THREATQUOTIENT™

ThreatQ™ for Financial Services

When it comes to cyberattacks, the financial services industry is an attractive and lucrative target. For three years in a row, it has been the most-attacked industry[1] with customers suffering 65% more cyberattacks than any other industry.[2]

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 $18.37 million – the highest cost of any industry.[3] 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.[4]

KEY CHALLENGES

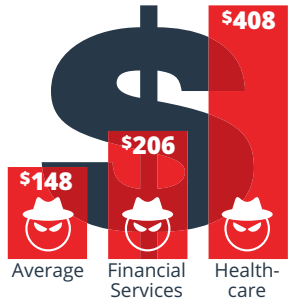
INCREASE IN ATTACK SURFACES

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.

COST PER RECORD BREACHED



The financial services industry has the second highest cost per record breached at $206; the average is $148.[4]

Approximately 36% of financial institutions suffered a security incident or detected unauthorized access in their infrastructure in 2018, up 24 percent from 2017.[5]

Banks and financial services organizations were the targets of 25.7% of all malware attacks last year, more than any other industry.[6]

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:

- **CONSOLIDATE** 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 Investigations at threatq.com/demo.

1 IBM, "2019 IBM X-Force Threat Intelligence Index," https://www.ibm.com/account/reg/us-en/signup?formid=urx-36763

2 The World Bank, "Cybersecurity, Cyber Risk and Financial Sector Regulation and Supervision," 2018, http://www.worldbank.org/en/topic/financialsector/brief/cybersecurity-cyber-risk-and-financial-sector-regulation-and-supervision

3 Accenture, "The Cost of Cybercrime," 2019 https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf#zoom=50

4 IBM, "2018 Ponemon Cost of a Data Breach Study," https://www.ibm.com/security/data-breach

5 Security Boulevard, "Cybersecurity Investment to Shoot Up in Financial Industry in 2019; Top Firms Already Spend $1 Billion," https://securityboulevard.com/2018/12/cybersecurity-investment-to-shoot-up-in-financial-industry-in-2019-top-firms-already-spend-1-billion/

6 Helpnetsecurity, "Which cyber threats should financial institutions be on the lookout for?," https://www.helpnetsecurity.com/2019/04/30/2019-cyber-threats-finance/

ABOUT THREATQUOTIENT™

ThreatQuotient's mission is to improve the efficiency and effectiveness of security operations through a threat-centric platform. By integrating an organization's existing processes and technologies into a single security architecture, ThreatQuotient accelerates and simplifies investigations and collaboration within and across teams and tools. Through automation, prioritization and visualization, ThreatQuotient's solutions reduce noise and highlight top priority threats to provide greater focus and decision support for limited resources. ThreatQuotient is headquartered in Northern Virginia with international operations based out of Europe and APAC. For more information, visit https://threatquotient.com.

THREATQUOTIENT™

11400 Commerce Park Drive, Suite 200, Reston, VA 20191 • ThreatQ.com
Sales@ThreatQ.com • +1 703 574-9885