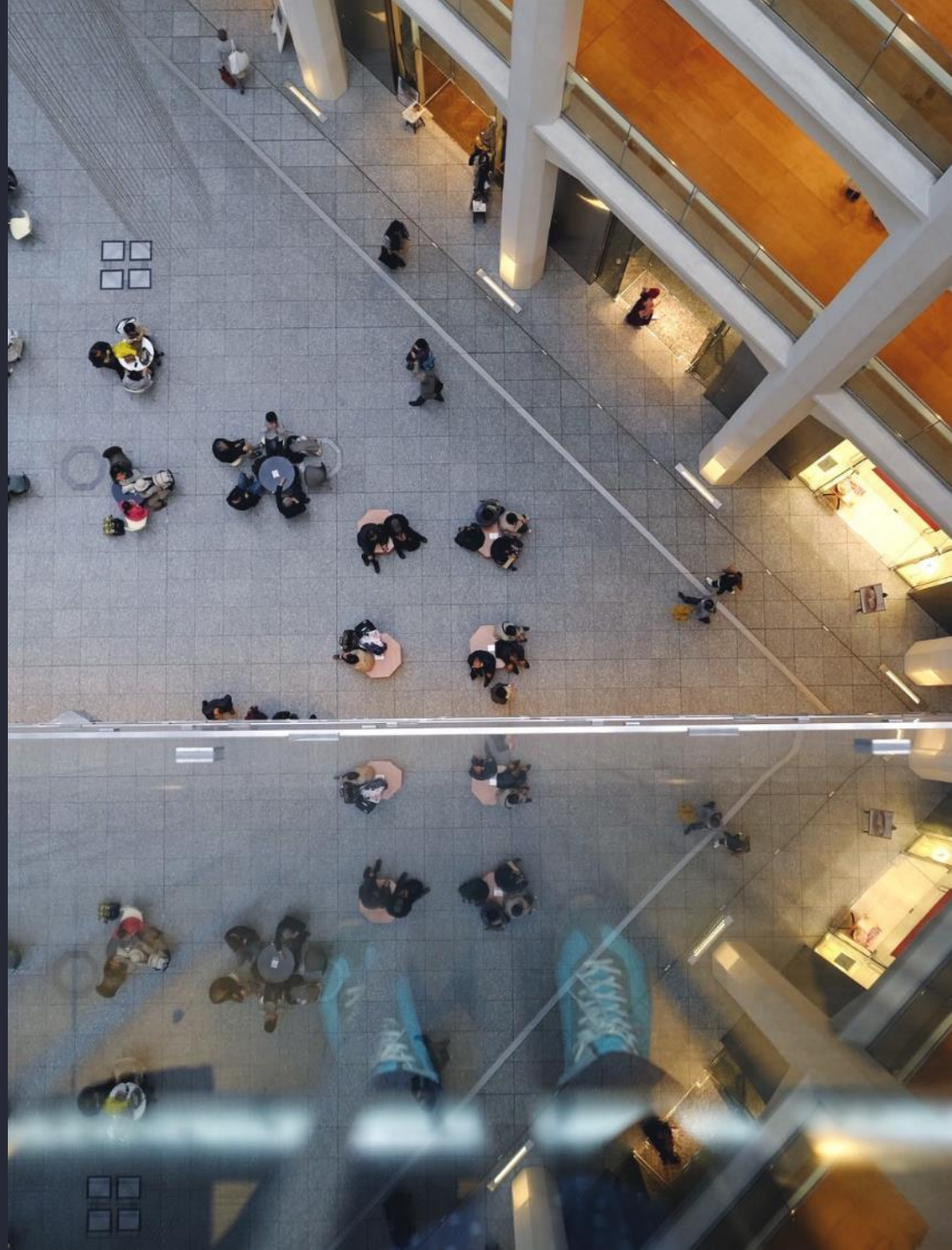
The Ransomware Effect

Key Next Steps and How Cyber Insurance Can Help Respond

FEI Madison

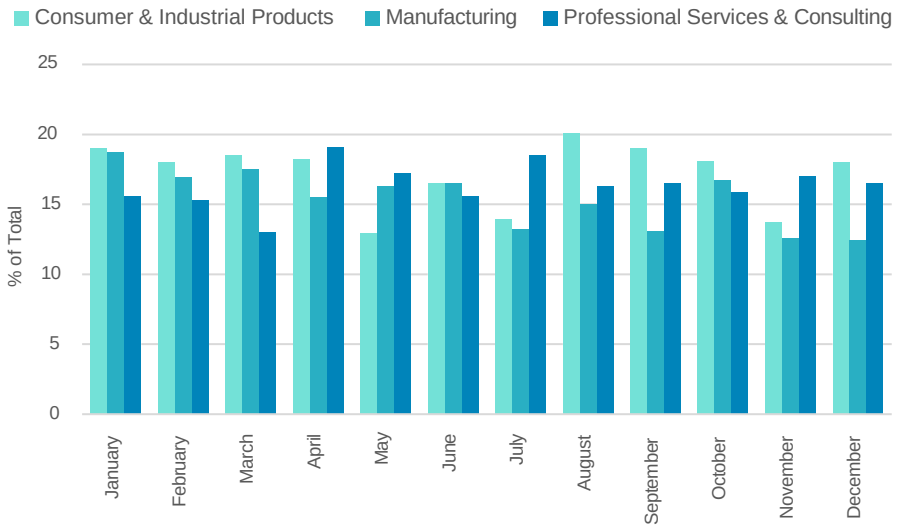
March 10, 2025



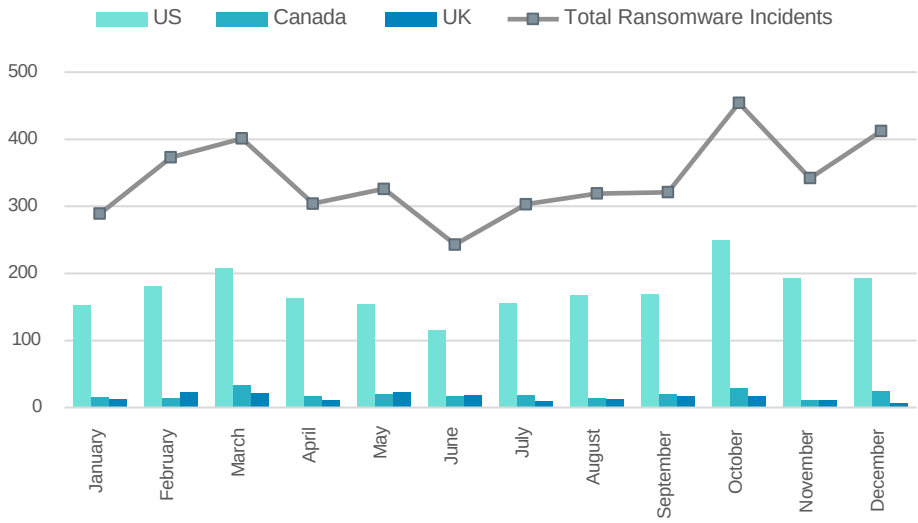
Observed Ransomware Breach Trends

YE 2024

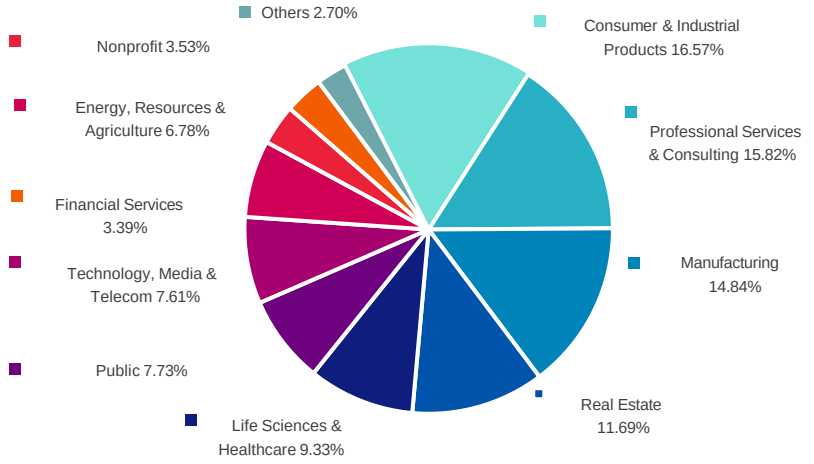
Top Targets by Sector



