
- Engage in scenario planning—and rehearse—before there is a breach.
- Assume a breach might be made public beyond your control. Have different iterations of holding statements (the company's formal acknowledgement of the breach) prepared in advance.
- Have the right person deliver the message—the appropriate business owner for your organization.
- Learn from other companies' experiences.
- Don't crucify your IT department—you need them.

When it's over, digest the results and adapt your breach response protocols to reflect the lessons learned.

How prepared are retailers?

A number of Forum panelists and participants discussed several key aspects of cyber preparedness: 1) the ability to detect incidents; 2) a business-centric response plan; 3) teams that are ready and able to execute that plan; and 4) putting in place cyber insurance, if appropriate, to mitigate some of the business impact.

Retail Preparedness

The following survey data shed some light on the degree to which retailers are prepared

- Investment in continuous security event monitoring is one of the top five areas of investment, suggesting that many companies have identified deficiencies.
- 80% have documented incident response plans and 20% admit to either having no incident response plan or an ad hoc one.
- Even when they do have preparedness plans, organizations may not be proactively reviewing, providing training for, or rehearsing their plans. Cyber war-game simulations have only been conducted by 23% of survey respondents.
- Despite challenges finding and retaining talent, more than 80% of companies handle incident response internally rather than outsourcing. More than 45% are retaining an outside firm in order to access talent as needed, and another 20% plan to engage one within the coming year.
- 57% of respondents have some kind of a cyber insurance ranging from less than $5m to more than $100m.

While the survey results show that most companies do have incident response plans, Forum discussions revealed that they likely need to evolve their plans so that they are better able to minimize the effects of a crisis. Several Forum panelists shared first-hand accounts of real-world cyber crises. A common thread across all these cases was the importance of strong business leadership during the response period. Participants acknowledged that companies are sometimes not even in control of when a public disclosure happens. In the past, companies had three to 60 days to respond. Today they might have less than 48 hours before someone else publishes the news. From a customer management perspective a cyber incident is something of a loyalty test, one that is inevitably played out via social media, rapidly magnifying brand and reputation damage.

A cyber war-game simulation exercise conducted on the second day of the Forum helped to highlight the importance of having—and rehearsing—a business-led incident response plan that includes legal counsel, Chief Executive Officer (CEO), Chief Compliance Officer (CCO), Chief Risk Officer (CRO), Chief Information Officer (CIO), Chief Technology Officer (CTO), and Chief Marketing Officer (CMO), as well as representatives from public relations, loss prevention, store operations, and potentially other functions. While technical teams are crucial in analyzing the events and supporting the decision-making process, the degree of business impact a breach causes depends on how quickly and effectively the organization acts to protect various aspects of the business, as well as how it handles interactions with customers, regulators, law enforcement, suppliers, the media, and other stakeholders.

III. External intelligence sharing will play a crucial role in the war against cyber threats

One of the major themes throughout the Forum was the need for greater collaboration and information sharing regarding cyber threats. Information sharing, said Ed Powers, is the "holy grail" of threat intelligence. It needs to become an ongoing aspect of threat management—both among retailers and distribution companies, and with public sector agencies. Sharing information is not just important once a crisis is underway—it is critical for understanding the industry-wide trends that ultimately shape a sound cyber risk program.

Eighty-six percent (86%) of survey respondents indicated that information sharing falls within the purview of the CISO's role, but the general sense among Forum participants was that few organizations are actively collaborating. Most companies are reluctant to share because of intellectual property, confidentiality, or regulatory concerns. Information sharing tends to begin when there is a triggering event that shakes the entire industry.

Failure to share information can have serious repercussions. Time and again, cyber attackers have been able to take advantage of companies' natural competitiveness and their tendency to hold any information about breaches close to the vest. One participant, talking about a breach that had occurred at his company, said they discovered in hindsight the rippling impact of the information-sharing gap. It turned out that many companies had been breached using precisely the same tactics within a short time frame. As the participant said, "they just picked us off one by one."

Also referencing the need to overcome the competition barrier, another individual agreed: "This is not something we want to happen to our competitors—because if it could happen to them, it can happen to us."

