REPORT

Contrast SECURITY

Cyber Bank Heists: Threats to the financial sector

Table of contents

Forward

Foreword by Derek Booth,
Assistant to the Special-Agent-in-Charge, U.S. Secret Service,
Head of the Mountain West Cyber Fraud Task Force

Organized cybercrime is growing exponentially since more businesses are opening themselves up to exposure trying to please their customers and making their products more accessible to their customers.

The more critical the organization and the information that is stored within that organization, whether it's private companies, healthcare, financial institutions or municipalities, the more valuable that data becomes to the cybercriminals and nation-states.

The increase of online threats, phishing, ransomware attacks, account takeovers and business email compromises are growing every day, and we can see in real time the damage this is doing to the longevity of businesses and the impact it's having on our economy.

Just as the Butch Cassidys and John Dillingers of the world exposed the country for vulnerabilities in banks and methods of commerce, cybercriminals are exposing the weaknesses in e-commerce and financial institutions by stealing as much as they can.

Executive summary

This annual report sheds light on the cybersecurity threats facing the financial sector. The report provides cyber ground truth, specifically manifesting an eye-opening perspective on the changing behavior of cybercriminal cartels and the defensive shift of the financial sector. In this year's report, financial sector security leaders from around the world revealed during a series of interviews the type of attacks they're currently seeing, what threats they're most concerned about and how they're adjusting their security strategy.

The findings of the Cyber Bank Heists report reflect the impact that the cybercrime events of the past year have had — and continue to have — on financial institutions (FIs) around the world. Since last year's edition, security has become a top-of-mind issue for business leaders amid rising geopolitical tension[1], an increase in destructive attacks utilizing wipers[2] and a record-breaking year of zero-day exploits[3].

[1] Defend from within | Intrusion suppression with runtime protection, continuous monitoring & application security | Contrast Security
[2] Secrets of the Wiper: Inside the World's Most Destructive Malware | Threatpost
[3] Zero Day Protection | Zero-day partiers are rocking your system | Contrast Security

01

Notable cyberattack trends

Over the past year, attacks have included[4] banking trojans, ransomware, account takeover, theft of customer data and cybercrime cartels deploying "trojanized" finance apps to deliver malware in spear-phishing campaigns. Given that backdrop, cybercriminals became punitive, escalating intrusions by launching destructive attacks against FIs.

60%

60% have been victimized by integrity/destructive attacks. Destructive attacks are launched punitively to destroy data.

In the past year, 60% of FIs were victims of destructive attacks. It is worth noting that cybercriminals in the financial sector will typically leverage destructive attacks as an escalation to burn the evidence as part of a counter-incident response. Destructive malware variants seek to destroy, disrupt or degrade victim systems by taking actions such as encrypting files, deleting data, destroying hard drives, terminating connections or executing malicious code.

60%

60% have been targeted by watering-hole attacks. Similar to how predators stake out watering holes to attack their prey, in watering-hole cyberattacks, adversaries hijack and boobytrap a website or mobile app used by e-finance customers. Eventually, financial customers who visit the compromised site or use the poisoned application get infected with the malware that adversaries have planted to compromise their data or systems.

64%

64% saw an increase in application attacks. Application attacks such as Class Loader manipulation[5], Expression Language Injection[6] and untrusted deserialization[7] are becoming more common. The new threats to supply chains are targeting software development, integration and delivery infrastructure. Research[8] shows that applications are attacked 433 times a day.

