FORTRA

Terranova Security®

Building Cyber Security Awareness: Why Training is a Must for the Retail Sector

BUILDING CYBER SECURITY AWARENESS: WHY TRAINING IS A MUST FOR THE RETAIL SECTOR

Shift Happens: The Retail Sector Today

As retailers sprint ahead with next-gen technologies and digital engagement, they're unwittingly stepping into a minefield: cyber threats have intensified, lurking at every digital corner. This new retail realm, while brimming with opportunities, is also fraught with unprecedented challenges.

The numbers paint an exciting picture. In the past three years, the retail sector has seen a decade's worth of growth, according to NRF President and CEO Matthew Shay, who anticipates continued positive trends, albeit at a more moderated pace.

Global eCommerce sales are projected to hit $8.1 trillion by 2026—marking a 56% surge.

But with every silver lining, there's a cloud. The very advancements that propel retail into the future are also its vulnerabilities.

New Opportunities Bring New Risks

2022 marked retail's grim milestone: it became the second most targeted industry by ransomware globally. Here's a snapshot of the stark reality:

77% of retail organizations surveyed worldwide faced an attack—a significant jump from the previous 75% benchmark.

Cyber attacks in the retail sector shot up by 117% in 2021, as reported by Positive Technologies.

As retail opportunities multiply and online shopping grows, the rate of cyber crime incidents increases in parallel. Retailers are engaging more third-party services to bridge in-store and online shopping experiences, and, on top of that, a significant 28.2% of employees have adapted to the hybrid model.

The crux of the matter is data. With heightened online activity, retailers are entrusted with more credit card details, financial records, addresses, birthdates, and purchase histories than ever before. As they weave through third-party services, they inadvertently spawn more digital pathways, inviting a slew of cyber threats.

The cache of stored data is a magnet for cyber criminals. Their arsenal includes theft, fraud, and even selling data on the dark web. And as the cyber threat intensifies, legislators are holding retailers accountable for the security of this data, urging them to bolster their defenses.

Recognizing the Need for Cyber Security Awareness

Retailers often believe that a robust firewall and updated antivirus software are sufficient for cyber security.

However, while technology is crucial for cyber security protection, it's not enough to address the most significant vulnerability: people.

Verizon's 2023 Data Breach Investigations Report (DBIR) showed that nearly three out of four breaches (74%) involved a human element.

Retailers need to align their views with recent cyber security trend data. In 2022, Verizon pinpointed a sharp rise in social engineering attacks targeting the retail sector. From just 7% of all attacks in 2016, these tactics surged to encompass 29% by 2022.

The Purpose of This Guide

This eBook is built to help guide retail leaders through common objections to cyber security training. It demonstrates why security awareness training programs are critical to reducing human risk, changing unsafe online behaviors, and protecting sensitive data.

Retail leaders who act now will help protect their organizations, stay compliant with data privacy legislation, and strengthen arguably the most important factor in modern business success: consumer trust in a brand.

CHAPTER 1

The Root Causes of Current Cyber Security Concerns

While many retail leaders are cognizant of cyber security challenges, some are yet to fully embrace the concept of a cyber security awareness program. Reservations vary, but the most common are tight budgets, the loss of valuable employee time, employee disinterest, and small company size.

Retailers have long grappled with various forms of fraudulent activity, refining their defenses over the years. However, the cyber threats of today are exponentially more sophisticated than they were just a few years ago, let alone two decades prior.

This rapid evolution means that even seasoned retailers may find themselves unprepared, underscoring the critical need for updated cyber security awareness and training.

Several reasons account for this sense of confidence.

Overreliance on Technology

As people become more at ease with technology, it propels the retail sector to new heights but also amplifies risks. While retailers and employees trust in technological solutions such as firewalls, password protections, and software safeguards, they often overlook the human factor.

This overconfidence can lead to unsafe online behaviors, and when guards are lowered, that's precisely when vulnerabilities are exposed and mistakes occur.

An Outdated View of the Retail Threat Landscape

Payment fraud and credit card theft are child's play for today's cyber attackers. These days, many cyber criminals play a longer and far more sophisticated game. An initial breach might involve stealing data or passwords, but this often paves the way for more devious follow-ups.

