THALES
Building a future we can all trust

2022 Thales Data Threat Report

Retail Edition

#ThalesRetailReport

cpl.thalesgroup.com

Introduction

Retail organizations have long been targeted by cyber criminals attracted to the industry because of its size, large quantities of online and point-of-sale (POS) credit card transactions, and millions of POS and IoT devices that can be easy targets due to unpatched vulnerabilities and configuration errors. This results in large and constantly expanding corporate attack surfaces. Moreover, retail organizations are dependent on high-value, constantly available systems, making them attractive marks for ransomware and other attacks that seek to leverage cybersecurity's weakest link: humans.

In this report, we summarize some of the most important findings of the 2022 Thales custom survey, obtained by surveying retail security leaders and practitioners worldwide, and explore ways to reduce the risk of cyberattacks.

451 Research

S&P Global
Market Intelligence

Source: 2022 Data Threat custom survey from 451 Research, part of S&P Global Market Intelligence, commissioned by Thales

Contents

65% of retailers chose malware as the top security threat, followed by ransomware at 52%."

Remote Working Worsens the "Human Factor" Weakest Link

Unsurprisingly, the "human factor" remains cybersecurity's weakest link — and widespread remote work makes the situation worse. A large percentage of successful cyberattacks gain footholds into organizations due to user error, often beginning with a successful phishing attack that progresses into a full-scale ransomware or malware attack. Thirty-six percent of retail respondents chose human error as their top threat, close to the percentage across all industries.

In a stack ranking of retail respondents' top perceived threats, malware was at the top (65%, 9 percentage points higher than overall percentage), with ransomware second (52%, 3 points below all respondents), and phishing/whaling third (41%, close to total). Retailers are clearly experiencing more issues with malware, as evidenced by their significantly higher response rate than the total. Seventy-four percent of respondents were very or somewhat concerned about security risks from employees working remotely, 5 points lower than all respondents. This is likely due to a smaller proportion of retail employees working remotely, compared with other industries.

When ranking the top security technologies to combat threats, only 33% of retailers prioritized multi-factor authentication (MFA) as most effective for preventing cyberattacks, similar to the total. In production, MFA is used by 59% of retail organizations, 4 percentage points higher than the overall survey. However, only 8% of retail organizations use modern authentication, including MFA, for the majority (>60%) of on-premises applications, 2 points lower than the total. Only 20% use it for a majority of cloud services, similar to respondents in all industries. While modern authentication includes more than just MFA, the disparity between MFA deployment on-premises and in the cloud is curious, given that MFA is a relatively simple way to quickly improve overall security posture by countering ransomware and other attacks that rely on user error— and it should be deployed throughout the organization in order to be most effective.

Viewing modern authentication use by role, the most cited category was remote/mobile non-IT employees (63%, 5 points lower than the overall average), followed by privileged employees and IT staff (55%) and third parties (49%), similar to overall averages.

The combination of malware and ransomware is particularly nefarious for retailers as malware can be used to capture and exfiltrate sensitive data, followed by a ransomware attack that disables business-critical systems."

Malware and Ransomware Attacks Increase and Get More Complex

Forty-five percent of retail respondents reported that the volume, severity and/or scope of cyberattacks had increased in the previous 12 months. Nearly a third (32%) of respondents had experienced a security breach in the previous 12 months, close to the percentage of total respondents, while 55% had experienced a breach at some point, 2 percentage points higher than the total. Malware tops the list of attack types on the rise, with 65% ranking it as an increasing threat, 9 points higher than the total across all industries. Ransomware ranked second, at 52%, 3 points lower than the total, with 20% of retailers reporting a ransomware attack at some point, similar to all respondents.

> **Nearly a third of retailers experienced a security breach in the previous 12 months."**

However, of those that had a ransomware attack, 29% reported more severe incidents with external impacts such as media coverage and affected customers, 6 points higher than the global percentage. While retailers rank malware as a greater threat than ransomware, in practice many ransomware attacks begin with a malware component, so they are closely linked.