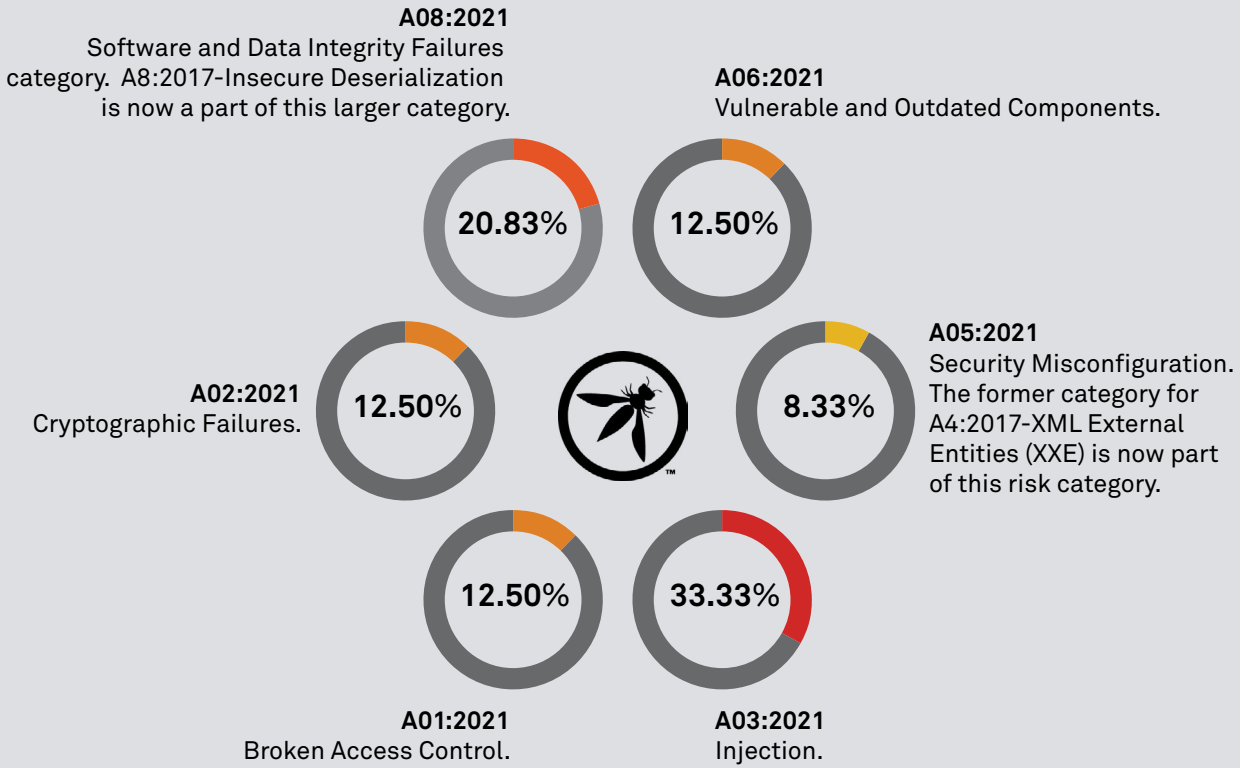
[4] Timeline of Cyber Incidents Involving Financial Institutions - Carnegie Endowment for International Peace
[5] Contrast Protect Blocks Spring4Shell | Contrast Security
[6] Expression Language Injection | OWASP Foundation
[7] Deserialization of untrusted data | OWASP Foundation
[8] Observability Report Page

The CISOs who participated in this study were most concerned with:

1. Injection vulnerabilities similar to Log4j, such as other Java Naming and Directory Interface (JNDI) injection attacks[9] that have been discovered in other libraries since the Log4j library was found to be vulnerable[10]. One example is the notorious banking trojan ZLoader[11], which exploits Microsoft's digital signature verification to inject malicious code into a signed system dynamic-link library (DLL).

2. Insecure deserialization, such as that found in AWS Lambda[12] in August 2022.

A breakdown of the most concerning **OWASP risks.**



[9] Hardening Log4j defenses with new Contrast Protect JNDI Injection rule | Contrast Security

[10] One year after Log4Shell, firms still struggle to hunt down Log4j | Contrast Security

