Turnaround and transformation in cybersecurity: Retail and consumer

Key findings from The Global State of Information Security® Survey 2016

The frequency of data breaches against retail and consumer products companies shows no signs of slowing. In fact, organizations detected 154% more incidents in 2015 than the year before, according to The Global State of Information Security® Survey.

The good news? Retail and consumer companies are taking decisive action to bolster their cybersecurity capabilities. Many are moving to strengthen their cybersecurity posture by implementing technologies such as cloud-based cybersecurity, advanced authentication and Big Data analytics. What's more, the vast majority—90%—have adopted one or more risk-based cybersecurity frameworks to help enhance security capabilities.

Another measure of progress is a willingness to invest in cybersecurity. This year, average information security spending soared 67%. Given the rash of high-profile breaches, it was not surprising that companies boosted security spending; the real challenge, however, may be achieving sustained results from these investments.

Securing payment channels

Many organizations are focusing on improving the security of payment channels. In the US, companies were rushing to complete the migration to the EMV (Europay, MasterCard and Visa) standard for payment card systems as we prepared this report. When participants took the survey in May and June of 2015, 63% said they expected to meet the October 2015 deadline for adoption of the new chip-based payment system.

In addition to the EMV migration, retail and consumer companies said they also were exploring other technologies and processes to protect customer data. Many are focusing on advanced technologies such as point-to-point encryption, next-generation firewalls and tokenization. Others are working to enhance security processes for payment cards and mobile payment systems, as well as improve employee security training programs.

Addressing risks of business partners

Assessment of the security capabilities of third-party business partners—cloud providers, in particular—has emerged as a top priority for many retail and consumer companies. This year, 68% of respondents said they assess third-party cloud providers to ensure compliance with security and data-protection policies. Most said they conduct assessments twice a year or more frequently.

Many are using risk-based security frameworks to improve third-party cooperation. These guidelines can help companies more easily exchange information with third-party business partners and suppliers, and communicate expectations and concerns about services that are being provided. Others are monitoring third-party security through the use of Big Data analytics, which respondents said delivers improved understanding of internal and external threats and enhanced visibility into network activity.

The elevated roles of the CISO and Board

Internally, businesses are expanding the roles of the Chief Information Security Officer (CISO) and the Board of Directors to improve understanding of cyberthreats and help build resilient risk-based cybersecurity capabilities.

Today's CISO is a senior business manager with experience in communications, risk management and overall business objectives. For instance, 41% of survey respondents said their CISO communicates information security risks and strategies directly to executive leaders, and 34% said CISOs deliver quarterly updates to Boards, which are increasingly engaged in security

In fact, we saw double-digit gains in Board participation in most aspects of information security. Almost half (47%) said their Board participates in the overall information security strategy and 46% said the Board is involved in discussions on security budgets. The latter may account, in part, for the sizable increase in security budgets this year. Other benefits of Board participation include support for an organizational culture of security and an improved ability to identify and communicate key risks.

pwc

How retail and consumer organizations are responding to rising cyber-risks

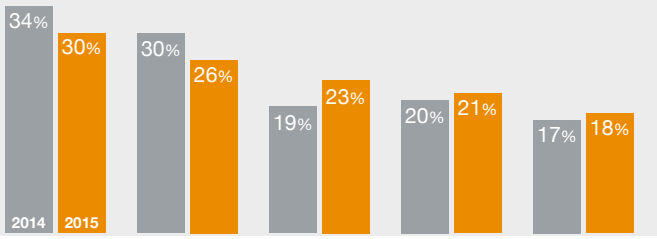
72%

While employee and customer records remain the top targets of cyberattacks and continue to increase, damage to brand/reputation was up **72%** in 2015.

154%

In 2015, the number of detected security incidents skyrocketed **154%** over the year before.

The number of respondents who attributed security incidents to employees dropped over the year before, while those who cited current service providers/consultants/contractors increased.



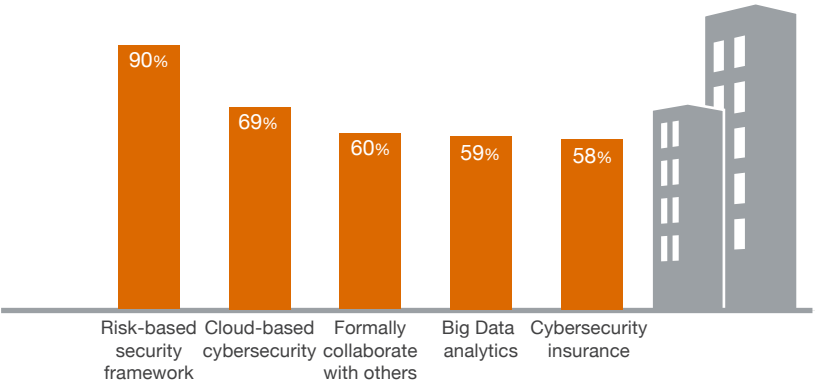
159%

Estimated financial losses as a result of all security incidents soared **159%** over the year before.

67%

After a decline last year, respondents boosted their information security budgets by **67%** in 2015.

Many organizations are implementing strategic initiatives—such as risk-based frameworks and cloud-based cybersecurity—to improve security and reduce risks.



Businesses are investing in core safeguards to better defend their ecosystems against evolving threats.

For a deeper dive into the 2016 Global State Information Security Survey findings go to pwc.com/gsiss or contact:

Alexander Coassin
Principal, Cybersecurity and Privacy
alexander.t.coassin@pwc.com

Bryan Oberlander
Principal, Cybersecurity and Privacy
bryan.s.oberlander@pwc.com

PJ Ritters
Principal, Cybersecurity and Privacy
paul.j.ritters@pwc.com

Source: The Global State of Information Security® Survey 2016