Cyber OverVue Report

for

Coinbase, Inc.

Finance and Insurance

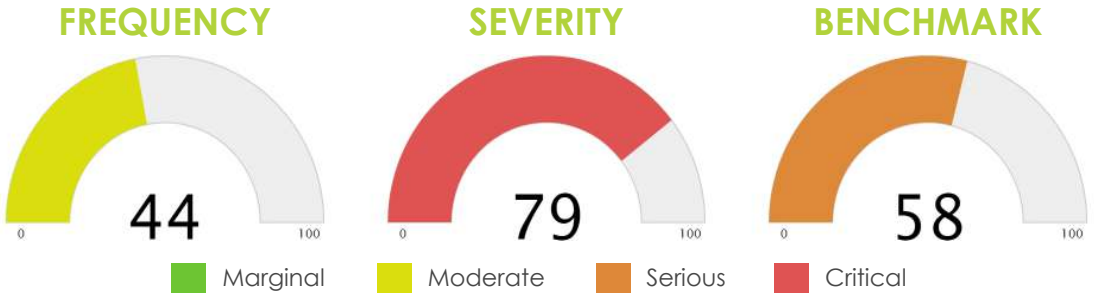
$100M to < $250M

March 3, 2020

Advisen
Transforming • Insurance™

TABLE *of* CONTENTS

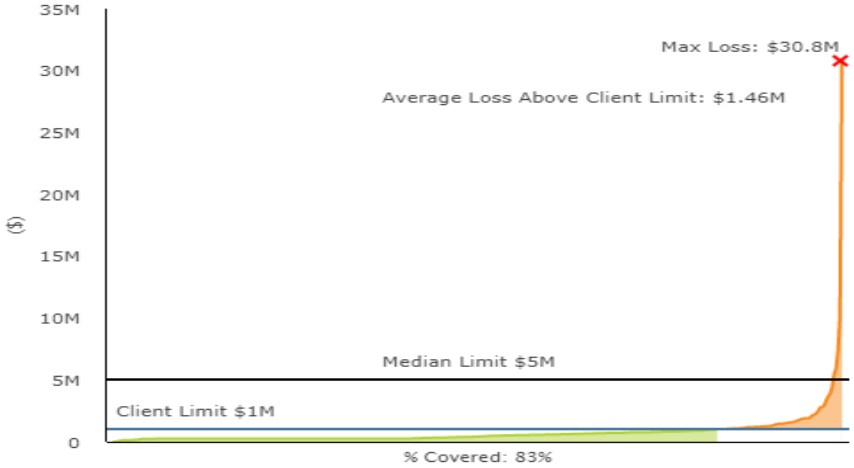
Executive Summary



LOSS SUMMARY AND BREAKDOWN

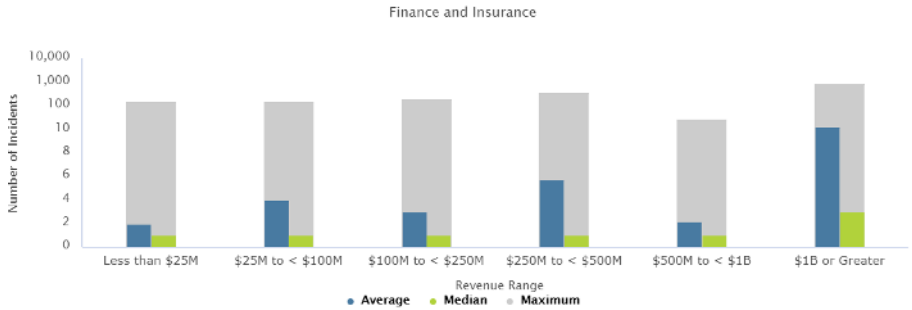
Incident Type	Asset	Potential Impact		1st Party	3rd party
Data Privacy	PII	**Low**	$137,398	$122,284	$15,114
		Mid	$806,451	$717,741	$88,710
		High	$2,052,259	$1,826,511	$225,748
Network Security	Business Income	**Low**	$159,095	$141,595	$17,500
		Mid	$912,971	$812,544	$100,427
		High	$2,263,671	$2,014,667	$249,004
Tech E&O	Business Income	**Low**	$160,819	$143,129	$17,690
		Mid	$957,772	$852,417	$105,355
		High	$2,432,139	$2,164,604	$267,535

