Forbes insights

Retailers Struggle To Keep Up With Cybersecurity Threats

In association with

vmware®

Nowhere is the disruption of the digital economy being felt more severely than with retailers.

Many existing store chains are threatened with extinction as executives struggle to achieve the right balance between having an online and a brick-and-mortar presence. E-commerce, online shopping and online transactions are only increasing, and in-store transactions, supply-chain interactions and payment processes are becoming highly digitized. This digitization of all phases of retail makes for an exponentially expanded attack surface for hackers and other malicious actors.

"In retail, the rise of e-commerce has meant both new opportunity for companies willing to adapt as well as increased cyber risk," says Gregg Garrett, head of U.S. and international cybersecurity and retail sector specialist for BDO USA. "Unfortunately, the retail industry has yet to make sufficient investments in its cybersecurity policies, plans, procedures and methods of defense, especially with respect to supply chain partners. Yet the average cost to respond to a cyber data breach in retail continues to climb each year, as does the average cost of cyber liability insurance coverage."

Retail organizations are particularly vulnerable to financial cybercrimes, according to Michael Coden, managing director and head of the cybersecurity practice at BCG Platinion. "The attractiveness of retail companies to financial criminals is the ability to quickly monetize the exploit or compromise," he says. "Digital skimmers, for example, allow financial criminals to gain payment information undetected by websites or consumers. The only evidence is the eventual fraudulent purchases made with a consumer's credit card, but most consumers do not check their bills or detect these fraudulent transactions. An additional problem for retailers is the high turnover of employees, which makes it very difficult to provide sufficient cybersecurity awareness training, and makes them more susceptible to phishing attacks than any other industry."

To better understand how organizations are approaching cybersecurity, Forbes Insights surveyed 1,001 security practitioners and security executives, in partnership with VMware. Data from this survey, which covers a range of industries, is presented in our report "Cybersecurity Trailblazers Make Security Intrinsic To Their Business," which also outlines how organizations can improve their enterprises' security posture.

This brief details the findings among the 213 retail respondents. Where appropriate, retail results are contrasted with the overall sample.

The average annualized cost of cybercrime to retail organizations is estimated at $9.3 million.[1]

[1] "Cost of Cyber Crime Study," Accenture, June 26, 2018.

“In retail, the rise of e-commerce has meant both new opportunity for companies willing to adapt as well as increased cyber risk.

Unfortunately, the retail industry has yet to make sufficient investments in its cybersecurity policies, plans, procedures and methods of defense, especially with respect to supply chain partners.”

Greg Garrett,
Head of U.S. and International Cybersecurity,
BDO USA

The Situation

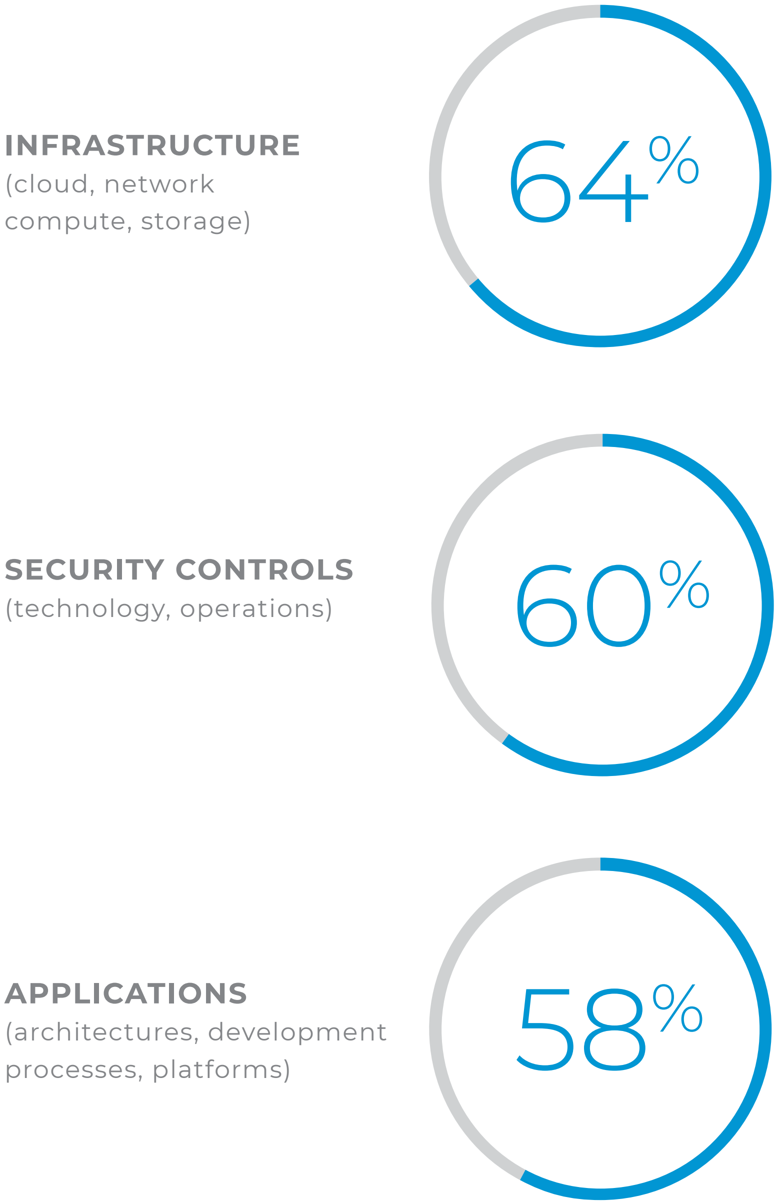
THE SITUATION

While an intense focus on e-commerce and customer experience is transforming retailers from the outside, much of this transformation is being seen internally as well. A majority of retail executives say infrastructure, security controls and applications have significantly changed in recent years as a result of digital transformation (Figure 1).

