Quantum Dawn

A FAIR approach to Quantum Dawn

Table of Contents

What is FAIR? FAIR is an Open Group industry standard that provides an analytic model for understanding, analyzing, and measuring information and operational risk. Unlike risk assessment frameworks that focus their output on qualitative color charts or numerical weighted scales, FAIR builds a foundation for developing a more consistent and scientific approach to information risk management.

What is Quantum Dawn? Quantum Dawn is a series of annual cybersecurity exercises that enable financial institutions to practice and improve coordination with key industry and government partners in order to maintain critical financial services market operations in the event of a low probability, high-impact systemic cyber-attack. In 2011 the Financial Services Sector Coordinating Council (FSSCC) hosted the first nation-wide cyber disruption exercise called Quantum Dawn. Building on the lessons learned of the first exercise and the increasing threat posed to the sector by a coordinated, large scale cyber-attack, SIFMA expanded the outreach to the broader financial services marketplace and coordinated second and third generation cyber disruption exercises, Quantum Dawn 2 and Quantum Dawn 3.

Over 650 participants from over 80 financial institutions and government agencies took part in Quantum Dawn 3. Participating entities included government partners such as the Department of the Treasury, Department of Homeland Security, FBI, federal regulators and the Financial Services Information Sharing and Analysis Center (FS-ISAC). This was a "closed loop" simulation and no real world systems were utilized or impacted.

This document focuses on a financial services firm with ~$30B in assets and their preparation and response to Quantum Dawn 3. Executive management, operational risk personnel, and information security 1st line of defense all participated in the exercise.

Quantum Dawn 3 objectives:

1. Simulate the degradation of critical infrastructure by effecting the availability and accuracy of critical systems allowing participants to remediate or resolve the situation.
2. Rehearse firms' internal response capabilities to a cyber-attack scenario which requires coordination of business continuity, operations and information security practices.
3. Exercise the interaction between firms, government entities, and FSISAC with a focus on sharing information or requesting assistance.

Day of the exercise:

This one-day exercise simulated three business days within the markets. Participants first experienced firm specific attacks, such as a malicious insider compromising critical infrastructure, distributed denial of service (DDoS), a domain name system (DNS) poisoning and breach of personally identifiable information (PII).

Preparation for Quantum Dawn

Prior to the exercise, senior executives asked some very basic questions:

1. What are considered critical assets affected by Quantum Dawn simulated attacks?
2. Who is attacking us and what is their capability?
3. What are the effects of this type of attack, i.e. business interruption, confidentiality breach, etc.?
4. What is the risk, or more specifically, how much financial exposure do we have?
5. How do we prioritize mitigation options, and what is the cost of each mitigation option?

A FAIR approach to Quantum Dawn

Keeping within scope of the Quantum Dawn objectives, members of the technology risk team first identified the scenarios that could result in potential loss to the organization and then performed a RiskLens FAIR-based analysis.

Firm Selected Scenarios

1. DNS Attack – DNS Poisoning: This scenario is for a single loss event resulting from a Domain Name System (DNS) attack on the server.
2. DDoS Attack – This scenario is for a single loss event resulting from the threat and limited demonstration of a Distributed Denial of Service (DDoS) attack to the retail customer-facing online banking website.
3. Insider PII/PCI Breach Online Banking Platform - This scenario is for a single loss event resulting from a malicious employee stealing Personally Identifiable Information (PII) and Payment Card Information (PCI) from core banking system.
4. Ransomware Loss of Availability - This scenario is for a single loss event resulting from ransomware being opened on a workstation at HQ.
5. Malicious insider compromise of network infrastructure - This scenario is for a single loss event resulting from lost availability/connection to a major trade processing provider.
6. Privileged insider malware attack resulting in data integrity failures - This scenario is for a single loss event resulting from a Settlement System compromise.

Quantum Dawn Scenario #1: DNS Attack

Quantum Dawn Scenario #1: DNS Attack

Scenario: This scenario is for a single loss event resulting from a Domain Name System (DNS) attack on the server. Normally, the firm's customer log-on for cash management is re-directed from the website to bank holding company website for online banking (customer log-on for Secure Messaging is also on the website). In a DNS attack on the Online Banking site, the legitimate IP address is replaced with that of another, rogue address in order to redirect traffic to a malicious website, collect information or initiate another attack.

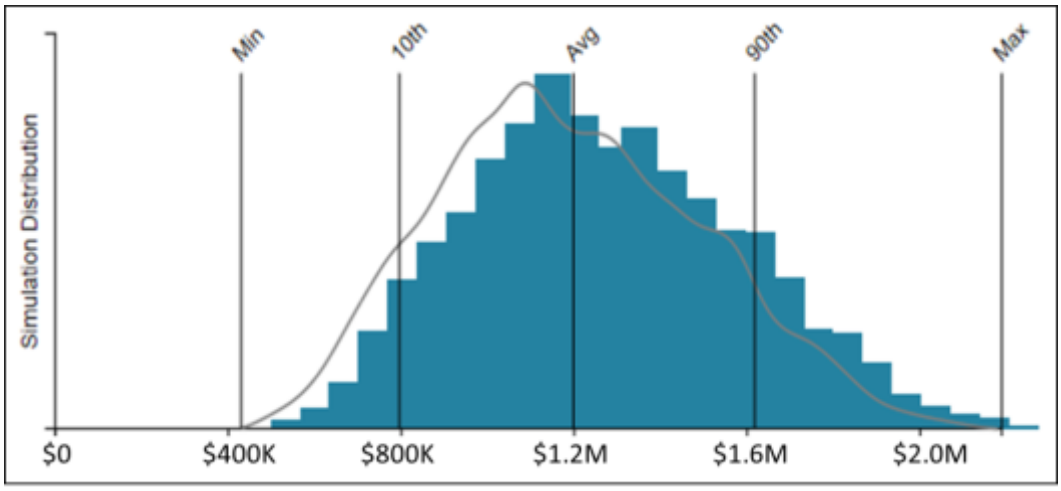
Asset at Risk: Online Banking, Cash Management Systems, Customer Secure Messaging

Threat Actor: The threat actor was determined to be a professional cybercriminal.