The industry is responding to the need to facilitate collaboration and information sharing. For example, the National Retail Federation (NRF) has established an IT Security Council to foster better networking and collaboration and to share timely security information through a regular webinar series. The council also works with organizations like the Financial Services-ISAC, Department of Homeland Security, and the US Secret Service and has established a Retail Threat Alert System designed to push critical information related to cyber incidents, threats, and vulnerabilities to its members. NRF, Retail Industry Leaders Association (RILA), and American Apparel & Footwear Association (AAFA) also participate, in an advisory capacity, in the nascent Retail Cyber Intelligence Sharing Center (R-CISC) organization.

Threat intelligence is more than a feed

- If your security organization is decentralized, start with internal threat information sharing between groups.
- Participate in industry intelligence sharing communities where you can.
- If competitive interests are an inhibitor, consider establishing information sharing with partners and suppliers.
- Reach out to local and federal law enforcement; know which relationships will help you be prepared, and where to go in a crisis.
- Put threat feeds in context by providing analysts with the tools they need to be effective.

"Information sharing is the holy grail of the intelligence piece. But how do you get to the point where organizations offer information rather than just consume it? Most industries advance when there's a triggering event—an event that leads organizations to start to establish trust."

—Ed Powers, principal, Deloitte & Touche LLP

There is a tendency, according to Mary Galligan, director, Deloitte & Touche LLP and former FBI Special Agent in Charge of Cyber and Special Operations, New York Office, for the private sector to expect that the government can and should provide more threat information, but in reality, it needs to be a collaborative process. Executives are surprised to learn that at least 40% of breaches are identified by a third party, such as a law enforcement agency, a financial institution or a telecommunications carrier. This tends to lead some to suspect that law enforcement may not be sharing information in its entirety. But in many cases, she said, the government sees only one piece of the puzzle. Arriving at a more complete picture often requires the company to combine third-party information obtained from the government with their own internal information.

There are challenges, however, that can dampen collaboration with law enforcement. Reporting a breach can result in numerous adversarial legal actions. Companies may have to ultimately defend themselves in government investigations. The current lack of immunity, Galligan noted, is a significant inhibitor of public/private collaboration. Incentive to share is further weakened by the fact that government agencies are often not in a position to reciprocate in sharing information.

Only time will tell if we can develop better methods of sharing information with companies and if companies will be more open to sharing information with one another.

"By 2020, I don't think it's a stretch to suggest that you won't be able to protect physical infrastructure any more. Obviously, we cannot keep doing things the way we've been doing them. We need a different approach. If we can spot anomalies in human behavior or in the Internet of Things, and we can spot anomalies in the flow and use of data, then we can respond timely enough to prevent loss. This is where security is headed."

—Art Coviello, Executive Vice President, EMC Corporation and Executive Chairman of RSA

IV. Cyber risk is a business issue

The engagement of senior executives in the Forum is indicative of the greater attention being paid to cyber risk at the leadership level. Board members are becoming more concerned about breach preparedness, and have gone from focusing solely on compliance to asking hard questions about what can be done to truly minimize risk and prevent crises and demanding that business leaders update them regularly. More than one-third (37%) of survey respondents cite a requirement to report to the board on a quarterly basis, and 43% report that often to the CEO. But despite growing executive concern, and despite the number of organizations that describe their program missions to be business-aligned, there are some indications that organizations still have further to go in establishing the dialogue, governance, and reporting to actualize this goal.

- Routine weekly and monthly reporting on cybersecurity or risk posture is mainly directed toward the CIO.
- 44.1% never report to business stakeholders.
- A combined 70% say they either don't track program metrics, or use technical metrics that are not aligned to business value. Only 6% say they have business-aligned metrics and report on a regular basis.
- 63% of the respondents either don't have a documented cyber program strategy or don't have their strategy document approved.
- 71.4% cite lack of sufficient funding as a primary barrier to more effective program execution. While resource constraints can't magically be eradicated, this high percentage may indicate that decision makers do not see a financial justification for investing in these programs.
- Over 25% cite lack of support from business stakeholders as a barrier, suggesting that many business stakeholders may not be as engaged in the conversation as they need to be.

