Cyber Risk Definition and Classification for Financial Risk Management

Filippo Curti, Jeffrey Gerlach, Sophia Kazinnik, Michael Lee and Atanas Mihov*

July 14th, 2020

* Filippo Curti, Jeffrey Gerlach, Sophia Kazinnik, and Atanas Mihov are at the Federal Reserve Bank of Richmond. Michael Lee is at the Federal Reserve Bank of New York. Email addresses: filippo.curti@rich.frb.org; jeffrey.gerlach@rich.frb.org; sophia.kazinnik@rich.frb.org; michael.j.lee@ny.frb.org; atanas.mihov@rich.frb.org. We thank Tom Barkin, Nida Davis, Michelle Gluck, Greg Gupton, Marco Migueis, Keith Morales, Nika Lazaryan, Hema Parekh, Will Robinson, and David Stabenaw for helpful comments and suggestions. We thank Cooper Killen and James Schulte for excellent research assistance. The views expressed in this article are solely those of the authors. They do not necessarily reflect the views of the Federal Reserve Bank of Richmond, the Federal Reserve Bank of New York, or the Federal Reserve System.

INTRODUCTION

Cyber incidents pose a major threat to the financial system. Cyberattacks on traditional financial institutions and cryptocurrency exchanges alike are estimated to have resulted in the theft of billions of dollars. The hacks of major financial firms, consumer credit reporting agencies, retailers and government agencies have compromised the personal information of hundreds of millions of individuals. Data breaches of third-party service providers put intellectual property and confidential information of their serviced financial firms at major risk. Ransomware attacks have infected hundreds of thousands of computer systems globally.

A number of factors contribute to cyber risk at financial institutions, including an increasing trend in globalization, the use and early adoption of quickly evolving technology, the significant dependencies and interconnections within both the financial system and information technology infrastructure, the growing sophistication of cyber criminals, and the intrinsic nature of financial institutions' business and services. Aware of the risks associated with cyber incidents, supervisors and regulators across the world have started taking steps intended to mitigate cyber risk at financial institutions, including enhancing resiliency capabilities and implementing plans for effective response to and recovery from cyberattacks.

Even though cyber risk is recognized as a significant threat to financial stability, the measurement and analysis of cyber risk in the financial sector has not matured to the point where it can be consistently measured and managed against corporate risk appetites and viewed from a system perspective by regulators and supervisors. This impedes efforts to effectively measure and manage such risk, diminishing institutions' individual and collective readiness to handle system-level cyber threats. In order to begin to classify such risk, this document provides a preliminary cyber risk definition and classification of cyber risk for risk management purposes. As such, the proposed definition and classification would ensure adopting institutions are utilizing common language and allowing consistent data collection and sharing.[1,2] This work can additionally support the application of modeling frameworks such as Factor Analysis of Information Risk (FAIR) to quantify and measure risk in the financial sector. The cyber loss definition and classification provided in this document, however, are intended to standardize, not necessarily replace, current bank practices. It is also

[1] Data on cyber losses in the financial industry do not exist in a consistent and comprehensive way. Available data products are largely based on publicly available information. Vendors include CyberDB (https://cyberdb.co/), ORX (https://managingrisktogether.orx.org/), Advisen (https://advisenltd.com/) and Verisk (https://verisk.com/).

[2] Appendix C: Classification Examples provides an illustration of the proposed classification scheme through examples. Appendix A: Data Collection Form provides examples of prospective data collection forms that are deemed useful from a financial risk management perspective. The Federal Reserve System or other regulatory agencies might be particularly well-positioned to facilitate and coordinate data collection efforts due to their secure information technology and data warehouse infrastructure, commitment to information and data confidentiality, and non-profit business orientation. Collected data could be additionally analyzed and used by the Federal Reserve or other regulatory agencies to provide horizontal perspectives on cyber risk management and mitigation for the benefit of participating financial institutions.

important to note that this initiative is not intended to address information technology or system engineering dimensions of cyber risk, but rather to focus on financial risk management aspects of cyber risk.

OBJECTIVE OF CYBER RISK DEFINITION AND CLASSIFICATION

The objective of this paper is to formalize a cyber risk definition and classification in order to support the work of regulatory agencies and private sector participants to facilitate cyber risk management in the financial sector. A cyber risk definition and classification could be useful to support work in the following areas:

Cross-sector shared recognition and identification of relevant cyber risks. A common definition and classification could be useful to foster a common understanding of cyber risks and their underlying triggers. A common definition and understanding across the financial sector, including among authorities and private participants, could further facilitate information sharing and appropriate cooperation in cyber risk management.

Assessment and monitoring of financial stability risks. As regulatory and supervisory agencies assess and monitor financial stability risks associated with cyber incidents, this work could be supported by a common definition and classification of cyber risks. For instance, as part of their assessment of vulnerabilities in the US financial system, regulatory and supervisory agencies consider the potential for operational risks, including cyber risks, to result in shocks that could be transmitted across the financial system.

Data collection and information sharing. A definition and classification that supports a common understanding across the financial sector can help advance data collection and information sharing critical to enhancing a collective knowledge on cyber risk by offering a coherent framework for creating and managing data and enabling systematic and compatible aggregation of information.

Regulatory guidance related to cyber risk management. A common classification could enhance the work of regulatory and supervisory agencies in providing guidance related to cyber security and cyber resilience, including identifying effective practices and/or emerging threats. For example, utilizing common language helps foster effective regulatory approaches while reducing the risk of duplicative and potentially conflicting regulatory and supervisory requirements.