Top Targets by Country



Ransomware Victims by Sector



Top Ransomware Groups

Group	Number of Published Victims
LockBit 3.0	404
RansomHub	387
Play	308
Akira	250
Hunters International	195

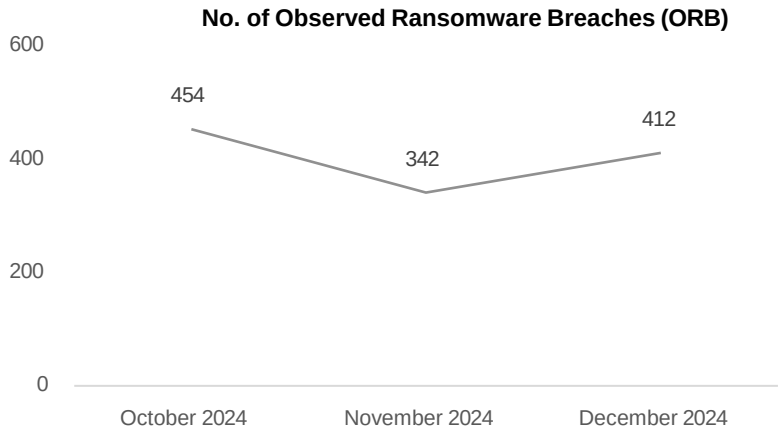
Source: *Aon Intelligence team analysis of information posted on ransomware leak sites on the dark web. Larger sample size.

