AON

Lex Mundi Forum

Cyber Risks & Insurance for Law Firms

March 17, 2022

Agenda

1. **Introduction & update on cyber threat landscape for law firms**

2. **Cyber coverage – what to look for**

3. **Cyber event readiness:**

   At the onset of a cyber event – what are the major issues and priorities?

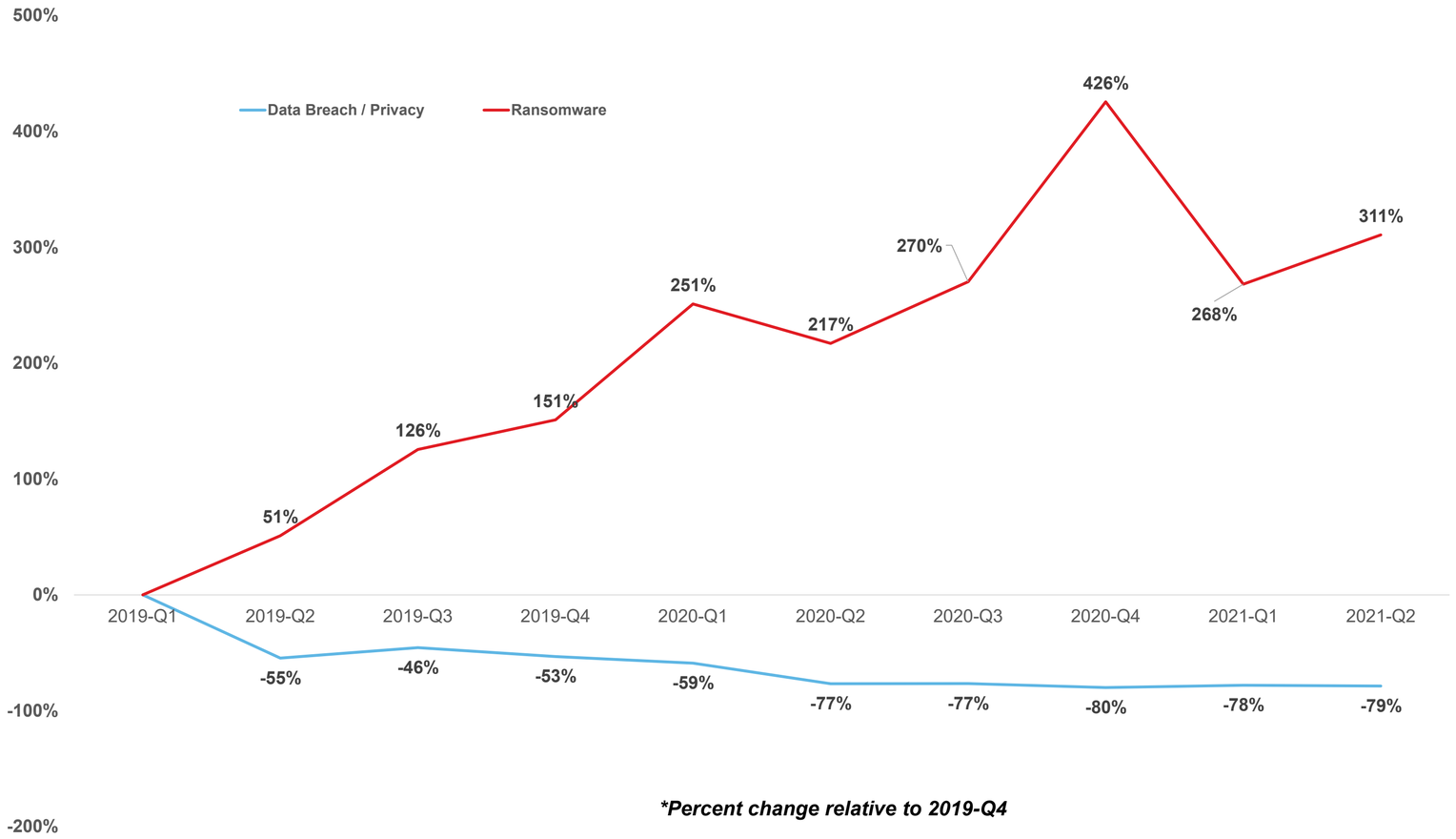
   How does the process run for law firm managing a claim?

   What decision-making structure should a law firm have in place?