In general terms, a common definition and classification will facilitate work in the areas outlined above. While the cyber risk definition and classification are intended to support work that regulatory and supervisory agencies and private sector participants determine to undertake in those areas, they are designed as helpful tools and their use is not mandatory.

CYBER RISK DEFINITION

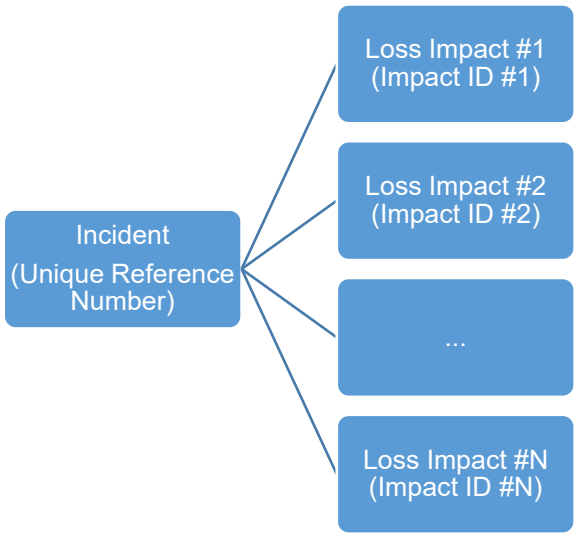
While definitions exist in different contexts (e.g., Financial Stability Board's *Cyber Lexicon*), for financial risk management purposes, this document regards cyber risk as a form of operational risk and defines it as the risk of loss resulting from digital incidents caused by internal, external or third parties, including theft, compromised integrity and/or damage to information and/or technology assets, internal and external fraud, and business disruption. Notably, this definition is largely consistent with known concurrent private sector efforts to define cyber risk (e.g., ORX's Cyber and Information Security Risk Initiative). Cyber risk incidents may impair the confidentiality, integrity and/or availability of data and information, and the proper functioning of information technology infrastructure.

We define *cyber incident* as an observable occurrence in an information system that a) jeopardizes the cyber security of an information system or the information the system processes, stores or transmits; or b) violates the security policies, security procedures, or acceptable use policies, whether or not it is a result of malicious activity.[3] A *cyber incident* is assumed to result in a financial loss. In contrast, a *cyber event* is defined as an observable occurrence in an information system that does not necessarily result in a financial loss.

A single cyber incident may have multiple loss impacts. Figure 1 illustrates this point. For example, a single cyberattack might be associated with the disruption of services at the attacked institution, a data breach, and theft of customer funds.[4] A cyber loss impact is defined as a financial loss (excluding insurance or tax effects) resulting from a cyber incident and includes all expenses associated with a cyber incident except for opportunity costs, forgone revenue, and costs related to risk management and control enhancements implemented to prevent future cyber losses.[5] Inherent in this definition are elements of legal risk, including privacy protection risk as applicable.[6] This definition excludes strategic and reputational risk.

[3] Adapted from the Financial Stability Board Cyber Lexicon.
[4] In this instance, the cyber loss incident has three separate impacts.
[5] We aim to capture these indirect costs separately (for example, please see Table 1).
[6] Legal risk includes, but is not limited to exposure to fines, penalties, or punitive damages resulting from supervisory actions as well as private settlements.

Figure 1: Cyber Incident Structure



CYBER LOSS CLASSIFICATION

1. Classification Principles

An important underlying principle of creating a cyber loss impact classification scheme is to create categories that aggregate loss impacts that are relatively similar in nature and contain similar drivers in order to facilitate actionable steps from a risk management perspective. Specifically:

a. A cyber loss impact should be uniquely identified to belong to a particular classification category
b. A particular cyber loss classification category should have impacts with similar underlying drivers

If a single cyber incident has multiple loss impacts, each loss impact could be plausibly assigned to a different classification category. In cases of incidents with multiple loss impacts, there should be common identifier at the incident level (e.g., a unique reference number) to link these individual records to the same underlying incident. Figure 1 above illustrates this structure with impact identifiers assigned to the incident in chronological order.

2. Classification

The proposed cyber risk classification is organized around 5 main concepts:

a. ***Cyber incident consequence****:* the consequence of a cyber incident.

- Business Disruption, System and Execution Failure (BDSEF, CN01): Any type of internal or external incident that disrupts the business or causes a software/hardware/IT failure where there was no initial data, technology or monetary loss.
- Data Breach - PII (CN02): Any type of data loss or exposure involving Personally Identifiable Information (PII). [7]
- Theft or Loss of Non-PII Information (CN03): Any type of theft or loss of technology, intellectual property, business proprietary information or any other information that is not PII.
- Theft of Funds (CN04): Any type of incident that led to an immediate and direct loss of funds and was carried out via a digital channel.

b. ***Cyber incident cause****:* the method through which a malicious cyberattack is carried out.[8]

- Denial-of-Service (CA01): A denial-of-service (DoS) attack floods systems, servers, or networks with traffic to exhaust resources and bandwidth. As a result, the system is unable to fulfill legitimate requests. A distributed denial-of-service (DDoS) is when attackers use multiple compromised devices to perform the attack.
- Man-in-the-middle (CA02): A Man-in-the-middle (MitM) attack, also known as eavesdropping attack, occurs when attackers insert themselves into a two-party transaction. Once the attackers interrupt the traffic, they can filter and steal data.
- Phishing (CA03): Phishing is the practice of sending fraudulent communications that appear to come from a reputable source, usually through email. The goal is to steal sensitive data like credit card and login information or to install malware on the victim's machine.
- Drive-by attack (CA04): In a Drive-by download attack, hackers look for insecure websites and plant a malicious script into HTTP or PHP code on one of the pages. This script might install malware directly onto the computer of someone who visits the site, or it might redirect the victim to a site controlled by the hackers. The "Watering Hole" is the most common strategy to execute this type of attack.[9]
- Password attack (CA05): A password attack happens when an unauthorized parties obtain the access to a person's password by looking around the person's desk,

[7] PII here is defined as any information about an individual that can be used to distinguish or trace an individual's identify and any other information that is linked or linkable to an individual. Source: NIST SP 800-163 under Personally Identifiable Information (NIST SP 800-122).