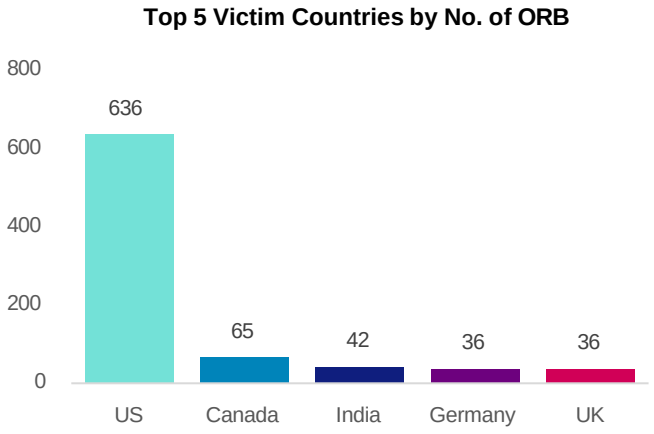
Observed Ransomware Breach Trends

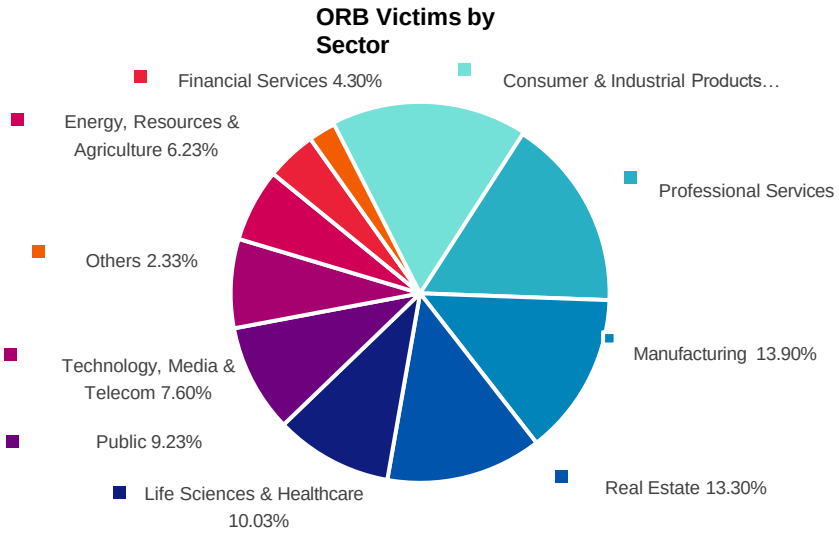
Q4 2024

Observed Ransomware Breaches

Observed ransomware breaches (ORBs) represent instances of organisations being named and/or having their data published on ransomware group data leak sites due to not paying ransoms.







Top 10 Ransomware Groups by

RW Group	No. of ORB
RansomHub	182
Kill Security aka KillSec	84
Akira	79
Play	73
Funksec	66
Fog	52
Hunters International	51
Medusa	40
Meow team	35
Black Basta	34

Source: *Aon Intelligence team analysis of information posted on ransomware leak sites on the dark web. Larger sample size.

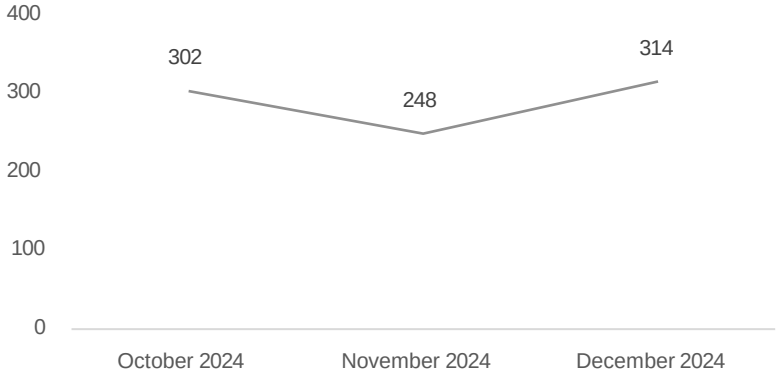
Access Claim Trends

Q4 2024

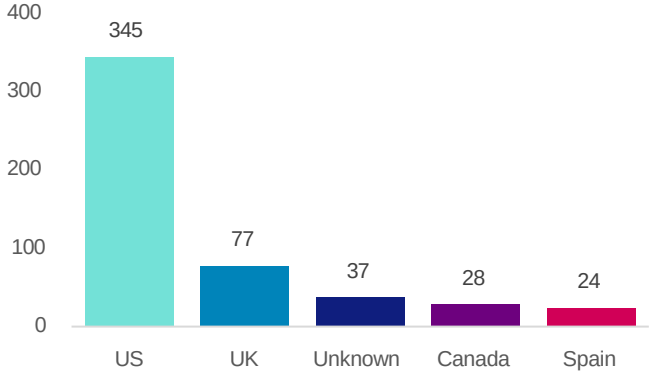
Access Claims

Access claims represent instances identified on underground marketplaces and hacker forums of claims by threat actors to have gained access to a network.

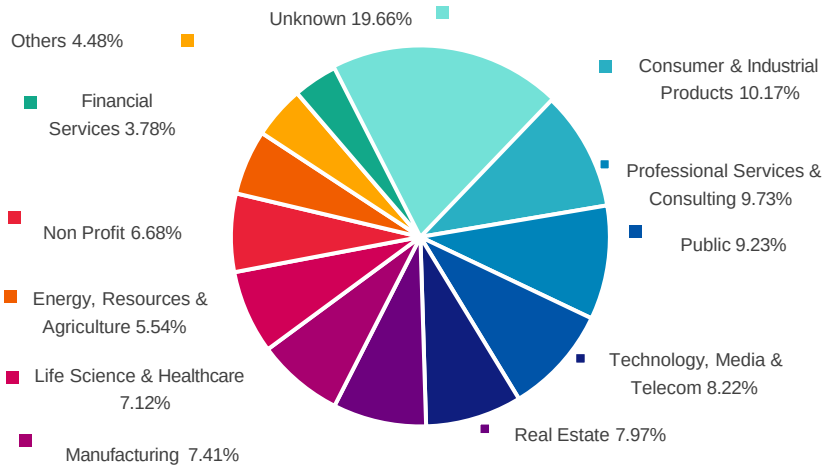
No. of Access Claims



Top 5 Countries of Target Victims by No. of Access Claims



Target Victims by Sector



Top 10 Technology Types Targeted

Technology Type	Percentage Impact
RDP Tools	51.1%
Not Listed	21.5%
Corporate Remote Access Portals	14.0%
Corporate Application	3.9%
Remote Access Services	3.5%
Unspecified Technologies	1.1%
Other	1.0%
RMM Tools	0.8%
Email Platforms	0.7%
Government Application	0.6%

Source: *Aon Intelligence team analysis of information posted on ransomware leak sites on the dark web. Larger sample size.

