Reducing Cyber Risk for the Financial Service Industry

The financial services industry is a leading target for cyber criminals because there's more than one way one way to profit from an attack. Whether it's the direct theft of funds and customer data, extortion, or fraud, financial institutions have a metaphorical bullseye on their backs when it comes to cybercrime, and that only gets worse when you add third parties into the mix.

Third parties are one of the top attack vectors and according to a recent Ponemon report, in the last three years, the financial services industry experienced the second most third-party breaches despite spending the most time on assessments (over 17,000 hours/year).

The head of the European Central Bank (ECB) warned that a combined cyberattack on vital banks could trigger a worldwide financial crisis and complete industry instability. Using well-known social engineering methods such as ransomware, phishing, data leakage, and unsecured applications, bad actors are perpetrating destructive and disruptive attacks that cripple the industry's ability to provide critical services.

Financial Services are Under Attack

Cyber Incidents in the Banking Industry

DATA LOSS

12,405
Dataloss Incidents

189.4%
Increase

Attacks of inadvertent usage that result in exposure or loss of sensitive information.

Examples: Unauthorized access, disclosure of personally identifiable information, theft of intellectual property, accidental disclosure of personal health information.

DISRUPTIVE ATTACKS

12
Disruptive Incidents

0%
Constant

Attacks that degrade performance or interrupt the flow of information, reducing overall system effectiveness.

Examples: Denial of service attacks, domain name system hijacking, and website defacement.

DESTRUCTIVE ATTACK

185
destructive incidents

-41.7%
Decrease

Attacks that render a device or application unusable without complete rebuild, or that deny access to a system.

Examples: Ransomware, logic bombs, source code destruction, destructive malware.

FRAUD

219
fraud incidents

-23.4%
Decrease

Attacks that use deception or target the integrity of business process, leading to non-compliance, asset loss, or financial manipulation and misrepresentation.

Examples: Social media disinformation campaigns, CEO fraud ("Business E-mail compromise"), wire transfer compromise, financial statement manipulation.

Regulations in the Financial Services Industry

NYDFS Cybersecurity Regulation

In response to the growing threats, regulators are implementing more controls in the form of legal and regulatory efforts. To put it a different way, in order to strengthen the industry's defenses, there are more compliance requirements than ever before. Included in those regulations, is the requirement to perform due diligence commensurate to the threats associated with third parties, meaning just outside-in passive scanning is not enough. Third parties need a combination of outside-in scanning and control responses with validation applied to attack scenarios so that financial institutions have a mechanism to prioritize the risk mitigation efforts.

The NYDFS Cybersecurity Regulation (23 NYCRR 500) is one example. This regulation applies to all entities operating under or required to operate under DFS licensure, registration, or charter, or which are otherwise DFS-regulated, as well as, by extension, unregulated third-party service providers to regulated entities.

A cybersecurity program that's in compliance with the NYDFS Cybersecurity Regulation will adhere to several requirements that are based on the NIST Cybersecurity Framework:

- Identify all cybersecurity threats, both internal and external.
- Employ defense infrastructure to protect against those threats.
- Use a system to detect cybersecurity events.
- Respond to all detected cybersecurity events.
- Work to recover from each cybersecurity event.
- Fulfill various requirements for regulatory reporting.

In order to satisfy an important part of NYDFS Cybersecurity Regulation, third-party assessment services help banks with cyber risk management, including due diligence and ongoing monitoring, two areas where auditors and regulators focus their time. More specifically:

- **Coverage & Quantity (Due Diligence):** Is the financial services company managing risk against their entire population of third parties? Do they have complete visibility to do this?
- **Consistency and Quality (Ongoing Monitoring):** Is the bank performing the proper level of due diligence commensurate to the threats from the third parties? Are these third parties being re-assessed at least annually to determine if their security posture has changed?
- **Comprehension across third party ecosystem:** Does the financial services company have the ability to identify which third parties are susceptible to newer vulnerabilities? Can they compare third parties across their peers and identify which ones are more likely to be compromised?

APRA CPS 234

Another example is the Prudential Standard CPS 234, released by the Australian Prudential Regulation Authority (APRA), which requires regulated entities to have information security capability commensurate with the size and extent of threats to its information assets including those managed by third parties. APRA CPS 234 specifically calls out lot of requirements for managing third-party risk. A regulated organization must:

- Maintain a third-party risk management policy along with other information security policies. The third-party risk management policy should clearly highlight that entities will take steps to ensure the third-party's security capabilities are commensurate to the information's security risks. The entity should ideally include this as part of the contract with the third party.
- Review the contracts with their third parties and update the requirements for third parties for maintaining information security capabilities. Furthermore, the entity should clearly define the timelines (<72 Hours) and responsibilities of the third parties in the case of any incident or a material information security control weakness within 10 business days of identification.
- Have visibility into the services that are consumed from third parties. They should evaluate which third parties have access to information assets and classify the entire third-party population based on size and extent of threats to its information security assets by the third-party relationship (i.e. type of services, type of data they access, how they access, etc.).
- Assess the information security capabilities (both design and operating effectiveness) of the third parties; at the time of onboarding, when there's a change in the service, as well as periodically on an ongoing basis.
- Provide visibility to the board and senior management on the risk associated with their third parties.