This has profound implications for cybersecurity, with a greatly increased attack surface and a need to view security through a new lens. “The rise of technology has flipped the traditional rules of business on their head, forcing retailers to reinvent themselves and reimagine business strategies,” says Garrett. “In today’s world, industries are blurring together as technology infiltrates and interconnects them all. To a certain degree, then, there are more companies—and customers—for hackers to target, and more pathways through which to target them.”

FIGURE 1

Retail Enterprise Areas Seeing Transformational Change



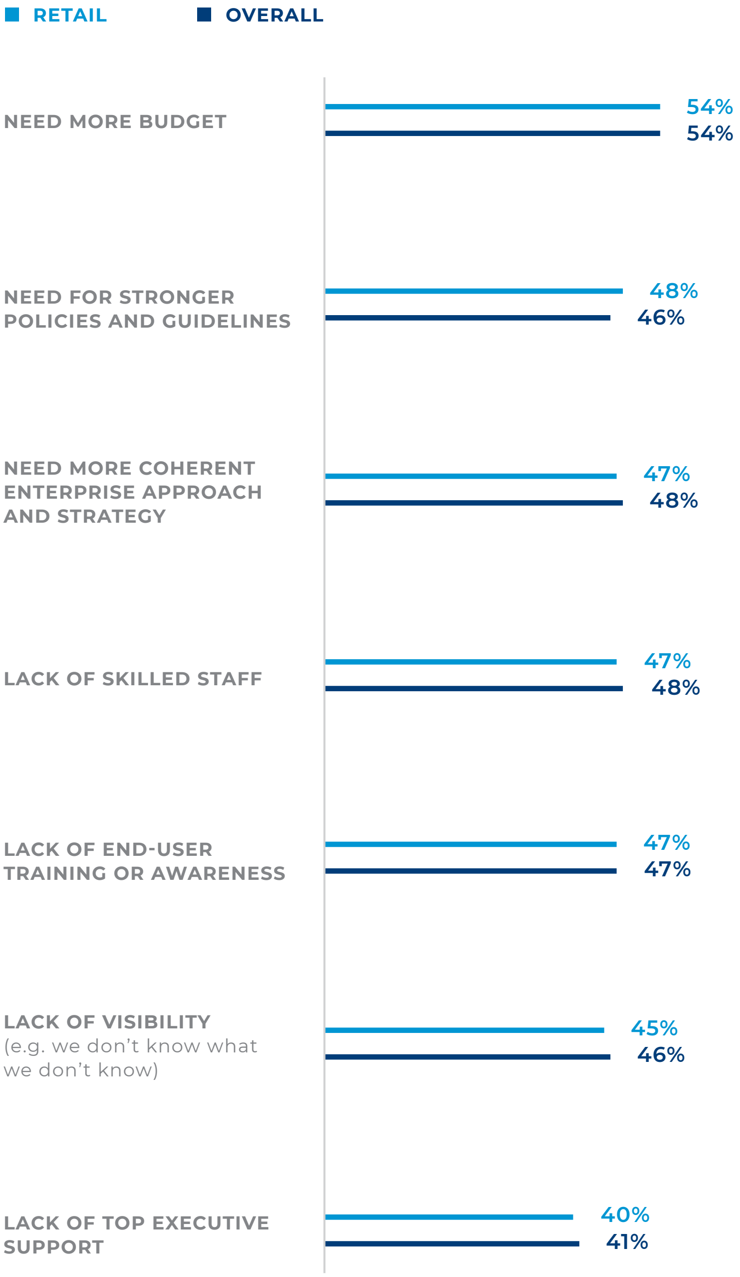
The main organizational challenge retail executives face with their cybersecurity strategies mirrors that of their colleagues from other industries—finding enough funding to move forward with their initiatives. More than half of retailers, 54%, say the need for budget is the biggest factor hampering cybersecurity efforts. In addition, close to half, 48%, cite a need for strong policies and guidelines for their efforts; a similar percentage of retail executives say their efforts need a more coherent enterprise focus (Figure 2).

54% of retailers say the need for budget is the biggest factor hampering cybersecurity efforts.

FIGURE 2

Retail Cybersecurity Organizational Pain Points

(Represents/highly represents)

