MARSH & McLENNAN AGENCY

Recent Cyber Trends and Breach Response Recommendations

September 16, 2020

Jim J. Giszczak, Member, McDonald Hopkins

Alex Ricardo, Breach Response Business Development; Cyber & Executive Risk, Beazley

Mario Paez, Director, Cyber & Technology E&O, Marsh & McLennan Agency

Disclaimer

This presentation and content is not meant to be considered professional legal advice.

The presenter is not a licensed attorney and all information obtained from this presentation should be considered for informational purposes only.

You should consult with a licensed privacy counsel for any decisions surrounding your corporate privacy initiatives, incident response plan or data breach response methodology.

Agenda

- Current Cyber Risk Statistics
- Threat Landscape
- Emerging Trends
- Incident Response Best Practices
- Q&A

Current Cyber Threats & Stats

- FBI and U.S. Secret Service have recently issued alerts for the growing threats on Business Email Compromise and Malicious Email Attacks.
- Ransomware attacks jumped 148 percent in March from the previous month (VMWare)
- Q1 2020 Coronavirus-Related Phishing Email Attacks Are Up 600% (KnowBe4)
- Ransomware demands have continually increased over the past year due to increased sophistication of attacks (such as infiltrating critical systems and backups) with multi-million dollar demands becoming more common.
- Increase of 60% from Q1 2020 to Q2 with average demand being over $178,000 (Coveware)
- The majority of SMBs (83%) said they do feel prepared for a ransomware attack. Forty-six percent of SMBs have been targeted by ransomware, 73% have paid the ransom (Infrascale)

Current Cyber Threats & Stats

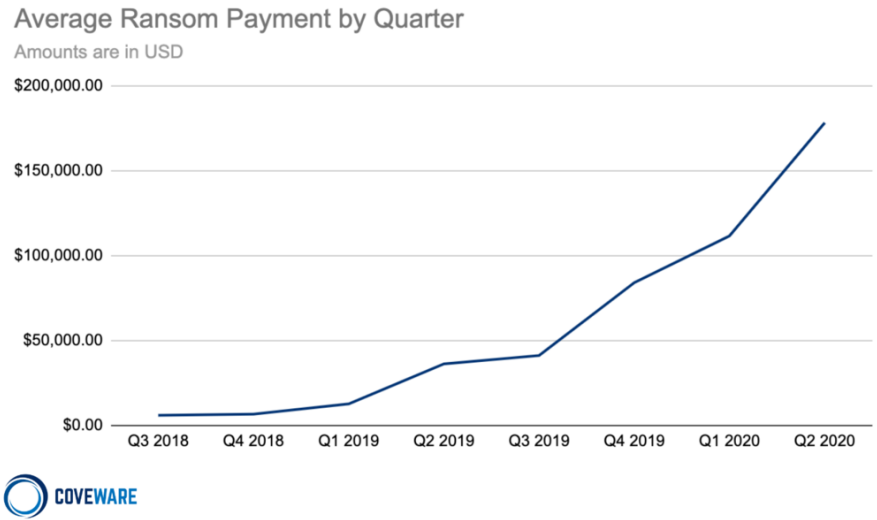
- Cloud-based cyber-attacks by external actors on businesses went up by 630% between January to April 2020.
- During May, a total of 108 data breaches exposed 841,529 sensitive records and 68,298,815 non-sensitive records.
- Around 16 billion records have been exposed so far this year. According to researchers, 8.4 billion were exposed in the first quarter of 2020 alone, a 273% increase from the first half of 2019 which saw only 4.1 billion exposed.
- Average estimated probability of a successful breach for organizations in the US is 45% (ESI Thoughtlab June Report)

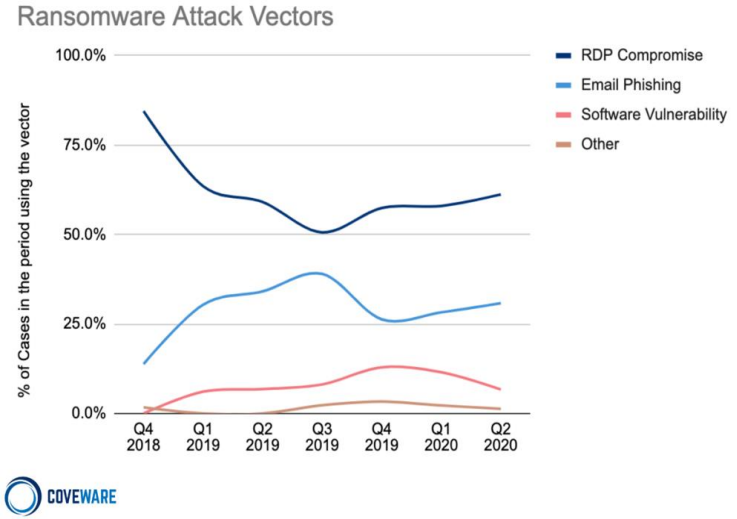
Current Threats & Stats (cont.)

