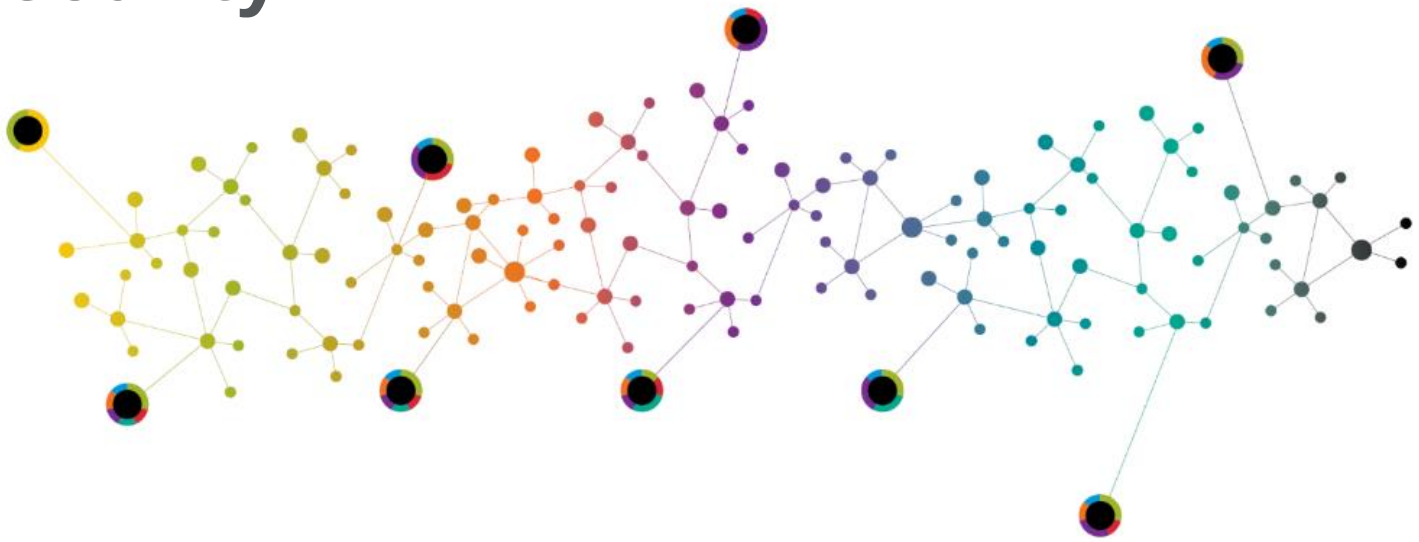
BakerHostetler

CALIFORNIA J · P · I · A

Introduction to Cyber Security



M. Scott Koller, CISSP, CIPP | Partner

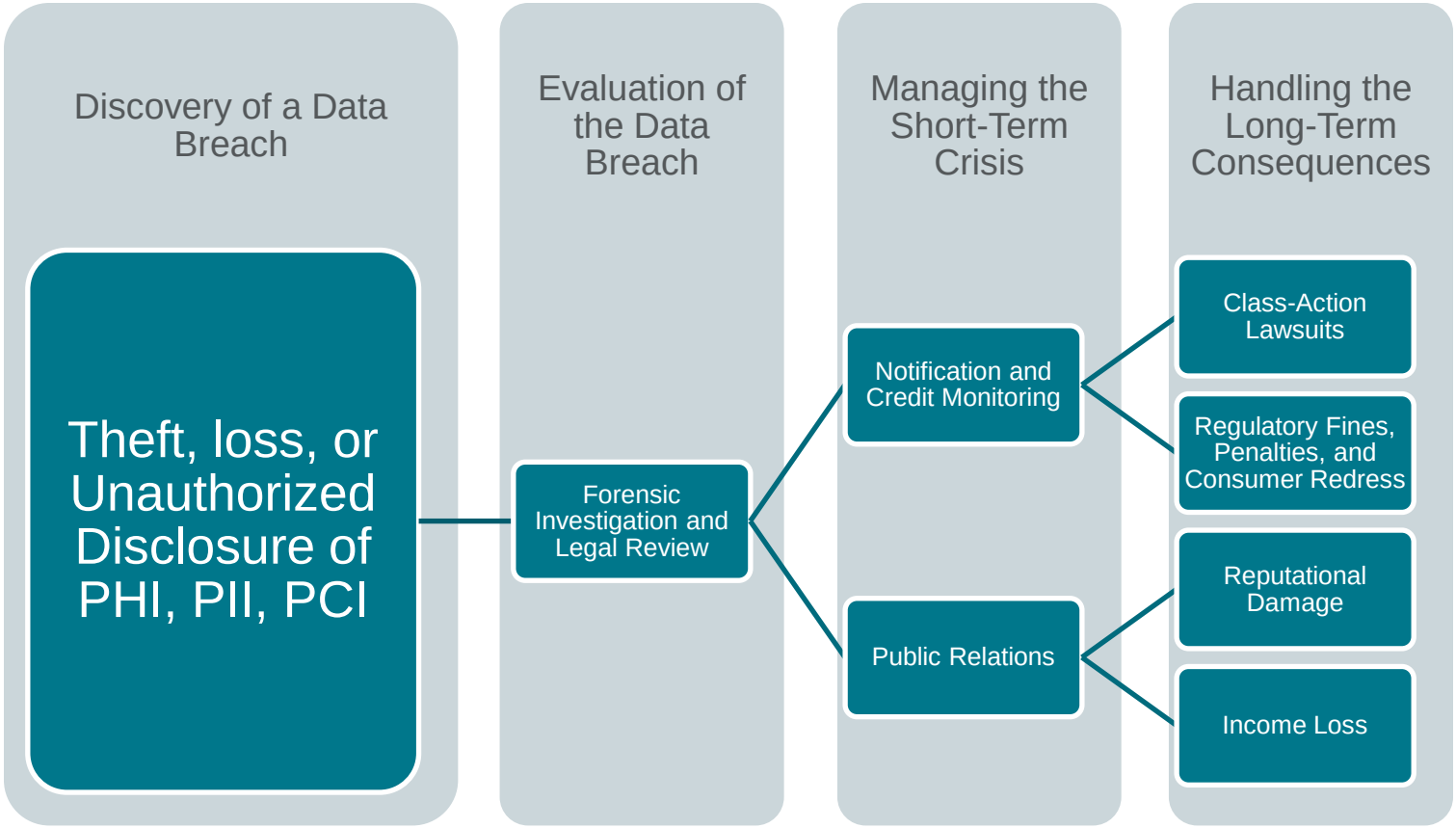
ADVANCE TRAINING ON INCIDENT RESPONSE AND CYBER SECURITY

Introduction

M. Scott Koller, CISSP, CIPP
Partner, Digital Risk Advisory and Cybersecurity Team
Baker & Hostetler, LLP

- Advised companies in more than 1,000 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