Access Claim Trends | Q4 2024

Marketplace Minimum Expectations

Multi-Factor Authentication (MFA)	Endpoint Detection and Response (EDR)	Phishing Exercise/ Cyber Awareness Training
Vulnerability Scanning & Patch Management	Secure RDP/VPN	Incident Response Plan/ Ransomware Exercise
Access Control/ Service Accounts	Disaster Recovery/Backups	Email Filtering & Security (DMARC / DKIM)
Zero Day Vulnerabilities and Supply Chain Risks	Network Segmentation/ Network Monitoring	M&A Due Diligence and Integration

Top 10 Critical Red Flags

YE 2024

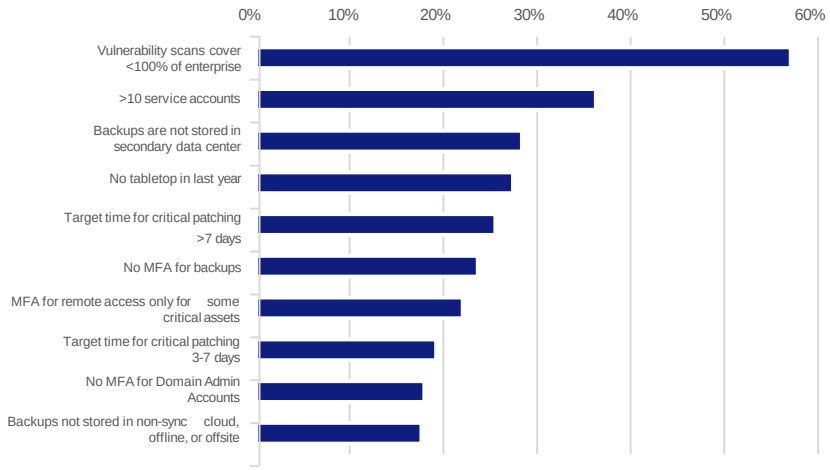
Global & Enterprise

57%

reported **vulnerability scans cover <100%** of the enterprise

36%

reported **>10 service accounts**



Key Observations:

- Although the number of service accounts is greater in larger organizations, privileged service accounts tend to be better managed.
- When a client has less than 100% covered in vulnerability scanning, segmentation is reviewed which is not captured in the above.

Data for over 270 existing and new Global and Enterprise US clients.

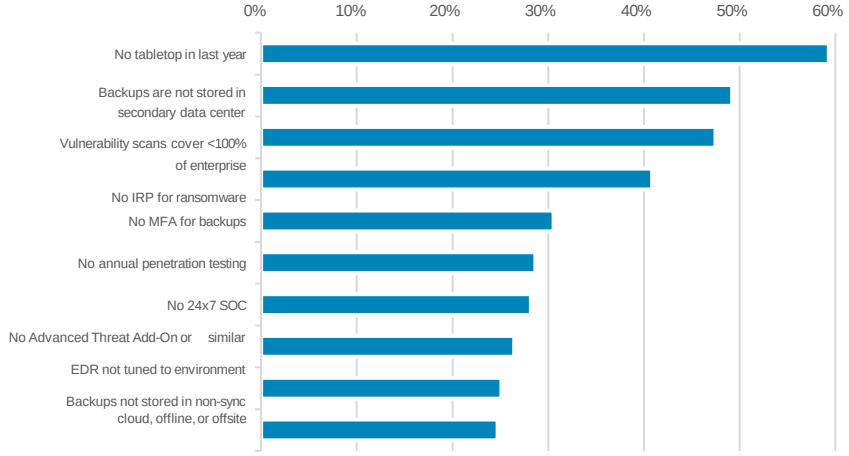
Middle Market & SME

59%

reported to lack annual **tabletop exercise**

49%

reported to lack **secondary data center for backups**



Key Observations:

- Privacy, while not necessarily from a risk perspective is an increased focus of carriers in terms of the controls that are in place around how insureds collect user information.
- *IBM's Cost of a Data Breach Report found that having an incident response team and formal incident response plans enables organizations to reduce the cost of a breach by almost half a million US dollars (USD 473,706) on average.

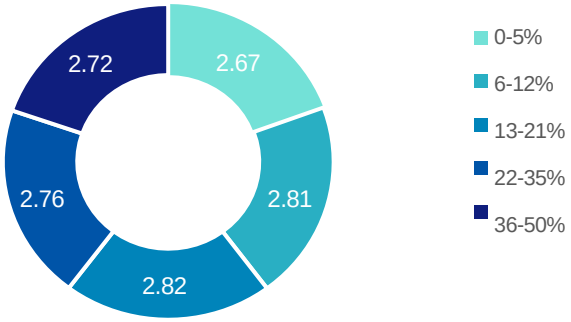
Data for over 1650 existing and new Middle Market and SME US clients.