The situation may be improving somewhat. While funding may never seem adequate, 48.6% saw their budgets increase this year by at least 6%. When asked to name their top program priorities, only 40% name compliance initiatives among them, indicating that regulatory issues may be loosening their grip as the major program driver. There are several indicators that illustrate a shift in focus:

- 71% said they plan to conduct a cyber risk or security assessment.
- Many organizations are investing in capabilities relating to threat detection (23%), security event monitoring (34%), and incident response (31%).
- Over one-quarter are focused on strategy; 23% say they are focused on governance; and an equal number are focused on metrics.

Source: Retail Cyber Risk Survey, Deloitte & Touche LLP, November 2014

In fact, risk metrics were such a hot topic at the Leadership Forum that an impromptu session was added to the agenda. According to Kiran Mantha, principal, Deloitte & Touche LLP, ″Metrics and key risk indicators, when tied in a meaningful way to business risk, can provide actionable insight, and can help create a common language between technologists and business leaders on the state of enterprise security and technology-associated risk.″

Of course, having robust metrics doesn't equate to a business-driven cyber risk program, but the fact that so many retail leaders are seeking guidance on how to establish meaningful metrics may be an indication that they are moving toward more accountability and alignment in their companies' cybersecurity programs. This is a much-needed shift; only 3% of survey respondents said they're focused on aligning program initiatives with the business, which may explain why support from business stakeholders may be lacking for some.

For a security program to truly be a business enabler, lowering the cyber risks associated with strategic innovations will need to become a fundamental part of the program, guided by business leaders. Survey data indicates that some organizations are placing a priority on "security related to technology advancements," such as mobile technologies and migration to cloud computing.

The survey also indicates that more than 70% are concerned about attacks originating from social engineering (e.g., phishing, pharming), suggesting that an organization's weakest link may be the human factor and that retailers need to be creative about cyber risk awareness. There has to be awareness, education, and training throughout the organization to combat cyber risk. One may have top-notch hardware and software to protect against cyber intruders, but it might take only one unaware employee opening an attachment with malicious software to shut down the organization's systems. The Forum participants agreed that the tone in combating this really does start at the top, with the board, CEO, and the CFO setting the governance and the organizational structure and making sure all employees are aware of their role in preventing cyber attacks. They echoed the need to incentivize openness, collaboration, and consider activities like war-gaming, digital applications, or other creative ways to raise awareness across the enterprise.

Engaging business and executive leadership

Effective next steps will vary for each company, depending on current level of maturity, organizational complexity, and culture. Some actions to consider might include:

Undertake a cyber incident simulation.
Testing the ability of the top leaders to respond to a staged attack can identify areas for improvement. The greatest initial outcome may be to wake people up to the complex challenge and importance of preparedness. Simulations can create an emotional "hook" that motivates people to be more engaged in an ongoing cyber risk program.

Put innovation under the microscope. The next time you build a new application or digital service, require that a cyber risk report be submitted before finalizing the project plan. Ensure that the plan adequately addresses key risks before work begins. Mandate progress reports, and establish change management processes to enforce periodic risk evaluation once the initiative is rolled out. Identify key risk indicators associated with the innovation, and use this as a pilot for ongoing reporting requirements.

Develop key risk and performance indicators. When communicating cyber risk, security leaders should highlight the most serious risks the business faces and the methods the organization is employing to manage them. One way to achieve this is to shortlist the top cyber risks your company faces and the risk indicators that signal your company's level of exposure to them. Additionally, one can identify whether your key risk indicators are trending up, down, or remaining flat quarter over quarter. It is also critical to explain how the company is managing security risks and keeping them within acceptable limits.

Hold a cyber risk heat mapping session. Bring senior business leaders together with threat intelligence experts with the goal of identifying the top areas of cyber risk. This can serve to both generate decisions on key areas of focus, or to begin an ongoing education and dialogue. Through the process, leaders may emerge who can spearhead pilot projects or play an ongoing role in building a corporate education program.