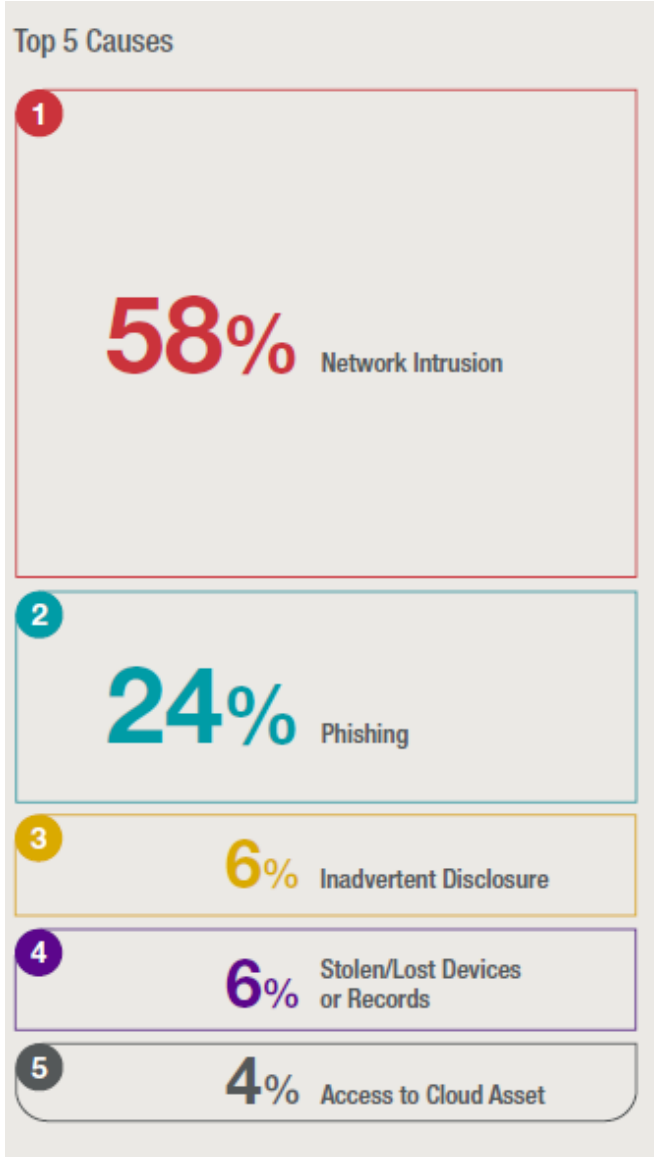


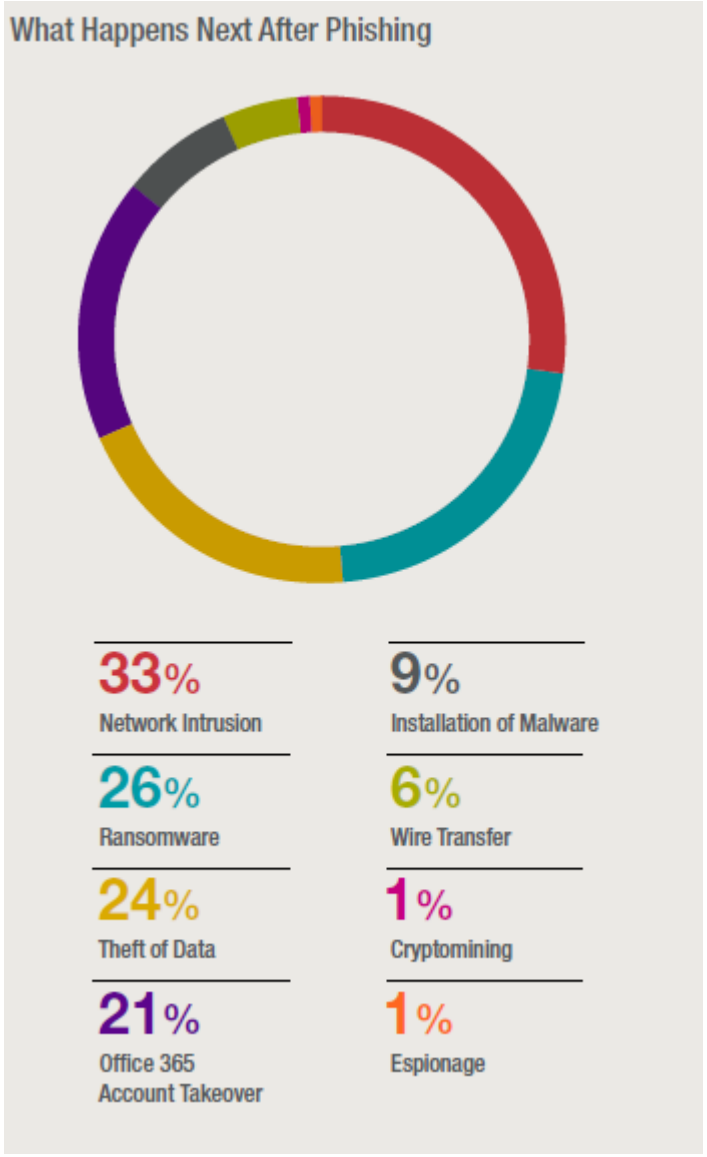
Incident Trends

BakerHostetler

Top Cause in 2019:
Phishing – 38%

Top Cause in 2020:
Network Intrusion – 58%





Source: BakerHostetler 2021 Data Security Incident Response Report

What Kinds of Information are at Risk?