Source: *CyQu's Red Flags data. Red flags are validated monthly by Aon's 'red flag committee' and quarterly by Aon's Underwriting Council compromised of three of its largest trading partners.
*IBM Cost of a Data Breach Report 2024

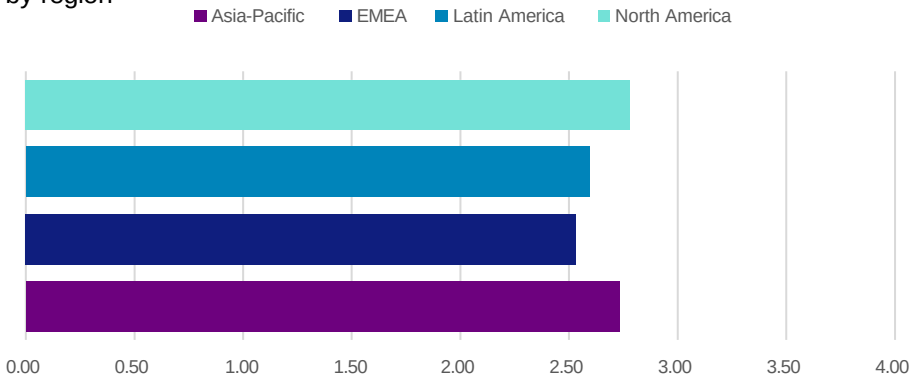
Cyber Maturity Analysis

2024 Global Data

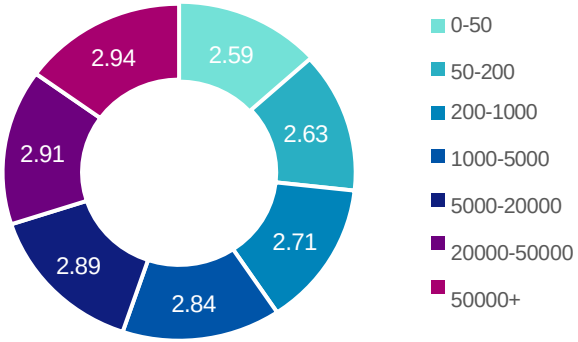
Total Score
by % of IT Budget Spent on Security



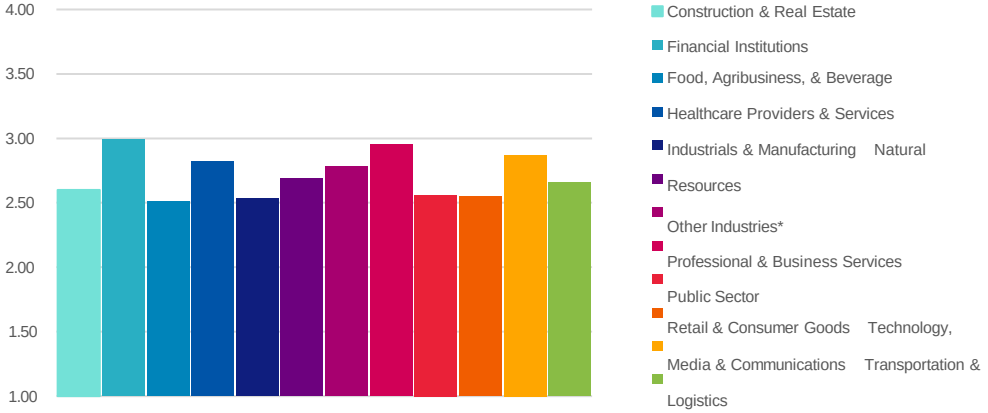
Total Score
by region



Total Score
by Employee Headcount



Total Score
by Industry



* 'Other Industries' category represents responses from clients in the following industries: Financial Sponsors, Hospitality, Travel & Leisure, Insurance, Life Science, Sports & Entertainment.

Data for over 3200 Aon global clients. North America and EMEA account for 94% of the data.
North America account for 76% of the Global & Enterprise ($2Bn and above) data, demonstrating higher maturing. EMEA has a larger pool of SME and Mid-Market clients.

Source: *CyQu Enterprise Edition response data analysis for 2024.

The Ransomware Effect

Potentially impacted insuring agreements stemming from a ransomware event

1st Party Insuring Agreements

Cyber Extortion	Reimbursement coverage for any extortion payment. **Tie-in** – Social engineering (whaling, spear phishing) and invoice manipulation are both direct phishing attempts.
Reputational Harm	Reimbursement coverage for loss income as a result of an adverse media report of a privacy incident. **Tie-in** – Ransomware groups hold all sorts of privacy records (Ex. Conti held passports for ransom). These threat actors intentionally exfiltrate data to initiate payment faster.
Network Business Interruption	Reimbursement coverage for net income loss, caused by computer system outage (Security or System Failure). **Tie-in** – Ransom negotiations can often become drawn out and result in a direct hit on the business's net income. 1st party business interruption coverage can help combat this element of an attack.
Computer Hardware Replacement / Bricking	Reimbursement coverage for insureds replacement of computer hardware due to unauthorized reprogramming/**ransomware** **Tie-in** – Ransomware or malware has the capability to corrupt and ruin all electronic equipment, turning the device into a 'brick'.
Digital Asset Protection	Reimbursement coverage for the insured for non-physical assets (software and data). **Tie-in** – Most ransom payments correlate with non physical assets being held hostage, similar to a network security failure.
Breach Event Expenses	Reimbursement coverage for insured's costs to respond to security incident . **Tie-in** – When ransomware is paid out, expenses can include computer forensics, legal expenses, expenses related to advertising.

