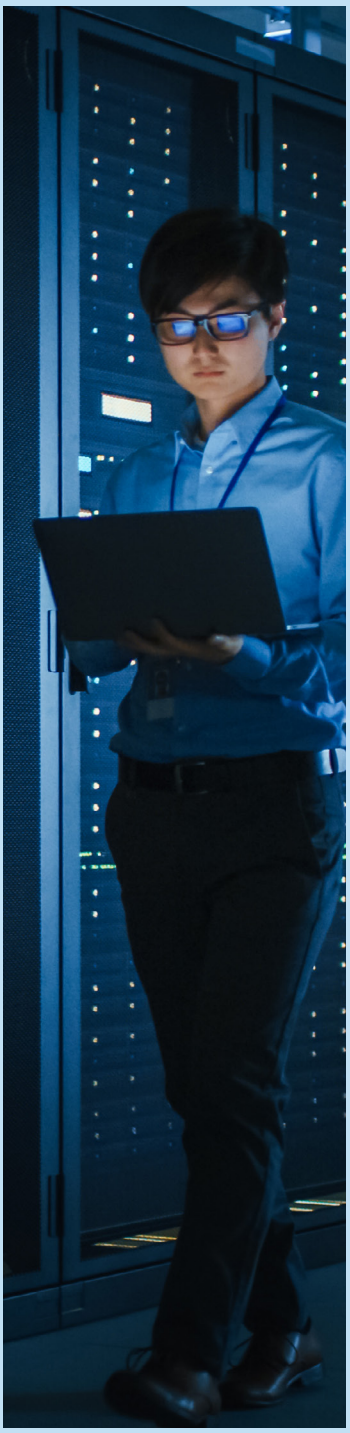
VIEW POINT



BETTER CYBER RESILIENCE MAKES FOR PROTECTED CUSTOMERS AND ENHANCED TRUST IN THE BFSI SECTOR

Infosys®
Navigate your next

Cyber Resilience in the BFSI (Banking, Financial Services and Insurance) sector

Cyber resilience refers to a hybrid discipline involving business continuity, enterprise resilience and information security, aimed at delivering the expected outcomes, withstanding, and recovering from adverse cyber events. It plays a pivotal role in having customers trust financial organizations to manage their assets and transactions while ensuring the CIA triad (Confidentiality, Integrity and Availability) through adequate controls and governance.

It has notably accelerated in the recent decades especially due to the significant evolution of the entire ecosystem including an expanded spectrum of stakeholders/ intermediaries, scaled up regulatory regimes globally, various technology advancements leading to a plethora of heterogenous IT systems, tools and processes, increased digitization (and virtual money), as well as new-age banking and enhanced customer experience. These apply to everyone in general – be it individual customers who deposit their paychecks and invest their savings for the future or a large corporate with portfolios worth billions of dollars and a large complex ecosystem often spread globally with wide spectrum of regulations and jurisdictions.

In this backdrop, let us look at the typical cybersecurity related risks in the BFSI space, why they happen and how to address them through preventive, detective and reactive controls

Key security risks in the Financial Services industry

1. Data and Identity Theft

In the current era of extreme digitization where "Data is the new Oil" and every individual / organization leaves digital footprints over the internet including various websites and social media, there is a high risk of critical data [including PII (Personally Identifiable Information) / PHI(Protected Health information) / SPI (Sensitive Personal Information) of individuals and confidential business data of organizations] getting compromised, leading to data breaches and/or stolen identities.

In the financial sector, this is extremely relevant and critical as digital trust is the foundation of most B2C or B2B transactions. Depending on the scale and severity of the breach, the impact could be very high especially if there are class action suits or regulator interventions (eg. penalties for data privacy issues governed through regulations like GDPR/CCPA).