4. **Q&A / Peer discussion**

Introduction
Cyber Threat Landscape

Threat Environment



Percent change relative to 2019-Q4

Key Observations:

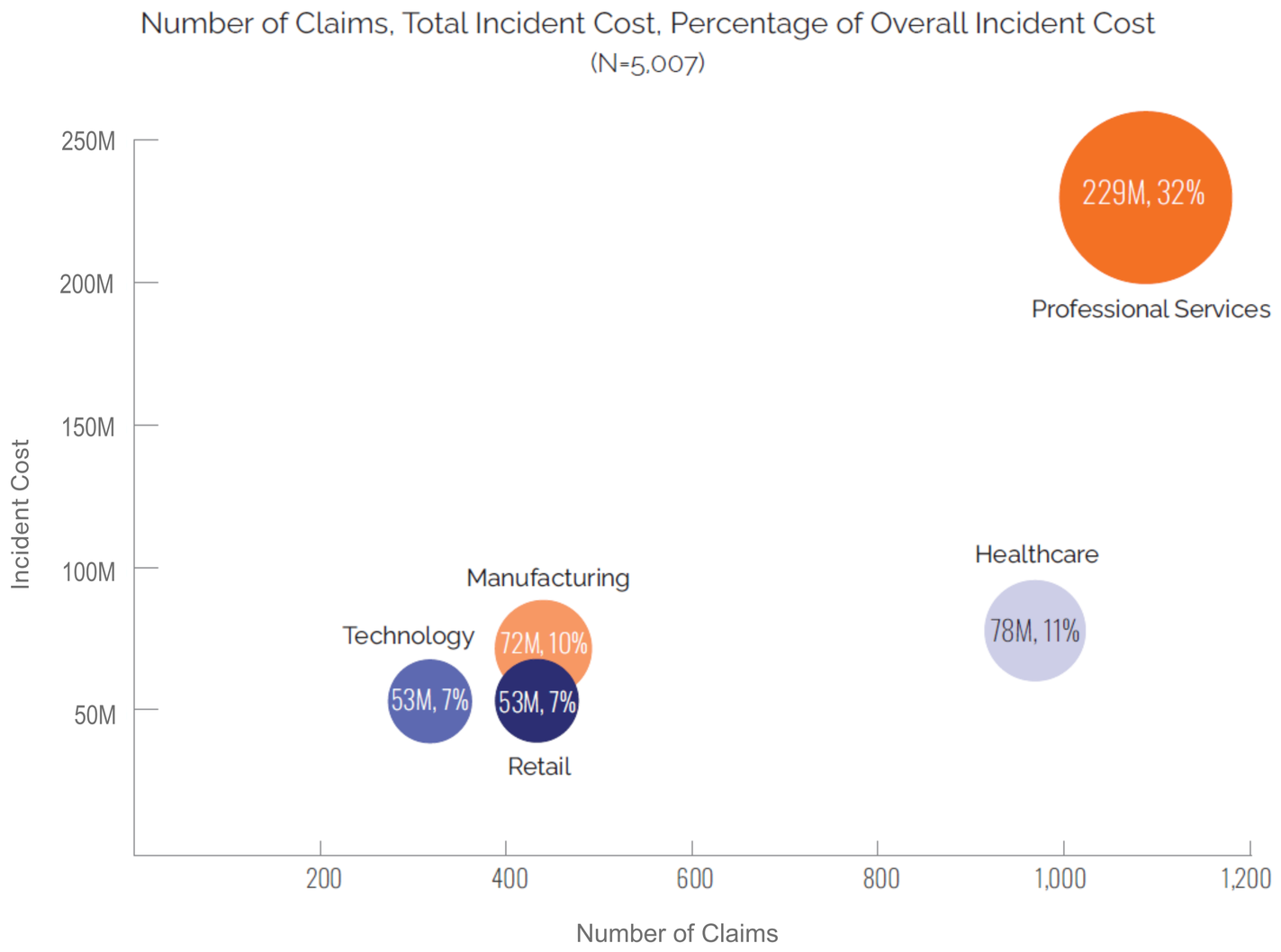
- Ransomware activity has dramatically **outpaced Data Breach/Privacy Event activity**.
- **Average Ransomware payment up 130%*** from Q3 2021 to Q4 2021 - now **$322,168.**
- Eight figure losses are commonplace – **business interruption is often the largest component of loss**.
- **Data exfiltration occurred in 84% of ransomware cases in Q4 2021.***
- **Average downtime**, **20 days** in Q4 2021.*

Source: Risk Based Security, analysis by Aon. Data as of 7/12/2021; Ransomware data exfiltration and downtime per Coveware Quarterly Ransomware Report as of 4/26/2021