3rd Party Insuring Agreements

Network Security Liability	Liability coverage for damages suffered by others stemming from a network security failure (confidential info, unauthorized access). **Tie-in** – Once the threat actors deploy malware and begin exfiltrating/holding an organization's data hostage, a large amount of that data may be 3rd Party information (client data), and can result in liability suits against the insured.
Privacy Liability	Often included in conjunction with Network Security Liability, Privacy Liability provides coverage for damages suffered by others to protect confidential 3rd party info. **Tie-in** – Data exfiltration is a key component of modern-day ransomware attacks, especially against organizations who house a large amount of sensitive 3rd party information.
Regulatory Proceedings Liability	Liability coverage for defense costs brought by a government agency/regulatory body due to a failure to protect private information. **Tie-in** - Third party coverage for actions/ investigations resulting from a violation of privacy law. If a government agency was to have a cyber breach; Ex, Police Department's files corrupted, would have to implement the regulatory proceedings coverage. Also will typically include coverage for GDPR, CCPA, and/or other state privacy laws where applicable.

Cyber Policy Design & Intent

Covered

- ✓ Third Party Claims for failure to protect employee or customer PII
- ✓ Interruption coverage for the loss of revenue due to the network failing because of a cyber attack and / or system failure
- ✓ Cyber extortion and ransomware related events (where insurable by law)
- ✓ Expenses to Digitally Restore or Recreate intangible assets / IT Network
- ✓ First Party Breach Response Expenses including: Forensics, Legal Guidance, Notification, Credit Monitoring, PR, and Call Center Services.

Not Covered

- × Property Damage and Bodily Injury
- × Theft of First Party Intellectual Property
- × Real Monies Lost (Crime)
- × Late Notice of Claim(s)
- × Pollution Liability

Important Notice

Claims Made Policies

Claims Made Policies

E&O/Cyber Liability policies often are claims made, which means that coverage applies to claims made during the policy period or extended reporting period (if applicable).

Reporting Requirements

E&O/Cyber Liability policies generally require reporting of claims during the policy period in which they were made. Failure to do so can result in denial of coverage.

Insurer Approval

E&O/Cyber Liability policies usually require the approval of the insurer(s) prior to selecting breach response vendors or defense counsel, incurring any defense costs, or agreeing to any settlement. Failure to do so can result in denial of coverage.

Note

These comments are general observations. Please refer to your policy for actual terms and conditions.

Claims Reporting Roadmap

Redacted Carrier

You are here: Your firm has suffered a security incident. The clock is now ticking. It's time to do right by your customers, employees, shareholders and others. A quick, effective response will help you to avoid lawsuits and regulatory inquiries.

Immediately gather your internal team and review your incident response plan.

Call the Insurance Carrier Breach Hotline; then contact the pre–approved expert privacy attorneys to determine legal applicability of actions, to respond to reporting requirements, and to maintain privilege. These lines are monitored seven (7) days a week. Leave a voicemail message. Contact your Aon broker to provide formal notice to Insurance Carrier.

Consult with your expert privacy attorney on the current situation and begin to determine what next steps are necessary.

Debrief with Insurance Carrier Cyber Claims. Some important things to cover:

- When and how discovered
- Type of event
- Who attacked
- Extent of attack
- Impact on business
- Type of data at risk
- # and location of people potentially impacted
- Ransom demand and threat actor

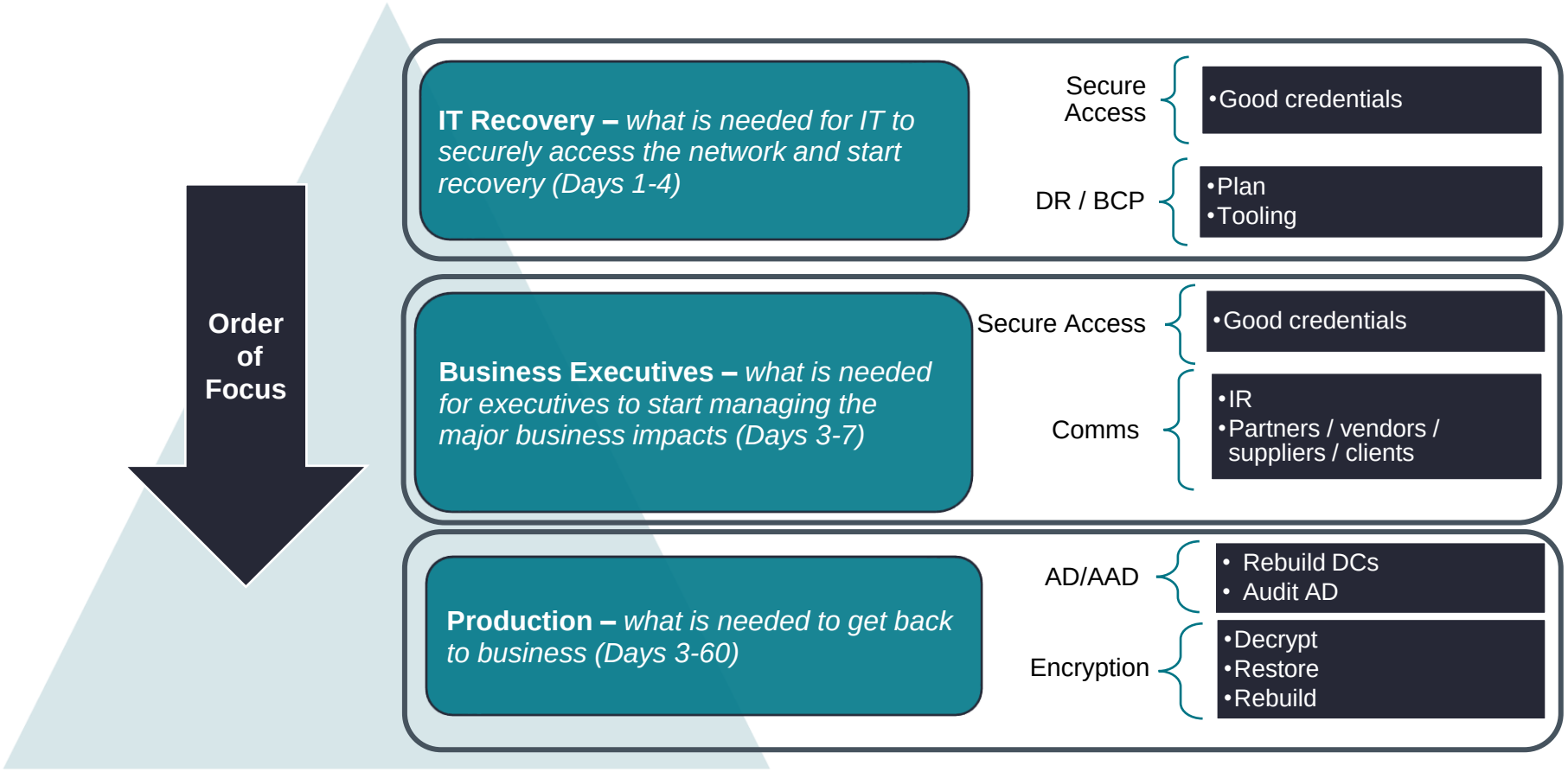
Insurance Carrier Claims Specialist will assist with identifying the resources needed to respond to the event and will provide consent as required.