[11] Microsoft disrupts Zloader malware in global operation

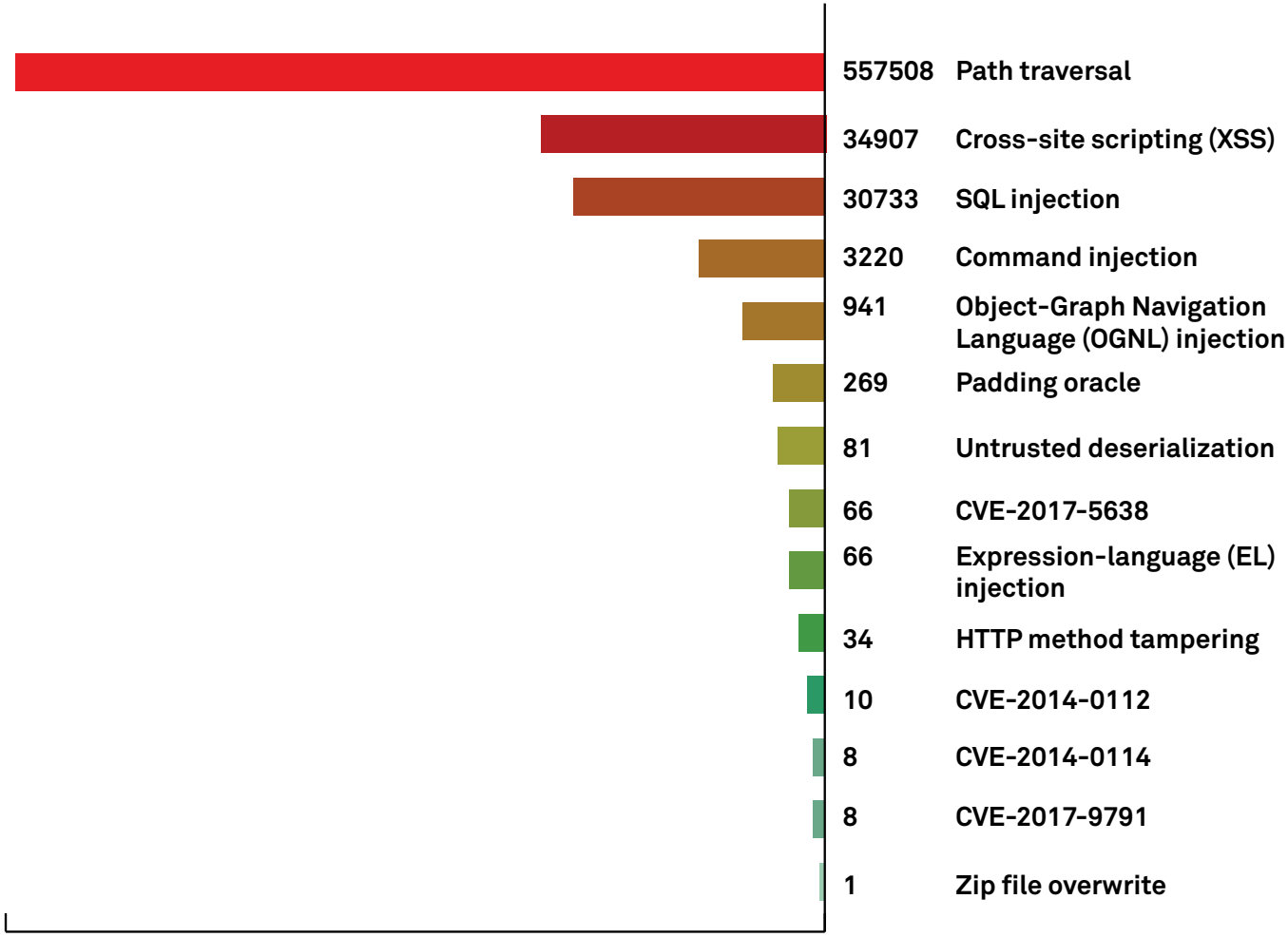
[12] Insecure Deserialization in AWS Lambda | What is the Vulnerability and How to Avoid It? | Contrast Security

Ground Truth

The Contrast Secure Code Platform continuously monitors and defends against application and application programming interface (API) attacks against Contrast's financial sector customers. On the right is a snapshot of real attacks launched against Contrast Security's FI customers over the past month.

"Malicious actors continue to leverage the most damaging attack vectors for the highest payout for them," said Contrast Security CISO Dave Lindner. "As we see more and more [Common Vulnerabilities and Exposures (CVEs)] released, we will see more widespread, coordinated attacks on known vulnerabilities that will affect a broad audience of technology segments.

"According to CVE.icu, in 2022, there was an increase in CVEs by ~25% YoY, with ~69 CVEs released per day for an average CVSS score of 7.19," Lindner pointed out. "These CVEs cover open source, [commercial off-the-shelf (COTS)] and everything in between. The increase of released CVEs YoY will continue in 2023, creating more potential avenues of attack for malicious actors, and requiring organizations to prioritize zero-day runtime protection now."