LIMIT ADEQUACY



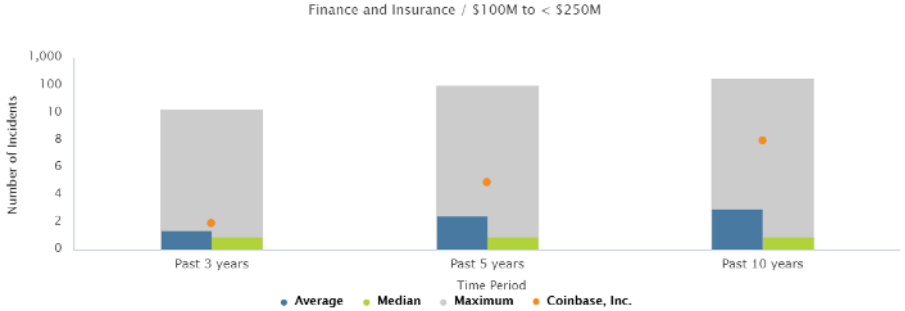
Frequency

INDUSTRY OVERVIEW



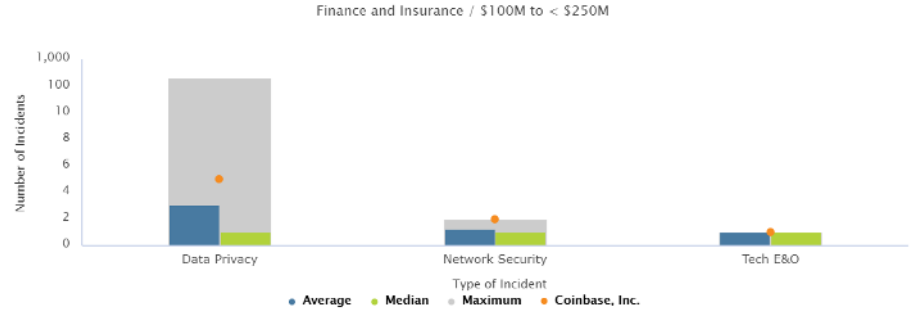
Revenue Range	Average	Median	Maximum	Standard Deviation
Less than $25M	1.96	1	154	8.7
$25M to < $100M	4.05	1	157	15.59
$100M to < $250M	3.02	1	201	14.72
$250M to < $500M	5.75	1	361	33.73
$500M to < $1B	2.15	1	28	3.08
$1B or Greater	12.67	3	870	47.74

TREND ANALYSIS



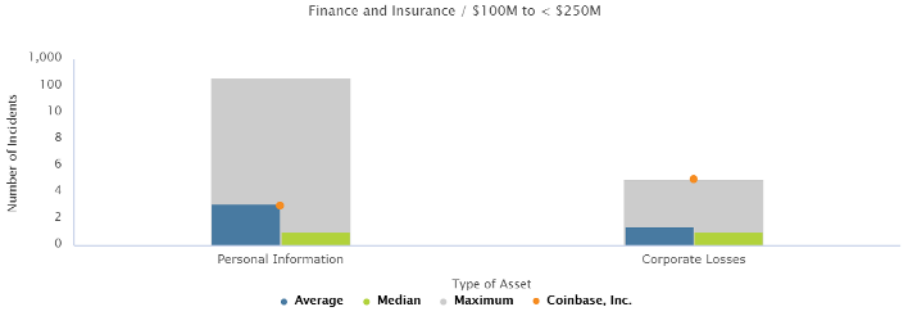
Time Period	Company Losses	Average	Median	Maximum	Standard Deviation
Past 3 years	2	1.49	1	14	1.79
Past 5 years	5	2.51	1	111	10.33
Past 10 years	8	3.02	1	201	14.72