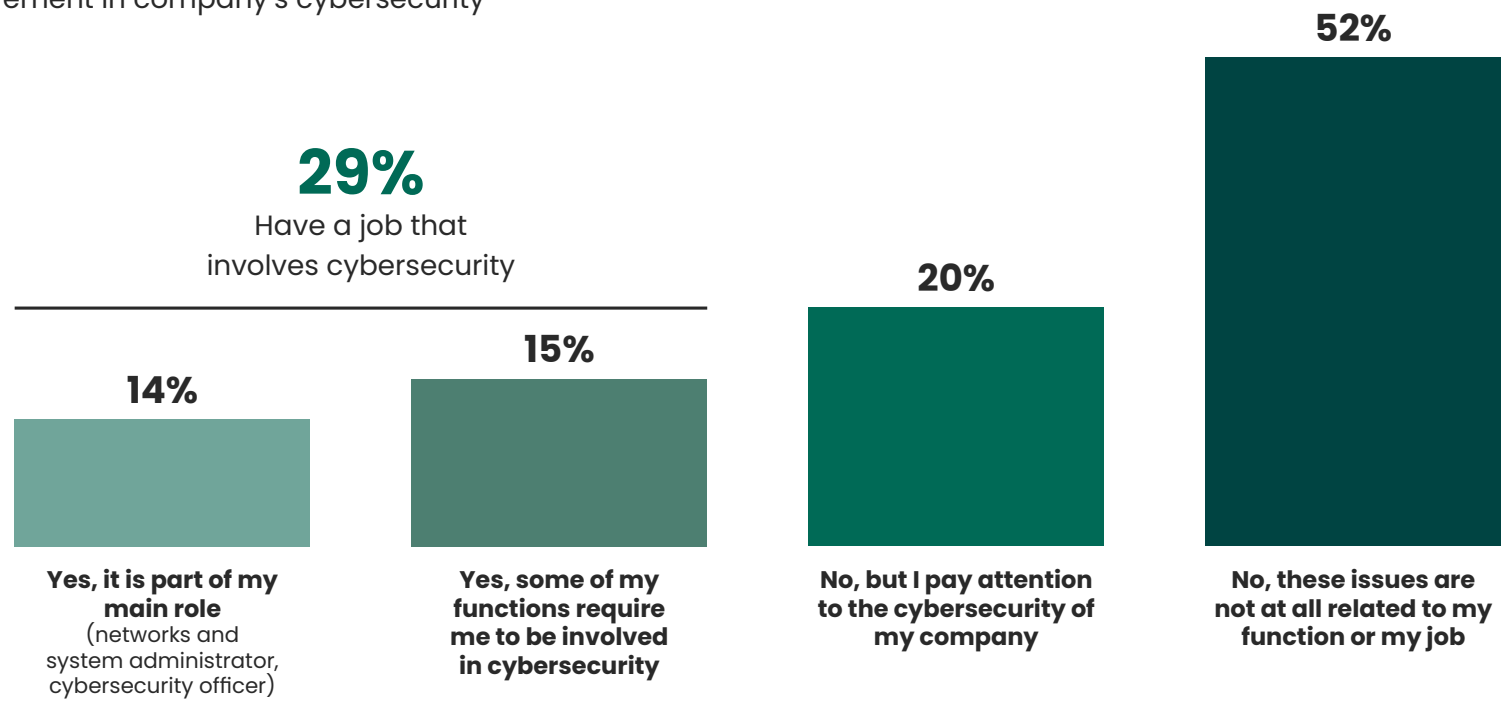
From encrypting systems and demanding hefty ransoms to targeting business partners, these attacks erode trust and relationships. It's more than just financial loss; a single attack can cripple a retailer through overwhelming legal fees, penalties, and irreparable reputational damage.

Misplaced Responsibility

As technology automates more business processes, a misconception persists. Most retail leaders and employees think the IT department controls all security aspects. A recent survey of employees showed 52% say their job has nothing to do with cyber security. When people play a role in most data breaches, that perception needs to change.

52% say their job has nothing to do with cybersecurity

Involvement in company's cybersecurity



In your company, are you involved in IT support in cybersecurity ?

Base=4000: All answering No filters applied

A cyber-aware mindset doesn't come out of nowhere. The whole organization needs to cultivate a security-aware culture, starting with retail leadership.