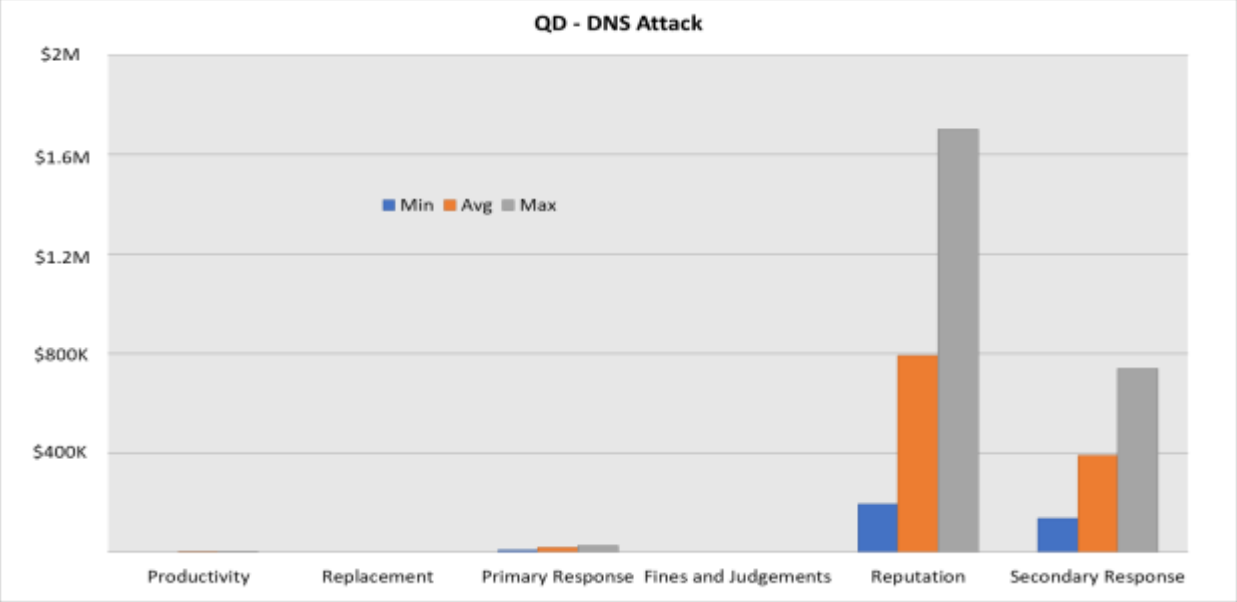
Threat Effect: Availability and Confidentiality

Aggregate Loss Exposure: The following estimate is an aggregation of all independently analyzed DNS attack simulations. The thresholds in the table below represent the results derived from the aggregation of thousands of Monte Carlo simulations ran against this particular scenario. That result set is used to compute the Average, Most Likely, 10th percentile, 90th percentile, and Minimum and Maximum loss exposure values.

Maximum	$2.2M
90th %	$1.6M
Average	$1.2M
10th %	$796K
Minimum	$430K



Scenario Loss Exposure Detail:



Primary Losses	Secondary Losses
***Productivity*:** Losses that result from a reduction in the organizations ability to execute its primary value proposition and/or the firm's employees are unable to perform their duties.	***Fines & Judgements***: Regulatory fines & judgements.
Replacement: No capital assets requiring replacement.	***Reputation***: Stakeholder impact – Effect on market share, cost of capital, stock price, and insurance premium adjustments.
Primary Response: Costs associated to managing the loss event, such as activating and engaging emergency response teams.	***Secondary Response***: Privacy Liability – Expenses incurred while dealing with customers, government, media, & business partners.

Materialized Areas of Loss:

In an effort to identify the nature of a loss event, the confidentiality, integrity, and availability (CIA) triad is the most useful for information security scenarios. The breakdown of loss in each of the three elements is listed below:

Confidentiality events when sensitive non-public information is disclosed, either through malicious acts or error, accounted for $1.16M or 97.3% of loss (Average).

Integrity events when information is either incomplete or inaccurate accounted for 0% of loss exposure (Average).

Availability events when assets are unavailable for use accounted for $32K or 2.7% of loss exposure (Average).

Relevant Assumptions

In this Quantum Dawn scenario, the minimum and maximum values for each specific risk analysis assumption built into the loss estimates are broken out below. All Control and Occurrence factors were set to reflect the fact that the event itself has already occurred, so the system assigns a 100% probability of loss.

- **Recovery Timeframe** (1 to 32 hours)
  - *The length of time it take to bring the assets back up (in hours) when an outage occurs.*
- **Affected Employees** (0 to 20 employees)
  - *The # of employees hindered in their ability to perform their duties when an outage occurs.*
- **Effect on Employee Productivity** (0 to 10%)
  - *The degree to which productivity is affected when an outage occurs that affects employees.*
- **Effect on Organizational Productivity** (10 to 20%)
  - *The % of the time that availability outages affect the organization's operational ability to deliver on its value proposition.*
- **Availability Secondary Effects Percentage** (100%)
  - *The % of outages that would be expected to have an adverse effect on secondary stakeholders (e.g., customers, business partners, etc.).*
- **Confidentiality Secondary Effects Percentage** (100%)
  - *The % of confidentiality breaches that would be expected to have an adverse effect on secondary stakeholders (e.g., customers, business partners, etc.).*
- **Person Hours** (64 to 280).
  - *The probable soft-dollar loss or cost (in terms of person-hours) that would be incurred as people repurpose their activities to respond to an event.*
- **Personally Identifiable Information** (80 to 100%)
  - *The % of sensitive records (restricted or protected data stored, processed or transmitted on these objects) which are classified as protected personal information (i.e. social security numbers)?*
- **Contractually Protected Data** (0 to 25%).
  - *The % of sensitive records (restricted or protected data stored, processed or transmitted on these objects) which are classified as Contractually Protected data (e.g., another company's intellectual property)?*

Scenario Summarized Results

In this particular scenario, where the firm's website traffic has been redirected to a bogus website, the average expected total loss would amount to $1.19M. Nearly two-thirds of that dollar amount, or $790,000, would result from an impact to stakeholders in the form of reputational loss. Nearly another third of the loss would be in the form of secondary response/privacy liability. In this event, there is a minimal impact to internal staff and their productivity, but it would require an average of 172 person hours to resolve.

Quantum Dawn Scenario #2: DDoS Attack

Quantum Dawn Scenario #2: DDoS Attack

Scenario: This scenario is for a single loss event resulting from the threat and limited demonstration of a Distributed Denial of Service (DDoS) attack to the customer-facing website. A DDoS attack is one in which a multitude of compromised systems attack a single target, thereby causing denial of service for users of the targeted system. The flood of incoming messages to the target system essentially forces it to shut down, thereby denying service to the website's legitimate users.

In this instance, attackers threaten to launch a DDoS attack if we fail to pay an internet bitcoin ransom within two hours. After that stated time had elapsed, the attacker has successfully launched a small-scale and relatively short "demonstration" attack that causes minor disruption to the company website. The group perpetrating the attack asserts that it has the capability to launch more powerful and sustained attack and demand payment of a larger ransom.

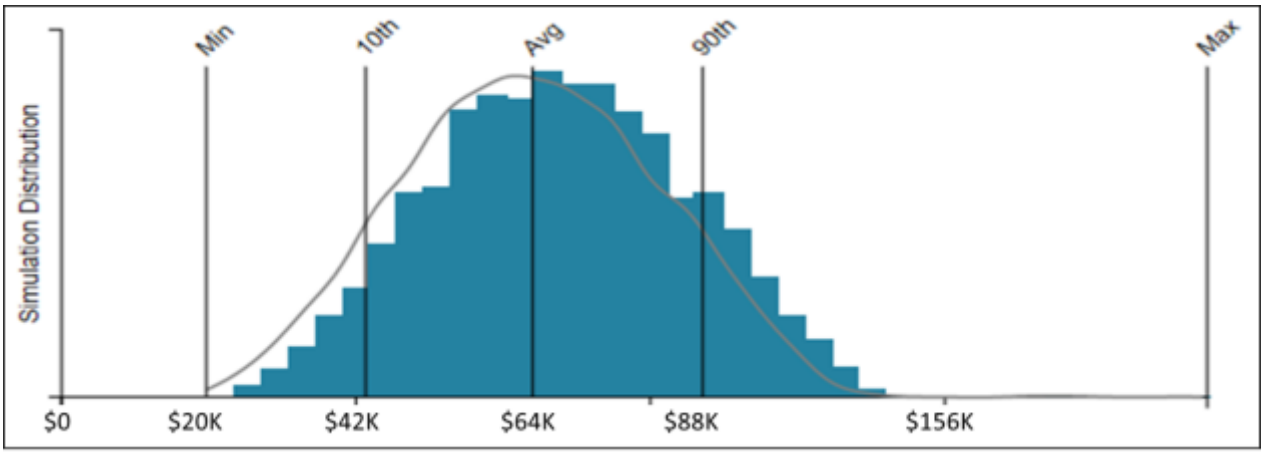
Asset at Risk: Customer Facing Website

Threat Actor: The threat actor was determined to be a professional cybercriminal.

