Cyber Security – A Growing Risk: What you Should Know and Do

CALIFORNIA J · P · I · A

Providing innovative risk management solutions for our public agency partners

INTEGRITY | EXCELLENCE | INNOVATION | TEAMWORK

California Joint Powers Insurance Authority

Programs and Services

Risk-Sharing Pools

- Liability Protection
- Workers' Compensation

Insured Programs

123 Municipal member agencies throughout California

519 In-person and virtual risk management trainings, webcasts and webinars provided in FY 20-21

"The Authority does more than simply provide insurance; the organization offers educational opportunities to prevent exposure. The risk mitigation and risk management presentations and speakers that the Authority puts on are just phenomenal."

- Marshall Goodman, City of La Palma Councilmember and California JPIA Executive Committee member

64 Risk Management evaluations and Loss Control Action Plans provided to member agencies in FY 20-21

BakerHostetler

2021 DATA SECURITY INCIDENT RESPONSE REPORT

Digital Assets and Data Management – Disruption and Transformation

1,250+

Incidents in 2020

U.S. Breach Notification Law Interactive Map

bakerlaw.com/BreachNotificationLawMap

EU GDPR Data Breach Notification Resource Map

bakerlaw.com/EUGDPRResourceMap

For the latest, visit our blog

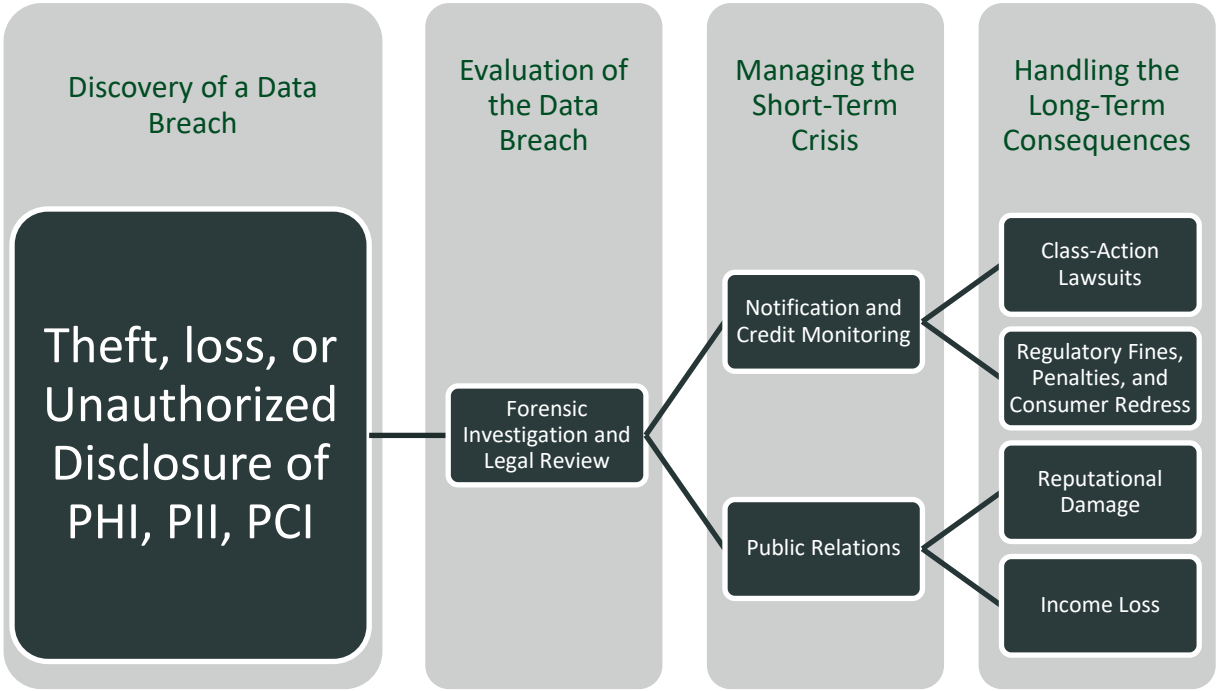
bakerdatacounsel.com

M. Scott Koller, CISSP, CIPP

Baker & Hostetler, LLP
Partner, Digital Risk Advisory and Cybersecurity Team
mskoller@bakerlaw.com

- Digital Risk Advisory and Cybersecurity Team
- Advised companies in over 1000 privacy and data security incidents involving malware, network intrusions, phishing, inadvertent disclosures, and ransomware.
- Defends clients on data protection issues and regulatory investigations (Office for Civil Rights (OCR), Financial Industry Regulatory Authority, Securities and Exchange Commission, the Federal Trade Commission (FTC), and various state Attorneys General.)

