THREATQUOTIENT™

ThreatQ for Retail & Hospitality

When it comes to cybersecurity, breaches in the retail & hospitality industry might be one of the most high-profile and are happening at an alarming rate. According to a report by Thales, a global technology leader, 55% of retailers have experienced a breach at some point and nearly a third of retailers have experienced a security breach in 2022.[1] Retailers and hospitality vendors are investing heavily in cybersecurity to protect payment card data and other personally identifiable information (PII). However, some of the most effective measures retailers can take to keep their brands out of the headlines are grounded in the adage, "Those who do not learn from history are doomed to repeat it." This is because cyber criminals reuse tactics, techniques and procedures (TTPs). In so doing, they leave a recognizable trail of breadcrumbs or indicators that provide insights into threats.

Subscribing to threat data feeds isn't enough. Organizations need a way to aggregate and de-duplicate all external and internal threat data, filter out the noise, assess and prioritize threat intelligence, and use that threat intelligence to act — decreasing time to detection and mitigation. The faster a team can streamline their ability to import, enrich, deploy and operationalize that information, the more pressure defenders are applying to the adversary, which leads the adversary to offensive mistakes and oversights. Operationalizing threat intelligence also allows teams to learn from industry peers and their own past experiences to discover adversarial TTPs and proactively reassess and strengthen defenses to mitigate future attacks.

A 2022 report by Thales finds that 45% reported increase in severity; 32% reported an incident in the previous 12 months.[1]

KEY CHALLENGES

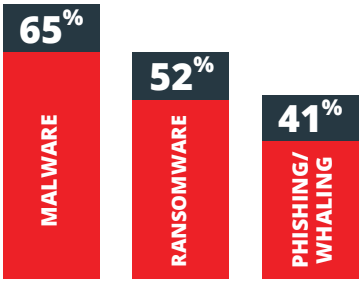
PERSONALLY IDENTIFIABLE INFORMATION AND PAYMENT INFORMATION

PII and credit card data is the lifeblood of the retail industry. Every transaction involves the exchange of valuable information, and this massive amount of data makes retailers lucrative targets for threat actors. Secure payment technology helps strengthen defenses, but it is not a silver bullet. When attacks do happen, research by Visa shows that they result in higher-impact breaches. Also of note, while Europay, Mastercard and Visa (EMV) chip technology increases security of point-of-sale (POS) transactions, it does nothing to protect "card not present" transactions involved in e-commerce.

SPEAR PHISHING

Many of the top threats to the retail and hospitality industry use spear phishing emails that are nearly impossible to discern from legitimate emails. Some campaigns engage in a rapid, wide-scale attack to target multiple merchants concurrently using a shotgun approach. Others target the merchant's POS vendor or integrator to gain access. Once inside the network, they take advantage of vulnerabilities for credential takeover and privilege escalation to steal payment card data or launch ransomware attacks.

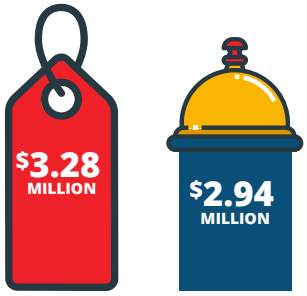
TOP SECURITY THREATS OF 2022



65% of retailers said that **malware** is the top security threat, 52% chose **ransomware**, and **phishing/whaling** was listed at 41%.[1]

VULNERABILITY PATCHING

Bad actors take advantage of the fact that IT and security teams struggle to keep up with patching of their POS systems, e-commerce payment applications and underlying internal infrastructure. As merchants strive to remain competitive, they invest in additional digital channels, applications and technologies that add complexity to the environment and further compound patching challenges. A lack of skilled cyber security professionals and organizational bureaucracy are often behind the inability to patch in a timely manner.



Cost of retail attacks

Cost of hospitality attacks

The average cost of cybercrime attacks per large retailing organization in the United States is estimated at $3.28M and hospitality at $2.94M.[2]

CREATING A LEADING THREAT INTELLIGENCE OPERATION

A robust data-driven security operations platform gives retailers and hospitality providers the context and prioritization they need to make better decisions, accelerate detection and response, and advance team collaboration and learning for continuous improvement. Serving as the hub of intelligence operations for many industries, the ThreatQ Platform aggregates and combines unstructured and structured data from any source, internal and external. There's no need to alter existing security infrastructure or workflows; all tools and technologies work seamlessly with ThreatQ's open architecture. Automation eliminates repetitive, time-consuming tasks so analysts can focus on high-priority and strategic work. The platform also provides flexibility to share curated threat intelligence, advisories and reports with a range of internal and external stake-holders, including retail and hospitality sectors, quickly.

ACHIEVE MORE WITH THREATQ:

- **CONSOLIDATE** all sources of external (e.g., R-CISC, RH-ISAC) and internal (e.g., SIEM) threat intelligence and vulnerability data in a central repository.
- **ELIMINATE** noise and easily navigate through vast amounts of threat data to focus on critical assets and vulnerabilities.
- **PRIORITIZE** what matters most for your environment.
- **PROACTIVELY HUNT** for malicious activity which may signal payment card fraud, denial of service attacks and other harm to consumers and merchants.
- **FOCUS** on known security vulnerabilities in currently active exploits which may impact regulatory status and security posture.
- **ACCELERATE ANALYSIS AND RESPONSE** to attacks against multiple targets, including POS systems, e-commerce applications, new digital channels and supporting infrastructure.
- **AUTOMATE** threat detection and response.

AVERAGE COST OF A SECURITY BREACH

Request a live demo of the ThreatQ Platform and ThreatQ TDR Orchestrator at www.threatq.com/demo.

1. https://cpl.thalesgroup.com/resources/encryption/2022/retail-data-threat-report
2. https://www.ibm.com/downloads/cas/3R8N1DZJ

ABOUT THREATQUOTIENT™

ThreatQuotient improves security operations by fusing together disparate data sources, tools and teams to accelerate threat detection, investigation and response (TDIR). ThreatQ is the first purpose-built, data-driven threat intelligence platform that helps teams prioritize, automate and collaborate on security incidents; enables more focused decision making; and maximizes limited resources by integrating existing processes and technologies into a unified workspace. The result is reduced noise, clear priority threats, and the ability to automate processes with high fidelity data.

ThreatQuotient's industry leading integration marketplace, data management, orchestration and automation (SOAR) capabilities support multiple use cases including threat intelligence management and sharing, incident response, threat hunting, spear phishing, alert triage and vulnerability management. ThreatQuotient is headquartered in Northern Virginia with international operations based out of Europe, MENA and APAC.

For more information, visit www.threatquotient.com.

THREATQUOTIENT™

20130 Lakeview Center Plaza, Suite 400 Ashburn, VA 20147 • ThreatQ.com
Sales@ThreatQ.com • +1 703 574-9885

TQ-IDB06-1023-02