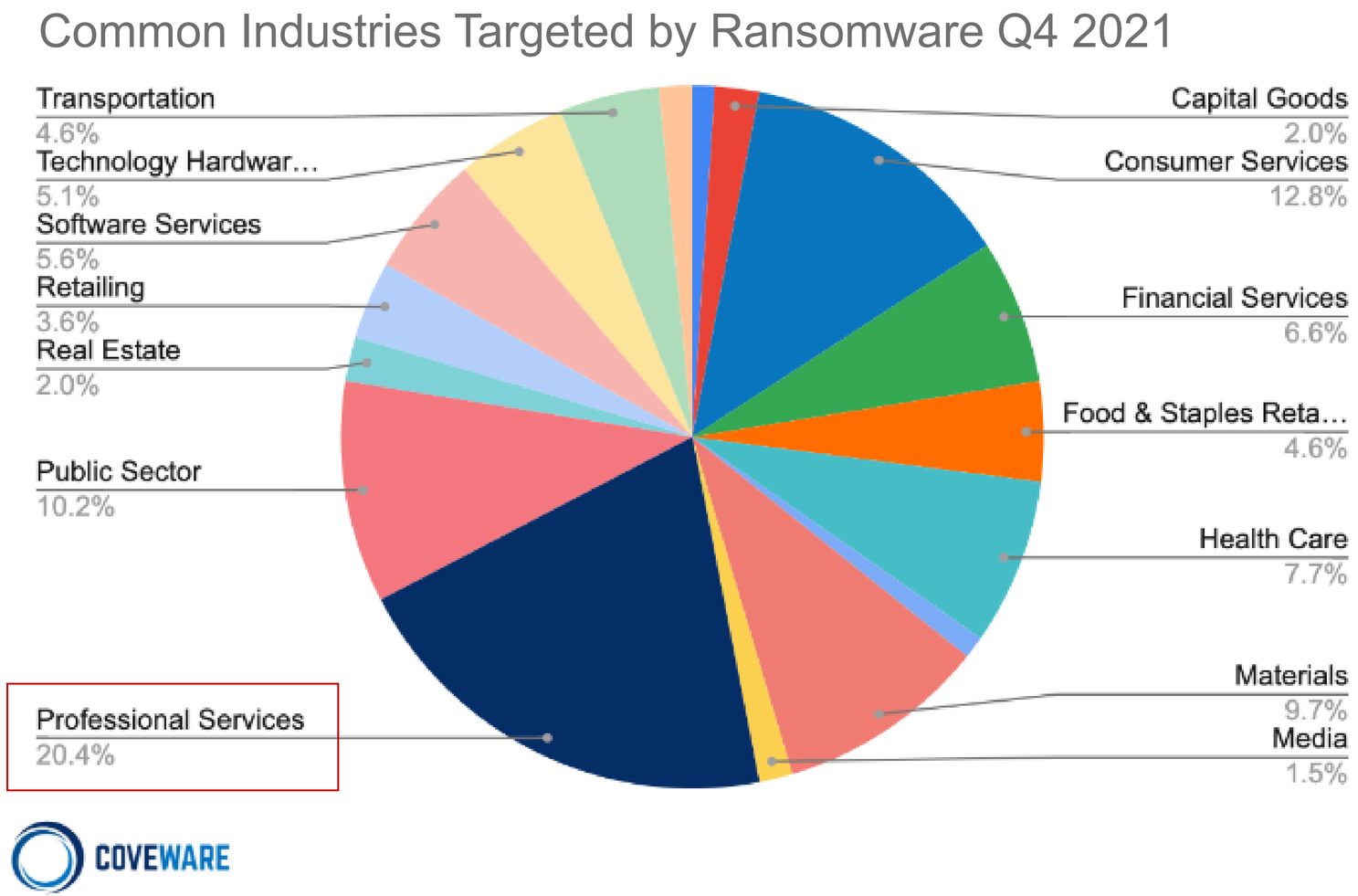
* Per Coveware online blog

Threat Environment

NetDiligence 2021 Cyber Claims Study Report



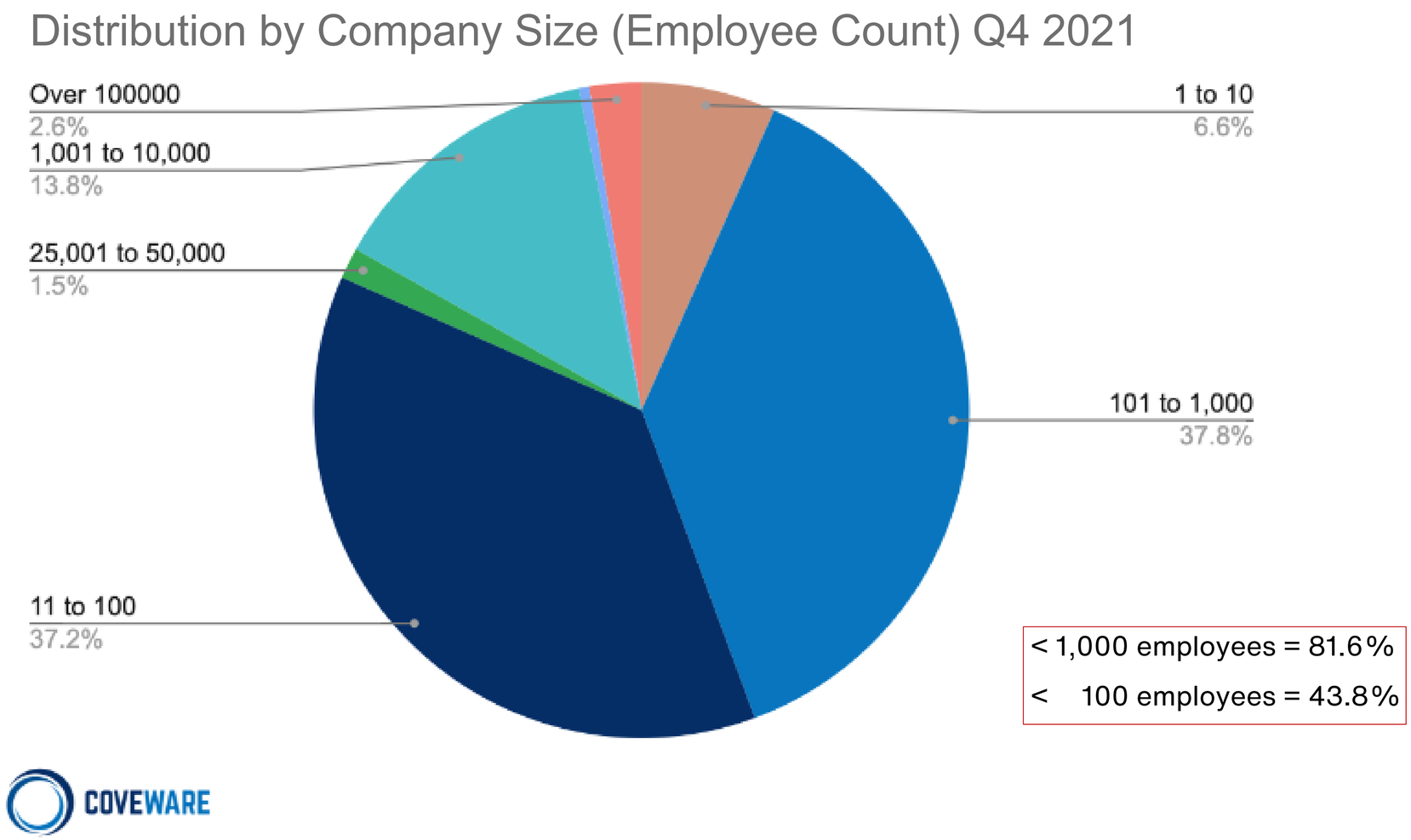