2. Ransomware

According to Boston Consulting Group research, financial service firms experience up to 300 times as many cyber-attacks per year compared to companies in other industries. This could lead to downtime of mission critical systems and extortion through exfiltration & encryption, with a cascading impact to lives and businesses. Usually, individuals and organizations are forced to pay ransom to restore data/ operations

3. ATM malware and jackpotting

ATMs have historically been one of the weakest links in securing the financial sector especially due to the unique/ proprietary underlying software systems needing specialized skills. At times, ATMs rely on obsolete/insecure platforms like Windows XP with a host of critical unpatched vulnerabilities (including those allowing remote code execution), mostly due to the way the systems are configured without giving due attention to security risks.

Ever since the Trojan Backdoor.Win32. Skimer appeared in 2009, criminals have been using such malware to empty cash dispensers and to skim cards in infected ATMs. The modus operandi often followed has 4 stages –

i) Gain access to the machine
ii) Inject malicious code in the atm
iii) Reboot the atm to gain control
iv) Carry out actual theft of money

4. Sophisticated/automated threats

According to the Verizon Data Breach Investigations report, about 88% of security incidents in the finance sector fall into just three categories where the level of sophistication has been high: web app attacks, distributed denial-of-service (DDoS) attacks, and payment card skimmers.

Automated attacks carrying out credential cracking, vulnerability scanning, bad bots, credential stuffing, and denial of service can potentially shut down a company's critical systems quickly.

5. Emerging technologies – IoT and Blockchain

Financial institutions have been increasingly innovating to offer improved customer experiences and efficiencies across the spectrum, by leveraging IoT led digitization through intelligent and interconnected devices (which otherwise get leveraged for smart cities, smart homes, self-driving cars etc). A case in point has been leveraging IoT driven sensors in vehicles which are either pledged against loans or insured - this can help control thefts and track driving behavior to trigger periodic revision of the insurance premium. This boon can become a bane when not adequately protected against the prying eyes and malicious acts of attackers.

Blockchain, though still an emerging technology, has the potential to revolutionize the financial industry due to the increased convenience and efficiency it offers – not only for bitcoins, but also across the spectrum for digital id verification, payments, stock trading, audits, credit reporting etc. With encryption being a key component of the technology, strengthening the underlying security is critical for further adoption and expansion, as any compromise on the keys can lead to hijacking the ownership of protected assets, with potentially disastrous consequences.

Just having a comprehensive description of the nature of attacks and their type, isn't enough. It's important to decipher the reasons why these attacks take place in the BFSI sector. Certain security aspects when overlooked result in devasting repercussions. By being aware of such aspects, organizations can expertly mitigate cyber threats and have a more secured and robust business environment. Following are the list of rationales that must be considered as reasons why the financial industry gets targeted.

Key reasons due to which the financial industry gets targeted

1. Missing or incomplete view of the threat landscape

- Gaps in monitoring threats due to(hardware/software) asset inventory being outdated or heterogeneous in nature

2. Inadequate controls regarding user privileges

- Absence of role-based access, allowing users to have higher system privileges than warranted
- Direct employee access to privileged accounts without enough controls, potentially leading to unintended errors affecting the entire system

3. Insider Threats

- People are often said to be the weakest link in cybersecurity. In fact, cybercriminals often work to exploit fear and uncertainty during major world events by launching cyber-attacks
- While almost 1/4th of all security breaches occur at financial institutions, this is often attributed to not having the right security culture in the organization and/or individuals not having the necessary awareness on the security aspects, apart from cases of those motivated by nefarious intentions through credential thefts and other means
- According to recent data, cyber-attacks against the financial sector increased by 200+%, amid the COVID crisis
- Significant portion of such reported incidents are often caused by negligent employees or contractors through phishing, losing work devices, mistake while using equipment or intentionally giving away or selling PII/PHI for profit
- As per a 2020 report, the overall cost of insider threats increased by 31% from $8.76 million in 2018 to $11.45 million in 2020

4. Third party ecosystem with inadequate controls

- There is a potential risk to the employee and customer data from the organization's suppliers, partners, contractors, joint ventures as these entities have access to privileged systems
- As the security protocols and controls are not mature enough within most of these third parties, they often get exploited. Cyber attackers view them as an easy and convenient route to laterally get access to the organization
- Often missing is an ongoing risk management process needed throughout the lifecycle of the relationship