[8] This list is by no means exhaustive. We plan to update it on a continuous basis.

[9] A "Watering Hole" attack targets a victim that belongs to a particular group (organization, industry, or region). In this attack, the strategy of an attacker is to guess or observe which websites the group often uses and infects one or more of them with malware.

''sniffing'' the connection to the network to acquire unencrypted passwords, using social engineering, gaining access to a password database or outright guessing (brute force or dictionary attack)

- SQL injection (CA06): A Structured Query Language (SQL) injection occurs when an attacker inserts malicious code into a server that uses SQL and forces the server to reveal information it normally would not.
- Cross-site scripting (CA07): Cross-site scripting (XSS) attacks use third-party web resources to run scripts in the victim's web browser or scriptable application.
- Birthday attack (CA08): Birthday attacks are made against hash algorithms that are used to verify the integrity of a message, software or digital signature.[10]
- Malware (CA09): Software designed with malicious intent containing features or capabilities that can potentially cause harm directly or indirectly to entities or their information systems.
- Zero-day exploit (CA10): An attack that exploits a previously unknown hardware, firmware, or software vulnerability.
- Other (CA99): Any other type of cyberattack that is not defined. This category would serve as a "catch all" category for cyberattacks with a known type but not captured by another existing category.
- Unknown (CA00): When the type of cyberattack is unknown to the institution.

c. ***Intent***: an indicator for whether the cyber incident was deliberate or accidental.
   - Intentional: when the cyber incident is malicious/intentional.
   - Unintentional: when the cyber incident is not intentional.

d. ***Origin***: an indicator for whether the cyber incident originated at the institution or at an external entity.
   - External Party: When the cyber incident initiated at a third party/vendor or any other external entity.
   - Non-External Party: When the cyber incident initiated at the institution or its subsidiary.

e. ***Basel event type category***[11]: the Basel Event category assigned to the cyber incident.
   1. Internal fraud (ET1): Losses due to acts of a type intended to defraud, misappropriate property, circumvent regulations, the law, or company policy, excluding diversity/discrimination events, which involves at least one internal party.
   2. External fraud (ET2): Losses due to acts of a type intended to defraud, misappropriate property or circumvent the law, by a third party.

[10] This is a brute force type of attack where the success of the attack largely depends on the higher likelihood of collisions found between random attack attempts and a fixed degree of permutations, as described in the well-known birthday paradox problem.

[11] As previously discussed, cyber risk is considered a form of operational risk. In this regard, the Basel event type categorization is important from a consistency perspective of how to map cyber risk to the broader concept of operational risk. The Basel event type categorization also provides additional granularity to meaningfully differentiate cyber loss events already classified according to other classification concepts.

3. Employment Practices and Workplace Safety (ET3): Losses arising from acts inconsistent with employment, health or safety laws or agreements, from payment of personal injury claims, or from diversity/discrimination events.
4. Clients, Products & Business Practices (ET4): Losses arising from an unintentional or negligent failure to meet a professional obligation to specific clients (including fiduciary and suitability requirements), or from the nature or design of a product.
5. Damage to Physical Assets (ET5): Losses arising from loss or damage to physical assets from a natural disaster or other events.
6. Business Disruption and System Failures (ET6): Losses arising from disruption of business or system failures.
7. Execution, Delivery and Process Management (ET7): Losses from failed transaction processing or process management, from relations with trade counterparties and vendors.

Classification Matrix: Panel A – Intentional

	Intentional			
Incident Consequence	*External Party*	*Non-External Party*	**Basel Event-Type Category**	**Incident Cause**
BDSEF	An intentional business disruption at a third party provider causes disruption to the firm.	An intentional act causes business disruption at the firm.	ET6	CA 1-99
	Human error that led to an intentional business disruption at a third party /external provider.	An internal human error that led to an intentional business disruption at the firm.	ET7	CA 1-99
Data Breach - PII	An employee of a third party provider uses their physical access to steal PII classified data from the firm.	An employee of the firm uses their physical access to steal PII data from the firm.	ET1	CA 1-99
	An external party gains physical access under the control of a third party provider to steal PII data from the firm.	An external party gains physical access that enables him to steal PII data directly from the firm.	ET2	CA 1-99
Theft or Loss of Non-PII Information	An employee of a third party provider	An employee of the firm steals non PII	ET1	CA 1-99

	steals non PII data from the firm with remote access.	data from the firm with remote access.		
	An external party steals non PII firm data from a third party provider with remote access.	An external party steals non PII firm data from the firm with remote access.	ET2	CA 1-99
Theft of Funds	An employee of a third party provider uses their access to steal money from the firm or its customers.	An external party defrauds a third party resulting in monetary loss to the firm or the firm's customers.	ET1	CA 1-99
	An employee of the firm uses their access to steal money from the firm or its customers.	An external party defrauds the firm resulting in a monetary loss to the firm or the firm's customers.	ET2	CA 1-99

