INDUSTRY BRIEF

THREATQUOTIENT™

ThreatQ for Financial Services

When it comes to cyberattacks, the financial services industry is an attractive and lucrative target. Financial Services is often the most-attacked industry with customers suffering far more cyberattacks than any other industry.[1]

Despite regular testing and simulation of incident response capabilities, along with some of the fastest detection and response rates, financial institutions still experience compromises and breaches. The average cost of cybercrime for financial services companies has increased to <$18 million USD – the highest cost of any industry.[2] In addition to actual funds stolen, costs include detection, response and notification of the breach, fines and litigation, as well as lost business. In fact, post-breach, the industry experiences the second-highest customer churn rates after healthcare.

KEY CHALLENGES

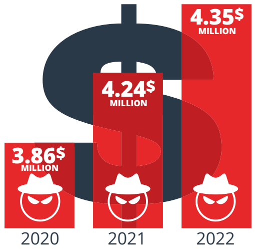
INCREASE IN ATTACK SURFACES

Customers expect 24/7 availability of services from any device, anywhere. Threat actors disrupt the flow of business with Distributed Denial-of-Service (DDoS) attacks. These campaigns are relatively easy to execute using third-party tools and services and are among the costliest attack type for firms to address. Increasingly, threat actors also target the social and mobile networks firms use to engage and support customers and run business operations. Taking advantage of the fact that few financial institutions incorporate these vectors into their threat model, cybercriminals leverage phishing scams, social engineering and malware to commit financial fraud, damage brands and even pose physical threats. To protect their expanding attack surfaces, financial institutions need visibility across the entire infrastructure as well as a proactive and anticipatory approach to closing gaps in defenses.

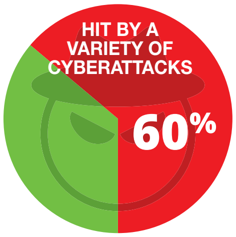
ATTRACTIVE TARGETS

Cybercriminals target financial institutions because that's where the money is and there are many ways to profit. They are actively exploiting vulnerabilities in ATMs, while networks like SWIFT (Society for Worldwide Interbank Financial Telecommunication) provide a means for criminal groups to steal directly from banks or surreptitiously shift money stolen from other sources. In addition, customer bank account information, payment card data and other personally identifiable information can be monetized quickly. Most security analysts suffer from alert overload and need the ability to focus on relevant, high-priority threats and to improve threat hunting capabilities.

AVERAGE COST OF A DATA BREACH



The average cost of a data breach reached a record high in 2022. The global average total cost of a data breach increased by USD 0.11 million.[3]



More than 60% of global financial institutions with at least $5 billion in assets were hit by a variety of cyberattacks over the past year, according to a new survey by Contrast Security.[4]

WEB APPLICATION ATTACKS

Financial services firms use web applications to provide a wide array of online and digital services to employees and customers. These applications allow users to submit and retrieve data from databases using their browsers. Threat actors exploit vulnerabilities in these applications and the devices used to access them to infiltrate networks and systems and steal confidential data and money. There is a wide variety of web application attacks, so financial institutions need real-time knowledge of how adversaries and campaigns operate and the infrastructure used, to accelerate response and prevention.

> *"We now have IOC data from trusted sources being sent proactively to detection-only watch lists in various internal security controls without daily oversight required by the team's personnel. What's more, because we're selectively exporting data to the tool specifically designed to consume it, we aren't pushing massive amounts of data across the network and slowing things down."*
>
> — Director of Threat Response,
> Fortune 500 Financial Services Company

BRINGING ORDER TO FINANCIAL SERVICES SECURITY OPERATIONS

A robust threat intelligence platform gives financial services providers the context and prioritization they need to make better decisions, accelerate detection and response and advance team collaboration and learning for continuous improvement. There's no need to alter existing security infrastructure or workflows; all tools and technologies work seamlessly with ThreatQ's open architecture.

ACHIEVE MORE WITH THREATQ:

- **CONSOLIDATION** all sources of external (e.g., FS-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 bank account data compromise, payment card fraud, DDoS 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 ATM systems, SWIFT network, web applications, new digital channels and supporting infrastructure
- **AUTOMATICALLY** push threat intelligence to detection and response tools

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

[1] Congressional Research Service, "Introduction to Financial Services: Financial Cybersecurity", January 5, 2023, https://crsreports.congress.gov/product/pdf/IF/IF11717

[2] Congressional Research Service, "Introduction to Financial Services: Financial Cybersecurity", January 5, 2023, https://crsreports.congress.gov/product/pdf/IF/IF11717

[3] IBM Security, "Cost of a Data Breach Report 2022" https://www.ibm.com/resources/cost-data-breach-report-2022

[4] ABA Banking Journal, "Larger financial institutions hit by variety of cyberattacks in 2022", February 7, 2023, https://bankingjournal.aba.com/2023/02/larger-financial-institutions-hit-by-variety-of-cyberattacks-in-2022/#:~:text=More%20than%2060%25%20of%20global,new%20survey%20by%20Contrast%20Security.

ABOUT THREATQUOTIENT™

ThreatQuotient improves security operations by fusing together disparate data sources, tools and teams to accelerate threat detection and response. ThreatQuotient's data-driven security operations platform 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 data management, orchestration and automation capabilities support multiple use cases including incident response, threat hunting, spear phishing, alert triage and vulnerability prioritization, and can also serve as a threat intelligence platform. ThreatQuotient is headquartered in Northern Virginia with international operations based out of Europe, MENA and APAC. For more information, visit www.threatquotient.com.