5. APTs – Including sophisticated threat actors

- The ever-expanding threat/vulnerability landscape gets exploited by leveraging abundant tools (including toolkits available on the Dark Web)
- When the keys become easily available in all forms and shapes, the doors and locks must be made stronger needing multiple layers to break open. Such a Defense in Depth approach is not often followed for security of critical systems. With multiple levels of security, organizations can detect, respond, and recover quickly even with eventualities of intrusions in the initial layer. This should be made available apart from adequate intrusion detection and prevention measures, following a Zero-Trust principle

6. Increased digitization

- Online banking has significantly increased (further accelerated by COVID-19) as financial organizations offer new age experiences through enhanced digitization
- This leads to social engineering, port scanners, packet sniffers, password cracking, trojans etc being leveraged to exploit a range of application vulnerabilities across data storage, authentication, and application code – thus expanding the threat surface
- Increased collection, storage, and transmission of PII/PHI due to increase in instant online/mobile banking (and less of brick-and-mortar branches) including cashless/contactless payments, compounds the risk to security and privacy

Key focus areas for mitigation

1. People - Educate, Enable, Empower and Examine

Initiatives to strengthen the security awareness among all stakeholders is key here. They should be empowered with adequate documentation and tools to take appropriate and swift action when required. Also needed are necessary controls to help track and report any interventions.

2. Process – Monitor, Measure, Assess, Analyze, Control, Correct and Prevent

Apart from enabling individuals, the security culture in an organization is greatly dependent on the processes and procedures it has and how they are designed, implemented and continuously improved over the entire lifecycle, right from monitoring to measuring, assessing, analyzing, putting in adequate controls, and taking corrective or preventive measures for any gaps observed.

3. Technology – Harden, Protect, Integrate, Standardize, Modernize

With IT/IS teams operating more as business enabling functions, it has become very critical to procure, secure, maintain, integrate, standardize and modernize the right set/size/spread of (application/infrastructure) technologies adequate to meet business goals and the emerging threat landscape.

4. Planning – Research, Document, Refine, Collaborate, Adapt, Enhance

Organizations should continue to strengthen their efforts in doing market research, document and refine this for better planning, increase internal/external collaboration, and enhance their enterprise cyber resilience capabilities.

5. Ecosystem – Evangelize, Integrate, Standardize, Enforce

With a rapidly evolving overall financial ecosystem of suppliers, vendors, partners, intermediaries, customers, regulators, governments etc, there is a need to work together as an integrated team towards higher levels of cyber resilience maturity. This includes mutual knowledge sharing to give different perspectives, design and enforce standards and best practices, so that none of the stakeholders become the weak link in the chain, with potential for overall disruption.

6. Management – Identify, Protect, Detect, Respond, and Recover

While it's important to take proactive measures as listed above (aligned with Identify and Protect phases as per NIST framework) to strengthen the security posture of the enterprise, no organization can have 100% assurance from any cyber security attack or impact. It's in this context that higher level of cyber resilience maturity requires adequate reactive measures be taken in the eventuality of an attack happening. It includes detecting, responding, recovering, and following a structured process to secure systems in an integrated ecosystem.

7. Governance – Strategize, Transparentize, Document, Optimize, Realize, Conform, Perform

As enterprise strategy and IT/security strategy gets increasingly integrated towards a common goal to minimize risks and maximize business value, there is an increased need for wider oversight from the enterprise leadership and the Board towards conformance (corporate governance aimed at accountability assurance) and performance (business governance aimed at value creation and resource utilization). This would involve defining the risk appetite, risk tolerance, ensuring there is adequate collaboration and transparency with all stakeholders including regulators, balancing across all these with appropriate prioritization.

Conclusion

Financial services organizations have been in the forefront of driving innovation by adopting state-of-the-art / emerging technologies (including AI/ML, IoT, Blockchain, RPA etc) and bringing in new ways of working, towards improved effectiveness and efficiencies, leveraging the economies of scale, and thereby optimizing customer costs and enhancing experiences. With the landscape continuing to be heterogeneous with co-existence of legacy systems that continue to be relevant and irreplaceable in some areas, ongoing changes or disruptions are expected at multiple levels, including risks related to compatibility or interoperability. Hence, it is imperative to have a constant focus towards strengthening the security posture in line with the ever-evolving ecosystem - through bringing in better "security first" organization culture, improving visibility of threats and vulnerabilities, and having solutions which are future-proof. This is the key to ongoing success, sustenance, and growth especially for organizations that are "built-to-last".