The combination of malware and ransomware is particularly nefarious for retailers because malware can be used to capture and exfiltrate sensitive data such as customer credit card information, followed by a subsequent ransomware attack that disables business-critical systems. Criminals are increasingly using exfiltrated data and other attacks such as denial of service as additional incentives to make ransom payments.

Ransomware has changed breach economics for retailers, which have low downtime tolerances. Survey data showed more intense aversions to "hard" rather than "soft" ransomware costs. Twenty-eight percent of retailers ranked financial losses, such as lost sales or penalties from lawsuits and legal expenses, as the greatest impact from ransomware, 4 percentage points higher than the total. Disclosure of sensitive information through exfiltration was second (20%, 3 points higher than for all respondents). Softer costs were not as critical to retailers, with brand reputation damage (9%, 2 points lower than total), loss of customers (6%, close to total) and long-term business impacts (3%, also close to total) ranking near the bottom of the list.

Paying ransom is a contentious issue, and 27% of retailers indicated a willingness to pay, 4 points higher than all respondents. Organizations may not have a good understanding of the overall effects of paying ransom, such as issues with cyber insurers, incident response firms, government regulators and ransomware attribution. For example, NATO considered NotPetya ransomware an act of war, causing some cyber insurers to refuse claims, and the U.S. Department of the Treasury's Office of Foreign Assets Control stated that facilitating ransomware payments to attackers on behalf of victims could risk violating regulations.

Ransomware's power comes from "kidnapping" of data and critical systems, and combating it requires a rapid, rehearsed response plan. However, only 48% of retailers have a formal ransomware plan, 2 points lower than the total across all industries.

27%

of retailers indicated a willingness to pay a ransom, 4 points higher than the global average.

Diverse Data Protection Strategies Need Better Alignment and Common Direction

The first step in a data protection strategy is identifying where data is stored, followed by classification, so that appropriate security protections can be employed. However, less than half (46%) of retailers have complete knowledge or are very confident they know where their data is stored, 7 points lower than the 53% average. Meanwhile, 53% of retail respondents indicated they could classify at least half of their data (1 point lower than the total for all verticals) and 23% said they could classify all of it (also 1 point below the total).

Deploying encryption technologies is key to ensure sensitive data is protected both at rest and in transit. Surveyed retailers indicated that encryption spending was 2 percentage points lower than the total on data-at-rest encryption, tokenization and data masking (19%); spending was 6 points lower on data-in-transit encryption (17%). There are clear advantages to encrypting data, both in terms of protection from ransomware and malware attacks and avoiding breach notifications through "safe harbor" provisions built into many compliance mandates.

When asked how their organizations protect sensitive cloud data, 60% of retailers selected encryption, while only 49% selected key management, similar to respondents across all verticals. While it is hard to comprehend how encryption and key management would not be equally deployed, the discrepancy is likely because organizations are unaware of how their keys are managed. For example, some cloud providers largely abstract key management, making it less visible. A focus on key management is critical. Simply deploying encryption to "check a box" can result in improper key management, leading to vulnerabilities and increased risks of attack. Encryption is only as good as the keys in use — and how they are managed.

59%

of retailers reported having five or more key management solutions.

Most organizations have multiple key management tools, resulting in higher costs, complexity and risk. Fifty-nine percent of retailers reported having five or more key management solutions (2 percentage points higher than the total), while 11% had eight or more (compared to 17% for all verticals). While fewer retailers have an excessive number of key management tools, five or more tools is still cumbersome (and expensive) to manage.

Security concerns regarding quantum computing continue to increase; all respondents expressed some concern about quantum-related risks. Retailers indicated top concerns are risk of network decryption (54%), future encryption compromise (52%), risk of blockchain attack (51%) and future decryption of today's data (48%).

46%

of respondents said that they have complete knowledge or are very confident they know where their data is stored.

Only

23%

of retail respondents indicated they could classify all their data.

Zero-Trust Adoption Continues, Particularly in Cloud Environments

Retail organizations typically have some of the most highly distributed infrastructures. These include brick-and-mortar storefronts, warehouses, e-commerce sites, offices, distribution centers/warehouses, thousands of IoT/OT devices and a growing hybrid workforce that can work from anywhere. High dependence on logistics and suppliers to keep goods flowing is also an important issue.