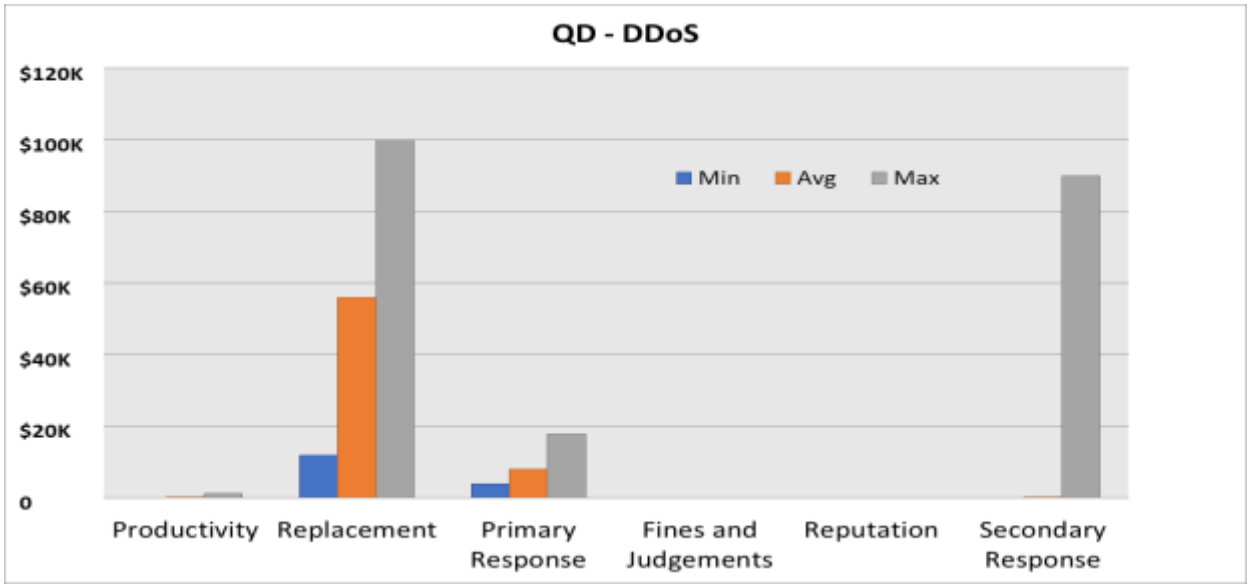
Threat Effect: Availability

Aggregate Loss Exposure: The following estimate is an aggregation of all independently analyzed DDoS attack simulations. The thresholds in the table below represent the results derived from the aggregation of thousands of Monte Carlo simulations ran against this particular scenario. That result set is used to compute the Average, Most Likely, 10th percentile, 90th percentile, and Minimum and Maximum loss exposure values.

Maximum	$156K
90th %	$88K
Average	$64K
10th %	$42K
Minimum	$20K



Scenario Loss Exposure Detail:



Primary Losses	Secondary Losses
***Productivity*:** Business Interruption - Losses that result from a reduction in the organizations ability to execute its primary value proposition and the firm's employees unable to perform their duties.	***Fines & Judgements***: Regulatory fines & judgements. Not applicable within the scope of this scenario.
Replacement: The cost to replace capital assets or activate recovery resources.	***Reputation***: Stakeholder impact – Limited outage with no significant impact.
Primary Response: Crisis Management - Costs associated to managing the loss event, such as activating & engaging emergency response teams.	***Secondary Response***: Expenses incurred while dealing with customers, government, media, & business partners

Materialized Areas of Loss:

Confidentiality events when sensitive non-public information is disclosed, either through malicious acts or error, accounted for 0% of loss (Average).

Integrity events when information is either incomplete or inaccurate accounted for 0% of loss exposure (Average).

Availability events when assets are unavailable for use accounted for $64K or 100.0% of loss exposure (Average).

Relevant Assumptions

In this Quantum Dawn scenario, the minimum and maximum values for each specific risk analysis

assumption built into the loss estimates are broken out below. All Control and Occurrence factors were set to reflect the fact that the event itself has already occurred, so the system assigns a 100% probability of loss.

- **Recovery Timeframe** (2 to 16 hours)
  - *The length of time it takes to bring the assets back up (in hours) when an outage occurs.*
- **Affected Employees** (0 to 10 employees)
  - *The # of employees hindered in their ability to perform their duties when an outage occurs.*
- **Effect on Employee Productivity** (0 to 25%)
  - *The degree to which productivity is affected when an outage occurs that affects employees.*
- **Effect on Organizational Productivity** (0 to 10%)
  - *The % of the time that availability outages affect the organization's operational ability to deliver on its value proposition.*
- **Availability Secondary Effects Percentage** (0.5 to 2%)
  - *The % of outages that would be expected to have an adverse effect on secondary stakeholders (e.g., customers, business partners, etc.).*
- **Replacement Cost** ($10K to $55K)
  - *Capital expense costs that would be incurred to replace the asset(s) at risk.*
- **Person Hours** (30 to 175 hours)
  - *The probable soft-dollar loss or cost (in terms of person-hours) that would be incurred as people repurpose their activities to respond to an event.*

The following averages were derived based on the shape of the distribution we selected to match the data provided – Recovery Timeframe (9 hours); Affected Employees (1.5 employees); Effect on Employee Productivity (3.75%); Effect on Productivity (1.5%); Availability Secondary Effects Percentage (.73%); Replacement Cost ($55K); Person Hours (51.75 hours).

Summarized Results

The average aggregate loss exposure for this scenario, where attackers threaten before ultimately launching a DDoS attack on the company website, came out at just over $64,000. The largest area of potential loss, accounting for 87% of the total, was the aggregation of capital expense costs incurred to replace the assets at risk. Even though the number of affected employees would be minimal, the average number of person hours or response-related cost would be high (nearly 52 hours).