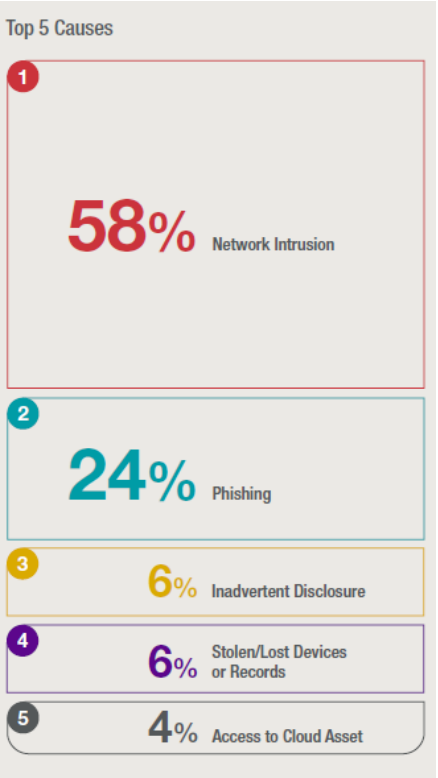
A Simplified View of a Data Breach

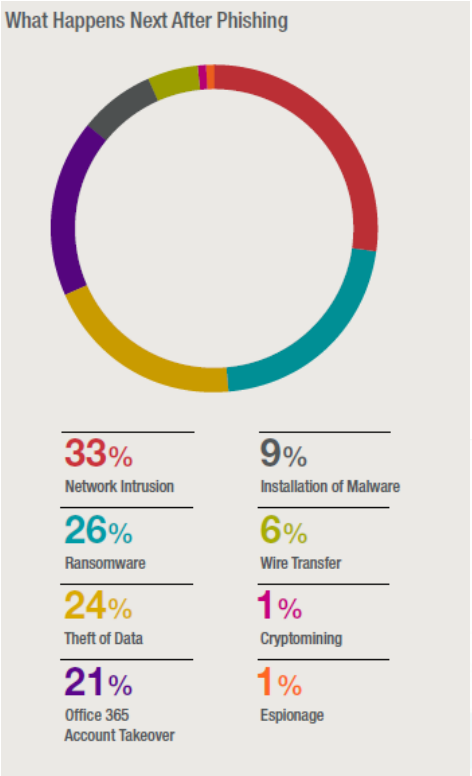


Incident Trends

Top Cause in 2019: Phishing – 38%

Top Cause in 2020: Network Intrusion – 58%





Source: BakerHostetler 2021 Data Security Incident Response Report

Third-Party Service Providers

Shopify Tablet SolarWinds Radial Accellion
Citrix Blackbaud Finastra Mimecast

of total incidents involved vendor-causes

of vendor-caused incidents had notice requirements

of notices had regulatory inquiries

Contract Terms

- Specify who does what
- Compliance with law
- Separate higher limit for breach of confidentiality/privacy/security
- Indemnification
- Exclude consequential damages disclaimer from indemnification for confidentiality/privacy/security

Legal & Regulatory Risks

20 lawsuits filed related to incidents disclosed in 2020 (compared with 14 in 2019)

- 3 lawsuits arose from incidents that started with unauthorized access to Office 365 inboxes
- 2 lawsuits involved payment card data
- 9 lawsuits involved SSNs
- 9 lawsuits involved medical/health information
- 7 lawsuits involved ransomware
- 3 lawsuits were vendor related