Classification Matrix: Panel B – Unintentional

	Unintentional			
Incident Consequence	*Third Party*	*Non-Third Party*	**Basel Event-Type Category**	**Incident cause[12]**
BDSEF	An unintentional business disruption at a third party provider causes disruption to the firm.	A software or hardware failure at the firm causes business disruption.	ET6	0 - Not Applicable
Data Breach – PII	A human error allows for unintentional business disruption at a third party provider, exposing PII data.	A human error allows for unintentional business disruption at the firm, exposing PII data.	ET7	0 - Not Applicable
Theft or Loss of Non-PII Information	A third party provider loses non PII firm data as a result of a hardware or software failure.	The firm loses non PII data as a result of a hardware or software failure.	ET6	0 - Not Applicable

[12] Incident cause is inapplicable here because the table lists unintentional (non-malicious) incidents only.

	A third party provider loses non PII firm data as a result of a faulty process or human error.	The firm loses non PII firm data as a result of a faulty process or human error.	ET7	0 - Not Applicable

Appendix C: Classification Examples provides an illustration of the proposed classification scheme through examples.

Lastly, it is important to emphasize that the proposed classification scheme is expected to evolve and be periodically updated as new technologies, their applications in banking and finance, and associated cyber threats continue to develop and emerge.

APPENDIX A: DATA COLLECTION FORMS

From a financial risk management perspective, two separate data collection schedules would be deemed useful:

1. A detailed "loss incident" schedule. This schedule would track cyber risk incidents that realized into financial losses and would be particularly useful for financial loss modeling. An example of such a schedule with the associated prospective data fields is presented in *Table 1*.
2. An aggregated monthly schedule. This schedule would track both the cyberattacks that resulted in financial losses (incidents) and the ones which did not result in financial losses (events) at a monthly frequency. Such a schedule would be particularly useful for tracking cyber risk trends in addition to financial loss modeling. An example of such a schedule with the associated prospective data fields is presented in *Table 2*.

Table 1: Cyber Loss Incident Data Collection Schedule (Loss Incident Level)

Field Reference	Field Name	Description	Format N:Numeric C: Character A: Alphanumeric
A	Unique Identifier	Report the unique identifier for each row of data in the institution's data submission. The unique identifier should remain constant with the specified row of data in subsequent submissions and become a permanent element of the data. The unique identifier should not include any white spaces, tabs, or special characters.	A
B	Reference Number	Report the unique institution-established identifier assigned to each loss incident. The reference number should not include any white spaces, tabs, or special characters.	A
C	Chronological Order ID	For incidents with multiple impacts, please assign a cardinal order that reflects the chronology of the different impacts starting at 1. For incidents with a unique impact, please assign 1.	N
D	Occurrence Date	Report the date that the cyber loss incident occurred or began. The Occurrence Date must be submitted in the following format: MM/DD/YYYY. For example, "January 5, 2011" should be "01/05/2011."	Date MM/DD/YYYY
E	Discovery Date	Report the date that the cyber loss incident was first discovered by the institution. The loss incident's discovery date should not be earlier than its occurrence date. The Discovery Date must be submitted in the following format: MM/DD/YYYY. For example, "January 5, 2011" should be "01/05/2011."	Date MM/DD/YYYY
F	Remediation Date	Report the date that the cyber loss incident was fully remediated by the institution. The loss incident's remediation date should not be earlier than its occurrence and discovery dates. The Remediation Date must be submitted in the following format: MM/DD/YYYY. For example, "January 5, 2011" should be "01/05/2011."	Date MM/DD/YYYY
G	Accounting Date	Report the date that the financial impact including remediation cost of the cyber loss incident was first recorded on the institution's financial statements. The accounting date should be consistent with, and no later than, the date a legal reserve is established. Generally, the loss incident's accounting date should not be earlier than its occurrence date or discovery date; however, there are cases where accounting date can accurately be reflected prior to discovery date. The Accounting Date must be	Date MM/DD/YYYY

Field Reference	Field Name	Description	Format N:Numeric C: Character A: Alphanumeric
		submitted in the following format: MM/DD/YYYY. For example, "January 5, 2011" should be "01/05/2011."	
H	Applicable Loss Data Collection Threshold	Report the institution-established loss data collection threshold that was applicable to the respective business line/ function and in effect at the time the loss incident was captured.	N
I	Gross Loss Amount ($USD)	Report the total financial impact of the cyber loss incident before any recoveries and excluding insurance and/or tax effects. The GLA should include all expenses associated with a cyber loss incident except for opportunity costs, forgone revenue, provision and provision write backs, and costs related to risk management and control enhancements implemented to prevent future cyber losses. Also, the following type of incidents should **not** be included in the Gross Loss Amount or the institution's completed schedule: *Near Misses:* A cyber risk incident that did not result in an actual financial loss or gain to the institution. *Timing Incidents:* A cyber risk incident that causes a temporary distortion of the institution's financial statements in a particular financial reporting period but that can be fully corrected when later discovered (e.g. revenue overstatement, accounting and mark-to-market errors). *Forgone Revenues/ Opportunity Costs:* Inability to collect potential future revenues due to cyber risk related failures. *Gains*: Situations where a cyber risk results in a financial gain for the institution. In addition, Gross Loss Amounts: Should be reported in units of one (not thousands), rounded to the nearest unit (for example, a one million dollar loss would be reported as 1,000,000).	N