Quantum Dawn Scenario #3: Insider PII Breach Online Banking Platform

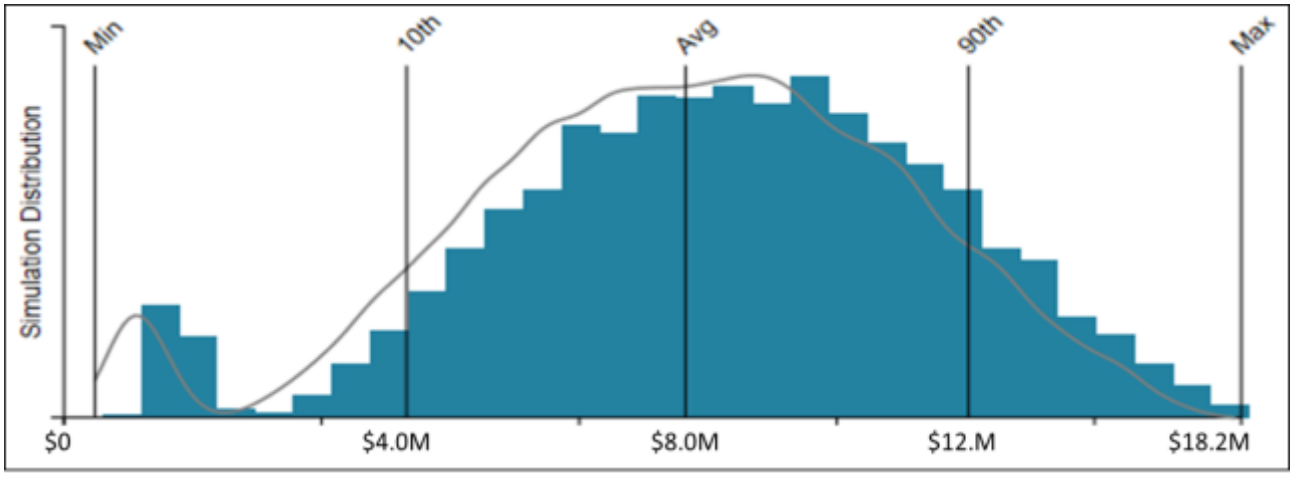
Quantum Dawn Scenario #3: Insider PII Breach Online Banking Platform

Scenario: This scenario is for a single loss event resulting from a malicious employee stealing Personally Identifiable Information (PII) from the Online Banking Platform. PII is information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context.
In this case, a malicious insider has gained unauthorized access to key customer account information and has posted it online in exchange for Bitcoin Internet Currency. Up to 220 thousand records are at risk as a result of this breach.

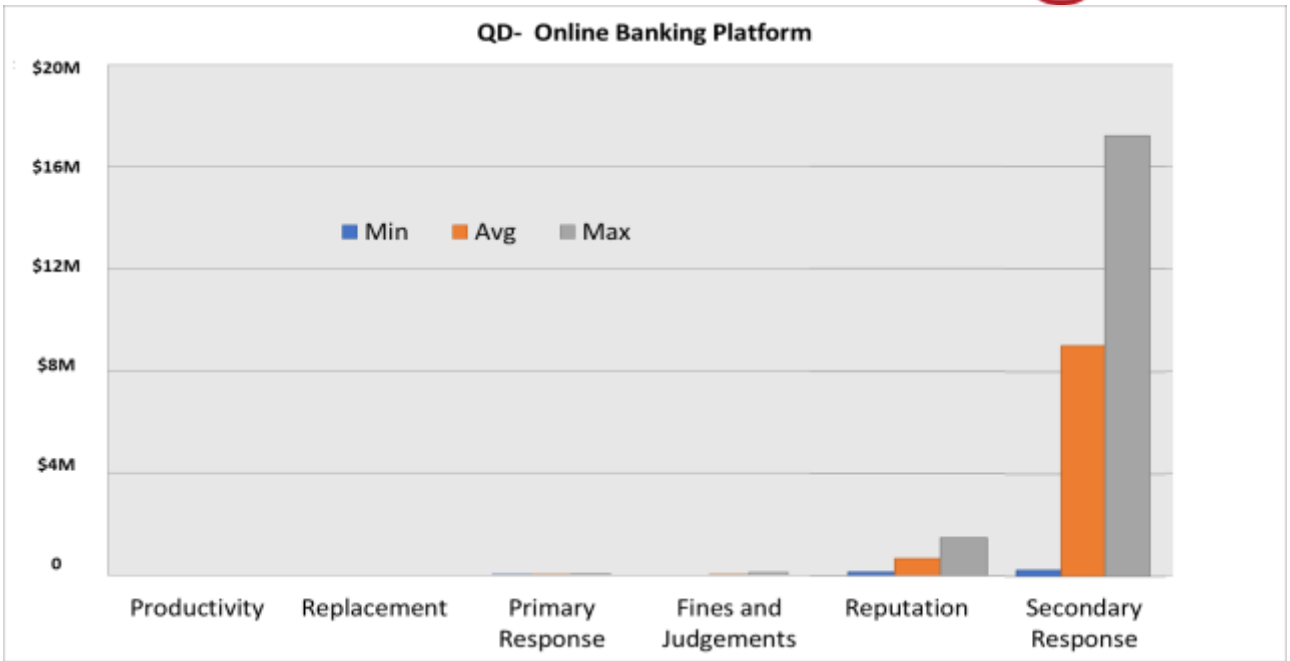
Asset at Risk: *Online Banking Platform*
Threat Actor: *The threat actor was determined to be a privileged insider with malicious intent*
Threat Effect: *Confidentiality*

Aggregate Loss Exposure: The following estimate is an aggregation of all independently analyzed PII Breach simulations. The thresholds in the table below represent the results derived from the aggregation of thousands of Monte Carlo simulations ran against this particular scenario. That result set is used to compute the Average, Most Likely, 10th percentile, 90th percentile, and Minimum and Maximum loss exposure values.

Maximum	$18.2M
90th %	$14.0M
Average	$9.6M
10th %	$5.4M
Minimum	$578K



Scenario Loss Exposure Detail:



Primary Losses	Secondary Losses
***Productivity*:** No production downtime, impact to customer engagement, or loss of employee productivity.	***Fines & Judgements***: Regulatory fines & judgements.
Replacement: No capital assets requiring replacement.	***Reputation***: Stakeholder impact – Effect on market share, cost of capital, and stock price.
Primary Response: Costs associated to managing the loss event, such as activating and engaging emergency response teams.	***Secondary Response***: Privacy Liability – Expenses incurred while dealing with customers (credit monitoring), and media.

Materialized Areas of Loss:

In an effort to identify the nature of a loss event, the confidentiality, integrity, and availability (CIA) triad is the most useful for information security scenarios. The breakdown of loss in each of the three elements is listed below:

Confidentiality events when sensitive non-public information is disclosed, either through malicious acts or error, accounted for $9.6M or 100.0 % of loss (average).

Integrity events when information is either incomplete or inaccurate accounted for $0 or 0.0 % of loss exposure (average).

Availability events when assets are unavailable for use accounted for $0 or 0.0% of loss exposure (average).

Relevant Assumptions

In this Quantum Dawn scenario, the minimum and maximum values for each specific risk analysis assumption built into the loss estimates are broken out below. All Control and Occurrence factors were set to reflect the fact that the event itself has already occurred, so the system assigns a 100% probability of loss.

- **Structural Integrity of Audit Results** (80% min, 90% most likely, 100% max)
    - The % of applications in compliance with secure coding standards or assets (workstations) found to be compliant with policies and standards based on an audit of patch levels and asset configurations.
- **Event Logging Detection Recognition** (0% min, 3% most likely, 20% max)
    - The % of logged/recorded events that would be identified or recognized timely and effectively enough to allow intervention before harm is done.
- **Sensitive Records** (220K most likely)
    - The # of sensitive records stored or processed on a system or application determined to be 'at risk' if a loss event should occur.
- **Confidentiality Secondary Effects Percentage** (100% most likely)
    - The % of confidentiality breaches that would be expected to have an adverse effect on secondary stakeholders (e.g., customers, business partners, etc.).
- **Person Hours** (25 min, 96 most likely, to 500 max hours)
    - The probable soft-dollar loss or cost (in terms of person-hours) that would be incurred as people repurpose their activities to respond to an event.
- **Personally Identifiable Information** (100% most likely)
    - The % of sensitive records (restricted or protected data stored, processed or transmitted on these objects) which are classified as protected personal information (i.e. social security numbers).
- **Contractually Protected Data** (25% min, 32% most likely, 40% max)
    - The % of sensitive records (restricted or protected data stored, processed or transmitted on these objects) which are classified as Contractually Protected data (e.g., another company's intellectual property).