TYPE OF INCIDENT



Type of Incident	Company Losses	Average	Median	Maximum	Standard Deviation
Data Privacy	5	3.1	1	201	15.19
Network Security	2	1.25	1	2	0.45
Tech E&O	1	1	1	1	0

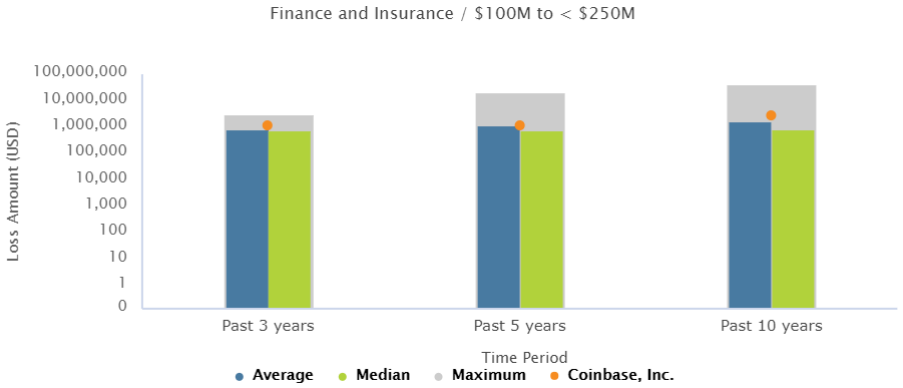
TYPE OF ASSET COMPROMISED



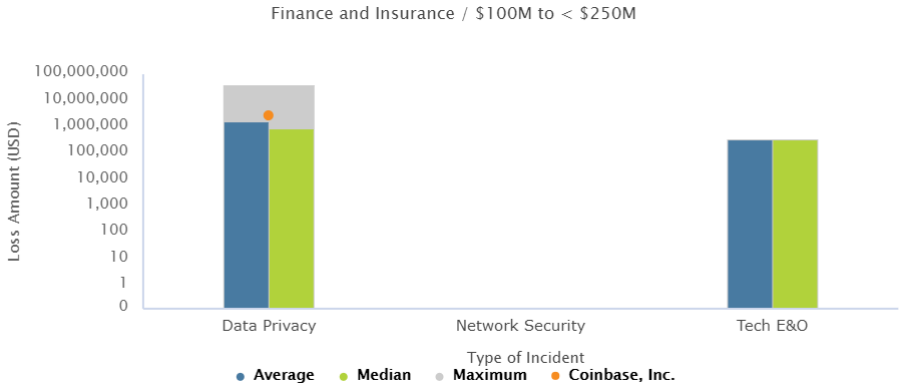
Type of Asset	Company Losses	Average	Median	Maximum	Standard Deviation
Personal Information	3	3.14	1	201	15.4
Corporate Losses	5	1.45	1	5	1

Severity

TREND ANALYSIS - LOSS AMOUNT



TYPE OF INCIDENT - LOSS AMOUNT



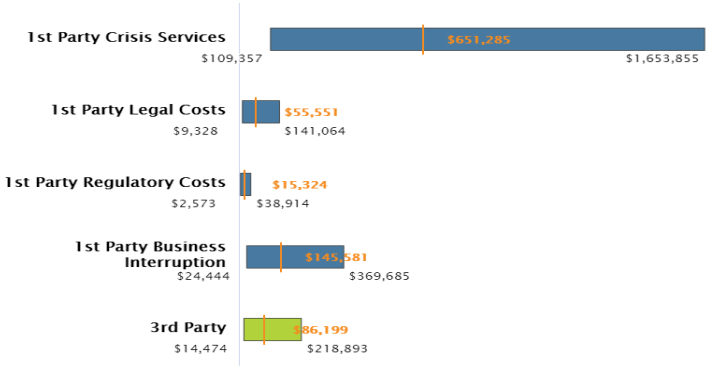
Time Period	Company Losses	Average	Median	Maximum	Standard Deviation
Past 3 years	$1,177,713.93	$798,469.06	$753,277	$2,978,423.55	$575,165.63
Past 5 years	$1,177,713.93	$1,110,086.04	$715,782	$20,001,093.46	$2,297,266.78
Past 10 years	$2,710,822.95	$1,638,541.92	$842,744	$41,975,215.48	$3,931,565.66