Field Reference	Field Name	Description	Format N:Numeric C: Character A: Alphanumeric
		Must be reported in US dollars. Loss amounts recorded in foreign currency should be converted to US dollars using a foreign exchange rate as of the accounting date associated with the respective loss. Cannot be reported as a negative value, except cases where it represents a decrease in reserves.	
J	Remediation Cost ($USD)	Report the direct remediation cost of the cyber loss incident before any recoveries and excluding insurance and/or tax effects. The Remediation Cost should be included in the Gross Loss Amount and represents all the expenses the institution bear to fully remediate the cyber incident. The costs related to risk management and control enhancements implemented to prevent future cyber losses should not be included.	N
K	Indirect Cost ($USD)	Report the indirect costs of the cyber loss incident. The Indirect Cost should include expenses related foregone revenues and/or opportunity costs. *Forgone Revenues/ Opportunity Costs:* Inability to collect potential future revenues due to cyber risk related failures.	N
L	Recovery Amount ($USD)	A recovery is an independent occurrence related to the cyber loss incident, separate in time, in which funds or outflows of economic benefits are received from a third party, excluding funds received from insurance providers. Recovery Amounts: • Should not be included in the Gross Loss Amount column or netted into the gross loss amount. • Should exclude provisions and provision write backs. • Should have the same reference number as the associated loss incident. • Should be reported in units of one (not thousands), rounded to the nearest unit (for example, a one million dollar loss would be reported as 1,000,000). • Should be reported in US dollars. Recoveries recorded in foreign currency amounts should be converted to US dollars	N

Field Reference	Field Name	Description	Format N:Numeric C: Character A: Alphanumeric
		using a foreign exchange rate as of the accounting date associate with the respective recovery. • Cannot be reported as a negative value.	
M	Insurance Recovery ($USD)	Report funds recouped as a result of existing insurance coverage as related to the cyber risk incident.	N
N	Cyber Incident Consequence Category	All loss incidents reported by the institution must be mapped to one of the four "Cyber Incident Consequence" categories in Reference Table 3. This field must contain the respective Cyber Incident Consequence code specified in Reference Table 3 (i.e. CN01, CN02, CN03, and CN04). The exact code provided must be used (e.g. "CN01") with no additional characters or spaces added.	A
O	Cyber Incident Cause Category	All loss incidents reported by the institution must be mapped to one of the twelve "Cyber Incident Cause" categories in Reference Table 4. This field must contain the respective Cyber Incident Cause code specified in Reference Table 4 (i.e. CA01, CA02, CA03… CA99). The exact code provided must be used (e.g. "CA01") with no additional characters or spaces added.	A
P	Intent Indicator (Intentional vs. Unintentional)	For all loss incidents originally caused by an intentional act please select 1, otherwise 0.	N
Q	External Party Indicator	For all loss incidents originally caused by an external or third party failure please assign 1, otherwise 0.	N
R	Basel Event-Type Category: Level 1	All loss events reported by the institution must be mapped to one of the seven "Level 1 Event Types" in Reference Table E.1.a. This field must contain the respective Level 1 Event-Type code specified in Reference Table E.1.a (i.e. ET1, ET2, ET3… ET7). The exact code provided must be used (e.g. "ET1") with no additional characters or spaces added.	A
S	Basel Business Line Level 1	All loss events reported by the institution must be mapped to one of the nine "Level 1 Business Lines" in Reference Table E.1.b. This field must contain the specific Level 1 Business Line code identified in Reference Table E.1.b (i.e., BL1, BL2,	N

Field Reference	Field Name	Description	Format N:Numeric C: Character A: Alphanumeric
		BL3,….BL9) which corresponds to the Level 1 Business Line.	
T	Acquired or Merged Entities	If the loss incident being reported originated from an acquired or merged entity, then include the name of the respective acquired or merged entity in this field. If not, then insert "NA" (not applicable). "Incidents originating from acquired or merged entities" refer to loss incidents that have a capture date prior to the acquisition/merger date. This requirement should also apply to loss incidents originating from acquired or merged entities that have capture dates after the acquisition/merger date, if those losses have not yet been integrated into the business lines/functions of the merged entity.	C
U	Detailed Description of Loss Incident (required for incidents > $250k)	For all cyber loss incidents with gross loss amounts greater than or equal to $250 thousand, include a detailed description of the loss incident. Generally, the "short-form" descriptions captured in an institution's internal loss database should suffice.	C
V	Detailed Description of Remediation Action (required for incidents > $250k)	For all cyber loss incidents with gross loss amounts greater than or equal to $250 thousand include a detailed description of the remediation action taken to address the cyber risk incident (including technical details for information technology fixes). "Short-form" descriptions should suffice.	C
W	Threat Actor	Type of Threat Actor, either entity or person that caused or contributed to the event.	A
X	Primary Control Failure [13]	Code for the primary control which was set to prevent the event from occurring (NIST).	A
Y	Secondary Control Failure	Code for the secondary control failure which was set to prevent the event from occurring (NIST).	A
Z	Event Status	An indicator denoting that all necessary information related to the event is known and has been submitted (1 for the open event, 0 for the closed).	N

[13] See Table 8 for the complete controls list.