Summarized Results

In this particular scenario, a malicious employee has stolen key customer account information (PII), the average expected total loss would amount to $9.6 million. Nearly 90% of the total loss amount, or $2.6 million, would be the result of an impact to our stakeholders in the form of secondary response (credit monitoring). Another 8% of the loss would be in the form of reputational harm. In this event, there is a minimal impact to our internal staff and their productivity, but it would require an average of 96 person hours to resolve.

Quantum Dawn Scenario #4: Ransomware

Quantum Dawn Scenario #4: Ransomware

Scenario: This scenario is for a single loss event resulting from ransomware being opened on a workstation at HQ. Ransomware is computer malware that installs covertly on a victim's computer, encrypts the victim's data, and demands a ransom payment to decrypt it or not publish it.

In this instance, ransomware was opened on an executive-level workstation at HQ (enabling more access to shared drives than a standard branch employee), resulting in an encryption of the victim's files, making them inaccessible, and demanding a ransom payment in order to receive the decryption key.

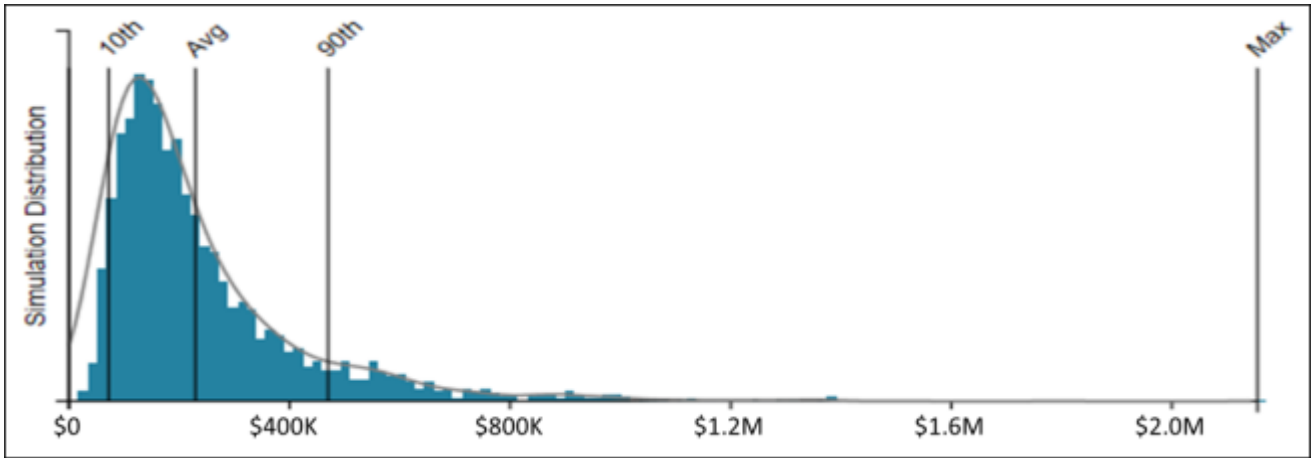
Asset at Risk: Executive employee workstation and corporate shared drives

Threat Actor: The threat actor was determined to be a professional cyber criminal

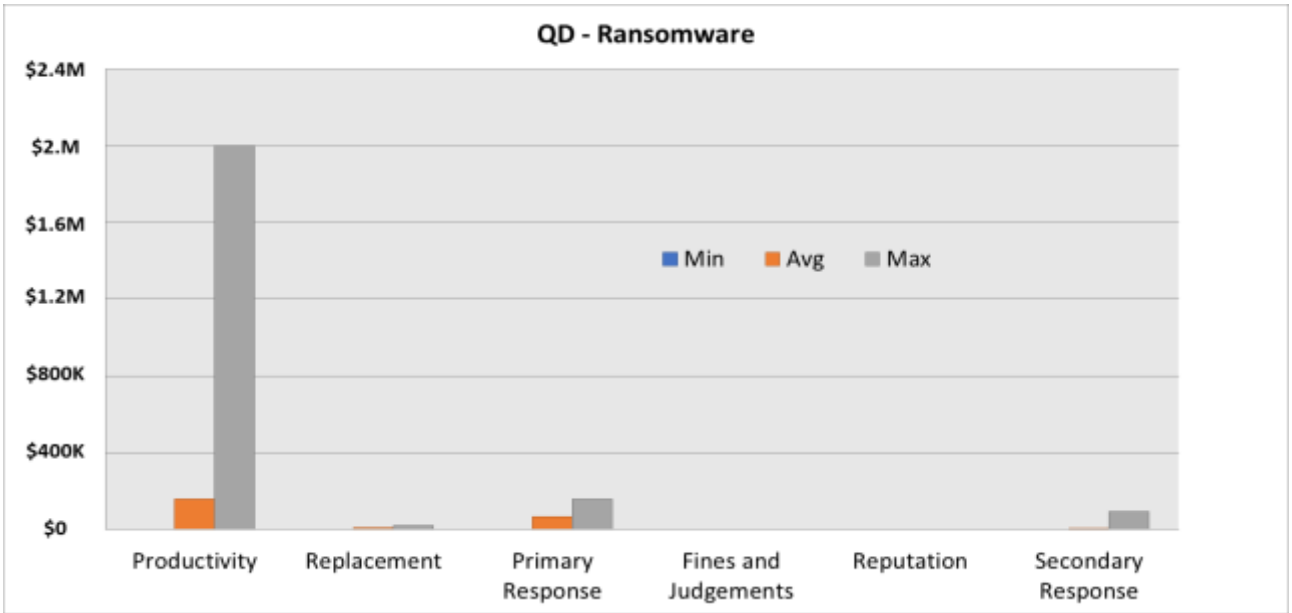
Threat Effect: Availability

Aggregate Loss Exposure: The following estimate is an aggregation of all independently analyzed Ransomware simulations. The thresholds in the table below represent the results derived from the aggregation of thousands of Monte Carlo simulations ran against this particular scenario. That result set is used to compute the Average, Most Likely, 10th percentile, 90th percentile, and Minimum and Maximum loss exposure values.

Maximum	$2.2M
90th %	$570K
Average	$230K
10th %	$72K
Minimum	$0



Scenario Loss Exposure Detail:



Primary Losses	Secondary Losses
***Productivity*:** Business Interruption - Losses that result from a reduction in the organizations ability to execute its primary value proposition and the firm's employees unable to perform their duties.	***Fines & Judgements***: Regulatory fines & judgements. Not a factor within the scope of this scenario.
Replacement: The cost to replace capital assets or activate recovery resources.	***Reputation***: Stakeholder impact – Limited outage with no significant customer facing impact.
Primary Response: Crisis Management - Costs associated to managing the loss event, such as engaging emergency response teams.	***Secondary Response***: Expenses incurred while dealing with customers, government, media, & business partners

Materialized Areas of Loss:

In an effort to identify the nature of a loss event, the confidentiality, integrity, and availability (CIA) triad is the most useful for information security scenarios. The breakdown of loss in each of the three elements is listed below:

Confidentiality events when sensitive non-public information is disclosed, either through malicious acts or error, accounted for 0% of loss (Average).