Type of Incident	Company Losses	Average	Median	Maximum	Standard Deviation
Data Privacy	$2,710,822.95	$1,656,955.82	$851,963	$41,975,215.48	$3,956,310.42
Network Security	$0	$0	$0	$0	$0
Tech E&O	$0	$325,115.36	$347,840	$364,310.58	$54,252.88

SCENARIO ANALYSIS

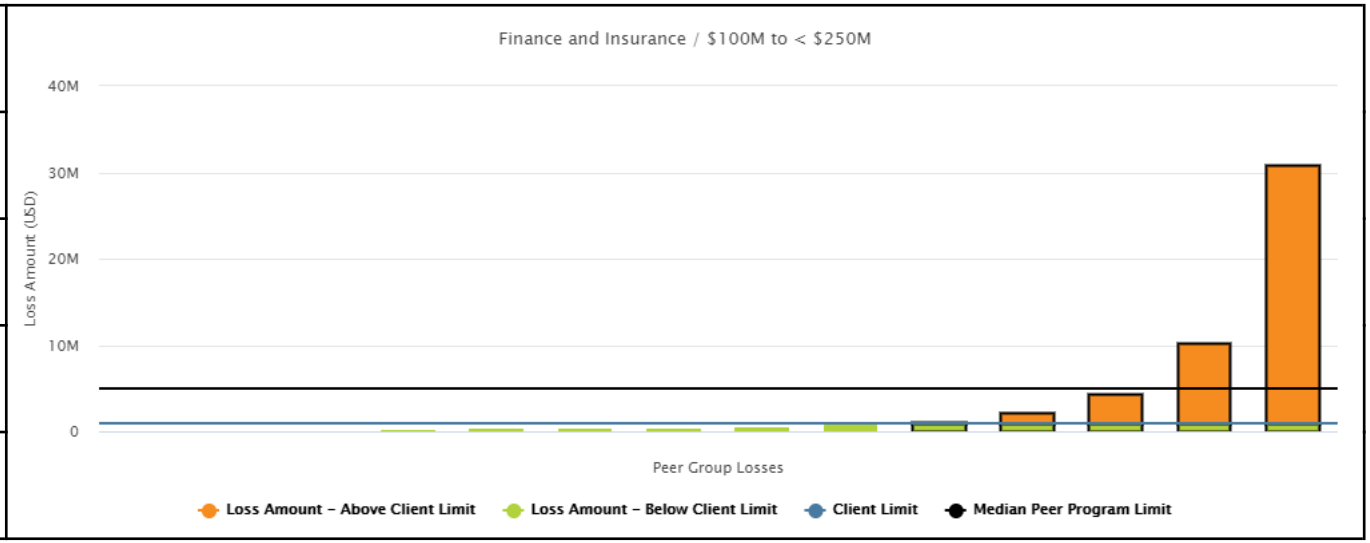
Score - **0-25:** Marginal **26-50:** Moderate **51-75:** Serious **76-100:** Critical

Records Exposed	Incident Type	Asset	Potential Impact		Score
2,000	Tech E&O	Business Income	Low	$160,819	75
			Mid	$957,772	79
			High	$2,432,139	81



Benchmark

LIMIT ADEQUACY - ACTUAL

Client Limit **$1,000,000**	
Median Limit **$5,000,000**	
% Covered **64%**	
Max Loss **$30,800,000**	
Average Loss Amount in Excess **$8,740,836**	

LIMIT ADEQUACY LOSS DETAILS

Company Name	Type of Incident	Incident Date	Records Exposed	Loss Amount	Type of Loss
Xoom Corporation	Data - Malicious Breach	12/01/2014	1,000	$30,800,000	Personal Financial Identity (PFI)
Metallinvestbank, Pao	Data - Malicious Breach	02/01/2016	43,078*	$10,200,000	Corporate Loss of Financial Assets
Nic Asia Bank Limited	Data - Malicious Breach	10/16/2017	12,365*	$4,400,000	Personal Financial Identity (PFI)
MAPFRE Life Insurance Company of Puerto Rico	Data - Physically Lost or Stolen	08/05/2011	2,209	$2,204,182	Personal Health Information (PHI)
Coinbase, Inc.	Data - Malicious Breach	01/05/2019	17,712*	$1,100,000	Corporate Loss of Business Income/ Services

* represents simulated values.