Table 2: Event/Incident Collection Schedule (Aggregated Monthly Level)

Field Reference	Field Name	Description	Format N:Numeric C: Character A: Alphanumeric
A	Reporting Date	Report the last day of the month during which the cyberattacks occurred.	Date MM/DD/YYYY
B	Cyber Incidents Cause	All cyber incidents reported by the institution in this schedule must be mapped to one of twelve "Cyber Incident Cause" in Reference Table 4. This field must contain the respective Cyber Incident Cause code specified in Reference Table 4 (i.e. CA01, CA02, CA03… CA99). The exact code provided must be used (e.g. "CA01") with no additional characters or spaces added.	A
C	Number of Cyberattacks	Report the number of total attacks that the institution has been targeted with during the month of the reporting date	N
D	Number of Successful Cyberattacks	Report the number of successful attacks that the institution has been targeted with during the month prior of the reporting date	N
E	Total Gross Loss Amount	Report the total gross amount lost across all the successful cyberattacks. Should be reported in units of one (not thousands), rounded to the nearest unit (for example, a one million dollar loss would be reported as 1,000,000).	N
F	Total Recovery Amount	Report the total recovery amount across all the successful cyberattacks. Should be reported in units of one (not thousands), rounded to the nearest unit (for example, a one million dollar loss would be reported as 1,000,000).	N
G	Total Defense Cost	Report the total defense cost amount spent during the quarter preceding the current submitted schedule.	N

APPENDIX B: REFERENCE TABLES

Table 3: Cyber Incident Consequence

Incident Consequence	Code	Definition
BDSEF	CN01	Any type of incident where there was no initial data, technology or monetary loss and was caused by a software/hardware/IT failure OR external disruption.
Data Breach – PII	CN02	Any type of data loss or exposure involving Personally Identifiable Information (PII).
Theft or Loss of Non-PII Information	CN03	Any type of theft or loss of technology, intellectual property, business proprietary information or any other information that is not PII.
Theft of Funds	CN04	Any type of incident that led to an immediate and direct loss of funds and was carried out via a digital channel.

Table 4: Cyberattack Incident Causes

Incident Cause	Code	Definition
Denial-of-Service	CA01	A Denial-of-Service (DoS) attack floods systems, servers, or networks with traffic to exhaust resources and bandwidth. As a result, the system is unable to fulfill legitimate requests. A distributed Denial-of-Service (DDoS) is when attackers use multiple compromised devices to perform the attack. The most common DoS and DDoS attacks are: TCP SYN flood attack, teardrop attack, smurf attack, ping-of-death attack and botnets.
Man-in-the-Middle	CA02	Man-in-the-Middle (MitM) attacks, also known as eavesdropping attacks, occur when attackers insert themselves into a two-party transaction. Once the attackers interrupt the traffic, they can filter and steal data. The most common types of Man-in-the-Middle attacks are: session hijacking, IP Spoofing, Replay.
Phishing	CA03	Phishing is the practice of sending fraudulent communications that appear to come from a reputable source, usually through email. The goal is to steal sensitive data like credit card and login information or to install malware on the victim's machine.
Drive-by Attack	CA04	In a Drive-by download attack hackers look for insecure websites and plant a malicious script into HTTP or PHP code on one of the pages. This script might install malware directly onto the computer of someone who visits the site, or it might re-direct the victim to a site controlled by the hackers.
Password Attack	CA05	A password attack happens when an unauthorized parties obtain the access to a person's password by looking around the person's desk, ''sniffing'' the connection to the network to acquire unencrypted passwords, using social engineering, gaining access to a password database or outright guessing (brute force or dictionary attack)
SQL Injection	CA06	A Structured Query Language (SQL) injection occurs when an attacker inserts malicious code into a server that uses SQL and forces the server to reveal information it normally would not.
Cross-site Scripting	CA07	XSS attacks use third-party web resources to run scripts in the victim's web browser or scriptable application.
Birthday Attack	CA08	Birthday attacks are made against hash algorithms that are used to verify the integrity of a message, software or digital signature.
Malware Attack	CA09	Malicious software can be described as unwanted software that is installed in your system without your consent. The most common malwares are: macro virus, file infectors, system or boot-record infectors, polymorphic viruses, stealth viruses, Trojans, logic bombs, worms, droppers, ransomware, adware, spyware
Zero-day Exploit	CA10	A zero-day exploit hits a previously unknown hardware, firmware, or software vulnerability. Attackers target the vulnerability before a patch or solution is implemented.

Other	CA99	Any other type of attack that is not defined in this table
Not Applicable	CA00	Not applicable

Table 5: Basel Event-Types

Basel Event-Type Category	Code	Definition
Internal Fraud	ET1	Losses due to acts of a type intended to defraud, misappropriate property or circumvent regulations, the law or company policy, excluding diversity/discrimination events, which involves at least one internal party.
External Fraud	ET2	Losses due to acts of a type intended to defraud, misappropriate property or circumvent the law, by a third party.
Employment Practices and Workplace Safety	ET3	Losses arising from acts inconsistent with employment, health or safety laws or agreements, from payment of personal injury claims, or from diversity/discrimination events.
Clients, Products & Business Practices	ET4	Losses arising from an unintentional or negligent failure to meet a professional obligation to specific clients (including fiduciary and suitability requirements) or from the nature or design of a product.
Damage to Physical Assets	ET5	Losses arising from loss or damage to physical assets from a natural disaster or other events.
Business Disruption and System Failures	ET6	Losses arising from disruption of business or system failures.
Execution, Delivery and Process Management	ET7	Losses from failed transaction processing or process management, from relations with trade counterparties and vendors.