Notifications vs. Lawsuits Filed

Regulatory Inquiries Following Notification

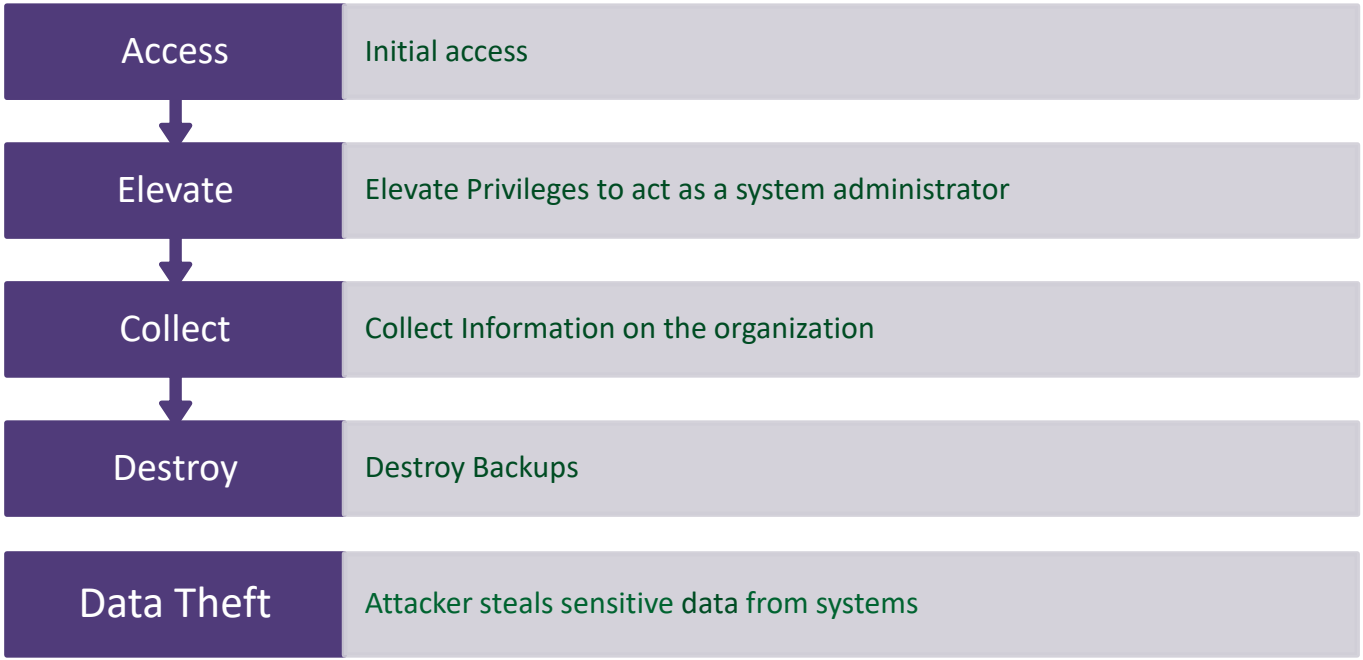
Number of Lawsuits by Individuals Notified

2	6	4
over 2 million	under 1,000	under 10,000

Ransomware Primer

How these attackers operate and evolve

Anatomy of an Attack – Phase 1



Anatomy of an Attack – Phase 2

Attacker deploys ransomware

Waits for contact

Negotiates payment

The Ransomware Epidemic

$65+ million — Largest ransom demand in 2020 (2019 was $18 million)

$15+ million — Largest ransom paid in 2020 (2019 was $5+ million)

$794,620 — Average ransom payment amount (2019 average was $303,539)

encryption key received after payment made

payment made by third party for the affected organization

75 threat actor groups/variants (2019 was 15)

67% of the time organization partially or fully restored from backup without paying ransom

