accentureconsulting

SECURING CUSTOMER TRUST

ACHIEVING CYBER RESILIENCE IN RETAIL

The retail security landscape

Retail leaders now understand that facing a cyberattack is not a case of if but when. And minimizing the impact on their business—and, especially, consumer trust—depends on how quickly they can detect it, isolate it, and coordinate an effective threat response.

According to our research, on average, retail companies are satisfied they are ready to tackle cyber threats. Eighty-seven percent of retail companies said they are confident that they have effective infrastructure security in place, and also express confidence about other aspects of the business, such as protecting against online fraud or securing sensitive corporate and customer data. They plan to increase their cybersecurity investments, too—nearly half said they are prepared to invest more in the cloud, protecting point-of-sale systems and preventing fraud. Yet, when we asked which types of security breaches their organizations had experienced within the past 12 months, 53 percent identified customer data—the lifeblood of their business and a growing challenge that is likely to put pressure on Chief Information Security Officers (CISOs).

As they migrate from tech-savvy specialist to business-outcome-focused advisor, CISOs must not only be brilliant at security basics, but also be equipped with the insight and foresight needed to keep the customer satisfied—and safe.

82% **of retail executives are, on average, confident about their cybersecurity capabilities; yet out of 33 cybersecurity capabilities, retail is high-performing in just 19.**

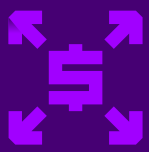
Enabling the business

Putting the business first is essential if retail CISOs are to handle upcoming threats posed by connected environments, broader ecosystems and the expanded use of data in all aspects of the retail environment.

72% of retail executives say that "cyberattacks are a bit of a black box, we do not quite know how or when they will affect our organization."

Three factors are important for retailers who want to reshape traditional operations and deal effectively with the next wave of cyber threats:

An evolving threat landscape demands constant vigilance



Digital prompts a new wave of security outsourcing

Retail CISOs need a seat at the (boardroom) table

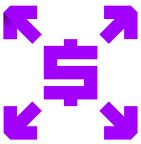
An evolving threat landscape demands constant vigilance

Retailers cannot be complacent about the enemy—or the shifting nature of cyberattacks. New business models, such as ransomware-as-a-service, mean that attackers are finding it easier to scale cybercrime globally. In May 2017, the WanaCrypt0r/WannaCry ransomware attack saw systems infected in more than 200,000 organizations across 150 countries. As many retailers digitize their stores, they open up not only the potential to improve customer experiences, but also new layers of vulnerability.

Spring 2018 saw several breaches that had a direct effect on customers: A sports clothing retailer experienced unauthorized access to personal information from 150 million users of the company's fitness app, and Saks Fifth Avenue and Saks Off Fifth exposed credit and debit card numbers that affected a reported five million customers.[1] Retail organizations recognize the risks: 81 percent of retail executives said that as companies adopt innovative business models, ecosystems, liquid workforces and so on, the risk and security attack surface area increases exponentially.

But it is a moving target; the number of attacks is rising along with the cost—between 2016 and 2017, there was a 23 percent increase in the cost of cybersecurity.[2] Hackers and cybersecurity techniques are constantly evolving and maturing to exploit new weaknesses in retail defenses. Retailers, busy managing competitive pressures, often lack the dedicated focus necessary to keep pace with the changing threat landscape.

Retail executives are defending 80% of targeted attacks and experiencing 32 security breaches a year, slightly more than the global average.



Digital prompts a new wave of security outsourcing

Increasingly, retailers are incorporating connected devices not only within their own stores, fleets, and distribution centers, but also using those technologies in their own sales environments. New value-added services like home-monitoring, smart doors for home delivery, and preventive maintenance of home appliances are all becoming attractive options for retailers who want to deliver more value and generate revenue.

But a connected environment brings its own complexities and exposure risks. Retailer CloudPets was made to realize the importance of customer data in its smart merchandise the hard way. It had to invalidate passwords created by owners of its soft toys following a breach and a ransom attack on its open database a year ago.[3] Data is no longer all in one place and security is not isolated to protect it. A distributed network of data that goes beyond the four walls of the organization, thanks to cloud computing and smart devices, places a burden on security teams who are already dealing with stretched resources and constrained budgets. Add in regulatory demands and the need for dedicated control and compliance and they are placed under further pressure.

Protecting high-value assets means looking after the data that is most critical to operations. Since retail executives already outsource many other areas of the business, such as security operations centers or risk management, it is a natural step to consider outsourcing to better meet security demands. Outsourcing will continue to grow as the data mountain grows—it is one way to keep pace with change.