Integrity events when information is either incomplete or inaccurate accounted for 0% of loss exposure (Average).

Availability events when assets are unavailable for use accounted for $235K or 100.0% of loss exposure (Average).

Relevant Assumptions:

In this Quantum Dawn scenario, the minimum, most likely, and maximum values for each specific risk

analysis assumption built into the loss estimates are broken out below. All Control and Occurrence factors were set to reflect the fact that the event itself has already occurred, so the system assigns a 100% probability of loss.

- **Event Frequency** (0.5 min, 2.75 most likely, 5 max)
    - The frequency with which Cyber Criminals (i.e., professional criminals focused on exploiting assets for financial gain) attempt to compromise the availability of information contained on or processed by company assets.
- **Non-Compliant Authentication Strength** (100% most likely)
    - The % of perceived resistance strength (ability to resist compromise) for accounts on company assets that are not compliant with organization policies and standards regarding passwords and authentication processes.
- **Non-Compliant Structural Integrity Strength** (30 min, 52.5% most likely, 75% max)
    - The % of perceived resistance strength (ability to resist compromise) for those systems or applications that are not compliant with organization policies and standards regarding configurations, patching and/or program code security.
- **Recovery Timeframe** (0.5 min, 7.6 most likely, 48 hours max)
    - The length of time it takes to bring the assets back up (in hours) when an outage occurs.
- **Affected Employees** (1 min, 105.8 most likely, 700 employees max)
    - The # of employees hindered in their ability to perform their duties when an outage occurs.
- **Effect on Employee Productivity** (10% min, 17.5% most likely, 60% max)
    - The degree to which productivity is affected when an outage occurs that affects employees.
- **Effect on Organizational Productivity** (0.5% min, 4.2% most likely, 25% max)
    - The % of the time that availability outages affect the organization's operational ability to deliver on its value proposition.
- **Availability Secondary Effects Percentage** (0.1 min, .85% most likely, 5% max)
    - The % of outages that would be expected to have an adverse effect on secondary stakeholders (e.g., customers, business partners, etc.).
- **Replacement Cost** (0 min, $2500 most likely, $5,000 max)
    - Capital expense costs that would be incurred to replace the asset(s) at risk.
- **Person Hours** (10 min, 273.5 most likely, 320 hours max)
    - The probable soft-dollar loss or cost (in terms of person-hours) that would be incurred as people repurpose their activities to respond to an event.

Summarized Results

In the event that ransomware is opened on an executive level workstation at our Headquarters location, the resulting average expected loss would total $230,000. The loss of productivity due to business interruption would account for nearly 70% of the total loss, or $158,000 and take an average of 7.6 hours to recover from. In addition, this event would affect just over 100 employees and require nearly 275 person hours to resolve. The majority of the remaining loss total could be attributed to the primary response or crisis management of the threat, and cost roughly $64,000.

Quantum Dawn Scenario #5: Loss of Connectivity to Funding Provider

Quantum Dawn Scenario #5: Loss of Connectivity to Funding Provider

***Scenario*:** This scenario is for a single loss event resulting from lost availability/connection to a major trade processing provider or custodian.

Asset at Risk: Critical network infrastructure supporting connectivity to bank funding Institution

Threat Actor: The threat actor was determined to be a malicious privileged insider

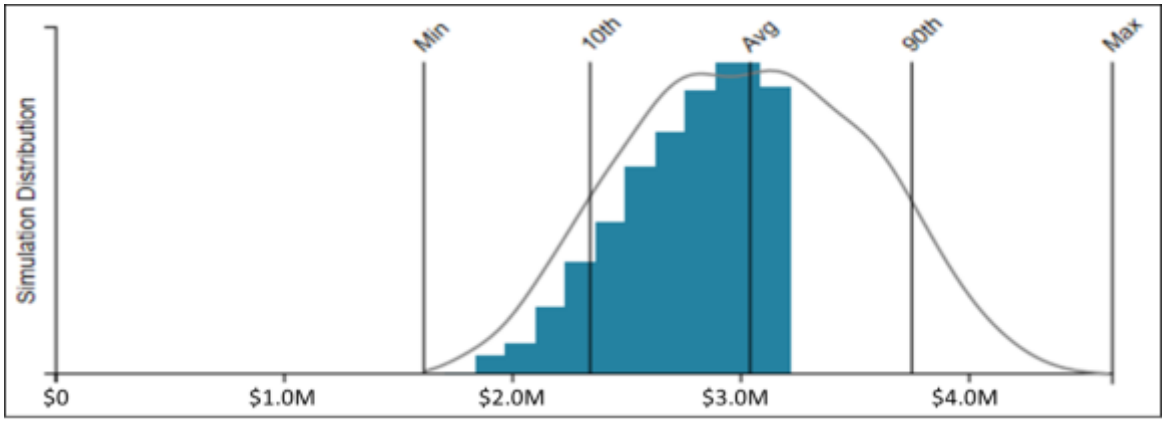
Threat Effect: Availability

In this case, a malicious insider compromised the exchange router and severed the connection to processor, resulting in a disruption of order processing. The following processes would be affected:

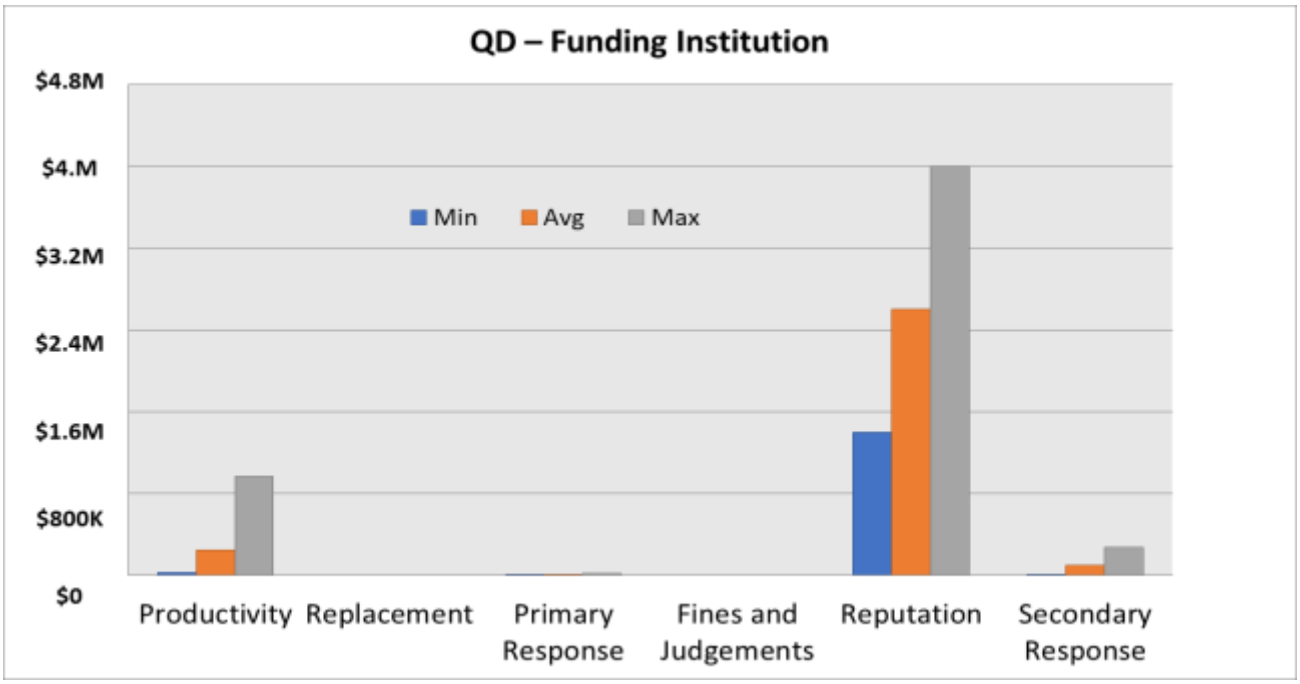
- Large cash management wires
- Funds management files and online banking (OLB) systems both customer impact and bank impact
- ACH batch import (Cash Mgmt)
- Customer cutoff for OLB is 2:30 pm PT (both customer and bank impact)
- Loan Accounting settlements
- Corporate account activity (remote deposit receipts, Image Cash Letter from lockbox, ACH)
- Branch remote check capture