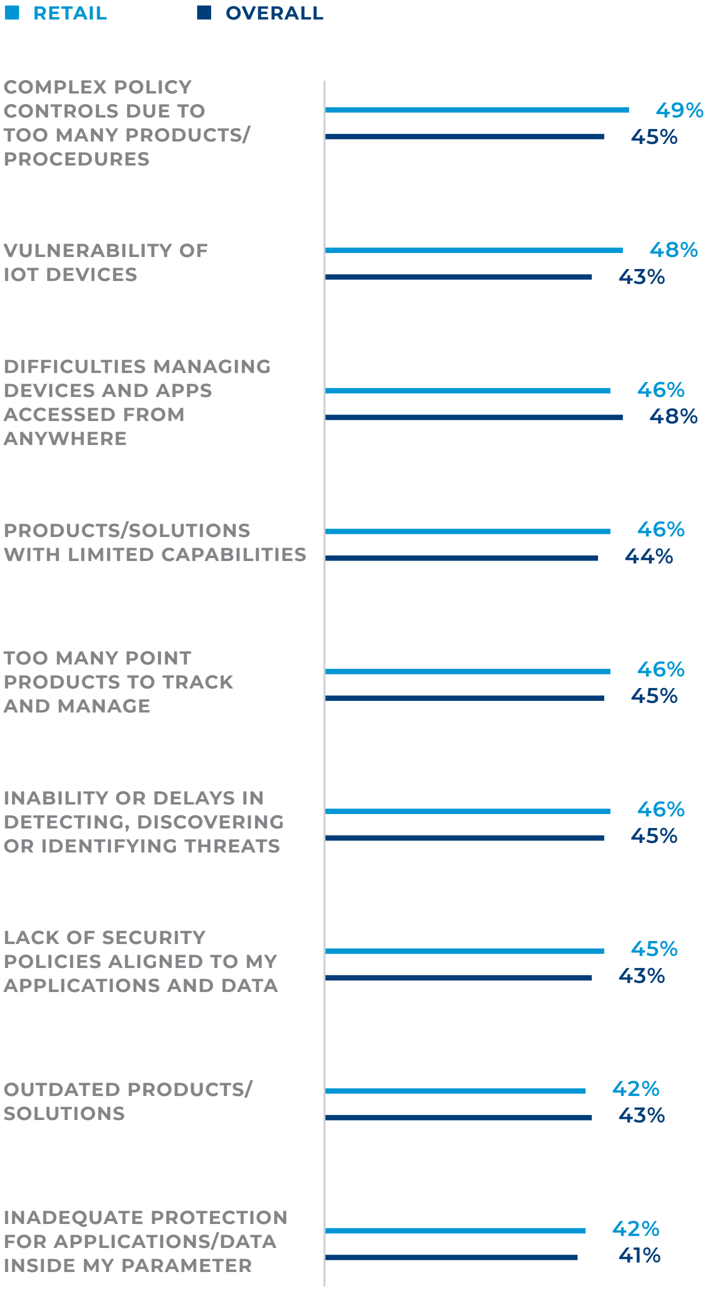


On the technical side, the effects of widening networks and increasing complexity are creating challenges for cybersecurity teams. Close to half, 49%, cite complex policy controls as a major pain point, and a similar percentage of respondents say vulnerability of IoT devices is a technical concern (Figure 3).

FIGURE 3

Retail Cybersecurity Technology Pain Points

(Represents/highly represents)

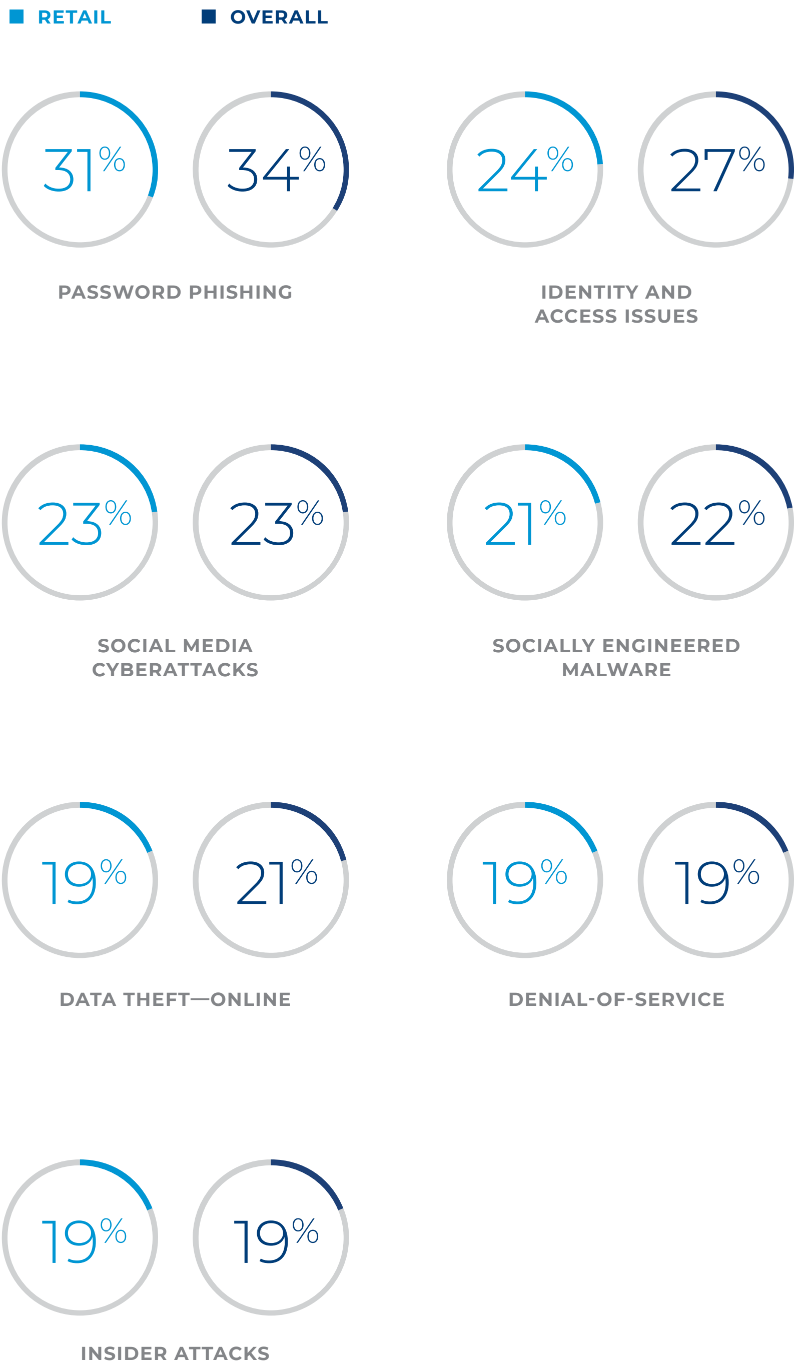


The leading threats to retail environments come from issues at the end-user level. Password phishing has been the most often-seen threat within retail organizations, cited by close to one-third (31%). Identity and access issues have also been experienced over the past three years. These issues have been seen somewhat less frequently within retail than in industries overall, the survey finds. Social media cyberattacks are also a frequent source of incidents, seen at close to one in four retail organizations (Figure 4).