58%

58% have been victimized by island hopping. The financial sector is being targeted by cybercrime cartels and nation-states that are evolving in both attack sophistication and organization. Cyber defenders must modify their response to these cartels and embrace situational awareness.

These are not the bank heists of old, as mere wire transfer fraud is no longer the ultimate goal. We've entered a new era of conspiracy, in which cyber cartels' target is to hijack the digital transformation of an FI.

The modus operandi is simple: Infiltrate the corporate environment via application attacks or API attacks and then use access to the environment to launch attacks against the customer base. This is called island hopping[13]. There has been a dramatic increase in island hopping — an increase that represents a tremendous operational and reputational risk to victim organizations. Cybercrime cartels have studied the interdependences of FIs and now understand which managed service provider (MSP) is used and who the outside general counsel is.

FIs are concerned with the security posture of their shared service providers. Shared service providers, when compromised, pose a systemic risk to the financial sector as their infrastructure can be polluted to attack dozens of FIs at a time. This type of island hopping is very concerning.

50%

50% have experienced attacks against their APIs. We should expect to see APIs increase as an attack vector for a number of reasons:

- The total number of public and private APIs in use is approaching 200 million.
- There is a shift in new development approaches to microservices architecture.
- Shadow APIs abound.
- Continuous development leads to sprawl and versioning issues.
- Hybrid apps spanning on-premises, cloud and serverless environments increase the attack surface.

In response to recent significant API vulnerabilities and breaches[14], we will see organizations fully include APIs in their Application Security (AppSec) practices. Organizations will move beyond legacy scan and firewall approaches in favor of inside-out solutions that can understand the full context of API code. Organizations will also expand their open-source security programs and runtime protection initiatives to specifically include APIs.

[13] Brand protection in an era of island hopping | Contrast Security
[14] T-Mobile hacked to steal data of 37 million accounts in API data breach

30%

30% have experienced attacks against their serverless environments. Serverless environments represent a high-value target for cybercrime cartels. Serverless computing is a cloud-native model that allows developers to write code and deploy applications without needing to manage servers and other infrastructure running the services.

Serverless enables teams to deploy powerful code extremely quickly and without a lot of controls. Security teams should work to ensure they understand their function inventory, have full vulnerability and library testing in place for functions, and ensure that functions are deployed with only the privileges necessary to fulfill their purpose.

API security best practices

1. Maintain a complete inventory of APIs running in your environments, in development and exposed in production.
2. Perform full security testing against running APIs during development to identify and remediate unknown vulnerabilities.
3. Identify security gaps in the software supply chain. Find known vulnerabilities in active third-party libraries, frameworks and services.
4. Protect against zero-day attacks from day one by ensuring all APIs are deployed with runtime protection in place.

Contrast SECURITY

Trends in e-fraud

50% have detected campaigns to steal non-public market information. Our report finds that cybercrime cartels have realized that the most significant asset of an FI is not wire transfers or the access to capital; rather, it's nonpublic market information. This encompasses corporate information or strategies that can affect the share price of a company as soon as it becomes public, such as earnings estimates, public offerings and significant transactions. Fifty percent of financial institutions experienced attacks that targeted market strategies. This threat aligns with economic espionage and can be used to digitize insider trading and to front-run the market. Front-running is the illegal practice of purchasing a security based on advance nonpublic information regarding an expected large transaction.

48% experienced an increase in wire transfer fraud. Wire transfer fraud is still a significant challenge to FIs, but business email compromise (BEC) and digital check fraud are the dominant funds transfer used by criminal conspiracies.

