Cyber threats continue to increase in sophistication and evolve and pose an existential risk to the government[1] and all industries, including the financial services industry. The Department of Homeland Security defines a cyber threat to mean "persons who attempt unauthorized access to a control system device and/or network using a data communications pathway."[2] NIST takes a broader view of the definition of the term cyber threat as "Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service."[3] Regardless of which definition is adopted by an institution, access can be directed from within an organization by trusted users or from remote locations by unknown persons using the Internet. Threats to control systems can come from numerous sources, including hostile governments, terrorist groups, disgruntled employees, and malicious intruders.[4]

According to *Forbes, "*the typical American business is attacked 4 million times per year, the typical American financial services firm is attacked a staggering 1 billion times per year." U.S. banks lost approximately $16.8 billion to cyber criminals in 2017[5], and the aggregate projected cost of damage from cybercrime worldwide across industries is estimated to reach $6 trillion by 2021.[6] A 2018 IMF study suggests that average annual potential losses from cyber-attacks may be as high as 9% of banks' net income globally.[7]

The effects of cyber-attacks include reduced availability or diminished response times of online banking services, identity theft, fraud, and theft of proprietary information. The costs and resources needed to mitigate the risks continue to increase as the attacks increase in frequency, scope and sophistication.

Cyber threats continue to target vulnerabilities in bank and third-party systems. Depending on their objectives, malicious actors may seek to expose or obtain large quantities of personally identifiable information and intellectual property, facilitate misappropriation of funds and data, corrupt information, and disrupt business activities. Failure to maintain proper cybersecurity controls, both internally and for third-party service providers, can lead to material adverse impacts on a bank or systemic risk. Banks are generally responding well to common cyber events, but malicious actors continue to improve their tools and tactics, requiring banks to continually reassess and validate their cybersecurity controls.[8]

---

[1] *See* "Secretary of the Navy, Cybersecurity Readiness Review," March 2019. https://www.navy.mil/strategic/CyberSecurityReview.pdf

[2] https://www.us-cert.gov/ics/content/cyber-threat-source-descriptions

[3] *See* CNSSI 4009-2015 under threat (NIST SP 800-30 Rev. 1)

[4] *Id.*

[5] *See https://www.forbes.com/sites/bhaktimirchandani/2018/08/28/laughing-all-the-way-to-the-bank-cybercriminals-targeting-us-financial-institutions/#239f0de16e90*

[6] https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

[7] *See* "IMF Working Paper Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment,"

[8] https://www.occ.gov/publications-and-resources/publications/semiannual-risk-perspective/files/pub-semiannual-risk-perspective-spring-2019.pdf

Cyber-attacks can have serious consequences for institutions, including:

- Reduced availability or diminished response times of online banking services;
- Identity theft;
- Fraud;
- Theft of proprietary information;
- Loss of customers/loss of revenue;
- Costs to remediate;
- Legal fees, judgments, fines/penalties;
- Increased regulatory scrutiny; and
- Loss of reputation

Cyber Risk Metrics

RMA's Operational Risk Council has compiled the following metrics to assist institutions in assessing and managing cyber risk across certain dimensions, namely, Vulnerabilities; Incidents; Events and Breaches; Patch and Account Management; Third Parties; Cyber Risk Awareness Training; and Audit Findings and Risk Ratings:

Vulnerabilities				
No.	**Metric**	**Description**	**KPI**	**KRI**
1	Critical/high vulnerabilities not patched within benchmark; e.g., SLA or risk acceptance time frame	Reflects the total number of critical and high vulnerabilities identified but not patched within the required SLA across the institution. **Note:** Critical/High severity designation is based on the vulnerability management model deployed by the institution.		√
2	Average number of high web application vulnerabilities per asset	Number of total scanned web application vulnerabilities over total number of web-facing assets.		√
3	Percent of high rated vulnerabilities past SLA or risk acceptance timeframe (Infrastructure)	High severity designation is based on the vulnerability management model deployed by the institution. The SLA duration is set in alignment with the institution's risk appetite for vulnerabilities, and the measurement of the time past SLA commences when a fix or workaround is available.		√

8 https://www.forbes.com/sites/bhaktimirchandani/2018/08/28/laughing-all-the-way-to-the-bank-cybercriminals-targeting-us-financial-institutions/#3da80a526e90