25% involved theft of data resulting in notice to individuals

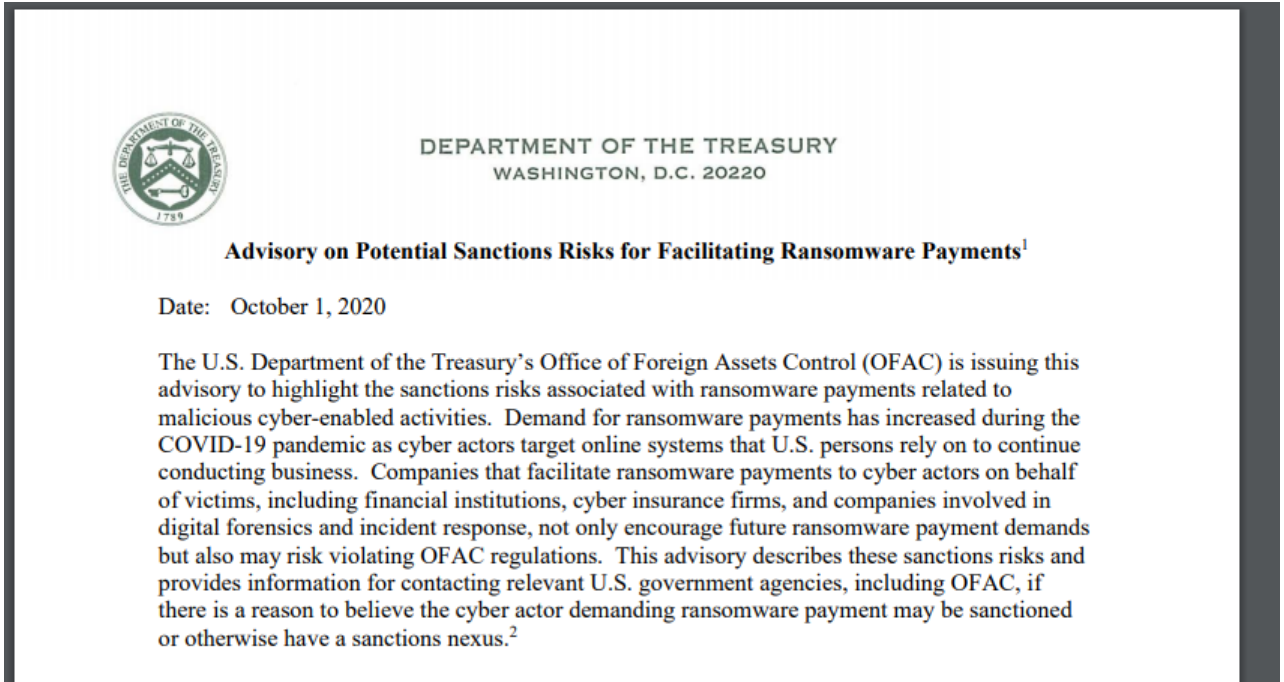
→ **20%** of matters involved a payment to a threat actor group even though the organization had fully restored from backup

70% of ransom notes contained claim of theft of data before encryption

90% found evidence of data exfiltration when there was claim of data theft in ransom note

Office of Foreign Assets Control

On October 1, 2020, the U.S. Department of Treasury's Office of Foreign Assets Control (OFAC) issued an advisory regarding ransom payments and the risk of sanctions associated with such payments.



DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments[1]

Date: October 1, 2020

The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) is issuing this advisory to highlight the sanctions risks associated with ransomware payments related to malicious cyber-enabled activities. Demand for ransomware payments has increased during the COVID-19 pandemic as cyber actors target online systems that U.S. persons rely on to continue conducting business. Companies that facilitate ransomware payments to cyber actors on behalf of victims, including financial institutions, cyber insurance firms, and companies involved in digital forensics and incident response, not only encourage future ransomware payment demands but also may risk violating OFAC regulations. This advisory describes these sanctions risks and provides information for contacting relevant U.S. government agencies, including OFAC, if there is a reason to believe the cyber actor demanding ransomware payment may be sanctioned or otherwise have a sanctions nexus.[2]

Preparing for Ransomware Infection

- Incident Response Plan
- Consider personnel awareness and training programs
  - Training for all levels of the organization
  - Include Identification of Types of Security Incidents
- Backups
  - Prepare backups resilient to current advanced ransomware attack methods (e.g., 3-2-1 backup strategy)
  - Test IRP and BCP/DR through tabletop or other simulation exercises.
- Identify service providers to be used in a ransomware event.
- Evaluate Cyber Insurance Coverage
- Consider options for access to critical response information (e.g., IRT and response vendor contact information) and communication methods (e.g., dedicated Google mail accounts for response) if Entity's systems are not operational.