Adopting zero-trust principles is a key strategy because it ensures "least privilege" access to highly distributed, high-value data and assets, both on- and off-premises. The adoption of connected POS systems and the conversion of many devices such as surveillance cameras and kiosks to IoT has greatly increased the size, complexity and elasticity of underlying networks, while also increasing the attack surface. These environments are generally well served by zero-trust security strategies.

Twenty-nine percent of retailers reported that they have adopted and are actively embracing formal zero-trust strategies, identical to all respondents. Only 23% of respondents reported zero-trust projects in planning and researching stages, 4 points lower than the total, although 30% are considering zero trust, 6 points higher than the total. When asked where they plan to use zero trust, respondents' top choices were cloud access (57%, 4 points lower than all verticals), on-premises access (51%, similar to the total), and remote access management (50%, same as the total).

More Apps and Data Move to the Cloud, Increasing Attack Surface and Complexity

Retailers ranked cloud databases, web apps and cloud-based storage as the attack targets that concern them most. A majority (57%) of respondents reported having more than 40% of workloads and data in the cloud, similar to the total. Even though two-thirds (66%) of respondents classified more than 40% of their cloud data as sensitive, only 18% of retailers reported that 60% or more of sensitive data in the cloud is encrypted — 4 points lower than for respondents across all verticals. Exacerbating the situation, 68% of retail respondents identified their environments as multicloud, and the same percentage (68%) said they have over 25 SaaS applications in use, leading to potential issues with the complexities of securing multiple cloud environments.

Only

18%

of retailers reported that 60% or more of sensitive data in the cloud is encrypted — 4 points lower than for respondents across all verticals.

68%

of retail respondents identified their environments as multicloud, and the same percentage (68%) said they have over 25 SaaS applications in use.

Moving Ahead

As organizations move forward, they will need visibility not only across their infrastructure, but throughout their organization."