With Infosys CyberSecurity, our clients have Digital-trust. Assured. We help strengthen the cyber resilience maturity of our customers with a 360-degree view, including managing the aspects mentioned above. By driving an enterprise mindset towards Secure by Design at every stage of the business lifecycle, we minimize security risks while maximizing visibility of the security threat, impact & resolution. We also optimize costs and amplify reach while making customers Secure by Scale, ensuring that our focus on innovating next-gen threat protection solutions in newer technologies will Secure the Future of customer's business.

Hundreds of our clients including Fortune 500 companies across BFSI and other industries have entrusted the security management of their critical systems to us and would bear testimony to our capabilities and delivery excellence.

References

https://enterprise.verizon.com/resources/reports/dbir/2020/data-breach-statistics-by-industry/financial-services-data-breaches/

https://www.attilasec.com/blog/banking-industry-cyber-threats

https://en.wikipedia.org/wiki/Cyber_resilience

https://cyberexperts.com/%EF%BB%BFcybersecurity-threats-in-the-banking-sector/

https://sqnbankingsystems.com/blog/the-5-biggest-threats-to-a-banks-cyber-security/

https://www.plugandplaytechcenter.com/resources/cybersecurity-threats-financial-institutions/

https://www.helpnetsecurity.com/2020/06/17/cybercriminals-sophisticated/

https://www.consumeraffairs.com/finance/identity-theft-statistics.html

https://www.theparliamentmagazine.eu/news/article/cybersecurity-the-trustbuilding-core-of-banking

https://dzone.com/articles/top-5-iot-security-challenges-to-expect-in-2020

https://youteam.io/blog/10-use-cases-of-blockchain-technology-in-banking/https://www.marketwatch.com/story/this-is-the-biggest-risk-to-the-financial-system-say-ceos-of-the-largest-us-banks-2019-04-10

https://www.kratikal.com/blog/why-cyber-security-in-banking-is-important/

https://www.arcjournals.org/pdfs/ijmsr/v3-i6/7.pdf

https://securelist.com/malware-and-non-malware-ways-for-atm-jackpotting-extended-cut/74533/

https://www.globalbankingandfinance.com/hackers-can-now-empty-out-atms-remotely-what-can-banks-do-to-stop-this/

https://thycotic.com/company/blog/2019/10/15/swift-controls-cyber-crime-privileged-access-management-pam/

https://www.kratikal.com/blog/insider-threat-the-biggest-contributor-to-cyber-attacks/

https://www.rsaconference.com/library/blog/navigating-the-threat-from-within-insider-threats-in-the-finance-industryhttps://www.enterprisetimes.co.uk/2020/12/22/why-insider-threat-presents-a-big-risk-to-financial-services-organisations/

https://www.observeit.com/solutions/financial-services/

https://www.observeit.com/wp-content/uploads/2020/10/2020-Proofpoint-Managing-Insider-Threats-in-Financial-Services-ebook-0512-002-01-01.pdf

About the author

Oommen Thomas
Associated with the Cyber Security Practice at Infosys

Oommen Thomas is associated with the Cyber Security practice at Infosys, where he is involved in managing GTM strategies of industry leading offerings and optimal business aligned solutions for global customers. He is an enthusiast on innovations in the Cyber Security space and has been actively associated with various security/privacy/management domains through forums like ISACA, IAPP and PMI. A continuous learner with close to 3 decades of IT industry experience handling multiple domains, roles and functions, Oommen has been certified in CGEIT, CRISC, CISM, CSX-P, CPISI, ISO27001-LA, DP/GDPR-LI, CIPP/E, TOGAF, PMP and ITIL.

For more information, contact askus@infosys.com

Infosys®
Navigate your next