

Cyberint

How The BFSI Industry Can Stop Threat Actors From Cashing In

Banks, financial services companies, and insurance enterprises are lucrative targets for threat actors.

This ebook covers the top 8 threats facing the BFSI industry and provides mitigation strategies to stop threat actors from making banks their cash cow.



USD

5M

Avg. cost of damages for
a breach in the financial industry

22%

Increase in phishing
attacks YoY

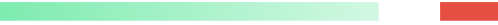
Cyberint

Introduction

With high annual revenues and large digital footprints, financial services companies have become favorite targets for threat actors.

While most financial institutions have sophisticated cybersecurity programs, there are still several major challenges: a surge in cyber attacks, a shortage of cybersecurity talent, massive and complex IT environments, and a distributed workforce that may not always adhere to corporate security policies.

These factors make it necessary for financial institutions to adopt a proactive approach that mitigates emerging threats prior to the development of full-blown attacks. A proactive security posture helps protect financial data across all touchpoints, and



makes it easier to monitor and defend against threats such as business executive targeting, compromised credit cards, phishing, fraud, and ransomware.

A prerequisite for increased cyber resilience is impactful threat intelligence. To pre-emptively configure cyber defenses, you must know the latest tactics and techniques of your adversaries. You must also have the visibility to identify attacks in the very earliest stages, giving you the opportunity to eliminate these threats before they can cause harm.

This report will highlight the 8 most pressing threats facing the banking, financial services, and insurance industries, and discuss how impactful threat intelligence can help proactively mitigate these risks.

50%

of all phishing attacks target the financial industry

151%

Increase in ransomware attacks



Fraud

With the acceleration of digital transformation in the banking industry, digital transactions and payments have become the default choice for individuals and businesses alike. This has turned financial institutions into highly profitable targets for threat actors.

Crafty cyber criminals have developed a number of scams to steal money from BFSI enterprises and their customers. Identity theft remains a prominent threat, as attackers use stolen PII and credit card details to make fraudulent payments. Other threats like insurance fraud, investment scams, and money laundering continue to present costly risks to the BFSI sector.

54%

of companies with global annual revenues over \$10 Billion that experienced financial damages from fraud during the past 24 months

PwC's Global Economic Crime and Fraud Survey 2022

Mitigation strategies:

Identify methods that threat actors use for fraud attempts

Discover weaknesses exploited by threat actors, as well as collaborations and transactions taking place in dark web forums, marketplaces, and dedicated messenger channels.

Thwart card clones and synthetic identity schemes

Expose the details of how threat actors obtained and abused cards and synthetic identities/aged accounts - and take measures to intercept or prevent their schemes.

Pre-emptively mitigate future attacks

Contextualize your threats with intelligence on entities, threat actors and attribution. Continuously monitor your adversary activity to ensure that no new attacks are being plotted for the future.



Phishing

Threat actors collect credentials using sophisticated phishing campaigns which trick users into surrendering their usernames and passwords. Attackers put enormous effort into creating convincing and up-to-date phishing sites, as well as phishing kits that make it much easier for other operators to launch phishing campaigns. There is a vast black market for phishing-related tools, products, and services on the deep and dark web.

16%

of corporate breaches begin with a phishing attack, costing an average of \$4.91 Million per incident.

IBM Cost of a Data Breach Report 2022

Mitigation strategies:

Monitor for lookalike domains

There's one clear indicator that threat actors are preparing a phishing attack against your organization: lookalike domains. Monitor the web for active domains, subdomains, and subdirectories that use your brand name or a lookalike variant.

Hunt for brand impersonation

When threat actors impersonate your brand— whether on a social media profile or a phishing site— the goal is almost always to steal credentials from your customers. Monitor the web for abuse of your brand trademarks and logos to fight these threats.

Optimize your takedown process

Once you've identified a phishing site, the next step is to respond and have the site taken offline. Establish a process and optimize it at every step to ensure a high takedown success rate and minimize your mean time to remediation.



Account Takeover

Obtaining and using credentials is a key attack vector for many types of cyber crime. Leaked credentials allow threat actors to enter an organization through the front door by taking over an employee or customer account. Once a threat actor is within the organization's network, effectively detecting them is more complex and even more urgent.

As such, threat actors are investing very big efforts to collect the freshest credentials, and extensive commerce in the deep and dark web is being conducted in specific markets, closed groups, and forums.

The fresher credentials are, the greater a threat actor's chances of successful account takeover - no stale passwords, obsolete users, etc.

25%

of U.S. adult consumers experienced identity theft in 2021. Among this subset of Americans, 64% experienced ATO fraud.