BakerHostetler

Information of Residents

- Social Security numbers
- Credit cards, debit cards, and other payment information
- Financial information such as account balances, loan history, and credit reports
- Protected healthcare information (PHI), including medical records, test results, appointment history, and insurance information
- Non-PI, like email addresses, phone lists, and home addresses that may not be independently sensitive, but may be more sensitive with one or more of the above

Employee Information

- Employers have at least some of the above information on all of their employees

Business Partners

- Any of the above with respect to Business Associates and/or Vendors

What's at Stake?

Time

- Time spent on incident response is time away from day-to-day operations

Money

- Responding to incidents can mean legal fees, forensic investigation costs, notification and call center costs, and paying for credit monitoring
- Lawsuits
- Regulatory investigation, fines, corrective action, and penalties

Reputation

- Residents and community trust

The Privacy “Patchwork” of Laws

- Federal & state laws may impact handling PII/PHI
  - Laws covering SSNs / disposal of PII
  - Employment-related laws (e.g., FMLA, ADA, GINA)
  - Other federal and state regulations (e.g., FTC Act, FCRA)
- Gramm-Leach-Bliley Act
  - Covers entities “significantly engaged” in providing financial products or services
- FERPA
- HIPAA / State Medical Information Breach Reporting Laws
- State Breach Notification Laws

Cyber Risk Landscape: Goals & Risks

BakerHostetler

GOALS

- Comply with all applicable laws and regulations
- Be thorough and descriptive without causing unnecessary concern.
- Provide reassurance without overpromising
- Strive for openness and transparency without creating unnecessary risk

RISKS

- Complaints
- Negligence, Invasion of Privacy Lawsuits
- Class Action Lawsuits
- Regulatory Action
- Damage to Reputation and Trust

What Will You Encounter?

- Law enforcement
- Class actions
- Issuing bank lawsuits
- Card network fines/assessments
- System remediation and revalidation
- Reporting of impact
- Regaining public trust

What Will You Encounter?

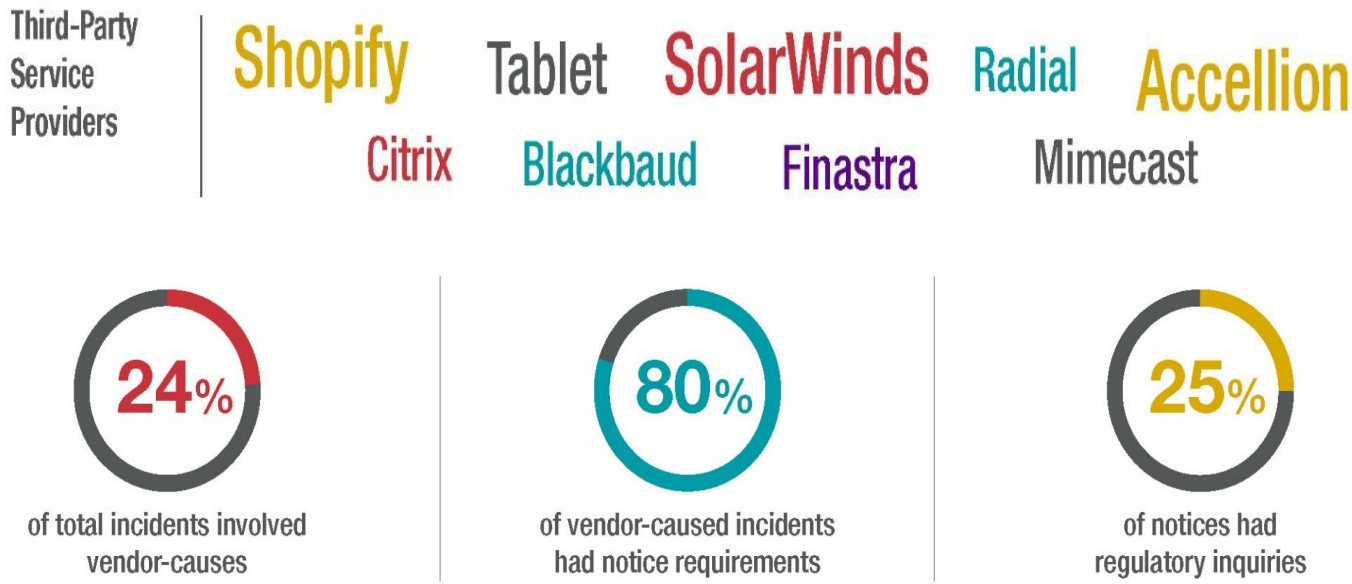
- Individual Complaints
- Forensic investigation
- Media inquiries
- Regulatory inquiries
- Operational challenges
- Decisions on public statements
- State breach notification law analysis