1. Engage a pre–approved computer forensics firm to determine existence, cause and scope of the breach.
2. Engage ransomware response vendor if necessary.
3. Determine if a public relations or crisis communication firm is required.
4. Consult with experts to determine if notifications are necessary. If so, decide who needs to be notified and utilize a pre–approved vendor.
5. After assessing the notification requirements, determine if a call center is required and contact a pre–approved vendor.
6. Decide if credit or identity monitoring is necessary. If so, contact the proper credit and identity monitoring firm.
7. Consider engaging forensic accountant; set up method to track and document cyber–related expenses.

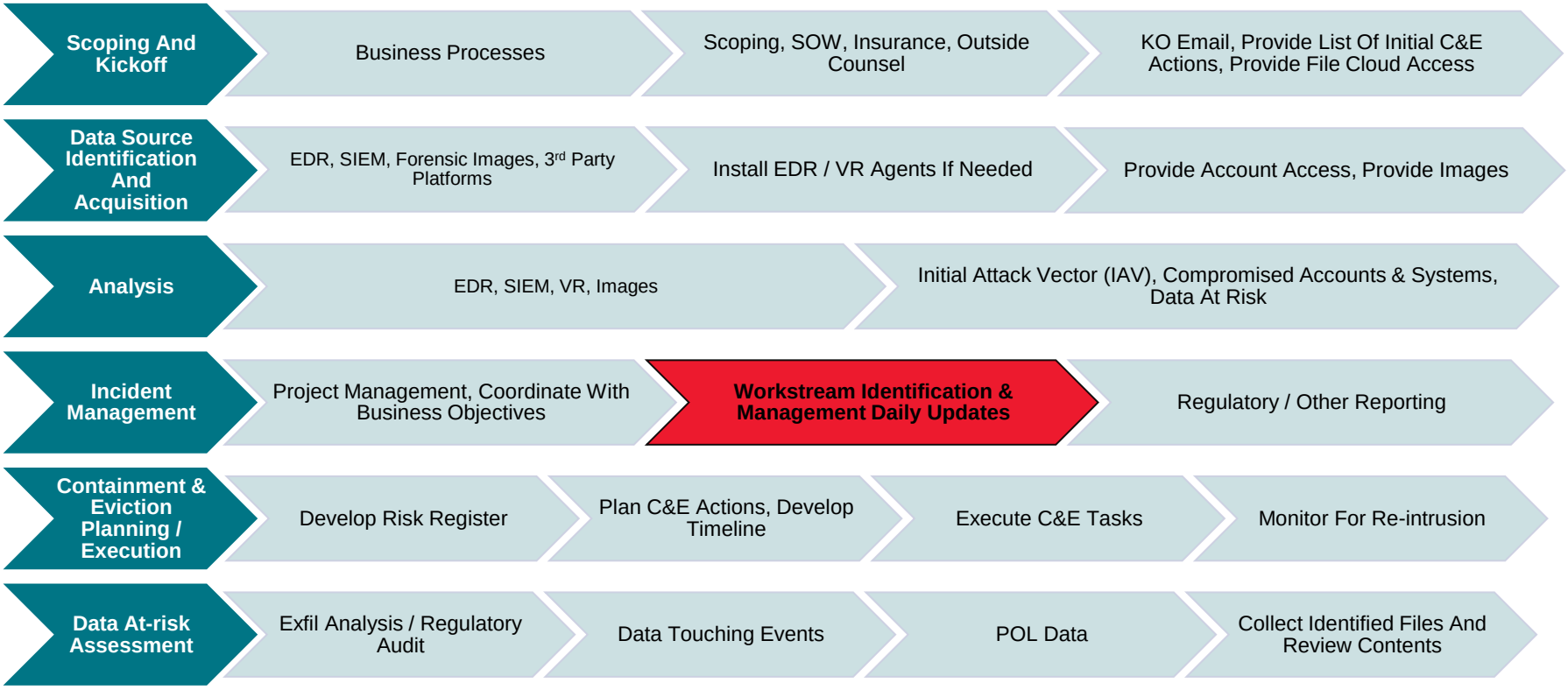
Execute your Response Plan.