The issue of cybersecurity regulations isn't something that is unique to the United States or Australia. In an attempt to assist financial institutions in their ongoing quest for cybersecurity, G7 governments released *Fundamental Elements for Third Party Cyber Risk Management* in the Financial Sector which is, "a set of Fundamental Elements for entities to tailor, as appropriate, to their specific risk profiles, operational and threat landscape, role in the sector, and legal and regulatory frameworks."

This document contains six elements of the Third-Party Cyber Risk Management Life Cycle:

Element 1: Governance – Entities' governing bodies are responsible and accountable for effective oversight and implementation of third-party cyber risk management.

Element 2: Risk Management Process for Third-Party Cyber Risk – Entities have an effective process for managing third-party cyber risks through the entire third-party risk management life cycle.

Element 3: Incident Response – Entities establish and exercise incident response plans that include critical third parties.

Element 4: Contingency Planning – Entities have appropriate contingency plans in place to address situations where third parties fail to meet cyber-related performance expectations or pose cyber risks outside the entity's risk appetite.

Element 5: Monitoring for Potential Systemic Risks – Third-party relationships across the financial sector are monitored and sources of third-party cyber risk with potential systemic implications are assessed.

Element 6: Cross-sector coordination – Cyber risks associated with third-party dependencies across sectors are identified and managed across those sectors.

How We Can Help

Reduce Risk & Scale your TPCRM Program with the CyberGRX Exchange

Developed by professionals with financial services industry experience, CyberGRX brings visibility, scalability, and accuracy to third-party cyber risk management programs (TPCRM) around the globe. We understand the importance of identifying and mitigating cyber risk due to third parties introduced because of Digital Transformation and the need to become more agile. Together with enhanced privacy controls, you can effortlessly meet third-party regulatory requirements that apply when data is shared with third parties, reducing your cyber risk even more.

The CyberGRX Exchange is a centralized hub where enterprises and third parties can easily access, order and share thousands of dynamic, cyber risk-based assessments to help manage risk across security, privacy, and business continuity. Coupled with these dynamic assessments, advanced analytics capabilities protect you against downtime and disruption with an up-to-date view of risk for continuous monitoring and mitigation insights. We provide invaluable visibility through the entire TPCRM life cycle.

Innovative solution that reduces the cyber risk of your third-party vendor ecosystem

- Maps to custom frameworks as well as over 30 industry standards and frameworks NIST –800.53, NIST-CSF, ISO 27001, PCI-DSS, HIPAA, NERC, GDPR, CCPA, NY-DFS, and CMMC
- Move past point in time assessments to continuous assessments and monitoring to mitigate any risk of disruption before it happens
- Utilize threat use cases built on MITRE tactics and techniques that streamline curation, reuse, and modularity, allowing CyberGRX to rank susceptibility to specific tactics or techniques
- Applies attack scenario modeling and inherent risk analysis against assessment results to create a prioritized control gap analysis
- Rapidly identify and prioritize the third parties who pose you the most risk with Auto Inherent Risk (AIR) Insights™
- Instantly create and prioritize a risk mitigation and assessment strategy upon ingesting your third party portfolio
- Manage your evolving ecosystem with a scalable exchange
- Review a before and after comparison of inherent and residual risk to identify the type of attacks to which your third parties are susceptible
- Provides ability to perform peer review across third-party controls and identify controls which are commonly failing across your ecosystem, allowing you to make informed decisions.
- Accurately identify third parties which are susceptible to newer vulnerabilities and threats, allowing you to take control of the risk associated with your third parties
- Accurately forecast spend due to a fixed pricing model and sharing of expenses with other companies via exchange economics, allowing organizations to do less with more
- Eliminate lengthy delays in receiving vital risk data and driving rapid decisions around third-party selection, renewal, and SLA terms

What This Means for the Financial Services Industry

Enterprise		Third Parties
Identify the third parties that pose you the greatest risk	✓	Never complete another shared spreadsheet again
Create a prioritized risk-based mitigation strategy	✓	Identify the remediation with the most yield
Continuously monitor your ecosystem to prevent supply chain disruptions	✓	Fill in one assessment, and share it with as many upstream partners as you like
Create a scalable program that can accommodate your entire ecosystem	✓	Drive business growth by demonstrating your proactive engagement with your security posture
Map Your CyberGRX assessments to other frameworks to show how you align to a variety of standards	✓	Quickly illustrate how your security posture maps to industry standards

Visit our website and contact us today for a free trial

www.cybergrx.com