For retailers, cybersecurity threats will continue to come from many different directions, Garrett points out. “Online retailers, and brick-and-mortar shops that process payments electronically, house mounds of consumers’ financial data,” says Garrett. “This data is susceptible to theft by cybercriminals who exploit unsecured—and unprepared—retailers and trade personal information for money on the dark web. As we’ve seen with numerous high-profile retail breaches, a major vulnerability lies within the supply chain, or rather, the weakest link in it. Hackers will target a retailer’s supply chain partners to try and pinpoint the weakest link and then enter the retailer’s network through that to steal sensitive information.”

FIGURE 4

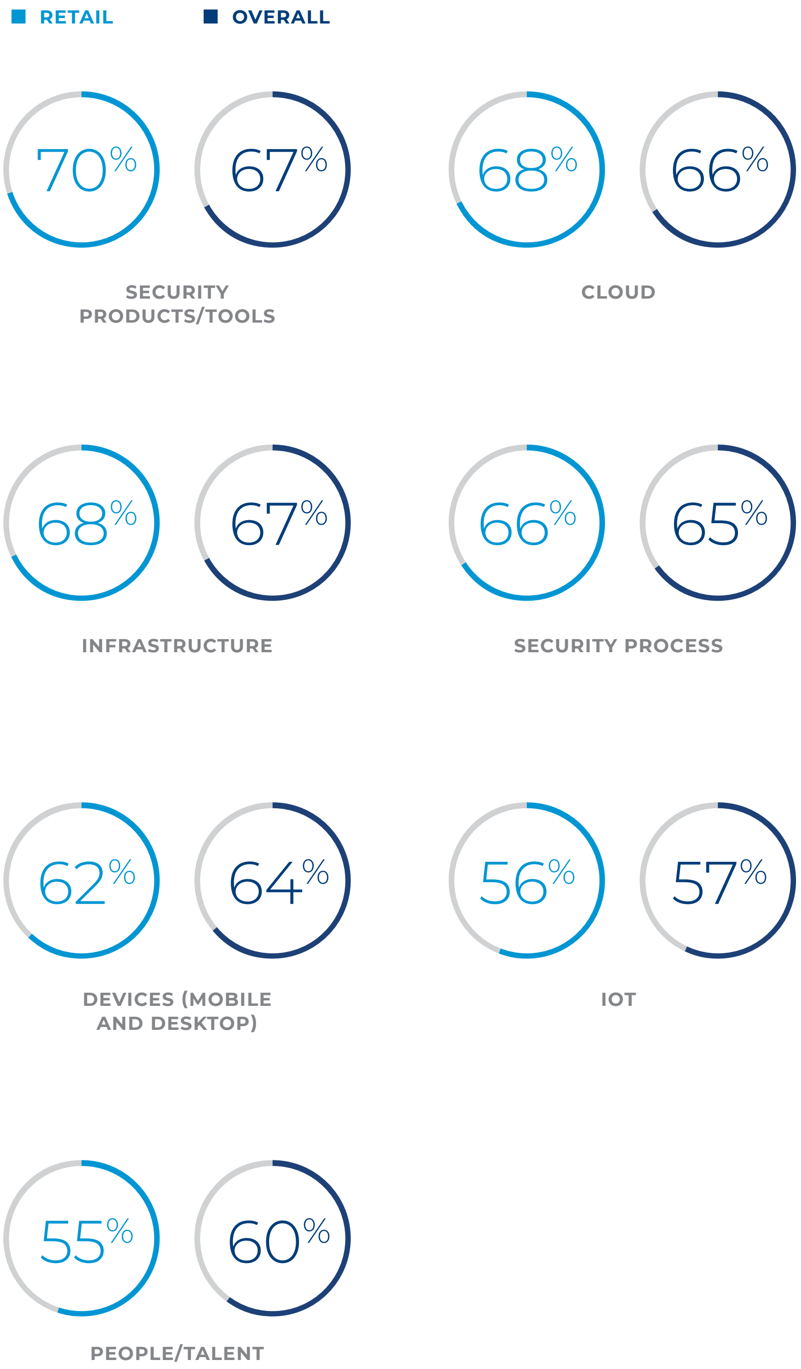
Top Incidents Experienced Over The Past Three Years



While exposures are increasing, a majority of retail respondents feel they are ready to meet these challenges—at least on a technical level. Retail leaders are most confident their security products are prepared to address emerging security challenges, cited by 70%. There is also a high level of confidence in both cloud and infrastructure, cited by 68%. However, retail executives express the least confidence in IoT and their own talent. This points to the need to formulate more holistic strategies that address the awareness and active participation of people within retail organizations (Figure 5).

FIGURE 5

Confidence In Addressing Emerging Security Challenges



The Technology

Retail respondents express a high level of confidence in the tools and services that address cybersecurity requirements, and they are ahead of the curve when it comes to implementing important technology solutions. Retail has a high focus on a zero-trust policy for application behavior, devices and access—71% of retail executives report having such policies, versus 66% across all industries.

Retailers also are more likely to be baking security into processes. Only 33% of retail executives fully involve their security organizations in decisions across their tech stack from the start. While this is still a higher number than the overall sample (25%), it's notable that two-thirds of retail organizations do not inherently build security into their technology-driven processes.

Retail has a high focus on a zero-trust policy for application behavior, devices and access—

71% of retail executives report having such policies, versus 66% across all industries.

To a large extent, many security functions within retail are being subsumed by cloud providers, the survey shows. More than three-quarters (78%) of retail executives say cloud providers handle some or many security measures (Figure 6). Retail respondents are most inclined to use cloud for web gateway services (74%), and the use of cloud for load balancing is also widespread (72%) (Figure 7).