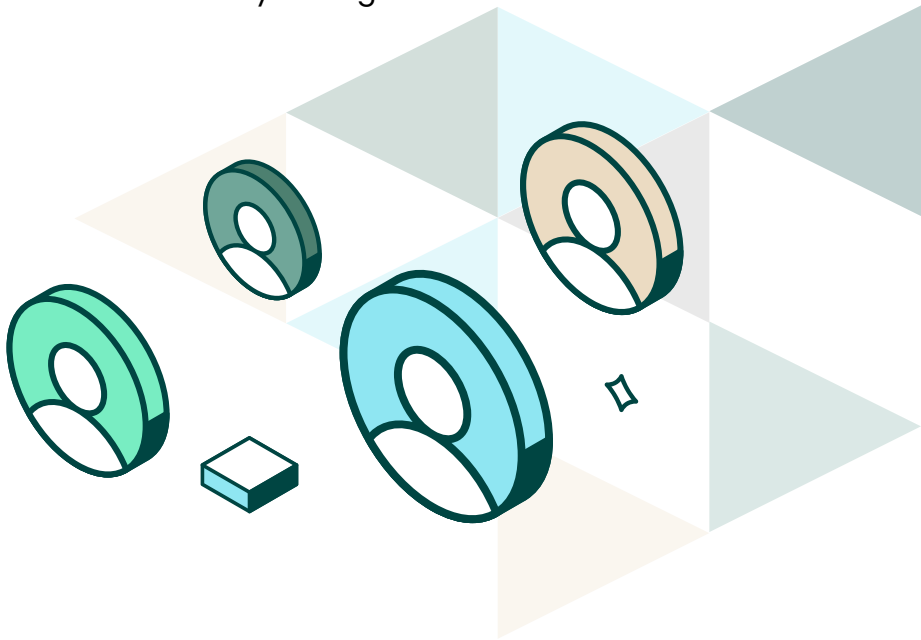
Increasing Third-Party Integration into an Evolving Threat Landscape

Store associates, merchandisers, social media managers, and Human Resources personnel all have access to your data. Sensitive business and customer information pass through third-party hands as well. Representatives from suppliers, fulfillment companies, payment providers, and payroll services need access to your data and systems. At the heart of this vast network? Your employees.

Every employee interaction can open the door to threats. For the sake of data security, it's vital that employees have the skills to navigate these situations safely. To keep business running smoothly, they need training to distinguish illegitimate communications from legitimate ones.

The external threat isn't theoretical—a recent report showed that 98% of organizations are connected to at least one vendor that has suffered a cyber security attack in the past 24 months. With third-party relationships becoming a rising vector for cyber attacks, retailers must prioritize and fortify their defenses in this domain.

Cyber attackers and cyber attempts are constantly evolving. Retailers that update their outlook and build a cyber-aware culture among their employees will be better positioned to handle new cyber threats as they emerge.



CHAPTER 2

5 Objections to Cyber Security Awareness Training

Some retailers don't consider cyber security awareness training a business essential. Often, retailers may not fully consider the comprehensive ROI of cyber risk management. While balancing available resources and meeting employee demands is crucial, it's equally important to assess the potential devastating costs of a data breach against the investment in robust security measures.

Often, balancing those factors ends with familiar objections, and the conclusion is that cyber security awareness training is wanted but not needed. The question is: Do these objections reflect current retail business demands, today's employees, and evolving risks?

To help retailers weigh the pros and cons, we dig into 5 of the most common objections to cyber security awareness training to see if they're warranted in today's threat landscape.

"Our employees understand enough about cyber security."

It's great to see employers show confidence in their staff. However, it's dangerous for retailers to assume their employees know about cyber security from previous jobs or daily life. In social engineering attacks, cyber criminals try to steal critical information from unsuspecting staff through carefully crafted emails, texts, or voice messages. They use manipulative messaging to get recipients to click links, divulge sensitive information, or download malware.

With inboxes inundated with customer queries, vendor updates, and delivery notifications, it's a tall order to expect retail employees to consistently distinguish genuine messages from deceptive ones. Many employees are unaware that their everyday communications could be the pathway to a store-wide data breach via a malware, ransomware, spear phishing, or another type of threat.

In 2013, for example, cyber attackers carried out a successful spear-phishing attack on a third-party vendor and gained access to Target's networks. They installed malware on the mega-retailer's systems and stole the payment data and personal information of 110 million customers.

A year later, a malware attack on hardware giant Home Depot compromised the payment information of 52 million customers. The cyber attackers had first gained access with a stolen username and password. In 2020, an online fraudster gained access to data from 4.6 million Neiman Marcus customer accounts, including usernames, passwords, contacts, and credit card details.