- March 28, 2020—As of March 28, the number of cyber attacks related to coronavirus grew from a few hundred daily to over 5,000 in one day alone (thenextweb.com)
- April 7, 2020—71% of security professionals report increased security threats or attacks since the COVID-19 outbreak (darkreading.com)
- April 21, 2020—In one month, over 2,000 COVID-related scams were taken down in the UK (BBC)
- May 2, 2020—As of May 2, the FBI reported a[n] 800% increase in reported cybercrimes (entrepreneur.com)
- May 6, 2020—In the next month, 49% of businesses expect to experience a data breach or cyber security incident due to a remote workforce (Baracuda.com)
- May 14, 2020—A 238% increase in cyberattacks against banks is linked to COVID-19 (ZDNET.com)
- August 11, 2020—Now, more than ever, ransomware attacks are more devastating (MonsterCloud.com)
- August, 2020 - 4 out of 10 Covid-themed emails are spam (BiteDefender)
- August, 2020 - 715% year-on-year increase in detected – and blocked – ransomware attacks (BiteDefender)

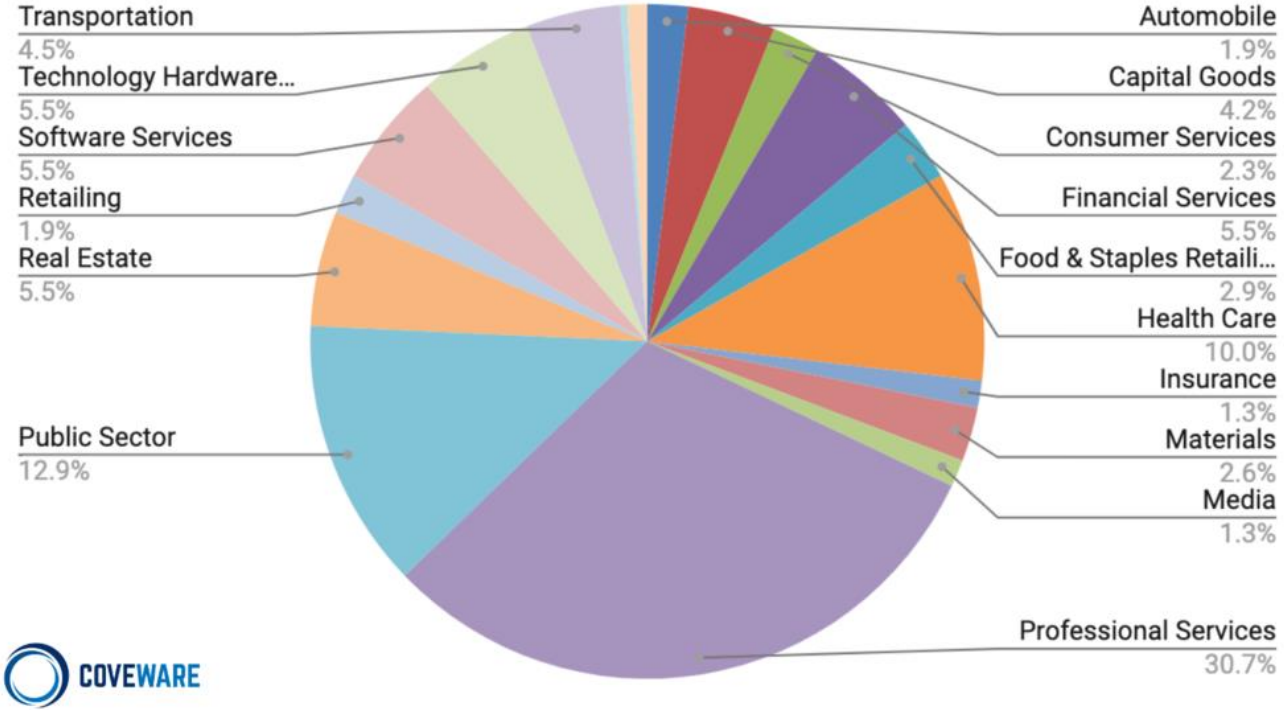
2nd Quarter 2020 Coveware Report

- Average ransom payment increased 60% from Q1 ‘20 to $178,254



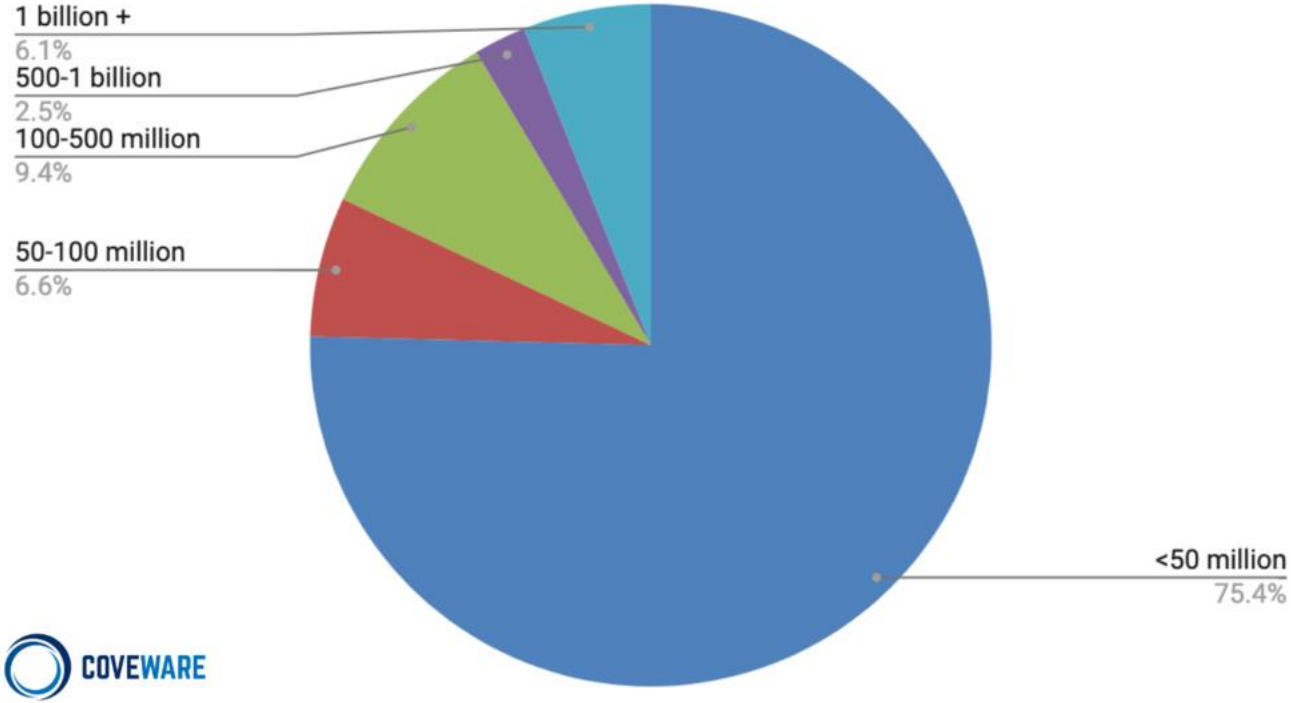


Common Industries Targeted by Ransomware in Q2 2020



COVEWARE

Distribution by Company Size (Revenue)



COVEWARE

2020 Ponemon-IBM Cost of a Data Breach Study (August 2020)

- This study is aimed at small to medium-size businesses, limiting the total record count of each eligible breach to 99,730 and separating “mega breaches” out to a different study.
- Key findings include that the most expensive place in the world to experience a data breach is the United States, where the **average total cost is $8.64 million** — more than double the global average.
- The Ponemon study found an expected increase of $137,000 in total data breach costs directly as a result of greater work-from-home implementation during the COVID-19 pandemic months that were covered (March and April 2020).