Losses

MOST RECENT PEER GROUP LOSSES

Company Name	Type of Incident	Incident Date ↓	Asset Compromised
Police & Nurses Limited	Data - Malicious Breach	12/12/2019	Personal Financial Identity (PFI)
Bank of England	Data - Malicious Breach	12/01/2019	Corporate Loss of Business Income/ Services
Amerisave Mortgage Corporation	Data - Malicious Breach	11/01/2019	Personal Financial Identity (PFI)
Factor Systems, Inc.	Network/Website Disruption	10/17/2019	Corporate Loss of Business Income/ Services
Credit Karma, Inc.	IT - Processing Errors	8/15/2019	Personal Financial Identity (PFI)

MOST RECENT COMPANY LOSSES

Company Name	Type of Incident	Incident Date ↓	Asset Compromised
Coinbase, Inc.	Phishing, Spoofing, Social Engineering	5/01/2019	Corporate Loss of Digital Assets
The California-based digital currency exchange Coinbase stops hack attack that could potentially have left the exchange woth loss of billion dollars. <P> <P>The said hack targeted over 200 employees in the exchange; however, swift action allowed the exchange to overcome the hacking attack that could have caused devastating losses to the company and investors. <P> <P>It all started back in May when emails were received by Coinbase's 200 employees. Those emails were sent from the United Kingdom's Cambridge University's compromised accounts by a group of hackers CRYPTO3/HYDSEVEN. <P> <P>Reportedly, the plan was well-executed and seemed to be carried out by a group of hackers who had considerable experience in developing exploits.			
Coinbase, Inc.	Data - Malicious Breach	1/05/2019	Corporate Loss of Business Income/ Services
A leading cryptocurrency exchange had been forced to halt trading of Ethereum Classic (ETC) after spotting double. <P> <P>San Francisco-based Coinbase first detected the suspicious activity on January 5, 2019, noting a "deep chain reorganization of the Ethereum Classic blockchain that included a double spend." <P> <P>However, soon after spotting the first reorg, the exchange halted send/receive activity in the blockchain to protect customer funds. <P> <P>The bigger picture problem was that by gaining majority control of the network, the attacker can raise questions about its integrity. <P> <P>ETC buy and sell activity was not affected by the shutdown, but at the time of writing sends and receives remained disabled by Coinbase while it monitored the situation. <P> <P>"The Coinbase team is currently evaluating the safety of re-enabling sends and receives of Ethereum Classic and will communicate to our customers what to expect regarding support for ETC," it said.			
Coinbase, Inc.	Network/Website Disruption	7/28/2017	Corporate Loss of Business Income/ Services
On July 28, 2017, San Francisco, California based digital asset exchange company Coinbase announced that it is suffering a suspected DDoS (Distributed Denial of Service) attacks. As a result of these attacks, customers were facing issues in withdrawing their funds. <P> <P>The attacks came days after Coinbase announced from August 1st, 2017; the company will implement Hard Fork. A "fork" is a change to the software of the digital currency that creates two separate version of the blockhain with a shared history. <P> <P>It is unclear who was behind the attacks. (HackRead - July 31, 2017)			
Coinbase, Inc.	IT - Processing Errors	6/21/2017	Corporate Loss of Business Income/ Services
On June 21, 2017, GDAX, the digital currency exchange run by Coinbase, experienced a flash crash in its USD - Ethereum market. <P> <P>Within seconds the price of ETH crashed from ~$320 to as low as $0.10. While the price recovered quickly, the rapid price movement caused many traders to experience margin calls or stop loss orders, resulting in potentially severe losses. <P> <P>While many initially thought the flash crash was the result of nefarious work, GDAX eventually confirmed that there was no indication of wrongdoing or account takeover. <P> <P>Instead, the flash crash was the result of someone placing a multi-million-dollar sell order at market price, meaning ETH would change hands at whatever price bidders were currently offering until the entire order was filled - no matter how much lower the price was than the current price of ETH.			
Coinbase, Inc.	Network/Website Disruption	1/25/2016	Corporate Loss of Business Income/ Services
Oklahoma Man Charged With Botnet Attack, Conspiracy Counts In U.S. Court In San Jose An 20-year-old Oklahoma man has been charged in federal court in San Jose with four counts related to his alleged creation of malicious software for use in launching denial-of-service attacks on the websites of high-profile companies. The indictment alleges Malone created a malware program known as Medusa IRC Botnet DDoS for use in overwhelming target websites with network traffic. <P> <P>Malone is charged with one count of transmitting his alleged malware program to a San Francisco company, Coinbase, on January 25, 2016, and three counts of conspiring to commit computer fraud and abuse by leasing his malware to unnamed co-conspirators later in 2016. (August 9, 2018 - www.sfgate.com)			