However, there is still confusion among retailers about the role of cloud, Coden states. “What many organizations do not understand is their responsibility in using cloud. A cloud service provider is only providing a secure data center, secure servers and an up-to-date patched secure operating system. It is the responsibility of the retail company to provide all application security, all data security—encryption in transit and at rest—and all access control security,” he says. “Too many recent security compromises are because retail companies put systems onto clouds but did not encrypt the database, or did not keep their own encryption keys secure, or kept their backups in the same data lake as the original data, or other mistakes in not taking responsibility for everything above the operating system.”

FIGURE 6

How Cloud Adoption Has Changed Security Strategies

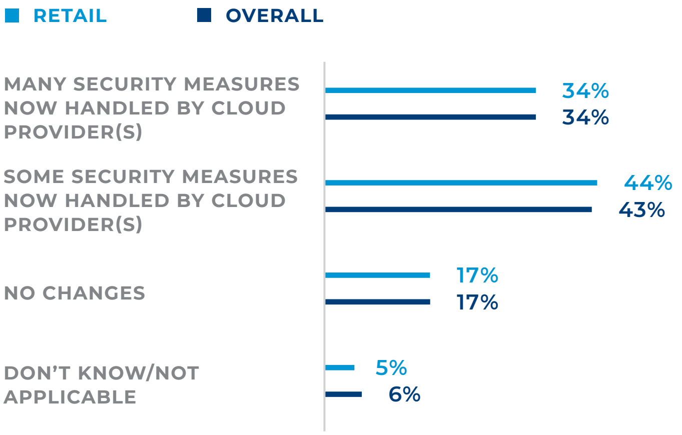
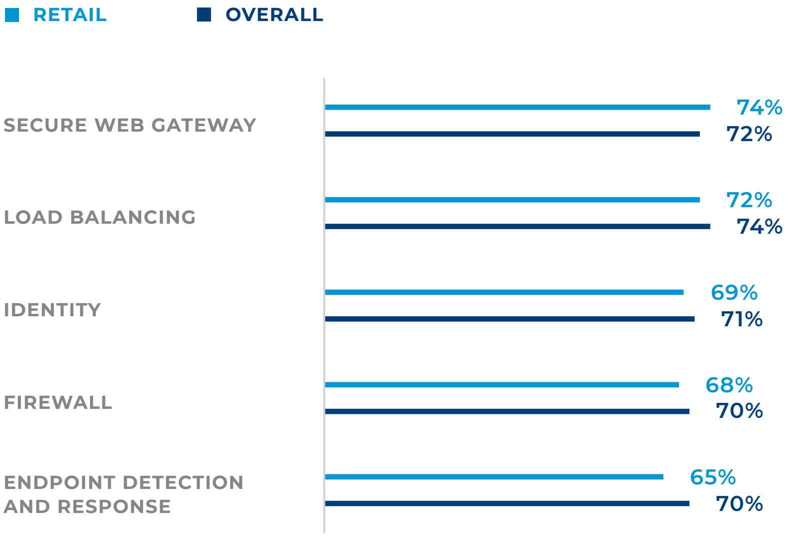


FIGURE 7

Security Services Provided By Cloud Providers

(Partially or in full)



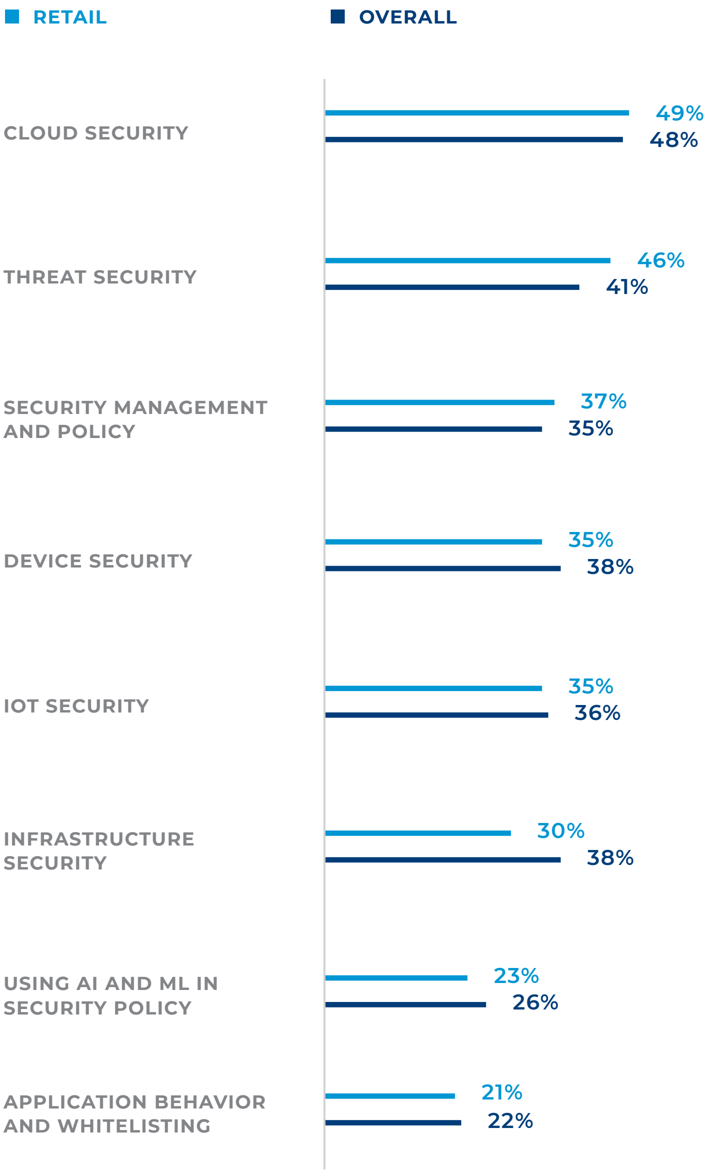
> “What many organizations do not understand is their responsibility in using cloud. A cloud service provider is only providing a secure data center, secure servers and an up-to-date patched secure operating system.
>
> It is the responsibility of the retail company to provide all application security, all data security— encryption in transit and at rest— and all access control security.”