Emerging directions

The retail sector may look back on this past year—what some have called the Year of the Retail Breach—as a catalyst for a more risk-focused approach to cyber security. Both the survey and the Forum reflect what seem to be significant shifts:

Cyber risk management is more than keeping hackers at bay

Both the survey and Forum reflect significant shift in organizations' strategies. In 2015, there is widespread awareness that compliance, while essential in shaping a foundation, should not define the cyber risk program. In addition to continued focus on improving protection controls, there needs to be greater emphasis and investment in threat detection and incident response preparedness. Organizations should consider expanding risk management around cyber to guard against not just external malicious breaches, but also inadvertent internal breaches and third-party partner breaches. Further, retailers must build the cyber risk strategy as a component of business strategy with a more active focus on establishing a business-aligned cyber risk initiative.

Talent crisis will continue making it harder for retailers to address cyber threats

More than 70% of survey respondents identified skills gaps as a barrier to addressing existing and foreseeable threats. The top factors negatively affecting their ability to develop, support, and retain cyber security professionals include inadequate salary and promotion structure; lack of a defined career path; and higher salaried positions outside the organization. As cyber threats increase in sophistication and become more evasive, the demand will increase for highly skilled analysts. As innovation continues, organizations will need security professionals who can help them rapidly adjust to the security requirements of new technologies. In other words, the problem is likely to get worse, not better. Organizations need to take a strategic approach to sourcing decisions and vendors to evolve solutions that can help rapidly fill the gap.

A move towards cohesive payment security strategy

As merchants and issuers try to move from magnetic stripe transactions to chip-based transactions, cost of conversion is a critical factor. While timelines and mandates for this conversion continue to evolve, the payment landscape is also changing. While the sector is currently focused on the costly conversion of magnetic stripe transactions to other forms, there needs to be an acknowledgment that it is not the panacea. Everyone agrees that it is important to address current challenges, but one needs to ask the question as to how effective the current initiatives and safeguards will be in the years to come as digital takes over the payments. The dialogue needs to expand to developing a broad secure payments strategy that covers all retail channels.

'Data science' movement within retail to transform how retailers detect infiltrations and threatening activity

As the web of connectivity between retailers, distributors, and customers becomes increasingly more complex and mobile, and as threats become more elusive, detection approaches that rely on signatures and predefined correlation rules will become increasingly ineffective. The marketing side of many organizations actively leverage Big Data analytics to better understand and reach customers. Organizations should consider applying similar analytic approaches to threat detection, along with developing sophisticated correlation and analysis capabilities from a variety of data and threat sources.

Improved collaboration and information sharing

Retailers have taken the first steps in establishing an information sharing center. While one can understand the myriad of legal complexities an organization may face to share information, one can agree that such intelligence is of paramount importance for defense against cyber attacks. Retailers could benefit from greater collaboration across the industry, as well as with government, to protect the industry as a whole, despite competitive interests.

Adoption of emerging standards and better overall program governance practices

The survey data indicates that besides PCI and ISO 27001/2, the most common standards referenced are the SANS Top 20 and the new NIST Framework for CIS, indicating greater threat-focused programs. Some of these standards, while voluntary in nature, can help define how to identify, protect, detect, respond, and recover from cyber threats. While there is ongoing debate on whether NIST Framework for CIS or some other regulation should be mandated for retailers, the hope is that it will become a baseline leading practice for companies to use in assessing legal exposure to cyber risks. Organizations should consider increased adoption of such emerging practices to promote better program alignment between technical and business teams and drive an internal culture shift. Further, organizations must aim to better define roles and cultivate a shared cyber risk language.

Cyber aware workforce and customer

Survey data indicates that 54% of respondents provide cyber security training to employees and contractors based on job or function. Organizations should continue investments to train the workforce on good security practices and handling emerging threats. Also, in this age of big data and digital marketing, where organizations are building detailed profiles of individual consumers based on a plethora of data sources, even a single data breach can substantially damage consumer trust. With this in mind, organizations should consider being proactive in cultivating positive consumer perceptions of their data privacy and security practices to help offset their unease. One may even consider going the extra mile to educate their customers on being safe online by offering tips via various channels.

For more information, please visit
www.deloitte.com/us/retailcyberrisk

For more information, please contact:

Alison Kenney Paul
Vice Chairman and
US Retail and Distribution Leader
Deloitte LLP
+1 312 486 4457
alpaul@deloitte.com

Kiran Mantha
National Retail & Distribution
Cyber Risk Leader
Deloitte & Touche LLP
+1 212 436 6155
kmantha@deloitte.com