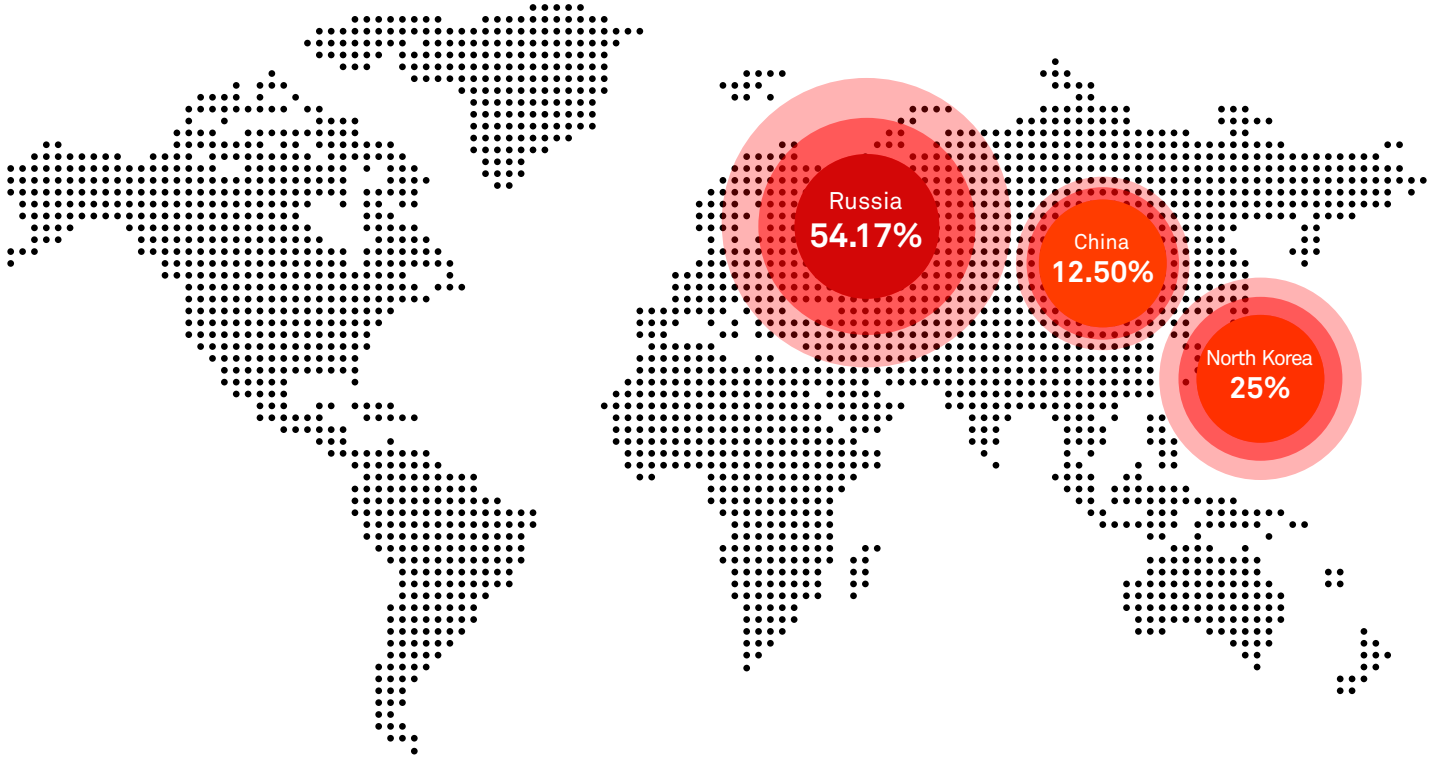
40% have been victimized by a ransomware attack. Five ransomware groups remained the most active this past year in the financial sector: Conti, LockBit, DarkSide, Yanluowang and Vice Society. Although these ransomware gangs represented a significant threat to FIs, the number of successful intrusions have diminished due to unprecedented efforts by Europol, the FBI, the U.S. Secret Service and the Cybersecurity and Infrastructure Security Agency (CISA) in disrupting and degrading the infrastructure, forums and alternative payments associated with these cybercriminals. In addition, FIs have invested heavily in extended detection and response (XDR) platforms and managed detection response (MDR) services that have enhanced their ability to defend against ransomware.

"The post-Conti fragmentation and proliferation of the Ransomware-as-a-Service ecosystem is a troubling development," notes Paul Sussman, Vice President and Global Lead of Cybersecurity Strategy at Booz Allen. "Access brokers have made breaches a commodity with an extremely high investment return, and disrupting this ecosystem requires vastly more effective countermeasures to address the innovation of threat actors.