When a single phishing email can have such disastrous results, retailers can't assume that having tech-savvy employees means their perimeter is secure. The only way to fill cyber security knowledge gaps is by cultivating a cyber-aware staff.

"We don't have the budget for cyber security awareness training."

When margins are tight, new expenditures are often viewed with skepticism. To many retailers, cyber security awareness training might appear as a non-essential cost or an investment to consider down the road.

Unfortunately, when security breaches do happen, recovery costs are high. IBM research shows that data breaches cost retailers an average of $3.28M in 2022 (up from $3.27M in 2021).

Direct financial losses from a breach (e.g., hiring people to build back databases, networks, and system controls) are just the tip of the iceberg. Retailers lose revenue from lost sales and wages during an ensuing shutdown. Data loss can bring stiff regulatory penalties, lawsuits, and legal fees. Marketing campaigns to fix reputational damage and re-establish customer trust can be costly, too.

The calculation is simple: Cyber security awareness training saves retail companies money in the long run by preventing reputation-damaging cyber breaches from occurring in the first place.

Top training programs are customizable so that any organization can improve its security posture at an achievable and practical price point.

"Training takes too much time away from work."

With eCommerce sales booming and retailers trying to accomplish more with fewer employees, cyber security training can seem like an extra burden that wastes time.

But consider this: An employee, amidst a busy workday, receives an email that appears to be from a familiar supplier. Without thoroughly checking the sender's details, they click on an embedded link. Or, during a short break, they connect to the coffee shop's public Wi-Fi to keep track of logistics without realizing it's been compromised. Just like that, the door is open to malware or a ransomware attack.

Ultimately, the claim that cyber security training occupies too much work time rings hollow compared to the significance of disruptions following a cyber attack. IBM's 2022 report indicates that businesses spent an average of 277 days identifying and recovering from a breach. During recovery periods or ransomware shutdowns, retailers often lose thousands, if not millions, in wages and sales.

For individual businesses, the longer a breach takes to detect, the longer and more costly the recovery. Veeam's 2022 Data Protection Trends report estimates the average cost of server downtime at $88,000 per hour or $1,467 per minute. Add legal fees, data breach penalties, and many other expenses, and it becomes evident that cyber security doesn't waste work time. In some cases, it saves the workplace.

Not all training programs are cut from the same cloth. Programs that adopt the self-serve approach understand the value of every second of employee time. They take workday rhythms into account with micro-lessons. Employees consult customized modules and take mini quizzes on demand when they have downtime. Instructor-led sessions, in contrast, can be inflexible and take a bite out of the workday.

"Our employees won't be interested in cyber security training."

This objection is propped up on two separate falsehoods. The first is that employees don't want to learn cyber security skills. The second is that disinterest is justified because training is dull, uninteresting, and unrelated to staff members' core duties. A survey conducted in 2022 by Ipsos and Fortra's Terranova Security indicated that the opposite is true. A clear majority of employees—79% of respondents—said they were interested in cyber security awareness training, whether their employer offered it.

Security experts prioritize engagement and relevance in program design to bring employees on board and keep people interested. Microlearning modules share content tailored to everyday work scenarios in small, easily consumable pieces. This construction helps learners see how cyber security awareness relates directly to protecting confidential data without sacrificing productivity.

Disinterest is not a factor when learning is fun and exciting. Gamified training keeps employees engaged as learners earn points by completing modules, winning challenges, and acing tests. Light competition drives participation, and leaderboards that display real-time results build team spirit.

Add personalization to the mix, and you boost engagement even further. Organizations can customize the visual style of training modules, provide content in different languages, and design special lessons for specific roles.

Employees feel good when they know they're doing something right for themselves and the organization. Cyber security awareness training is a crucial worker benefit. Giving your staff skills, knowledge, and techniques to protect their data—and that of friends and family—shows them that you care.

"Our company is too small to be a target of cyber attacks."