Ransomware Lessons Learned

- ***Practice downtime procedures***. We have found entities spend so much time trying to prevent attacks, and not nearly enough on training its workforce on downtime procedures. This is especially critical since everyone is so dependent on IT systems and applications.

- ***Give less access to IT accounts***. Five of our recent ransomware incidents involving ransomware all started after an IT account was compromised, allowing the threat actor to have unfettered access to the network, and move laterally undetected.

- ***Prepare for early preservation issues***. Have blank drives available to retain copies of encrypted systems—this will help ensure company preserves relevant evidence for potential litigation while not slowing down the restoration process.

- ***Better understand what data is stored where***. Entities are usually shocked to learn the amount of unencrypted PII that is stored outside the primary systems, such as in shared folders, as well as how dated the information is. Consider where large amounts of PII may be stored (such as backup files used during database migration projects) and clean up as much as you can.

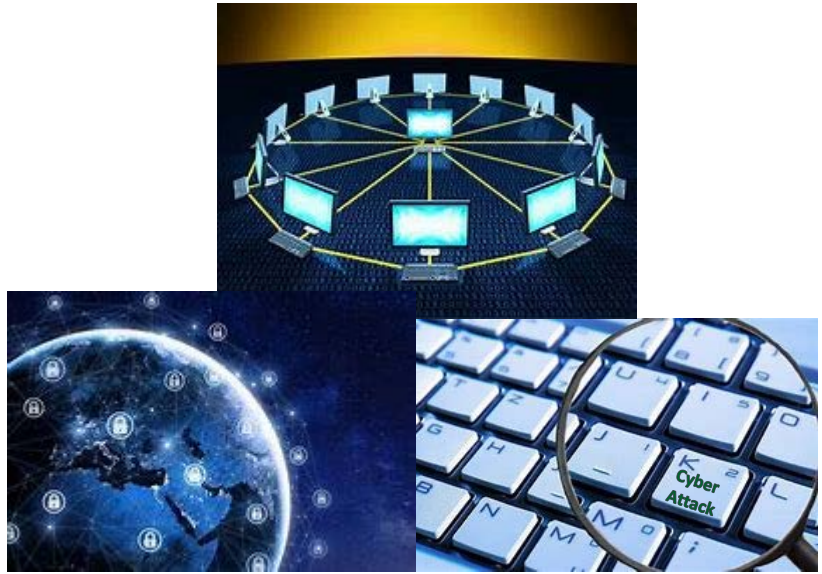
"Reasonable Security"

- **Align to a security framework** – such as NIST CSF. Many of the other items listed below are identified as components of one of these security frameworks.
- **Do risk assessments** – identify critical assets, threats, and vulnerabilities. Use assessment to prioritize cybersecurity roadmap/maturity plans. .
- **Know your environment** – if you do not know what devices you have you cannot defend them (e.g., avoids scenarios where you deploy an endpoint tool but it does not get provisioned on every device and then those are the devices that are first compromised).
- **Know what data you have and where it resides** – if you do not know what data you have and where it resides, you are not likely to implement appropriate measures (or even know when there is unauthorized access to it). A data inventory is also part of complying with the new obligations under CCPA and is part of a GDPR compliance program.
- **Multifactor authentication** – enable MFA where you can, especially for Office 365 (and disable backwards compatible apps that do not support MFA/modern authentication) and any other cloud-based application where logging in provides access to sensitive data (e.g., payroll services like ADP – apply MFA at least for HR admin users).
- **Manage cloud assets** – address access rights for cloud resources (make sure that they are not set to public access where anyone that knows the url can see what is in the bucket).
- **Endpoint security** – deploy an endpoint tool that goes beyond signature-based AV detection. Examples are FireEye's HX agent, CrowdStrike's Falcon, Carbon Black, Tanium, or Cylance.
- **Encryption** – encrypt portable devices (e.g., laptops, USB drives), sensitive data at rest (e.g., payment card numbers, SSNs), and passwords for online accounts (do not just hash).
- **Patch management** – use a tool for patching and evaluate patching cycle.
- **Logging and log monitoring** – use a SIEM and have a SOC (internal or outsourced) to provide 24/7 monitoring of logs and alerts. Talk to security firm that does forensic investigations about log retention and details to log (this identifies evidence sources that enable them to be more precise in their investigation).
- **Phishing** – use an email filter to reduce the amount of phishing emails that get through (e.g., Proofpoint, Mimecast, FireEye's ETP)
- **Security awareness training** – design and implement a program that teaches employees about phishing and social engineering. Test phishing exercises are pretty common.
- **Vendor management** – build a program that appropriately vets vendors (e.g., marketing cannot just sign up someone – other disciplines should be involved including legal and security), negotiate appropriate contractual protections and rights (you can build a data security addendum you add to vendor agreements to cover your core terms/needs), and oversee vendors after selection.
- **Business continuity** – ransomware has become very problematic. Have good backups that are readily available and not stored on each host they are a backup of.