Michael Coden,
Managing Director and Head of the
Cybersecurity Practice, BCG Platinion

With retailers' reliance on cloud providers, it makes sense that retailers are focusing their future investments on the cloud as well. Cloud security is the leading investment focus, borne by close to half of retail respondents. Threat security—the ability to guard against hackers—will also see greater investment, cited by 46%. Notably, retailers are less inclined than their counterparts across other industries to see artificial intelligence (AI) and machine learning (ML) as tools to manage their security environments. Twenty-three percent of retailers plan to integrate AI and ML into their security infrastructures, compared with 26% overall (Figure 8).

FIGURE 8

Top Areas For Security Investment Over The Next Three Years



The People & Processes

Retail organizations experience response times to security issues similar to industries across the board, the survey shows. Close to half of retail respondents, 48%, report being able to identify and resolve security incidents within one business day, while 52% report it takes longer (Figure 9).

There is a sizable segment of retail executives who want things to move faster when it comes to resolving such issues. More than one-third, 35%, report they are not, or are only somewhat, satisfied with their companies' ability to address security threats in a timely manner (Figure 10).

FIGURE 9

Length Of Time To Resolve A Security Issue

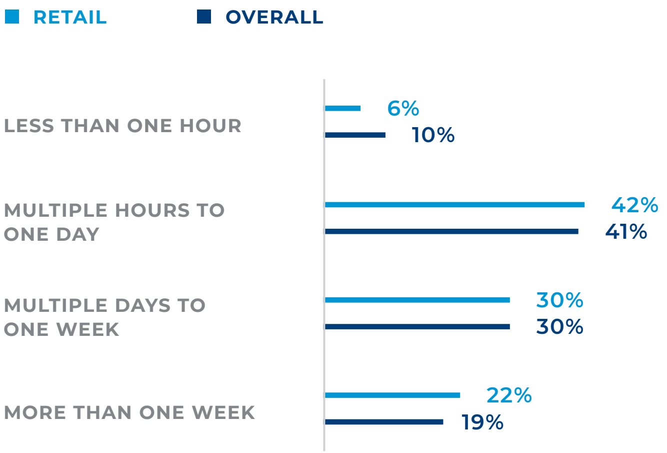
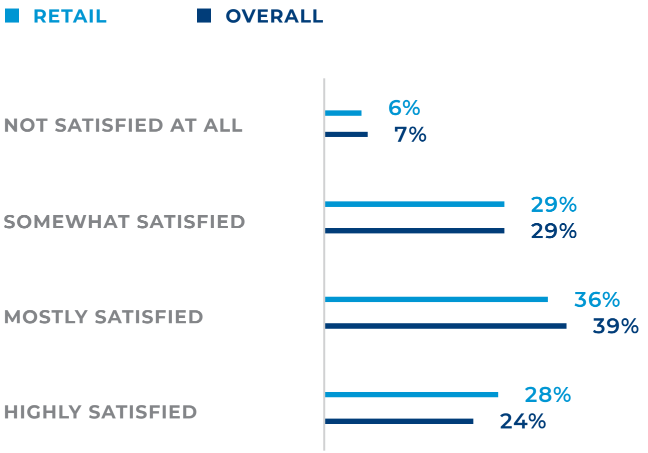


FIGURE 10

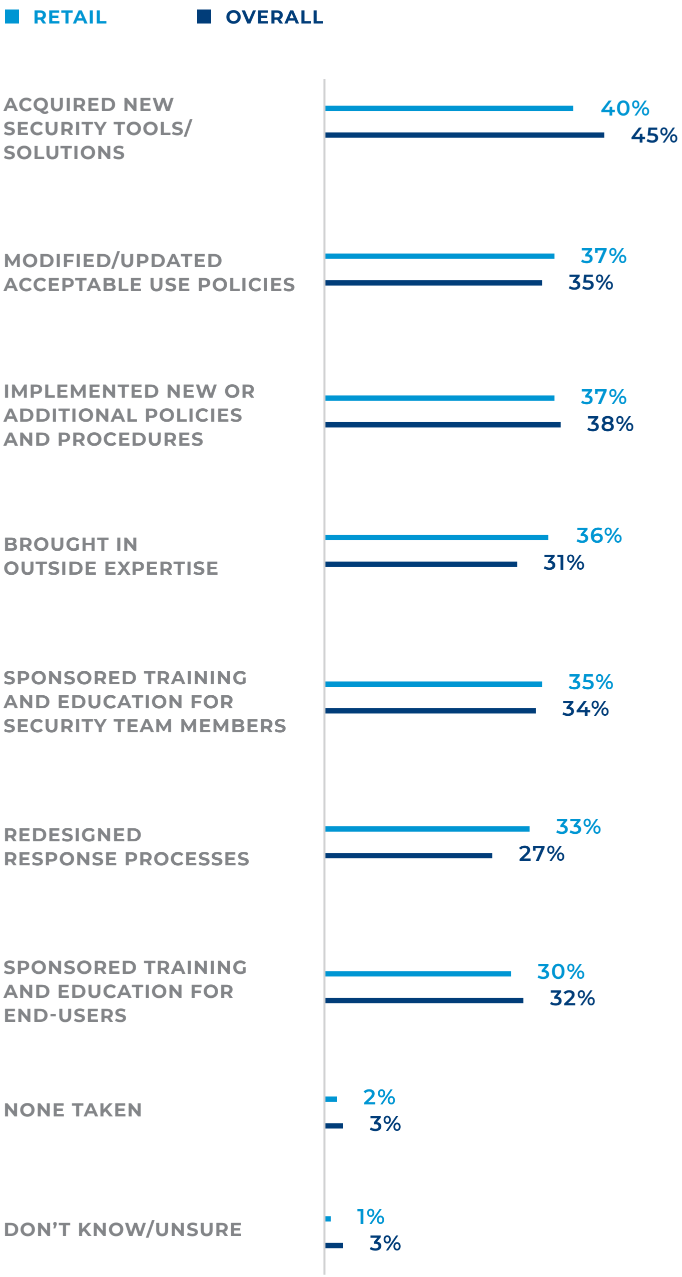
Satisfaction With Length Of Time To Resolve A Security Issue