Organizational Challenges

- Contracting
- Conflicts
- Large Size and Complexity
- Unclear Chain of Command
- Too Many Cooks in the Kitchen
- Slow Moving
- Limited Resources
- Maintaining large volume of citizen and employee data
- Preserving online availability and integrity of state services

Contract Terms

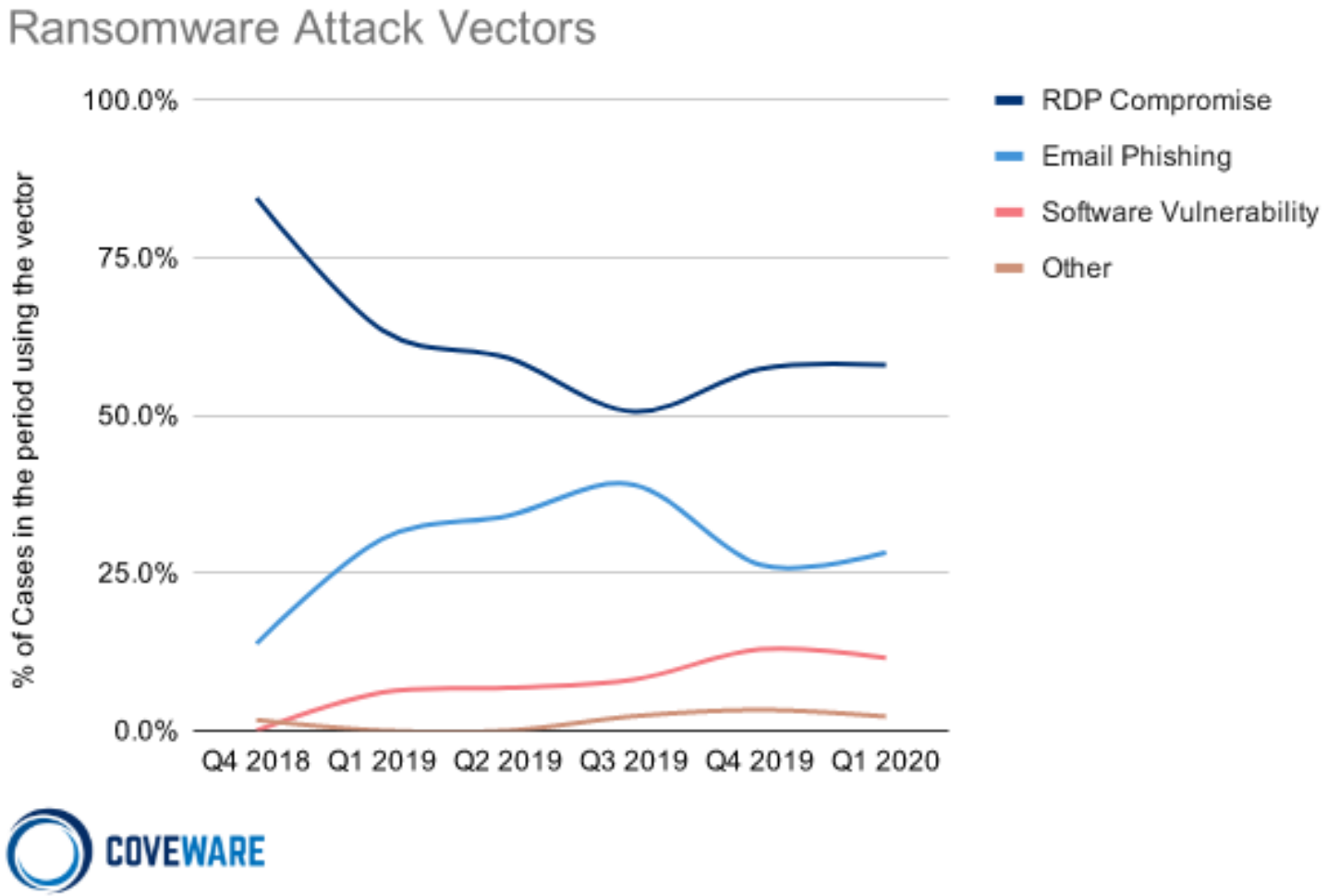
- Specify who does what
- Compliance with law
- Separate higher limit for breach of confidentiality/privacy/security
- Indemnification
- Exclude consequential damages disclaimer from indemnification for confidentiality/privacy/security