Threat Environment



COVEWARE

AON

Threat Environment



Threat Environment

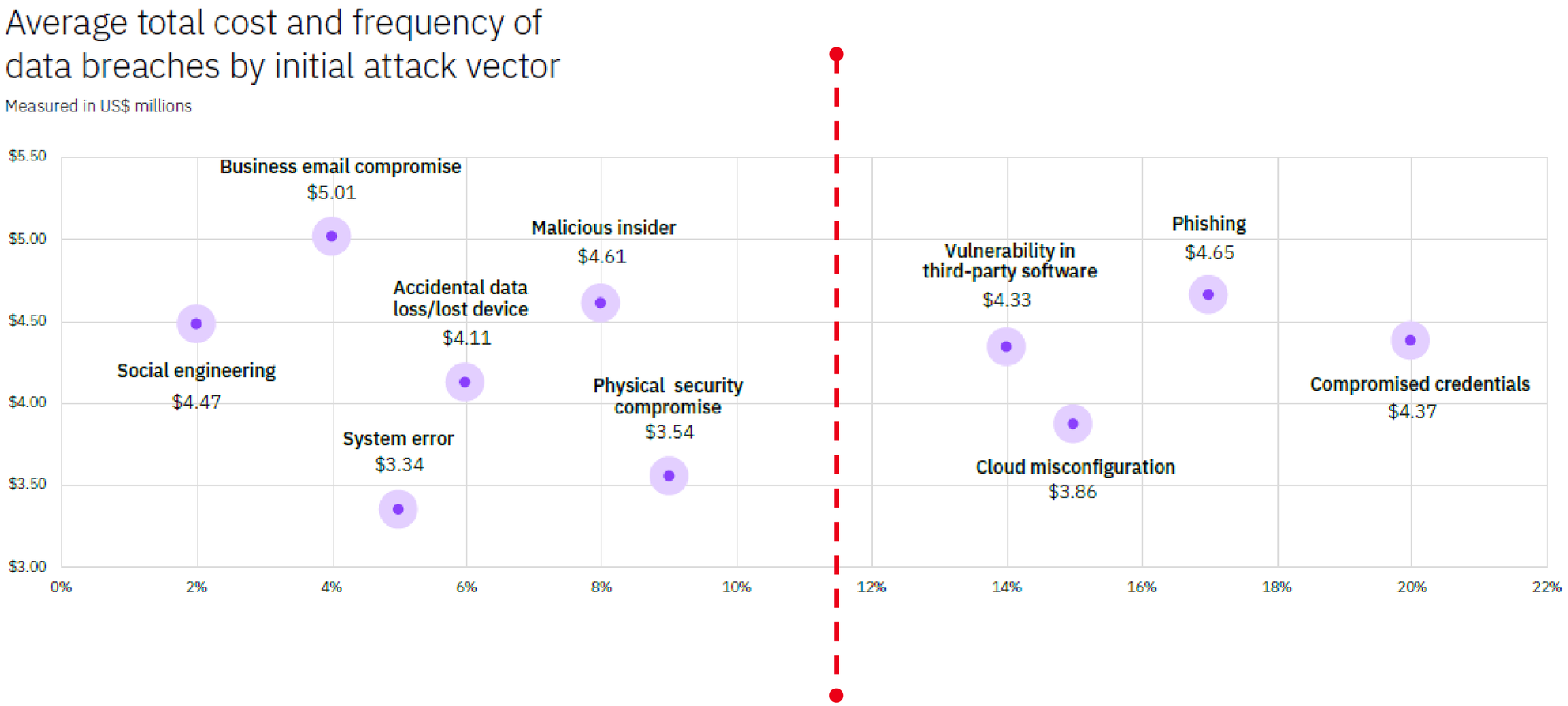
Baker Hostetler 2021 Data Security Incident Report