CYBER INSURANCE

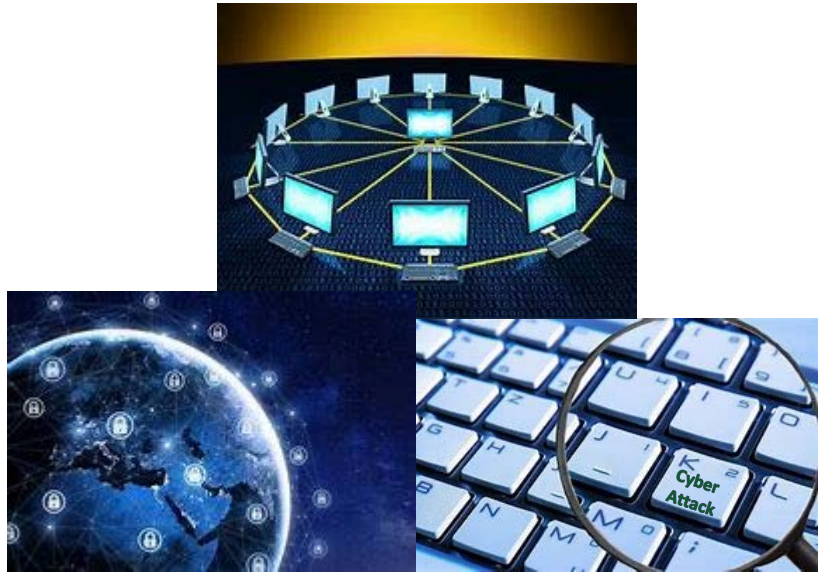
Example I

- Hackers access system through a single open port
- Hackers snooped for a long time
- Eventually launched malware that locked down ~200 devices
- Ransom demand of $50,000 per device (~$10M demand)
- There was a firewall between city hall and the police department so no police systems were compromised
- City hall closed for two weeks because they didn’t have access to computers



Example II

- An employee clicked a link they should not have clicked, and it launched ransomware, which shut down the police department IT function
- $50,000 ransom demand per server (3 servers) + $20,000 per end point device (more than 100 devices)
- >$2 million ransom demand
- No access to servers or any way to intake or process information the police were collecting (body cameras, reports, etc.)
- Potentially compromised investigation materials that were housed on the servers
- Several weeks to restore all devices to full functionality



Insurance Overview

First-Party Coverages

Cyber Incident Response Fund

Covers expenses to retain a computer forensics firm to determine the scope of a breach, to comply with privacy regulations, to notify and provide credit monitoring services to affected individuals, and to obtain legal, public relations or crisis management services to restore the company's reputation. In essence, coverage is provided for expenses used toward a computer forensics firm. In addition, this is the coverage for notifications and credit monitoring needs after a breach.