Retailers are just as inclined to see process or operational changes as key to moving their cybersecurity strategies forward as they are to be relying on the latest technology. Acquiring new tools is retail's most common action to improve security responsiveness, though they are less inclined than their counterparts overall. Additional actions include modifying and updating acceptable use policies, and implementing new or additional policies and procedures (Figure 11).

FIGURE 11

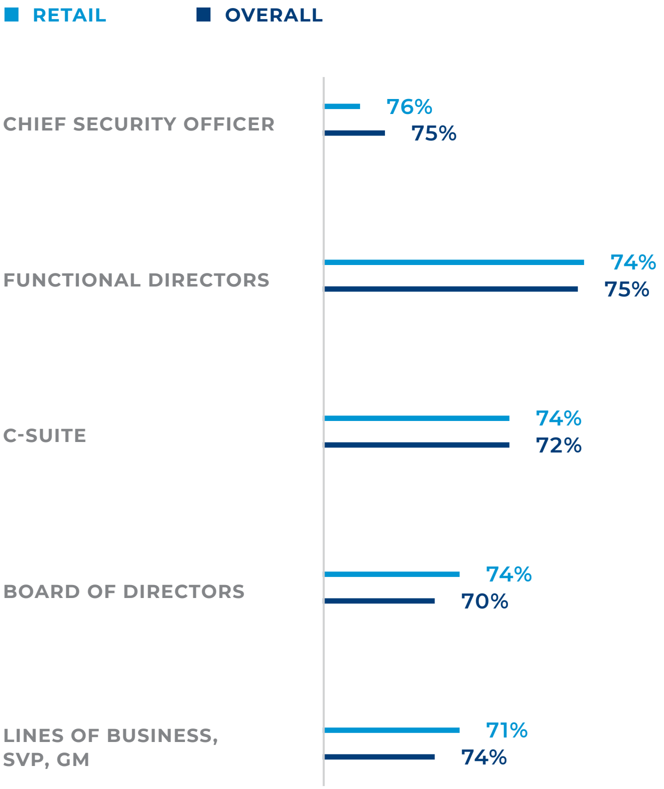
Actions Taken To Improve Responsiveness To Security Issues



In terms of commitment to cybersecurity, retailers have most constituents on board. Roughly three-quarters of retail leaders say major stakeholders are aligned to their security strategy (Figure 12).

FIGURE 12

Stakeholder Alignment In Security Strategies

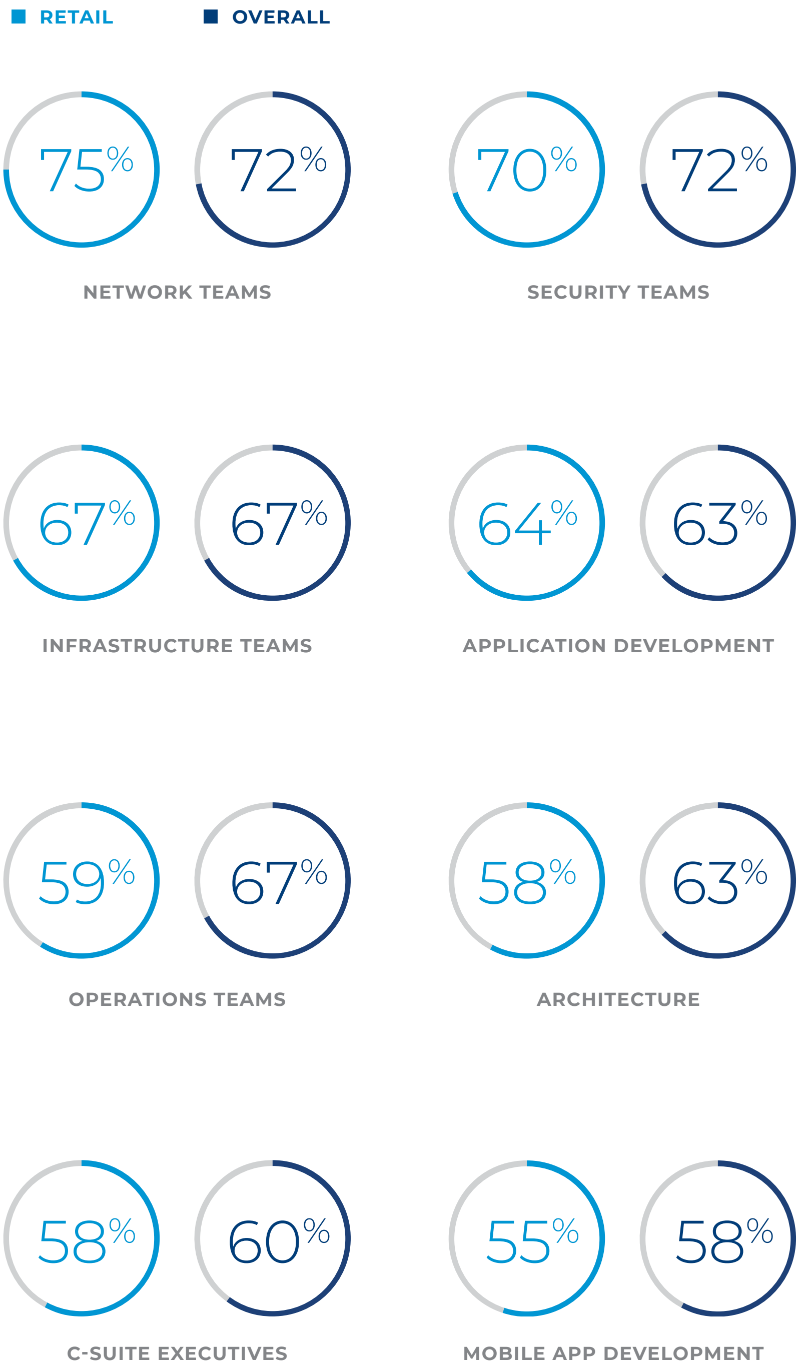


Network and security teams at retail organizations tend to be most collaborative; mobile app development teams lag those overall (Figure 13).