Email account compromises to facilitate wire transfer fraud (BECs) are still happening

$26 million	$453,468	$6 million	$758,365	28%
In wire transfers resulting from a BEC	Average wire transfer	Largest wire transfer	Average recovery	Matters that had recovered funds totaling over $12 million

Threat Environment

IBM-Ponemon 2021 Cost of a Data Breach Report



Threat Environment

NetDiligence Cyber Claims Study – 2020 Report

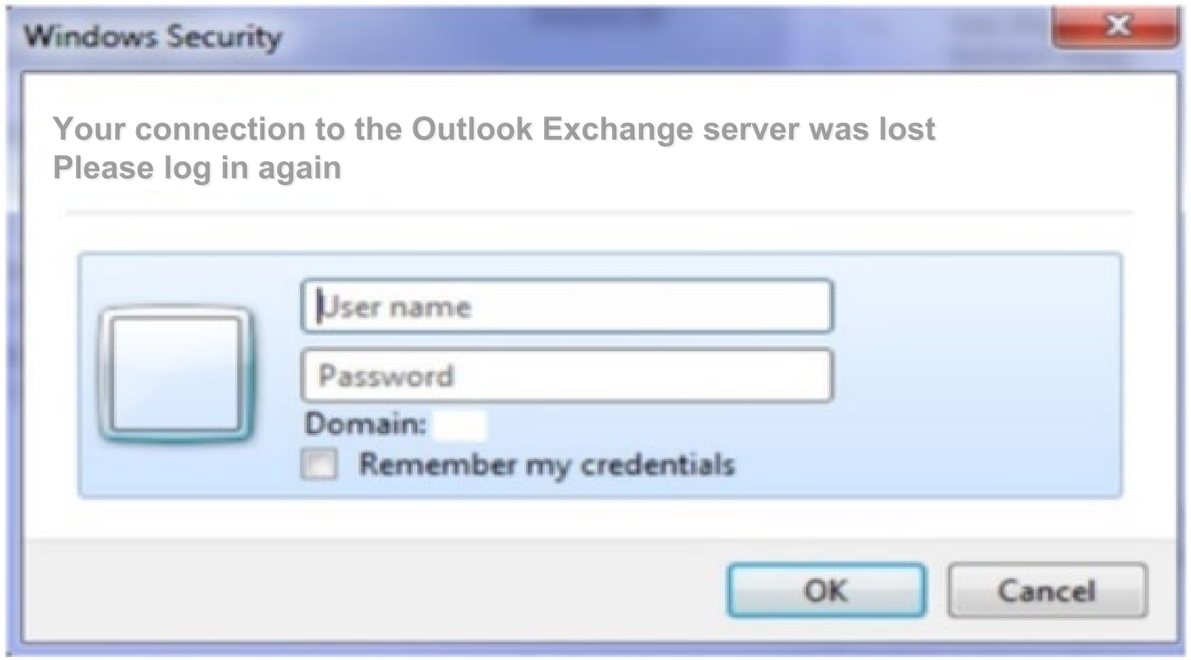
Incident Cost by Revenue Size
2015-2019

	Revenue Size	Claims	Minimum	Average	Median	Maximum	Total
SMEs	Nano-Rev (<$50M)	1,590	1K	91K	41K	7.1M	145.4M
	Micro-Rev ($50M-$300M)	594	1K	173K	62K	6.6M	102.9M
	Small-Rev ($300M-$2B)	199	3K	359K	105K	7.4M	71.3M
	Unknown	970	1K	211K	12K	120.2M	204.5M
Large Companies	Mid-Rev ($2B-$10B)	28	3K	3.6M	207K	64.0M	99.6M
	Large-Rev ($10B-$100B)	15	249K	20.3M	10.0M	97.0M	305.2M
	Mega-Rev (> $100B)	3	15.0'M	23.3M	15.0M	40.0M	70.0M

Case Studies

Case Study 1 - Phishing

- 77 Attorneys in a large law firm received an email from a client email address
- The email attached a Word document that had been shared multiple times between the client and firm
- 7 Attorneys were familiar with the matter in question and opened the document
- After opening the document, a pop-up box appeared showing a Microsoft error message:



Case Study 1 - Phishing

- 4 Attorneys entered their credentials and carried on working
- The credentials were received by a server in Zurich Switzerland
- Within hours hackers compromised the email accounts and started downloading information

Case Study 2 - Ransomware

Ransomware Attack Causes Law Firm to Close

The offices of Charlotte, NC-based Law Firm LLP lost access to thousands of stored legal documents when the CryptoLocker ransomware, delivered as an email attachment, encrypted them permanently. The email attachment appeared to be an automatically generated recording of a voicemail message and was delivered to the firm's receptionist. When the receptionist opened the attachment, the ransomware was launched, encrypting all the firm's data and backups.

The firm was not able to obtain Bitcoin to pay the ransom on time and missed the deadline to obtain the decryption key. The firm lost all of its data and subsequently went out of business.

Case Study 3 - Extortion

Attack on Secure File Transfer Application

In late 2020 threat actors identified and exploited a vulnerability in a widely used secure file transfer application. The threat actors initially targeted financial institutions in the Asia-Pacific region (including