Aggregate Loss Exposure: The following estimate is an aggregation of all independently analyzed Loss of Connection to a major trade processing provider. The thresholds in the table below represent the results derived from the aggregation of thousands of Monte Carlo simulations ran against this particular scenario. That result set is used to compute the Average, Most Likely, 10th percentile, 90th percentile, and Minimum and Maximum loss exposure values.

Maximum	$4.3M
90th %	$3.8M
Average	$3M
10th %	$2.4M
Minimum	$1.61M



Scenario Loss Exposure Detail:



Primary Losses	Secondary Losses

***Productivity*:** Business Interruption - Losses that result from a reduction in the organizations ability to execute its primary value proposition and the firm's employees unable to perform their duties.	***Fines & Judgements***: Regulatory fines & judgements. Not a factor within the scope of this scenario.
Replacement: The cost to replace capital assets or activate recovery resources.	***Reputation***: Stakeholder impact – Limited outage with no significant customer facing impact.
Primary Response: Crisis Management - Costs associated to managing the loss event, such as engaging emergency response teams.	***Secondary Response***: Expenses incurred while dealing with customers, government, media, & business partners

Materialized Areas of Loss: **In an effort to identify the nature of a loss event, the confidentiality, integrity, and availability (CIA) triad is the most useful for information security scenarios. The breakdown of loss in each of the three elements is listed below:**

Confidentiality events when sensitive non-public information is disclosed, either through malicious acts or error, accounted for 0% of loss (Average).

Integrity events when information is inaccurate accounted for 0% of loss exposure.

Availability events when assets are unavailable for use accounted for $3.0M or 100.0% of loss exposure (Average).

Relevant Assumptions

In this Quantum Dawn scenario, the minimum and maximum values for each specific risk analysis assumption built into the loss estimates are broken out below. All Control and Occurrence factors were set to reflect the fact that the event itself has already occurred, so the system assigns a 100% probability of loss.

- **Recovery Timeframe** (12 min, 14 most likely, 16 max hours)
  - The length of time it take to bring the assets back up (in hours) when an outage occurs.
- **Affected Employees** (75 min, 100 most likely, 125 max employees)
  - The # of employees hindered in their ability to perform their duties when an outage occurs.
- **Effect on Employee Productivity** (10% min, 40% most likely, to 70% max)
  - The degree to which productivity is affected when an outage occurs that affects employees.
- **Effect on Organizational Productivity** (100% most likely)
  - The % of the time that availability outages affect the organization's operational ability to deliver on its value proposition.
- **Availability Secondary Effects Percentage** (100% most likely)
  - The % of outages that would be expected to have an adverse effect on secondary stakeholders (e.g., customers, business partners, etc.).
- **Person Hours** (50 min, 72.5 most likely, 200 max hours)

- The probable soft-dollar loss or cost (in terms of person-hours) that would be incurred as people repurpose their activities to respond to an event.

Summarized Results

If an insider compromises the exchange router and severs our connection to the processor, resulting in a disruption of order processing, the resulting average expected loss would total $3 million. By far, the largest portion of loss in this scenario (88% or $2.6 million) would stem from an impact to our stakeholders in the form of reputational loss The loss of productivity due to business interruption would account for another 8% of the total loss, or $246,000 and take an average of 14 hours to recover from. Additionally, this event would roughly affect 100 employees and require nearly 72.5 person hours to resolve. The majority of the remaining loss would come from any secondary response/privacy liability, and cost roughly $96,000.

Quantum Dawn Scenario #6: Settlement System Compromise

Quantum Dawn Scenario #6: Settlement System Compromise

***Scenario**:* This scenario is for a single loss event resulting from an ACH Settlement System Compromise. A settlement system is a system used to facilitate the settlement of transfers of funds or financial instruments.

Asset at Risk: ACH Settlement System

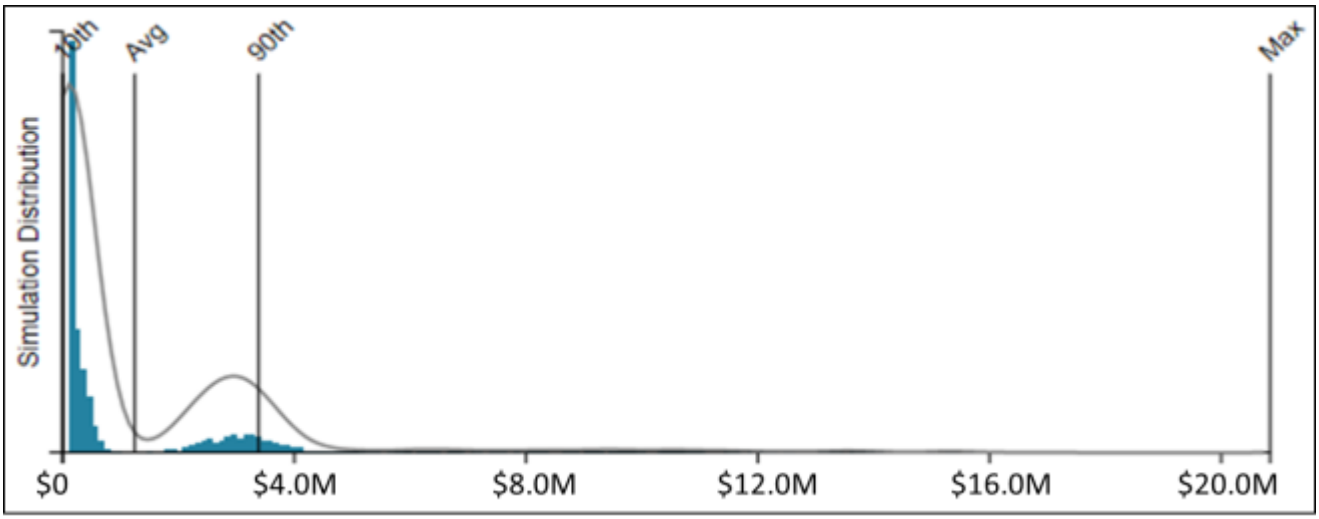
Threat Actor: The threat actor was determined to be an insider - staff