Please note that the above flowchart is intended to serve as a high–level guide throughout the claims management process. Please refer to your policy(ies) for more affirmative guidelines regarding claims reporting and the applicability of coverage for said incident. By no means does the above flowchart represent or guarantee the applicability of coverage for each event; coverage determinations are subject to the policy terms and conditions.

Example Recovery Priority



Common Sequence of Events

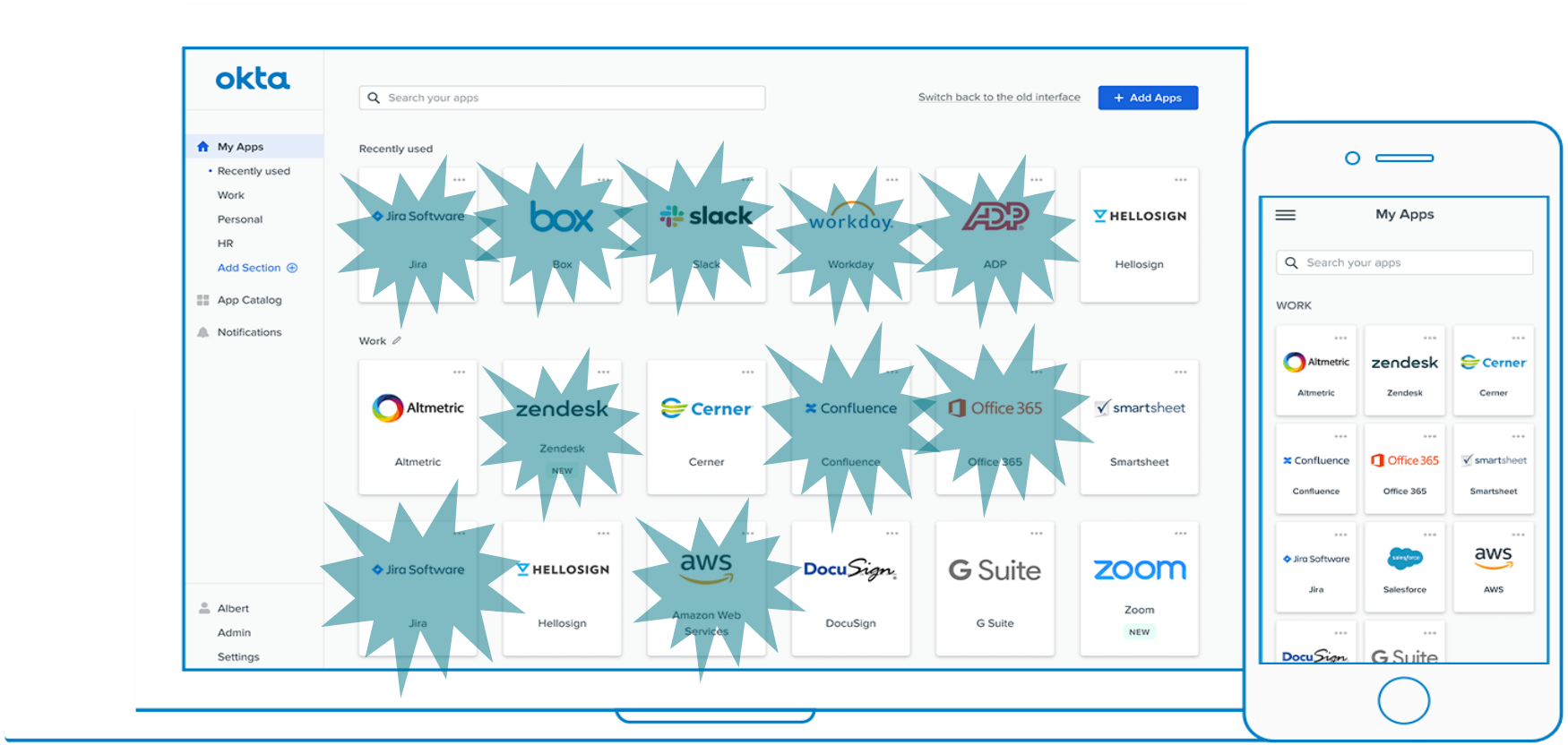


Common Large Incident Workstreams

Key:
All boxes: duration of the incident
Grey boxes: first 24 hours
Red box: external support
Green outline: SF/MSSP/MSP/client co-execution
Gold outline: SF/client co-execution

SSO Asynchronous Attacks

Bigger Blast Radius



Via: https://www.okta.com/okta-end-user-experience/

About Aon

Aon plc (NYSE: AON) exists to shape decisions for the better — to protect and enrich the lives of people around the world. Through actionable analytic insight, globally integrated Risk Capital and Human Capital expertise, and locally relevant solutions, our colleagues in over 120 countries with the clarity and confidence to make better risk and people decisions that help protect and grow their businesses.

Follow Aon on LinkedIn, X, Facebook and Instagram. Stay up-to-date by visiting Aon's newsroom and sign up for news alerts here.

www.aon.com

Contact Us

Will Miller
Vice President, Commercial Risk Solutions
william.miller@aon.com
+1 920 621 5904

Lee Carsten
Vice President, Cyber Solutions
lee.carsten@aon.com
+1 210 241 2491

Jacob Mast
Senior Broker, Cyber Solutions
jacob.mast@aon.com
+1 262 424 7634