In early 2021 the threat actors started targeting law firms in the USA. They identified that the application was being used to transfer large quantities of high-sensitivity data between law firms and their clients. The vulnerability allowed the threat actors to exfiltrate data.

The threat actors then reviewed public information about the firms involved to establish an initial extortion demand. Initial demands seen by Aon ranged from $5m to $50m and actual payments made ranged from less than $1m to between $4m and $5m.

The largest payment made by a law firm is understood to be over $10m

Aon Professional Services Practice Experience

Aon's Professional Services Practice has seen an increase in both frequency and severity of claims within our client base. These numbers are not statistically significant, but are reflective of the experience being reported by insurers and consultants, and by reports compiled from insurer and victim surveys

2020

14 incidents notified that turned into actual claims

9 were significant:

3 paid more than $500k but <$1m

2 exceeded $1m paid but <$2m

4 were $multi-million claims (>$3m, <$10m)

In addition to the above, notice was given on 9 incidents arising from ransomware hitting third party providers (Epiq eDiscovery and TBG Benefits). None of these resulted in a claim.

Several clients reported using the compromised version of SolarWinds Orion. No associated claims reported.

Total claims payments for the year >$21m

2021

6 significant incidents notified to insurers in H1

All 6 incidents involve extortion

3 are multi-million-dollar losses (>3m, <5m)

7 firms notified Microsoft OWA incidents, no associated claims reported

4 firms notified Accellion incidents, all 4 resulted in paid claims

Total claims payments for the year >$14m

2022 Q1

4 Incidents reported

1 Insider data theft

1 APT incident

2 Ransomware events

AON

Cyber Coverage

Coverage Provided by a Cyber Policy*

*Cyber policies vary greatly in coverage grants and terms & conditions

Insuring Agreements	
Event Management	• Breach Counsel • Forensic Investigation • Remediation • Crisis Communications consulting
Network Interruption	• Loss of Revenue • Reputational Loss / System Failure • Extra Expense • Forensic Accounting consulting
Extortion	• Extortion Negotiation consulting • Ransom payment
Cyber Crime	• Computer Crime • Social Engineering
Security & Privacy Liability	• Defense Counsel • Liability to third parties • Regulatory Defense • Fines & Penalties
Media Liability	• Defense Counsel • Liability to third parties