14%+ **of retail executives, on average, lack confidence that their organizations can protect a range of nine different security areas, from customer and payment card information, to secure store and corporate networks or eCommerce attacks.**

26% **of retail executives say that more than half of their cybersecurity program should be outsourced to providers in three years' time.**

Retail CISOs need a seat at the (boardroom) table

For CISOs to be successful, they must have access to the executive team and insight into where business decisions are being made. Retailers are focused on CISO engagement and feeling buoyant about the impact of their efforts. Yet, our research showed that although they are confident about their cybersecurity effectiveness and capabilities, they are only high-performing in just over half. Being more embedded in business decision making requires a fundamental shift in the CISO role. It is not just a case of dealing with threats as they arise, but taking a proactive, risk-based approach to data security and management that goes beyond the boundaries of a cybersecurity strategy. For instance, take the area of mergers and acquisitions. If security is not involved early on, CISOs lose visibility and control over whether security policies are being consistently applied across acquired entities.

CISOs must partner with different areas of the business to properly assess security and management controls. For the security team to be front and center of any strategic plans, CISOs need to develop a new mind-set within the workforce, so that they become guardians of cybersecurity strategies that fully represent the business. But having the right talent in place may prove to be part of the challenge in the cybersecurity voice being effectively heard. According to the (ISC)[2] Cybersecurity Workforce Study 2018, 63 percent of respondents report that their organizations have a shortage of IT staff dedicated to cybersecurity. Forty-eight percent of employers around the globe said they were looking to hire more cybersecurity staff in the next 12 months—an indication that talent demand could outstrip supply.[4] As hackers become more sophisticated, this talent gap is a bigger concern. Large, powerful, companies will have first pick of good talent, leaving smaller retailers with limited choices. Given that a lack of cybersecurity protection can destroy trust and brand image with a subsequent impact on revenue, this is a further area where retailers might want to consider outsourcing their cyber responsibilities to free up their focus on the business of retailing.

4 in 5 survey respondents say that the CISO role will evolve from "authoritative enforcer" to "influencer/coach" for C-suite colleagues. To do this, the CISO needs to speak to business leaders in their own language.[5]

Security first

To achieve cyber resilience, retail organizations must build cybersecurity qualities and values into their business. In doing so, they need to take three actions:

01

Harden and protect core assets

Become brilliant at the basics by hardening and protecting your core hardware and software assets. Be clear on your inventory and put security controls in place—establish whether new technologies are adding complexity or adding value.

02

Adopt a "protect and partner" approach

Use a data-driven approach and advanced threat intelligence to better anticipate potential attacks and develop a more proactive security posture. Shore up your third-party defences or outsourcing partners so that their approach is as secure as your own.

03

Evolve the role of the CISO

Make sure the next-generation CISO is business adept as well as tech-savvy. Infuse a security mind-set into the culture of the organization.

45% of retail executives recognize they need to improve on cyber threat analytics and 43% on security monitoring—the "basics" of security programs.

Cybersecurity resources and capabilities are fundamental to retailers' future.

As attacks become more frequent and more sophisticated, cybersecurity basics must be baked in to the fabric of the organization. Getting the fundamentals right, pressure testing, taking up new intelligence and breakthrough technologies, such as artificial intelligence (AI) and analytics, and evolving the CISO role to be more business focused are essential ingredients to counteract today's and tomorrow's cyber threats—and keep the customer satisfied.

Authors

Vish Ganapathy
Managing Director
Global Retail Technology Lead
vish.ganapathy@accenture.com

Tammy Moskites
Managing Director
North America Products Security Lead
tammy.moskites@accenture.com

Stay Connected

@AccentureConslt
@AccentureRetail

About Accenture

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions—underpinned by the world's largest delivery network—Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With 459,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives.
Visit us at **www.accenture.com**.

Notes

Unless otherwise stated, the statistics in this point of view represent retail respondents in the survey report "Gaining ground on the attacker: 2018 State of Cyber Resilience," Accenture 2018.

References

[1] Retailer Data Breaches in 2018:Was Your Store Hacked? Kiplinger, May 2, 2018. https://www.kiplinger.com/article/spending/T048-C011-S001-retailer-data-breaches-2018-favorite-store-hacked.html

[2] 2017 Cost of Cybercrime Study, Accenture and the Ponemon Institute.

[3] Children's messages in CloudPets data breach, BBC News, February 28, 2017. https://www.bbc.co.uk/news/technology-39115001

[4] International Information System Security Certification Consortium, Global Information Security Workforce Study, June 2017. https://www.isc2.org/News-and-Events/Press-Room/Posts/2017/06/07/2017-06-07-Workforce-Shortage

[5] Build pervasive cyber resilience: Securing the future enterprise today, Accenture 2018.