Aite-Novarica 2022 U.S. Identity Theft: Adapting and Evolving

Mitigation strategies:

Monitor deep and darkweb sources

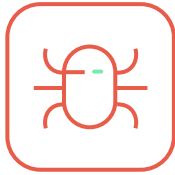
Monitor for dumps and combo lists on various sources in the deep and dark web. Monitor paste sites and Intercept Infostealers to catch credentials before being offered for sale. Take action as soon as leaked credentials are discovered.

Monitor and prevent emerging phishing campaigns

Monitoring emerging phishing campaigns can reduce the probability that actors steal credentials and gain privileged access in your organization's networks. Be prepared to take down phishing websites or pages the moment they go live.

Optimize your takedown process

Understanding what happened will help to prevent future recurrence. Find out everything you can about the leak: what emails and passwords, how many times each combination of email and password was seen, sources of credentials, the first time they were published, and so on.



Ransomware

Ransomware attacks are still the preferred way for actors to monetize their attacks. They keep increasing in volume and impact, leading to a cyber threat landscape that is evolving faster than cyber defenses. Financial companies are a preferred target as they possess a significant amount of valuable data.

Ransomware attacks target critical business data and PII, encrypt and/or exfiltrate that data, and extort ransom payments from the victim organizations. This data may be intellectual property, private employee or customer information, or passwords and access tokens that can be used to escalate privileges in the organization's internal IT systems.

\$1.98 Billion

in ransom payments were made to threat actors over the past 3 years.

Chainalysis 2023 Crypto Crime Report

Mitigation strategies:

Practice good security hygiene

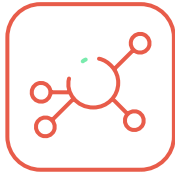
Maintain complete visibility on all of the publicly-visible servers and applications that you need to protect. Update software and services to eliminate known vulnerabilities. Take outdated websites, domains, and servers offline if they are not needed.

Detect misconfigurations in your attack surface

Continuously monitor your external attack surface to spot misconfigurations, exposed databases, high-risk open ports, old vulnerabilities, and other unnecessary risks. Be agile and remediate risks as quickly as possible.

Monitor the deep and dark web for evidence of a breach

The sooner you detect and respond to a breach, the lower the likelihood it will result in costly damages. Monitor the deep and dark web for evidence of an impending attack, such as leakages of employee credentials.



Malware

As consumer usage of finance apps rapidly expands, so too does their value as a target to cyber criminals. The threats are becoming more frequent, more complex, and more difficult to prevent using traditional security measures. Advanced strains of malware can easily bypass legacy security controls, anti-malware detection software, and user behavior analytics solutions.

Once deployed, malware like banking trojans, InfoStealers, and keyloggers begin stealing and exfiltrating sensitive data. This could be critical login and (multi-factor) authentication information, account holder and credit card details, account numbers, or other privileged information. With this valuable data in their possession, cyber criminals can launch additional attacks, sell their data to other attackers on the dark web, or attempt to extort the victim organization.

286,753,500

downloads from the Google Play Store of apps that are targeted by banking trojans.

Zimperium 2022 mobile banking report

Mitigation strategies:

Ensure continuous visibility of threat actor TTPs

Identify the use of rogue apps, malware, and banking trojans in app stores, as well as other tools that systematically stuff lists of credentials found in the dark web to gain access to your network.

Early detection of potential breaches and attacks

Get actionable alerts to prioritize attackware threats based on the motivation and capability of threat actors and the risk they present to your enterprise.

Mitigate and takedown threats

Discover, monitor and remediate against a broad range of threats that includes malware and other threats against your digital enterprise. Proactively remove threats when necessary.



Compromised Credit Cards

Although in decline due to the shift to digital wallets, compromised credit cards are still a prominent phenomenon. A variety of credit card tools and services are offered for sale in the deep and dark web: Phishing-as-a-Service (PhaaS), credit card sniffers for stealing information online, shimmers and skimmers for physical hacking of ATMs and POSs, and more.

Even if a threat actor isn't sophisticated enough to operate their own campaigns, they can simply purchase droves of compromised card details, including bin, holder name and PII, CVV, and more, for a nominal fee in dark web marketplaces. The surge in cyber crime over the past few years has lowered the barrier to entry and made it easy for unskilled threat actors to make a quick buck.

441,822

adults in the USA reported being a victim of credit card fraud in 2022.

US Federal Trade Commission Data Book 2022

Mitigation strategies:

Monitor for compromised credit cards

Identify and block compromised cards and the information associated with them (bin, account holder name and PII, cvv). Accelerate fraud mitigations and adapt fraud controls.

Learn about attackers' TTPs

Stay in the know about attackers tools and techniques. Learn who the key players are and what as well as who they're after. Understand how credit cards are getting stolen. Block, prevent, and prepare accordingly.