"The financial sector remains a primary target of cybercriminals," Sussman continues. "Recent benchmarks indicate that both the frequency and the severity of cyber incidents is growing — a 'multiplier effect' that indicates rising cyber risk in the industry. Notably, the rate of growth is lower in [the financial services industry] than in other sectors, showing some level of success for the industry, but not enough to turn the tide."

Contrast SECURITY

54% of the banks were most concerned with the cyber threat posed by Russia.
Russia was closely followed by North Korea and China.



Geopolitical tension is metastasizing in cyberspace. The majority of FIs stated that Russia posed the greatest concern.

Note: Whereas empirical data shows that the majority of attacks originated in the West, this reality is due to cybercriminals using compromised western hosts as proxies. Vast swaths of western digital infrastructure is compromised, as evidenced by the "access brokerage[15]" marketplaces on the dark web.

[15] Initial Access Broker Market Booms, Posing Growing Threat to Enterprises

02

Trends in cyber defense

72% plan to invest more in AppSec in 2023. As evidenced by the Verizon Data Breach Investigations Report (DBIR)[16], application attacks are the attack vector of choice for cybercrime cartels. FIs have traditionally been overly reliant on Web Application Firewalls (WAFs) to defend against application attacks. Cybercriminals are well aware that WAFs can be bypassed by launching attacks that push into backend systems such as Message Queue (MQ), thereby enabling attacks to enter applications and APIs without having to go through a WAF. Others use different encoding techniques and complex syntax to bypass WAF rules.

The FIs who participated in this study will increase investment in runtime protection and API security. This was underscored by a recent Forrester survey of Security Technology Decision Makers wherein the vast majority of FIs have either adopted or plan to adopt runtime protection[17].

> "While many FIs have excellent AppSec teams, they are being pressured by new technologies, rapid development, complex architectures, new threats and burgeoning software portfolios. Unfortunately, most FIs have large vulnerability backlogs, aren't detecting and stopping app/API attacks, and aren't yet managing supply-chain risks effectively. The situation has forced governments around the world to demand increased transparency and even [Sarbanes-Oxley Act (SOX)-style] attestations to force better security. I believe organizations need to act now to establish an AppSec program that they are proud of: one that will enable them to share with the world the details of why people should trust their code."
>
> **— Jeff Williams, CTO and Founder, Contrast Security**

[16] 2022 Data Breach Investigations Report | Verizon
[17] Contrast Protect | Application and API Protection

64% mandate cybersecurity requirements to their FinTech vendors. For far too long, FinTech vendors have not undergone sufficient scrutiny of the security of their products and services. The surge in attacks against APIs underscores this stark reality. The majority of FIs are now contractually mandating cybersecurity requirements to these vendors, in the form of Software Bills of Materials (SBOMs)[18], security attestation[19] and compliance with the new minimum AppSec security standard from the National Institute of Standards[20] and Technology (NIST).

Internationally, there have been significant developments as well. Recently, Japan and the USA signed an agreement on software security standards as attacks on applications surged and foreign adversaries polluted software supply chains to island hop into government agencies. This agreement is paramount in order to defend Japanese and US cyberspace from ongoing Chinese attack campaigns. This marked a historic moment wherein the U.S. and Japan dramatically enhanced the security of their software supply chains through international cooperation. Many see this as an extension of the Five Eyes Alliance[21] to which Japan has been added.

The governance issue still abounds: 64% of CISOs still report to CIOs. In this age of anywhere work and heightened security risks, we must provide chief information security officers (CISOs) with a direct line of access to the CEO, along with greater authority and resources. In CISA's Shields Up guidance[22], the need to empower CISOs is the top recommendation for corporate leaders and CEOs to better protect their organizations.

As detailed in CISA's guidance, "In nearly every organization, security improvements are weighed against cost and operational risks to the business. In this heightened threat environment, senior management should empower CISOs by including them in the decision-making process for risk to the company, and ensure that the entire organization understands that security investments are a top priority in the immediate term."

The defensive mindset is necessitated at the top. That's why proactive FIs have elevated their CISOs to report to the CEO.