Potential Coverage Restrictions*

*Cyber policies vary greatly in coverage grants and terms & conditions

Ransomware:
- Sub-limit
- Coinsurance
- Exclusion

Widespread event endorsement:
- Sub-limit
- Coinsurance

War Exclusion:
- Acts of foreign enemy
- Onus on the insured
- Collateral damage
- Cyberterrorism carveback

Governmental Acts Exclusion:
- State Actors
- Requisition

Dependent Business Interruption:
- Sub-limit
- Coinsurance
- Exclusion

Professional Liability:
- Exclusion

Media Liability:
- Electronic media only
- Exclusion

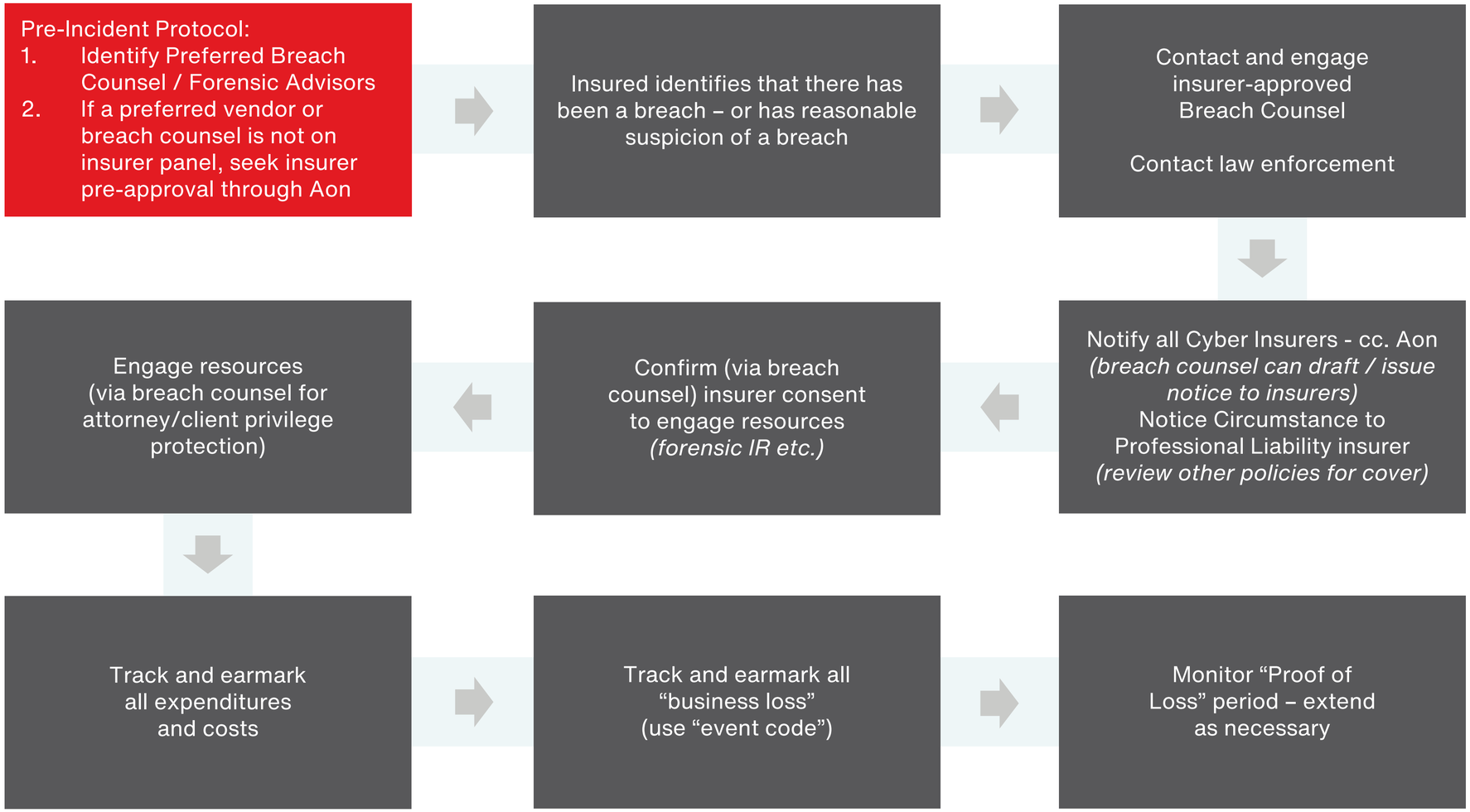
Wrongful Collection:
- Exclusion

Biometric Information:
- Exclusion

Controversial Practice Areas:
- Opioids
- Cannabis

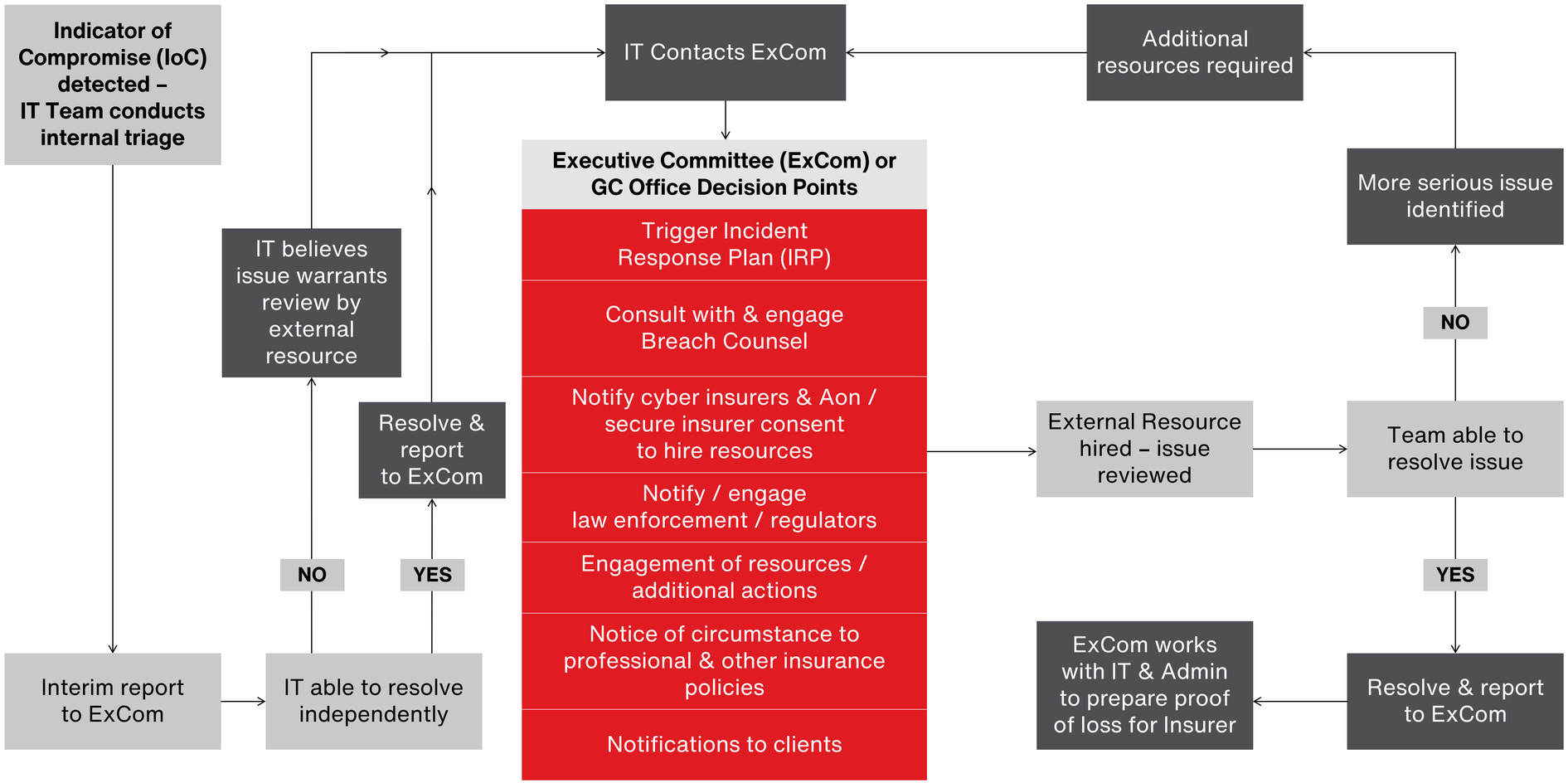
Event Readiness & Claims Process

Cyber Incident Flow Chart – Key Steps



Event Readiness Decision Making

This diagram illustrates how a cyber event response flow might work in a firm where it is coordinated through the Executive Committee or General Counsel's office. It can be modified to account for different internal reporting structures.



Common Missteps

- Treating a cyber attack solely as an IT problem
- Failure to engage breach counsel
- Delay notifying insurers
- Not securing insurer consent where required (especially extortion payments)
- Engaging non-approved or non-insurer-panel resources
- Failure to engage law enforcement in a ransomware attack
- Disregarding OFAC due diligence requirements (especially for extortion events)
- Using internal resources for breach counsel services
- Using an existing security services vendor for forensics

Q&A

For more information, please contact:

Tom Ricketts

Senior Vice President and Executive Director

+1.212.441.1744 (t)

+1 (646) 300 2894 (m)

tom.ricketts@aon.com

Professional Services Practice Website

Professional Services Practice Insights