Proactively search for brand impersonation

Threat actors impersonate your brand with the goal of stealing PII and credit card information from your customers. Monitor the web for abuse of your brand trademarks and logos to fight these threats.



Business Email Compromise

Businesses are increasingly relying on external vendors and 3rd party suppliers as part of their ongoing business. As one would expect, these 3rd party suppliers require payments from the business consuming the product or services.

Business email compromise is a specific type of cyber crime where attackers impersonate either a 3rd party supplier or a senior executive to request payment of an invoice. For instance, threat actors impersonate the CEO and send a spoofed email to the finance department, demanding that an invoice be paid immediately. The finance team may not realize the email is a fraud and send the funds, making a direct transfer to the criminals.

While it may seem like a far-fetched scheme, business email compromise causes billions of dollars in losses every year.

\$2.4 Billion

lost to business email compromise scams and invoice fraud in 2021.

FBI Internet Crime Report 2021

Mitigation strategies:

Monitor your organization's VIPs

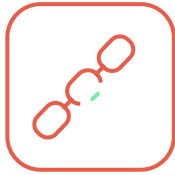
Protect VIPs and ensure that they are not being impersonated on social media. Monitor other discourse regarding your executives to maximize prevention of BEC campaigns.

Conduct security awareness training

Make sure your workforce understands the latest phishing and spear phishing TTPs. Train employees, especially those in the finance department, on how to spot a fake email and a fraudulent payment request.

Understand if and when you're being targeted

Investigate and contextualize your threats with adversary intelligence and attribution. Continuously monitor your threat actor activity to ensure that your organization is not being targeted in BEC attacks.



Supply Chain Risks

Threat actors are actively targeting software vendors, SaaS providers, and other business-to-business suppliers, as it amplifies the impact of a single breach. If attackers compromise 1 large supplier with many clients, this single breach could potentially give them access to dozens, hundreds, or even thousands of organizations' networks and data.

Mitigating 3rd party risks is a real challenge because the supply chain doesn't stop at your organization's immediate connections. If a supplier you do business with is using software created by a vulnerable vendor, and that vendor is breached, it could lead to a compromise of your supplier—and that, in turn, could result in a breach at your organization.

45%

of organizations worldwide will have experienced attacks on their software supply chains by 2025, according to Gartner.

Gartner

Mitigation strategies:

Continuously monitor the security posture of 3rd parties

Monitoring for the level of security hygiene of your supply chain partners and vendors sheds light on how much cyber risk they introduce for your organization

Track and assess security according to benchmarks

Identify benchmarks across industries and regions to compare them to your assessments of relevant third-party organizations. Ensure that your suppliers are beating the benchmarks.

Effectively prioritize and mitigate risks

Apply all knowledge and information gathered to effectively prioritize your risk mitigation. Do not hesitate to bring vulnerabilities, risks, and threats to the attention of your 3rd party suppliers.

Why Financial Organizations Choose Cyberint

Protect financial and banking data across all touchpoints in real time

Continuously monitor your most pressing threats, such as business executive targeting, payment card exposure or generation, ATM targeting, phishing, brand abuse, and fraudulent operations and scams.

Safeguard all facets of your online presence

Collect intelligence from a broad set of open sources and analyze potential threats using a combination of automated and manual techniques. Identify and remediate weaknesses in your external attack surface.

Mitigate and prevent fraud to reduce monetary loss

Detect the details of stolen customer credit cards, including credit card numbers, CVVs and expiration dates, together with the personal details of the cardholders on various deep and dark web forums. Block cards proactively to prevent their malicious use.



“With Cyberint, I have a level of assurance and trust that they are always there for me. The feeling that they always have my back is invaluable and has given me the confidence that we have enough visibility and can be proactive in dealing with different cyber threats.”

Mark Frogoso CISO, GCash



“With Cyberint, we know that we’re in safe hands. The Argos Edge platform provides us with very targeted and accurate alerts to stop cyber attacks. We also utilize Cyberint’s expert analyst team to help augment our intelligence needs.”

Bank Leumi



Cyberint

Recognized by the industry’s most respected analysts

Gartner

F R O S T
S U L L I V A N

FORRESTER

About Cyberint

Cyberint's impactful intelligence solution fuses real-time threat intelligence with bespoke attack surface management, providing organizations with extensive integrated visibility into their external risk exposure. Leveraging autonomous discovery of all external-facing assets, coupled with open, deep & dark web intelligence, the solution allows cybersecurity teams to uncover their most relevant known and unknown digital risks - earlier. Global customers, including Fortune 500 leaders across all major market verticals, rely on Cyberint to prevent, detect, investigate, and remediate phishing, fraud, ransomware, brand abuse, data leaks, external vulnerabilities, and more, ensuring continuous external protection from cyber threats.