Business Interruption Loss and Extra Expenses

Covers business income loss due to network interruption. In essence, coverage is provided to the member for the lost revenue that the member would have earned if no such loss had occurred, and/or reasonable expenses the member incurs to allow the business to continue operation during the period of restoration.

Digital Data Recovery

Covers the recreation of data lost due to a network interruption. In essence, this coverage pays on behalf of the member the cost to restore or recreate valuable information that is damaged or corrupted from a cyber event such as viruses, malicious code and Trojan horses.

Network Extortion

Covers extortion monies and associated expenses arising out of a criminal threat to release sensitive information or bring down a network. In essence, it covers the settlement of an extortion threat against the member's network and the cost of hiring a specialty security firm to investigate and negotiate with blackmailers.

Insurance Overview

Third-Party Coverages

Cyber, Privacy and Network Security Liability

Covers loss arising out of the organization's failure to protect sensitive personal or corporate information in any format. Provides coverage for regulatory proceedings brought by a government agency alleging the violation of any state, federal, or foreign identity theft or privacy protection legislation. In essence, this is the liability if the member is involved in breaching someone's privacy rights, either protected by regulations or protected by the member's own privacy statement. Coverage is provided if the member is fined by regulators because of the member's wrongful act. In addition, this is for liability that may result from a security breach of the member's system or of information the member holds.

Electronic, Social and Printed Media Liability

Covers infringement of copyright or trademark, invasion of privacy, libel, slander, plagiarism or negligence arising out of the content on the organization's internet website. In essence, this is for liability that may result from the member's online activities, such as plagiarism, libel and slander.

Coverage Limits and Deductible

For both first- and third-party coverages, each member has a $1,000,000 per incident and for all claims during the coverage year. This limit is subject to an aggregate limit of $5,000,000 for all claims by all members during the coverage year. The member deductible is $250,000 per incident.

Resources

Crisis Hotline

- Assists entities when they believe an incident or breach has occurred
- May be through an insurance carrier call center or directly with a service provider such as a law firm
- Agencies are then connected with an incident coach who helps navigate the process

Incident Response Plans

- Created in advance of a cyber incident to guide an agency through a cyber incident
- Templates are available though third-party vendors

Guidance and Data

- Even agencies with IT expertise may need outside guidance and resources
- Authority members have immediate online access to a library of resources including best practices, policy templates, white papers, training, and industry data

Source: SANS Institute

eRiskHub®

Direct Cyber Insurance Snapshot and Future Expectations

Pricing and Terms

Rates

Average premium increase in (US/UK)
1Q20: **5.6% / 11%**
2Q20: **7.2% / 18%**
3Q20: **10.6% / 13%**
4Q20: **17.2% / 17%**
1Q21: **35.1% / 29%**
2Q21: **59.5% / 51%**
3Q21: **97.1% / TBD**

Limits/ Coverage

Many carriers are reducing capacity exposed. Some carriers are scaling back ransomware-related coverages (or not offering coverage at all) for clients that don't have adequate controls.

Future Expectations

Anticipate increases to accelerate, likely **75% or greater** in Q3 and beyond. Risk specific terms dependent on risk profile & controls.

Claims

Frequency

Ransomware tactics are more accessible for bad actors. Short tail nature of losses is changing insurer profitability on an ongoing basis.

Severity

Ransom payments in the millions. Business interruption and data recovery loss. SolarWinds & MS Exchange attacks have increased carrier uncertainty around systemic nature of cyber risk.

Future Expectations

Ransomware attacks will continue to increase in sophistication; systemic risks concerns; privacy risk concerns.

Underwriting

Information Needs

Full application & responses to ransomware Q's. Underwriters focusing on supply chain exposures and CBI controls.