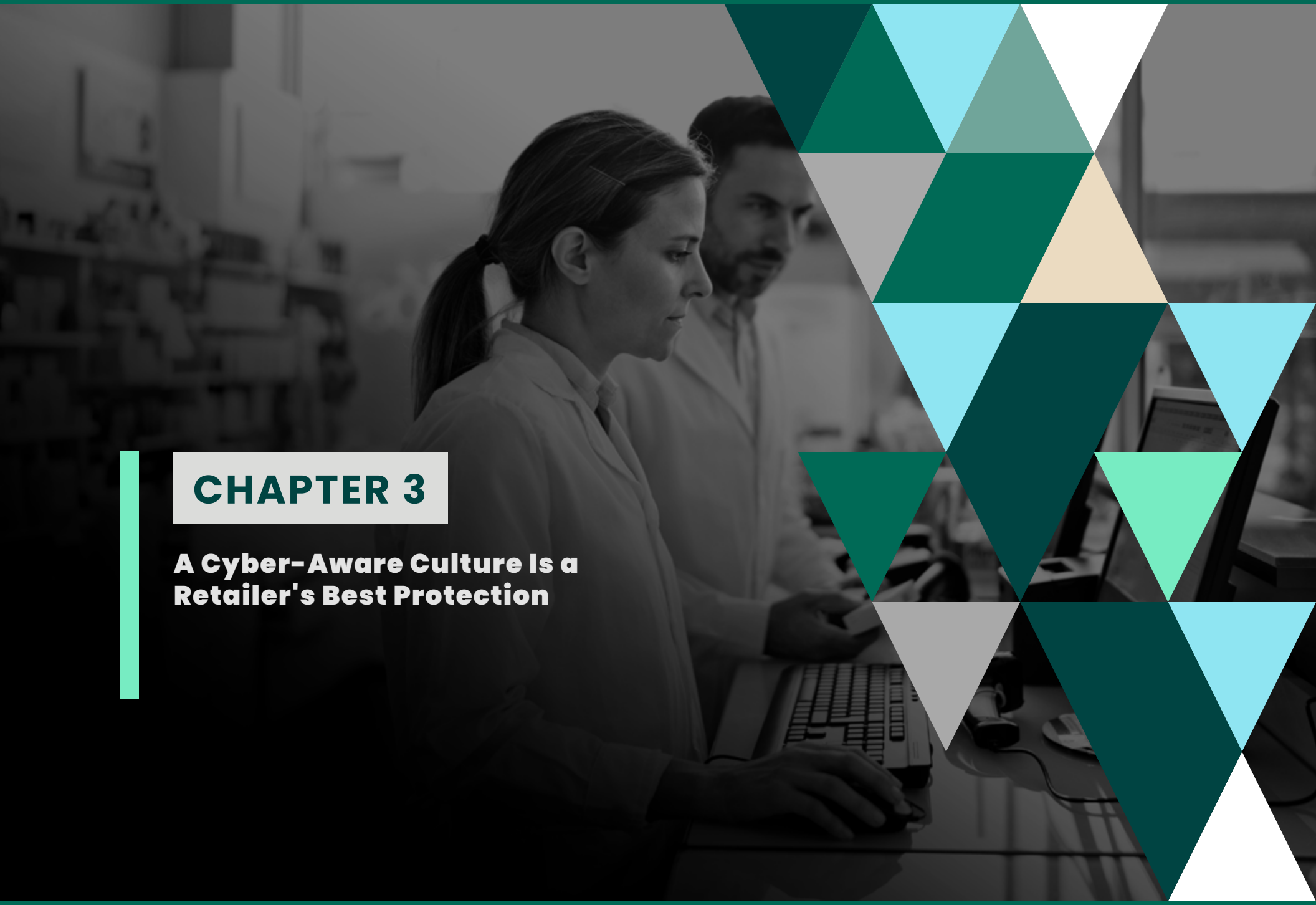
Small retailers sometimes mistakenly think they're immune from cyber crime. With fewer employees, less digital infrastructure, and less data, they believe they're not worth attacking. A survey by Digital, for instance, shows that 36% of small business owners are "not at all concerned" about cyber attacks.

While attacks on large-scale businesses might dominate the headlines, the numbers show that small businesses are equally enticing hacking targets. In 2021, the FBI's Internet Crime Complaint Center received nearly a million (847,376) reports of cyber crime activity, most of the victims being small businesses.

Phishing attacks, in particular, are spiking as smaller online retailers turn to social media to advertise and connect with their customer base. At the same time, those new sales channels bring increased risk. According to Threat intelligence, 32.4% of cyber attacks in the retail sector target eCommerce.