4	No. of high rated vulnerabilities past SLA or risk acceptance timeframe/No. of total high rated vulnerabilities	This measure is for infrastructure-aligned vulnerabilities only, which tend to be more discreet and, therefore, more voluminous in nature.		√
5	Percent of high rated vulnerabilities past SLA or risk acceptance timeframe (Application)	High severity designation is based on the vulnerability management model deployed by the institution. The SLA duration is set in alignment with the institution's risk appetite for vulnerabilities, and the measurement of the time past SLA commences when a fix or workaround is available. **Note:** This is the same description as No.1 above, but is aligned to application-specific vulnerabilities only. These are segregated from infrastructure vulnerabilities because application vulnerabilities tend to be different in scope, impact and overall size of remediation (e.g., revision of code v. application of a patch/modification of a configuration).		√
6	No. of high rated vulnerabilities past SLA or risk acceptance timeframe/No. of Total high rated vulnerabilities	High severity designation is based on the vulnerability management model deployed by the institution. The SLA duration is set in alignment with the institution's risk appetite for vulnerabilities, and the measurement of the time past SLA commences when a fix or workaround is available. **Note:** This is the same description as No.1 above, but is aligned to application-specific vulnerabilities only. These are segregated from infrastructure vulnerabilities because application vulnerabilities tend to be different in scope, impact and overall size of remediation (e.g., revision of code v. application of a patch/modification of a configuration).		√
7	No. of open vulnerabilities	Based upon scan results. **Note:** This is a point-in-time measurement.		√
8	No. of Internet-facing systems with vulnerabilities	The total number if Internet-facing systems vulnerabilities from scans not patched within SLA for that month. **Note:** This is a total number of systems, not vulnerabilities.		√
9	Percentage of critical vulnerabilities patched within 30 days/total number of vulnerabilities	Highlights critical vulnerabilities for which a patch was published within the preceding 30-day period.	√	
10	Boundary assets with past due vulnerabilities	Percentage of boundary assets with one or more past due critical vulnerabilities		√

11	Core assets with past due vulnerabilities	Percentage of core assets with one or more past due critical vulnerabilities		√

INCIDENTS, EVENTS & BREACHES			**KPI**	**KRI**
1	High Severity Data Loss Protection Violations Blocked	Reflects the total number of Data Loss Protection Violations blocked across the institution on a monthly basis		√
2	No. of Information Security Events with Business Impact	Reflects the total aggregate number of high severity security events that occurred across the institution on a monthly basis		√
3	No. of Confirmed Security Breaches (Non-Fraud)	Calculated by adding (A) confirmed data breaches of an internal system and (B) notifications of a confirmed breach of a third party's system.		√
4	No. of Confirmed Security Breaches (Fraud)	Calculated by adding (A) confirmed data breaches of an internal system and (B) notifications of a confirmed breach of a third party's system.		√

PATCH & ACCOUNT MANAGEMENT			**KPI**	**KRI**
1	Average no. of open patches per device			√
2	Percentage of patches that are applied fully automatically	Measures the extent to which manual intervention is needed to install patches on IT assets; manual patching could result in extended exposure to risk.		√
3	Percentage of critical vulnerabilities patched within 7 days/total number of vulnerabilities		√	
4	Percentage of high severity vulnerabilities patched within 30 days		√	
5	Average no. of high severity missing patches per asset	Number of unique critical (patches to be applied within 7 days)/high severity (patches required to be applied within 30 days) patches open per asset		√
6	No. of emergency patches	Measured quarterly		√
7	Timely Removal of Network Access for Departing Employees	Measures the percentage of departing employees (voluntary and involuntary) whose network access was not removed on time per the institution's access administration policy; aggregated quarterly		√
8	Administrator IDs on workstations			√

THIRD PARTIES	**KPI**	**KRI**

1	Percentage of Tier 1 technology third parties with high residual risk	Identify the number of Tier 1 technology third parties that have a high residual risk. A Tier 1 third party is one which has access to sensitive or critical information.	√	
2	High risk overdue vendor findings			√
3	High risk vendor technology control gaps with no remediation plan			√

CYBER RISK AWARENESS TRAINING & PHISHING EXERCISES			**KPI**	**KRI**
1	Percentage of employees that completed phishing training on time			√
2	Percentage of employees that failed phishing test in a 30-day period	Reflects the percentage of employees who failed a phishing test with the total number of employees that received the test on a monthly basis		√
3	No. of employees that failed 2 or more phishing tests in a 12-month period			√

AUDIT FINDINGS & RISK RATINGS			**KPI**	**KRI**
1	Past due high severity issues	Reflects the total number if past due high inherent risk issues		√
2	Past due audit management action plans for critical/major findings	Reflects the total aggregate number of past due audit management action plans for critical/major findings		√
3	Security Rating	External cyber security rating (similar to a FICO score)		√