Retailers have an opportunity to lead the way with cybersecurity. “Retailers have the largest platforms for engagement with society,” says Ross Williams, head of information security at Bloomreach. “Having this access, retailers can help educate the population on best practices for protecting oneself in a digitally connected world. Cybersecurity is a priority in the business. Make cybersecurity a priority in your budget and make cybersecurity a priority at every level in your organization.”

FIGURE 13

Who’s Collaborating On Cybersecurity



The Future

Retail security executives and practitioners need to prepare for the transformative changes that are sweeping organizations.

Here are the trends that will shape the industry over the coming years.

There is no one-size-fits-all for retail cybersecurity. Every retailer has its own unique mix of online and physical points of sale, and thus, cyber strategies need to be customized to fit each retailer's unique profile. "As digital transformation becomes a core part of retailers' strategies, they'll have to prioritize threat-based cybersecurity in tandem, concentrating investments according to their unique threat profile," says Garrett. "A framework will look different for a pure-play e-commerce entity than for a hybrid e-commerce or specialty retailer because the most likely attack vectors are different for each. By taking a threat-based approach to cybersecurity concerns, retailers can ensure that investments in innovation are backed by the appropriate safeguards, shielding the organization from both steep fines and reputational blemishes."

Increasing consideration of cloud or third-party options to deliver security capabilities. Until recently, security was seen as a drawback of moving to the cloud. Now, cloud providers can deliver far more security than on-premises sites. Retail organizations will need to work in close collaboration with cloud providers to ensure that all critical areas are covered.

Retail business and security team leaders will need to take a leadership role on security concerns. Cybersecurity is an ongoing challenge that affects every part of the enterprise. This requires that processes and work habits be constantly examined and adjusted to meet security needs. End-users can often be the first to spot issues and alert security teams. In addition, the enhanced attention to processes that occurs within a robust and holistic cybersecurity strategy can help streamline and improve the way business is conducted.

"Before being able to make the right investments, retailers need to have the right governance and leadership," says Nadya Bartol, associate director at BCG Platinion. "Without a responsible executive with authority, budget and access to the CEO and the board, nobody will be able to define the right investments."

Retailers will need to develop cyber risk strategy and crisis plans. "As awareness around cybersecurity grows, retail organizations are realizing they need to collaborate more if they're going to succeed in protecting their reputation and assets," says Garrett. "But in general, many are still entirely too siloed. A way to address this is by creating a cyber risk management strategy. This should include a crisis communications plan, a comprehensive coordinated incident response plan, and post-breach digital forensics and cyber investigations. For the strategy to succeed, the organization must foster communication between all enterprise stakeholders and bridge the divide between corporate counsel and the IT department. Designating team members to each component of the strategy to ensure lateral communication and coordinated action is also crucial."

There will be pressure to identify what is important and apply resources accordingly. All too often, when it comes to cybersecurity, many organizations tend to be too reactive instead of proactive, says Stuart Madnick, a professor with MIT Sloan School of Management and founding director of cybersecurity at MIT Sloan. "A lot of things that companies are doing—better firewalls or security codes—are all good things to do, but security needs to be looked at holistically. Obviously, there are thousands of things that are important. But if security is spread across everything, probably nothing is going to be protected very well. You need to ask, 'What are the crown jewels?' so you can understand what things need the most protection. It's the exceptional organization that's really thought that through."

For more information on how to turn security into a competitive advantage, read:

Cybersecurity Trailblazers Make Security Intrinsic To Their Business ⟶

METHODOLOGY

Forbes Insights surveyed 1,001 executives from across the globe representing manufacturing, retail, financial services, healthcare, government and education. Within this group, 213 respondents were with retail organizations. From the overall sample, more than four in 10 respondents were from the C-suite (including chief information security officers, chief information officers and chief technology officers), and nearly a quarter were in security management roles. Responses were weighted to reflect market size.

ACKNOWLEDGMENTS

Forbes Insights and VMware would like to thank the following individuals for their time and expertise:

Nadya Bartol
Associate Director, BCG Platinion

Michael Coden
Managing Director and Head of the Cybersecurity Practice, BCG Platinion

Gregg Garrett
Head of U.S. and International Cybersecurity, BDO USA

Stuart Madnick
Professor with MIT Sloan School of Management; Founding Director of Cybersecurity at MIT Sloan

Ross Williams
Head of Information Security, Bloomreach

Forbes Insights is the strategic research and thought leadership practice of Forbes Media, a global media, branding and technology company whose combined platforms reach nearly 94 million business decision makers worldwide on a monthly basis.

By leveraging proprietary databases of senior-level executives in the *Forbes* community, Forbes Insights conducts research on a wide range of topics to position brands as thought leaders and drive stakeholder engagement. Research findings are delivered through a variety of digital, print and live executions, and amplified across *Forbes’* social and media platforms.

Report Author:
Joe McKendrick

499 WASHINGTON BLVD. | JERSEY CITY, NJ 07310 | 212.367.2662 | FORBES.COM/FORBES-INSIGHTS