Carrier Flexibility

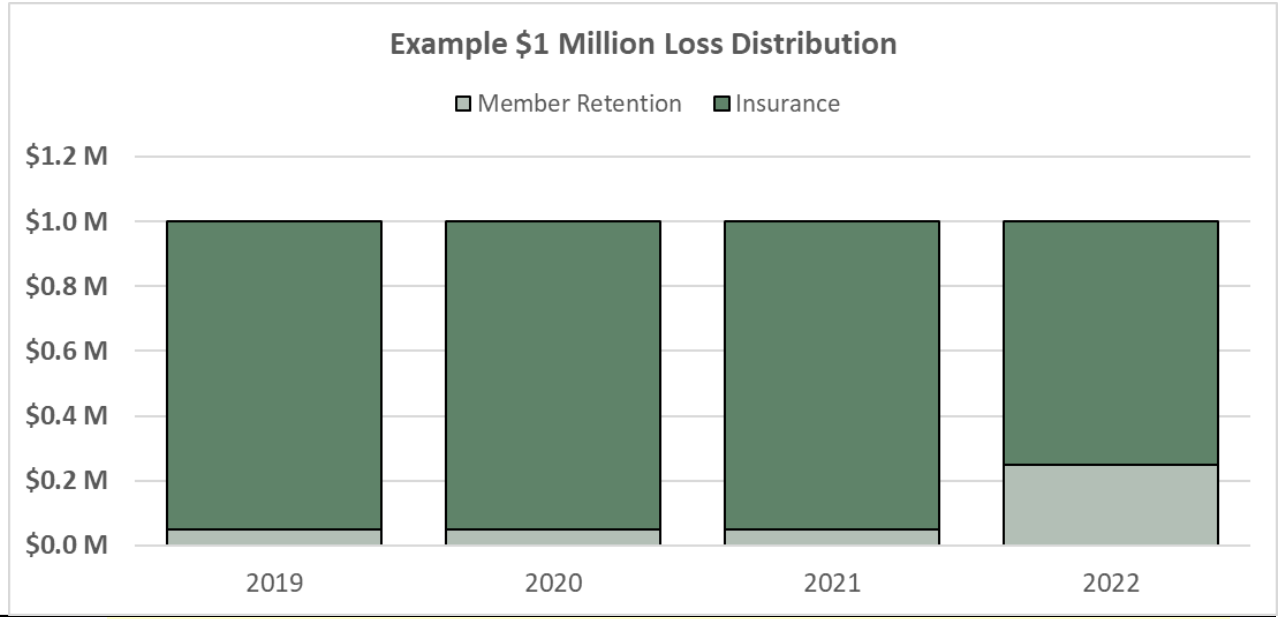
Ransomware responses required prior to quoting. Third party scans may lead to remediation requests. Adequate controls are required to obtain a quote.

Future Expectations

As technical acumen increases, underwriters will demand additional information to assess risk and may require certain cyber controls to quote.

Source: Guy Carpenter "Q3 Global Cyber Update"

Cyber Insurance Renewal Considerations



Member Retention	$ 50,000	$ 50,000	$ 50,000	$ 250,000
Insurance	$ 950,000	$ 950,000	$ 950,000	$ 750,000
Total Cost	$ 1,000,000	$ 1,000,000	$ 1,000,000	$ 1,000,000
Coverage Limit	$ 1,000,000	$ 1,000,000	$ 1,000,000	$ 1,000,000
Aggregate Limit	$ 10,000,000	$ 10,000,000	$ 10,000,000	$ 5,000,000
Premium Change ~	0%	0%	+100%	+50%

RANSOMWARE – To Pay or Not to Pay

PROS

- May be the only way to restore operations*
- Gets people back to work and productive
- May be a less expensive alternative from a financial standpoint*
- May speed up restoring operations
- Limits service interruptions…the longer it takes to restore operations, the more public outcry

CONS

- Potentially encourages future attacks*
- Does not guarantee restoration of data or return of stolen data without public disclosure*
- May violate the U.S. sanctions regime*
- Employees and/or the public may object to the moral aspect of paying a ransom

*Source: A Guide for Boards and Companies Facing Ransomware Demands (harvard.edu)

KEY TAKEAWAYS

1. Preparing and preventing a cyber breach may save $ millions in costs
    - Practice down time procedures
    - Train all employees on cyber risks
    - Prepare for early preservation issues
    - Understand what data is stored and where
2. Evaluate your cyber insurance coverage, including limits, sub-limits, and coverage components in relation to the risk that your agency can absorb
3. A cyber breach has financial, operational, and political implications