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)

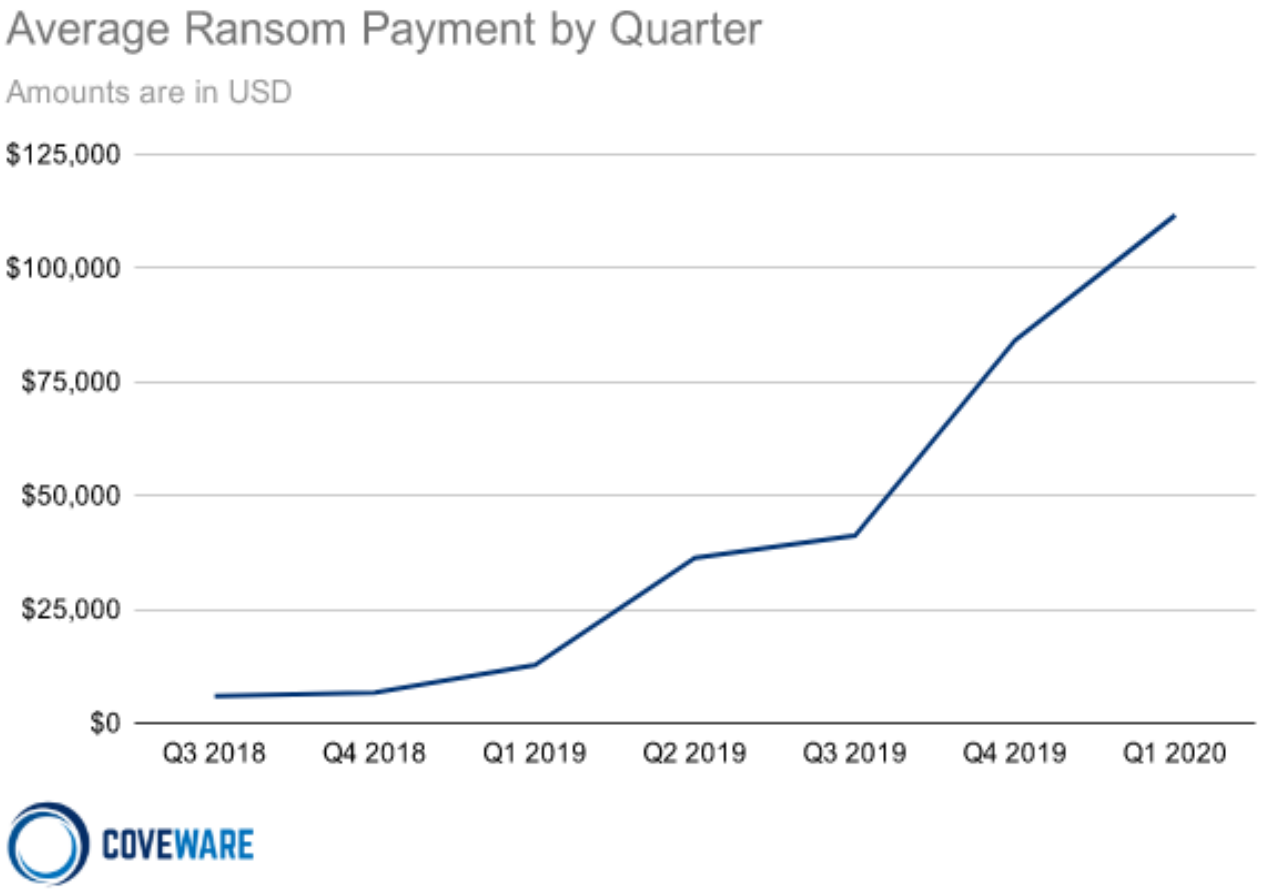
What Are The Most Common Ransomware Attack Vendors?