Appendix

Glossary

A

Accident Date

Date on which the incident occurred or began.

Actual Values

These values (**Records Exposed** and **Loss Amount**) have been taken directly from verified sources in the public domain.

B

Benchmark Analysis

Analyses that give insight on how an organization's program compares to its peers.

F

First-Party Losses

First-party losses are financial losses that directly impact the selected organization. For cyber incidents, these include dollars spent on:

- Crisis Services
  - o Forensics
  - o Credit/ID Monitoring
  - o Notification
  - o Legal Guidance/Breach Coach
  - o Recovery Expense
- Legal Costs
  - o Legal Defense

- Legal Settlement

- Regulatory Costs
  - Regulatory Defense
  - Regulatory Fines
  - PCI Fines (if applicable)

- Business Interruption

Frequency Analysis

Analyses based on the number of cyber incidents experienced over a given time period.

In general, the analyses seek to compare the loss experience of a company against the average, median, and maximum loss experience of its peer group.

L

Loss Amount

Refers to the financial loss amount corresponding to the particular cyber incident. These values could either be **Actual** or **Simulated**, and are identified accordingly.

Loss Profile

Based off of the historical loss experience, the loss profile gives an indication of a company or peer group's loss propensity.

Company Loss Profile

The historical loss experience for the selected company. In general, this is indicated by the orange dots in the various charts.

Peer Group Loss Profile

The historical loss experience for the peer group of the selected company. In general, this is indicated by the blue bars in the various charts.

P

Peer Group

A grouping of companies that share the same industry grouping (2 digit NAICS) and revenue range as the selected company.

R

Records Exposed

Refers to the number of individuals or systems affected. These could be based on the number of identities breached or stolen, social security numbers revealed, devices compromised, etc., depending on type of incident.

Revenue Bands

Company revenue in USD. The following bands have been identified and are consistently applied across all industries:

- Less than $25M
- $25M to < $100M
- $100M to < $250M
- $250M to < $500M
- $500M to < $1B
- $1B to Greater

S

Severity Analysis

Analyses based on either the loss amount or the number of records exposed as a result of cyber incidents over a given time period.

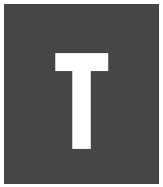
In general, the analyses seek to compare the loss experience of a company against the average, median, and maximum loss experience of its peer group.

Simulated Values

These are values derived from Advisen's proprietary model, which looks at a combination of more than 70 different variables across more than 100,000 cyber to simulate both the number of records exposed and financial loss amounts. The model incorporates quantile regression analyses that look at data relationships across different quantiles to establish a range of potential impacts. These values are identified by an * where relevant to differentiate them from **Actual Values**

Standard Deviation

The standard deviation quantifies the variation of a set of observations. A lower standard deviation indicates that observations tend to be closer to the mean, while a higher standard deviation indicates that observations are spread over a wider range of values in relation to the mean.