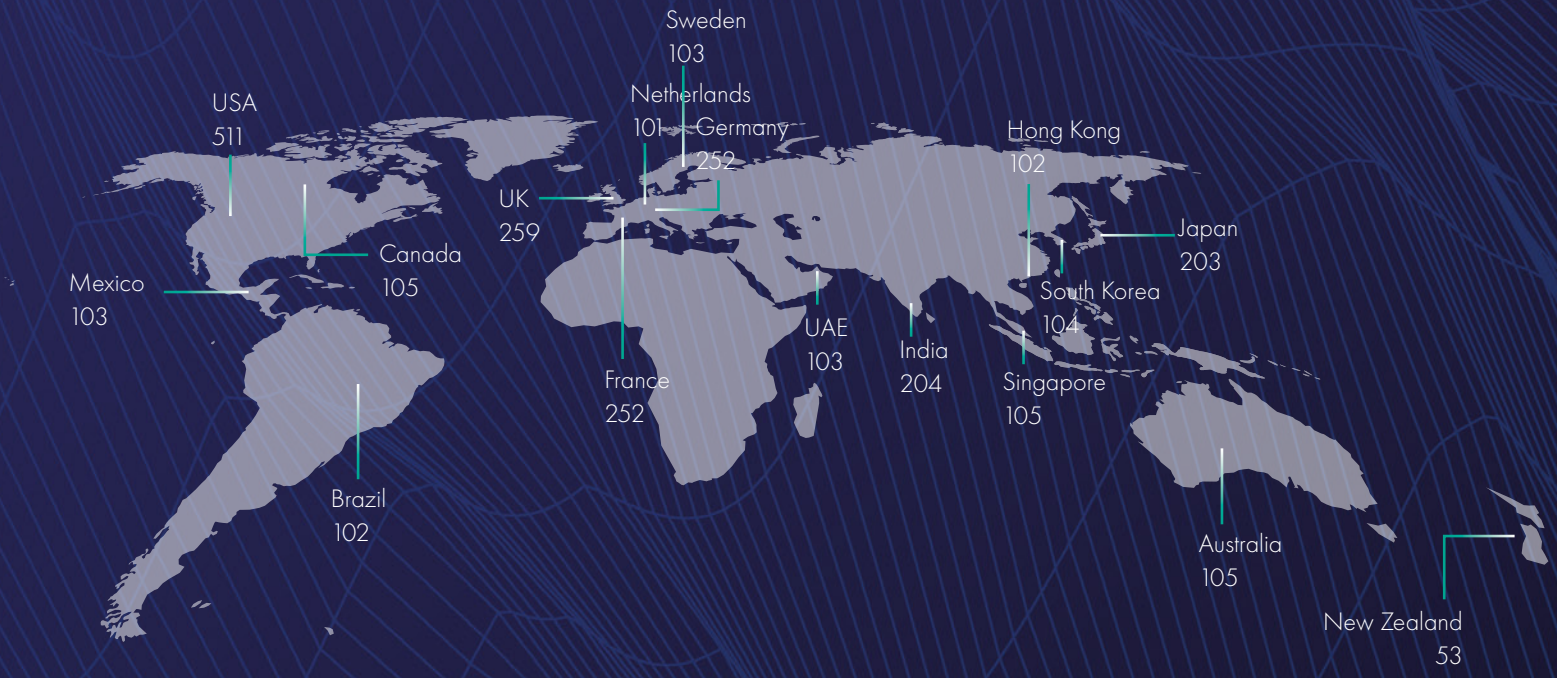
Retailers have been impacted by security issues due to highly distributed infrastructures, large and continually expanding attack surfaces, a prevalence of exploitable IoT devices and the human factor, which remains the weakest security link. Criminals need only find one human — preferably one with high privileges — using poor password hygiene or who can be tricked into releasing information, to gain a foothold. From there, ransomware, malware and other tactics can result in breaches, failed audits and unacceptable downtime. Data loss from breaches remains problematic due to low encryption rates and overly complicated key management practices, which tend to run at odds with one another. One effective defense, MFA, is progressing, although it is far from universally deployed.

Zero trust continues to gain momentum, particularly in remote access and cloud environments, but a true zero-trust strategy should be equally applicable to all users, devices and workloads, regardless of location. While implementing a zero-trust strategy focused on users and devices outside the organization is a fine starting point, it must permeate the entire IT estate to be truly effective. Additionally, in a zero-trust strategy, cloud-based assets should be protected independently from cloud infrastructure, preferably with encryption and enterprise key management to enforce auditable cryptographic encryption.

As retailers move forward, they will need visibility not only across their infrastructure, but throughout their organization. Establishing a common understanding is a key part of effectively setting priorities and executing security projects. When security teams are aligned with other key parts of the business, they can work together to address whatever issues the future holds.

About This Study

This research was based on a global survey of 2,767 respondents, fielded in January 2022, via a web survey with targeted populations for each country, aimed at professionals in security and IT management. In addition to criteria about level of knowledge on the general topic of the survey, the screening criteria for the survey excluded those respondents who indicated affiliation with organizations with annual revenue of less than US$100 million, and with US$100 million-$250 million in selected countries. This research was conducted as an observational study and makes no causal claims. A subset of this data was created that included 235 respondents who identified themselves as employees of retail organizations, including grocers, restaurant and food service and "classic" retailers.



Industry Sector

Critical Infrastructure	300
Manufacturing	157
Retail	154
Technology	127
Financial Services	120
Healthcare	115
Public Sector	109
Consumer Products	107
Computers/ Electronics/Software	106
Engineering	104
Federal Government	103

Revenue

$100 million to $249.9 million	162
$250 million to $499.9 million	802
$500 million to $749.9 million	865
$750 million to $999.9 million	458
$1 billion to $1.49 billion	254
$1.5 billion to $1.99 billion	58
$2 billion or more	168

THALES

Building a future we can all trust

Contact us

For all office locations and contact information,
please visit cpl.thalesgroup.com/contact-us

cpl.thalesgroup.com/retail