Threat Effect: Availability

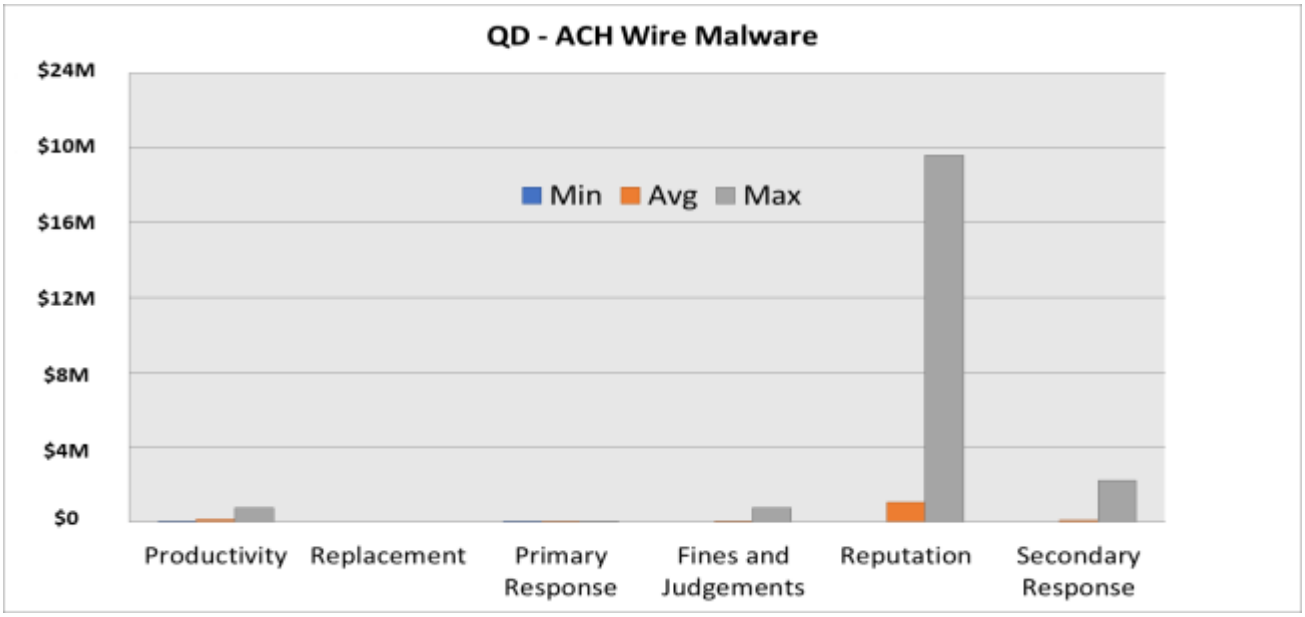
In this instance, an insider introduced malware into the clearing systems after the close-of-day summary and settlement reports were completed, therefore all data appeared to be correct going into our evening cycle. This malware caused major settlement failures (80-90%) and increased risk and uncertainty to all parties. The event was coupled with media reports (including multiple errors) being released to the public.

Aggregate Loss Exposure: The following estimate is an aggregation of all independently analyzed Malware simulations. The thresholds in the table below represent the results derived from the aggregation of thousands of Monte Carlo simulations ran against this particular scenario. That result set is used to compute the Average, Most Likely, 10th percentile, 90th percentile, and Minimum and Maximum loss exposure values.

Maximum	$10.8M
90th %	$3.4M
Average	$1.46M
10th %	$10K
Minimum	$4K



Scenario Loss Exposure Detail:



Primary Losses	Secondary Losses
Productivity**:** Business Interruption - Losses that result from a reduction in the organizations ability to execute its primary value proposition and the firm's employees unable to perform their duties.	***Fines & Judgements***: Regulatory fines, civil judgements, and fees based on contractual stipulations as a result of a loss event.
Replacement: The cost to replace capital assets or activate recovery resources. N/A in this scenario.	***Reputation***: Stakeholder impact – Effect on market share, cost of capital stock price and insurance premium adjustments.
Primary Response: Crisis Management - Costs associated to managing the loss event, such as engaging internal emergency response teams.	***Secondary Response***: Expenses incurred while dealing with customers, business partners, government, and media.

Materialized Areas of Loss: **In an effort to identify the nature of a loss event, the confidentiality, integrity, and availability (CIA) triad is the most useful for information security scenarios. The breakdown of loss in each of the three elements is listed below:**

Confidentiality events when sensitive non-public information is disclosed, either through malicious acts or error, accounted for 0% of loss (Average).

Integrity events when information is either incomplete or inaccurate accounted for $438K or 35.2% of loss exposure (Average).

Availability events when assets are unavailable for use accounted for $808K or 64.8% of loss exposure (Average).

Relevant Assumptions

In this Quantum Dawn threat scenario, the minimum and maximum values for each specific risk analysis assumption built into our loss model are broken out below. All Control and Occurrence factors were set to reflect the fact that the event itself has already occurred, so the system assigns a 100% probability of loss.

- **Recovery Timeframe** (10 min, 17 most likely, 24 hours max)
  - The length of time it take to bring the assets back up (in hours) when an outage occurs.
- **Affected Employees** (2 min, 2.6 most likely, 6 employees max)
  - The # of employees hindered in their ability to perform their duties when an outage occurs.
- **Effect on Employee Productivity** (30% min, 53% most likely, 75% max)
  - The degree to which productivity is affected when an outage occurs that affects employees.
- **Effect on Organizational Productivity** (0% min, 85% most likely, 100% max)
  - The % of the time that availability outages affect the organization's operational ability to deliver on its value proposition.
- **Availability Secondary Effects Percentage** (10% min, 25% most likely, 40% max)
  - The % of outages that would be expected to have an adverse effect on secondary stakeholders (e.g., customers, business partners, etc.).
- **Integrity Secondary Effects Percentage** (0% min, 5% most likely, 10% max)
  - The % of data integrity compromises that would be expected to have an adverse effect on secondary stakeholders (e.g., customers, business partners, etc.).
- **Person Hours** (10 min, 37 most likely, 63 hours max)
  - The probable soft-dollar loss or cost (in terms of person-hours) that would be incurred as people repurpose their activities to respond to an event.

Summarized Results

If an insider introduces malware into the clearing systems leading to major transaction/settlement failures and reputational impact, the resulting average expected loss would total $1.25M. Nearly 84% of the loss in this scenario, or $1.05M, would come as a result from the impact to our stakeholders in the form of reputational risk. The loss of productivity due to business interruption would account for another 9.6% of the total loss, or $120,000 and take an average of 17 hours to recover from. Lastly, while this event wouldn't affect a large number of employees, it would still require 37 person hours to resolve.

Ensuring cybersecurity for the financial services industry is an iterative process and a top priority for the industry, at both the largest and smallest firms at the highest levels in the corporate suite. The organization highlighted in this document had the wherewithal to first identify the critical assets within the organization, relate those assets to the exercise objectives, run quantitative risk analysis thus understanding the impact to the organization, and then decide if or what mitigation options were appropriate.

About RiskLens®

RiskLens is the leading provider of cyber risk quantification software. RiskLens empowers large enterprises and government organizations to manage cyber risk from the business perspective by quantifying it in dollars and cents. Our customers leverage RiskLens to understand their cyber risk exposure in financial terms, prioritize their risk mitigation, measure the ROI of their security investments, and optimize their cyber insurance coverage. RiskLens is the only cyber risk management software purpose-built on FAIR, the only standard quantification model for information security and operational risk.