Third-Party Losses

Third-party losses are financial losses that indirectly impact the selected organization. For example, an incident experienced by the organization could result in a breach or financial losses for its clients.

Type of Asset Compromised

The type of data, asset, or information that was compromised during a cyber incident. The two main groups are as follows:

Corporate Losses

A grouping of types of loss that relate to the compromise of corporate data or assets. These include:

Loss of Business Income / Services

Any interruption of normal business activities as a result of a cyber incident. These could be a consequence of Distributed Denial of Service (DDoS) attacks or reputational damage.

Loss of Digital Assets

Business and customer data, trade secrets, proprietary software and other confidential corporate data.

Loss of Financial Assets

Money, securities and other financial property, including digital currency such as Bitcoins that belong to either the company or its clients.

Personal Information

A grouping of types of loss that relate to the compromise of personal information. These include:

Personal Identifiable Information

Data containing identifying information, including name, address, e-mail, date of birth, gender etc.

Personal Health Information

Data specifically protected under health information laws and regulations (such as HIPAA), including medical records and health information

Personal Financial Information

Credit/debit card details, social security numbers, banking financial records (account numbers, routing

numbers, etc.)

Type of Incident

The type of cyber incident based on a number of characteristics. Advisen captures 13 different case types, which are defined below.

Incident Type Families

Groupings of multiple incident types that share similar characteristics. These include:

Data Privacy

A grouping of case types that deal with situations where there has been an unauthorized breach or disclosure of personal information of some sort. These case types are as follows:

Data - Malicious Breach

Situations where personal confidential information or digital assets either has been or may have been exposed or stolen, by unauthorized internal or external actors whose intent appears to have been the acquisition of such information.

Data - Physically Lost or Stolen

Situations where personal confidential information or digital assets have been included, or may have been included, with computer or peripheral equipment which has been lost, stolen, or improperly disposed of; the confidential information is incidentally included but unlikely to be the primary focus.

Data - Unintentional Disclosure

Situations where personal confidential information or digital assets have either been exposed, or may have been exposed, to unauthorized viewers due to an unintentional or inadvertent accident or error.

Identity - Fraudulent Use / Account Access

Actual identity theft or the fraudulent use of confidential personal information or account access.

Phishing, Spoofing, Social Engineering

Attempts to get individuals to voluntarily provide information which could then be used illicitly, e.g. phishing or spoofing a legitimate website with a close replica to obtain account information.

Privacy - Unauthorized Data Collection

Cases where information about the users of electronic services, such as social media, cellphones,

websites, etc. is captured and stored without their knowledge or consent

Skimming Physical Tampering

Use of physical devices to illegally capture electronic information such as bank account or credit card numbers for individual transactions.

Network Security

A grouping of case types that deal with situations involving the disruption or interference of corporate operations. These case types are as follows:

Network / Website Disruptions

Unauthorized use of or access to a computer or network, or interference with the operation of same, including virus, worm, malware, digital denial of service (DDOS), etc.

Cyber Extortion

Threats to fraudulently transfer funds, destroy data, interfere with the operation of a system/network/site, or disclose confidential digital information such as identities of customers/employees, unless payments are made

Industrial Controls & Operations

Losses involving disruption or attempted disruption to "connected" physical assets such as factories, automobiles, power plants, electrical grids, etc. (including "the internet of things")

Tech E&O

A grouping of case types that deal with situations involving the failure of corporate operations resulting from errors or oversights in the development, implementation, and/or maintenance of the organizations' IT environment. These case types are as follows:

IT - Processing Errors

Losses resulting from internal errors in electronically processing orders, purchases, registrations, etc., usually due to a security or authorization inadequacy, software bug, hardware malfunction, or user error.

IT - Configuration / Implementation

Losses resulting from errors or mistakes which are made in maintaining, upgrading, replacing, or operating the hardware and software IT infrastructure of an organization, typically resulting in system, network, or web outages or disruptions