For many small retailers, the financial fallout can be too much to bear. Statistics estimate that cyber attacks force 60% of small organizations out of business. Still, as a 2022 survey shows, of small businesses with fewer than 50 employees, only 8% had a cyber security budget, and 77% demonstrated a lack of cyber security knowledge.

Given the odds, eCommerce retailers need to take steps towards building a security-aware culture. Whether a company has 10 employees or 10,000, everyone must learn to detect, avoid, and report phishing and social engineering attempts. Continuous learning through cyber security awareness training bridges security gaps and builds resilience.



CHAPTER 3

A Cyber-Aware Culture Is a Retailer's Best Protection

Facing today's cyber threats, common objections fade into the background.

Retailers store massive amounts of sensitive customer data and payment information. They deal with a long list of third-party vendors. They often have a high employee turnover rate. All these factors make retail organizations an attractive target for cyber criminals.

Without proper training, recently onboarded staff are particularly vulnerable to one of the most common attack vectors: email phishing attacks. In one example, "Business Email Compromise" (BEC), skilled cyber criminals posing as trusted vendors use stolen email addresses to pressure unsuspecting employees into sharing system credentials or paying invoices to those criminals' bank accounts.

Novice staff are often responsible for ordering stock, dealing with third-party payment or delivery partners, and updating Point of Sale (POS) software. Unfortunately, hackers are experts at spoofing external websites to look like legitimate ones. With the help of AI tools, creating and proliferating a sophisticated email or spoofing brands is easier than ever before.

Consumers are becoming savvier, too. Those wary of identity theft are choosing retailers they know they can trust. 83% of US consumers said they would stop spending their money on a business several months after a security breach and 21% said they would never return to that business.

Grappling with the financial, regulatory, and reputational consequences of a data breach is a genuine distraction from your core business. Remediating a data theft or other data compromise is expensive, and the financial burden from lawsuits and regulatory penalties could spell the end for smaller retail stores.

By all accounts, retailers are better off doing everything they can to stave off cyber incidents before they happen. When 82% of breaches involve a human element, the most effective way to do that is through cyber security awareness training.

There are many benefits:

- **Employees learn about security best practices**
- **Employees feel encouraged to adopt cyber-secure behaviors**
- **You develop a robust cyber security-aware culture across your organization**
- **Human-initiated cyber security incidents are reduced**

Transforming awareness into action starts by acknowledging the crucial role of employees in cyber defense.

CHAPTER 4

Gaining Confidence with Fortra's Terranova Security Solution

As the threat landscape continues to evolve, retailers need a range of tactics and tools to mitigate security risks and improve the organization's security posture. Terranova Security's training solution teaches employees the significance of cyber security best practices and instills cyber-secure behaviors throughout the company.

Terranova Security experts, with over 20 years of domain experience, design every security program around four pillars of success:

Significant risk reduction:
Through consistent training and awareness, your team can identify and address vulnerabilities, substantially reducing the chances of a cyber incident.

Changing unsafe online behavior:
By targeting the habits that lead to vulnerabilities, training helps reshape employee actions for a more secure online environment.

Data breach prevention:
Equip your team with the skills to spot and respond to threats, directly minimizing the chances of costly data breaches that can tarnish brand reputation.

Enhanced defense at every touchpoint:
Solidify your security posture across all departments and interfaces, whether it's in-store terminals or online platforms, ensuring a safer shopping experience for every customer, every time.

In today's retail marketplace, business leaders have little choice but to grapple with cyber security risks and threats. The best way to do that is by continuously empowering your employees with security-aware knowledge and best practices to keep data and assets safe.

Terranova Security's training solution is affordable, engaging, time-saving, and effective. It transforms your retail business into a security-aware organizational culture.

To learn more about the foundational principles that guide Terranova Security's impactful training programs, download the Definitive Guide to Security Awareness Training by clicking here or scanning the QR code below:

Face the Future with Cyber Security Awareness Training

It's time for retailers to move beyond knee-jerk objections and consider the facts. Human error is still the number one cause of cyber security incidents. No matter how small your business, what security technology you implement, or how savvy your employees are, you can measurably reduce risk by implementing a professional cyber security awareness training program. Training your employees in cyber security best practices is affordable and accessible for retail companies of all sizes.

Talk to a cyber security expert to see Terranova Security's training solution can be a huge difference-maker for your organization.

BOOK MY DEMO

FORTRA™

Terranova Security®

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.

 | tns-ebook-retail-1123