Highest Initial Ransom Demands in 2020:

- $68 million
- $50 million
- $30 million

All involved encryption and data exfiltration.



Ransomware – Double Extortion

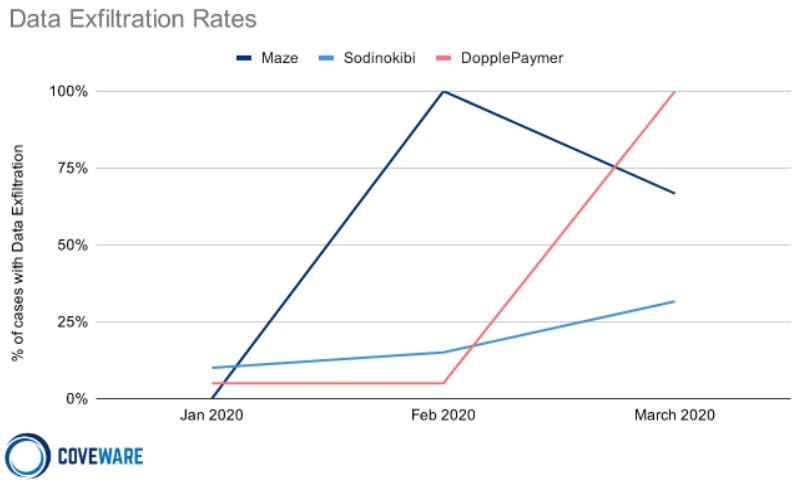
70% of ransom notes contained claim of theft of data before encryption

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

MAZE RANSOMWARE EXFILTRATES DATA - DID OTHER RANSOMWARE VARIANTS?

Cases with data exfiltration

8.7%



Data exfiltration, where data is downloaded from victim computers and is threatened to be released publicly, became a prevalent tactic during ransomware attacks in Q1 2020. This was a big change from the previous quarter where it was virtually non-existent.

Ransomware – To Pay or Not to Pay

BakerHostetler

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

- Does not guarantee restoration of data or return of stolen data without public disclosure
- Employees and/or the public may object to the moral aspect of paying a ransom
- May violate the U.S. sanctions regime
- Generally disfavored since payment fuels the ransomware industry and encourages future attacks.

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: There should be 3 copies of data; On 2 different media; With 1 copy being off site.)
  - 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.

Cyber Insurance – Typical Benefits

First Party Coverage

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.

Cyber Insurance – Typical Benefits

Third Party Coverage

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.

Cyber Insurance – State of the Market

- Increased Premiums
- Insurance Carriers Leaving the Market
- Underwriting becoming more strict, increased requirements
- Some entities face trouble renewing policies

Risk Management Strategies

- 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).

Risk Management Strategies – Continued

- 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).
- 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 and oversee them 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.


Q&A
You have
Questions
We have
Answers

BakerHostetler

bakerlaw.com

Atlanta | Chicago | Cincinnati | Cleveland | Columbus | Costa Mesa

Dallas | Denver | Houston | Los Angeles | New York | Orlando

Philadelphia | San Francisco | Seattle | Washington, D.C. | Wilmington

M. Scott Koller
mskoller@bakerlaw.com
310-928-7524