Table 6: Business Lines

Business Line Name	Code	Activity Groups
Corporate Finance	BL1	Mergers and acquisitions, underwriting, privatizations, securitization, research, debt (government, high yield), equity, syndications, IPO, secondary private placements
Trading & Sales	BL2	Fixed income, equity, foreign exchanges, commodities, credit, funding, own position securities, lending and repos, brokerage, debt, prime brokerage
Retail Banking	BL3	Retail lending and deposits, banking services, trust and estates; Private lending and deposits, banking services, trust and estates, investment advice; Merchant/ commercial/ corporate cards, private labels and retail
Commercial Banking	BL4	Project finance, real estate, export finance, trade finance, factoring, leasing, lending, guarantees, bills of exchange
Payment and Settlement	BL5	Payments and collections, funds transfer, clearing and settlement
Agency Services	BL6	Escrow, depository receipts, securities lending (customers) corporate actions; Issuer and paying agents
Asset Management	BL7	Pooled, segregated, retail, institutional, closed, open, private equity;
Retail Brokerage	BL8	Execution and full service
Corporate Level- Non-Business Line Specific	BL9	Losses originating from a corporate/firm-wide function that cannot be linked to a specific business line.

Table 7: Threat Actor[14]

Threat Actor Name	Code	Activity Groups
External Actor - Activist	TA1	An individual or entity intending to cause political/social change.
External Actor - Nation State	TA2	State-backed cybercriminals aimed at disrupting organizations and states.
External Actor – Organized Crime	TA3	Hacking groups, etc.
External Actor - Unstructured	TA4	Individuals or small groups of attackers with limited resource and without political/social agenda.
External Actor - Former Employee/ Contractor	TA5	An individual formerly employed by the firm on a permanent OR temporary basis (e.g. former consultant/contractor).
External Actor - Terrorist	TA6	Politically motivated actor(s) intending to cause severe disruption or widespread fear.
External Actor - Competitor	TA7	A commercial or economic competitor intending to gain a market advantage.
External Actor - Other	TA8	Other external actor.
External Actor - Unknown	TA9	Used when specific external actor cannot be identified.
Internal Actor - Employee	TA10	An individual employed by the firm at the time of the attack.
Internal Actor - Contractor/Consultant	TA11	An individual employed by the firm on a temporary basis at the time of the attack.
Internal Actor – Other	TA12	Other internal actor.
Internal Actor – Unknown	TA13	Used when specific internal actor cannot be identified.
Third Party Actor – Business Partner	TA14	For example, affiliates, brokers, agents, etc.
Third Party Actor – Services Provider (IT)	TA15	For example, software developing companies, IaaS, PaaS, or SaaS providers, backup services.
Third Party Actor – Services Provider (Other)	TA16	For example, advisors, data disposal, cleaning, HVAC.
Third Party Actor – Trusted Third Party	TA17	For example, payment gateways, clearing houses, etc.
Third Party Actor – Other	TA18	Other third party actor.
Third Party Actor – Unknown	TA19	Used when specific third party actor cannot be identified.

[14] Threat actor classification is following ORX's CISR event reporting framework.

Unknown	TA20	

Table 8: Control Failure Type

Control Type (NIST)	**Code**
Physical devices and systems within the organization are inventoried	ID.AM-1
Software platforms and applications within the organization are inventoried	ID.AM-2
Organizational communication and data flows are mapped	ID.AM-3
External information systems are catalogued	ID.AM-4
Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	ID.AM-5
Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	ID.AM-6
The organization's role in the supply chain is identified and communicated	ID.BE-1
The organization's place in critical infrastructure and its industry sector is identified and communicated	ID.BE-2
Priorities for organizational mission, objectives, and activities are established and communicated	ID.BE-3
Dependencies and critical functions for delivery of critical services are established	ID.BE-4
Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	ID.BE-5
Organizational cybersecurity policy is established and communicated	ID.GV-1
Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners	ID.GV-2
Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	ID.GV-3
Governance and risk management processes address cybersecurity risks	ID.GV-4
Asset vulnerabilities are identified and documented	ID.RA-1
Cyber threat intelligence is received from information sharing forums and sources	ID.RA-2
Threats, both internal and external, are identified and documented	ID.RA-3
Potential business impacts and likelihoods are identified	ID.RA-4
Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	ID.RA-5
Risk responses are identified and prioritized	ID.RA-6
Risk management processes are established, managed, and agreed to by organizational stakeholders	ID.RM-1
Organizational risk tolerance is determined and clearly expressed	ID.RM-2
The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	ID.RM-3
Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders	ID.SC-1
Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process	ID.SC-2
Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.	ID.SC-3
Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.	ID.SC-4
Response and recovery planning and testing are conducted with third-party providers	ID.SC-5

Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes	PR.AC-1
Physical access to assets is managed and protected	PR.AC-2
Remote access is managed	PR.AC-3
Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	PR.AC-4
Network integrity is protected (e.g., network segregation, network segmentation)	PR.AC-5
Identities are proofed and bound to credentials and asserted in interactions	PR.AC-6
Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	PR.AC-7
All users are informed and trained	PR.AT-1
Privileged users understand their roles and responsibilities	PR.AT-2
Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities	PR.AT-3
Senior executives understand their roles and responsibilities	PR.AT-4
Physical and cybersecurity personnel understand their roles and responsibilities	PR.AT-5
Data-at-rest is protected	PR.DS-1
Data-in-transit is protected	PR.DS-2
Assets are formally managed throughout removal, transfers, and disposition	PR.DS-3
Adequate capacity to ensure availability is maintained	PR.DS-4
Protections against data leaks are implemented	PR.DS-5
Integrity checking mechanisms are used to verify software, firmware, and information integrity	PR.DS-6
The development and testing environment(s) are separate from the production environment	PR.DS-7
Integrity checking mechanisms are used to verify hardware integrity	PR.DS-8
A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)	PR.IP-1
A System Development Life Cycle to manage systems is implemented	PR.IP-2
Configuration change control processes are in place	PR.IP-3
Backups of information are conducted, maintained, and tested	PR.IP-4
Policy and regulations regarding the physical operating environment for organizational assets are met	PR.IP-5
Data is destroyed according to policy	PR.IP-6
Protection processes are improved	PR.IP-7
Effectiveness of protection technologies is shared	PR.IP-8
Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	PR.IP-9
Response and recovery plans are tested	PR.IP-10
Cybersecurity is included in human resources practices (e.g., deprovisioning, screening)	PR.IP-11
A vulnerability management plan is developed and implemented	PR.IP-12
Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools	PR.MA-1
Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	PR.MA-2
Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	PR.PT-1
Removable media is protected and its use restricted according to policy	PR.PT-2

The principle of least functionality is incorporated by configuring systems to provide only essential capabilities	PR.PT-3
Communications and control networks are protected	PR.PT-4
Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations	PR.PT-5
A baseline of network operations and expected data flows for users and systems is established and managed	DE.AE-1
Detected events are analyzed to understand attack targets and methods	DE.AE-2
Event data are collected and correlated from multiple sources and sensors	DE.AE-3
Impact of events is determined	DE.AE-4
Incident alert thresholds are established	DE.AE-5
The network is monitored to detect potential cybersecurity events	DE.CM-1
The physical environment is monitored to detect potential cybersecurity events	DE.CM-2
Personnel activity is monitored to detect potential cybersecurity events	DE.CM-3
Malicious code is detected	DE.CM-4
Unauthorized mobile code is detected	DE.CM-5
External service provider activity is monitored to detect potential cybersecurity events	DE.CM-6
Monitoring for unauthorized personnel, connections, devices, and software is performed	DE.CM-7
Vulnerability scans are performed	DE.CM-8
Roles and responsibilities for detection are well defined to ensure accountability	DE.DP-1
Detection activities comply with all applicable requirements	DE.DP-2
Detection processes are tested	DE.DP-3
Event detection information is communicated	DE.DP-4
Detection processes are continuously improved	DE.DP-5
Response plan is executed during or after an incident	RS.RP-1
Personnel know their roles and order of operations when a response is needed	RS.CO-1
Incidents are reported consistent with established criteria	RS.CO-2
Information is shared consistent with response plans	RS.CO-3
Coordination with stakeholders occurs consistent with response plans	RS.CO-4
Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	RS.CO-5
Notifications from detection systems are investigated	RS.AN-1
The impact of the incident is understood	RS.AN-2
Forensics are performed	RS.AN-3
Incidents are categorized consistent with response plans	RS.AN-4
Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers)	RS.AN-5
Incidents are contained	RS.MI-1
Incidents are mitigated	RS.MI-2
Newly identified vulnerabilities are mitigated or documented as accepted risks	RS.MI-3
Response plans incorporate lessons learned	RS.IM-1
Response strategies are updated	RS.IM-2
Recovery plan is executed during or after a cybersecurity incident	RC.RP-1
Recovery plans incorporate lessons learned	RC.IM-1
Recovery strategies are updated	RC.IM-2
Public relations are managed	RC.CO-1
Reputation is repaired after an incident	RC.CO-2

Recovery activities are communicated to internal and external stakeholders as well as executive and management teams	RC.CO-3

APPENDIX C: CLASSIFICATION EXAMPLES

Table 9: Cyber Incident (Generalized) Examples

Classification Matrix: Panel A – Intentional		
Incident Consequence	**Intentional**	**Basel Event-Type Category**
BDSEF	Firm/third party is hit by DDoS attack that subsequently disrupts service.	ET6
	Neglect/human error on the part of the firm/third party enabled an attack that led to a system disruption.	ET7
Data Breach - PII	Neglect/human error on the part of the firm/third party enabled an attack that led to PII data exposure.	ET7
	Password protected computer is stolen from the firm/third party, and PII information becomes compromised.	ET2
Theft or Loss of Non-PII Information	An insider helps infiltrate firm's/third party computer system, installs software to record computer keystroke activity, thus gaining access to confidential (non PII) data.	ET1
	Hacker infiltrates firm's/third party computer system, installs software to record computer keystroke activity, thus gaining access to confidential (non PII) data.	ET2
Theft of Funds	Firm employee helps criminals to install a physical device within the firm/third party, which enables criminals to control the computer and transfer funds via Wi-Fi.	ET1
	Criminals use malware to gain access to firm/third party accounts and transfer funds.	ET2

Classification Matrix: Panel B – Unintentional		
Incident Consequence	**Unintentional**	**Basel Event-Type Category**
BDSEF	Firm/third party software update leads to an unexpected service disruption.	ET6
	Human error leads to an unexpected service disruption.	ET7
Data Breach – PII	Employee of the firm/third party loses a flash drive containing PII information.	ET7
Theft or Loss of Non-PII Information	Firm/third party sends confidential (non PII) information to unauthorized users due to a software error.	ET6
	Firm/third party sends confidential (non PII) information to unauthorized users due to a human error.	ET7