28% of these banks had a cybersecurity specialist on their board. Objective, holistic security guidance is fundamental in an era of cybercrime conspiracies and cyberespionage. Having a cybersecurity specialist on the board increases the authority and resources endowed to the CISO. It also provides an objective perspective on cyber risk and correspondent priorities. In 2023, the Securities and Exchange Commission (SEC) will likely require that FIs seat a cybersecurity specialist on their board of directors.

Offense must inform defense. Given the evolving cyber threat landscape to FIs, specific defensive countermeasures should be employed.

[18] Executive Order on Improving the Nation's Cybersecurity | The White House

[19] September 14, 2022 M-22-18 MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES FROM: Shalanda D. Young Director SUBJE

[20] AppSec Solution Guide for Complying with New NIST SP 800-53 IAST and RASP Requirements

[21] What is the Five Eyes Alliance?

[22] Shields Up | CISA

03

Top 10 countermeasures for Cyber Bank Heists

1. Deploy intelligent runtime protection[23].
2. Deploy an XDR platform.
3. Employ an MDR firm.
4. Conduct weekly threat hunting.
5. Microsegment your networks.
6. Deploy AppSec for serverless platforms.
7. Use multifactor authentication (MFA) and apply least privilege.
8. Defend your APIs.
9. Ensure code you develop is continuously tested for vulnerabilities.
10. Add a cybersecurity specialist to your board.

Cybercrime has a material impact on business operations. Cybersecurity can no longer be viewed as an expense but rather as a functionality of conducting business. This is no longer a question of duty of care but rather a duty of loyalty to the digital safety of your customers. Cybersecurity is a brand protection imperative. Trust and confidence in the safety of your institution depends on effectively mitigating and responding to cyberattacks.

[23] What Is RASP Security? Runtime Application Self Protection

04

Contrast report methodology

Participants interviewed for this study consisted of CISOs, SVPs of Cybersecurity, and Managing Directors of Information Security from global Tier 1 FIs (those with a minimum of $200 billion in assets) and Tier 2 FIs (those with between $5 billion and over $10 billion in assets).

About the author

Tom Kellermann is the Senior Vice President of Cyber Strategy at Contrast Security, Inc. Previously, Tom held the positions of Head of Cybersecurity Strategy for VMware, Inc. and Chief Cybersecurity Officer for Carbon Black, Inc., wherein he authored the "Modern Bank Heist Report" for the past five years. In 2020, he was appointed to the Cyber Investigation Advisory Board for the United States Secret Service. On Jan. 19, 2017, Tom was appointed the Wilson Center's Global Fellow for Cybersecurity Policy. Tom previously held the positions of Chief Cybersecurity Officer for Trend Micro, Inc., Vice President of Security for Core Security and Deputy CISO for the World Bank Treasury. In 2008, Tom was appointed a commissioner on the Center for Strategic & International Studies' (CSIS') Commission on Cyber Security for the 44th President of the United States. In 2003, he co-authored the Book "Electronic Safety and Soundness: Securing Finance in a New Age."

About Contrast Security

Contrast Security is the leader in modernized application security, embedding code analysis and attack prevention directly into software. Contrast's patented deep security instrumentation completely disrupts traditional application security approaches with integrated, comprehensive security observability that delivers highly accurate assessment and continuous protection of an entire application portfolio. This eliminates the need for disruptive scanning, expensive infrastructure workloads and specialized security experts. The Contrast Application Security Platform accelerates development cycles, improves efficiencies and cost, and enables rapid scale while protecting applications from known and unknown threats.

Contrast Security provides the industry's most modern and comprehensive Application Security Platform, removing security roadblocks inefficiencies and empowering enterprises to write and release secure application code faster. Embedding code analysis and attack prevention directly into software with instrumentation, the Contrast platform automatically detects vulnerabilities while developers write code, eliminates false positives, and provides context-specific how-to-fix guidance for easy and fast vulnerability remediation. Doing so enables application and development teams to collaborate more effectively and to innovate faster while accelerating digital transformation initiatives. This is why a growing number of the world's largest private and public sector organizations rely on Contrast to secure their applications in development and extend protection in production.

240 3rd Street
2nd Floor
Los Altos, CA 94022
Phone: 888.371.1333
Fax: 650.397.4133

Contrast SECURITY

contrastsecurity.com