- Organizations have tended to anticipate this, with 70% of respondents saying that they expected the cost of data breaches to increase while COVID-19 remote work policies were in place.

2020 Ponemon-IBM Cost of a Data Breach Study (August 2020)

- Organizations that had fully deployed security automation measures (technologies based on machine learning and AI that come to recognize abnormal patterns of behavior and execute security actions accordingly) saw an **average savings of $3.58 million** in data breach costs over organizations that had no form of security automation put in place.
- Incident response teams and testing are also another major expense mitigator. **Organizations with these teams and procedures in place saved $2 million** as compared to those that did not. Successful teams include those that deployed tools to help protect and monitor endpoints and remote employees.

Ransomware

A form of malware that encrypts files and demands a ransom in exchange for the key needed to decrypt files

- Common types: Ryuk, Sodokinibi, Dharma

Frequent, and still increasing in frequency

- Per McAfee report, ransomware incidents grew by 118% in Q1 of 2019
- Approx. 151.9 million ransomware events in Q1-Q3 of 2019

Trends: Victims

Significant increase in attacks in certain industries:

- Healthcare
- Managed Service Providers (MSPs)
- Manufacturing
- Municipalities
- Professional Service Providers
- Education (School districts, universities)
- Financial Institutions

Increase in attacks on small and mid-size businesses

Trends: Variants

New variants exfiltrate data prior to encryption and threaten to expose the data if ransom is not paid

- Ex. Maze, Sodokinibi, Dopplepaymer

Increase in the number of these types of events

Due to increase in exfiltration events, increase in “breaches” requiring notification

Trends: Ransom Demand, Cost

Average ransom demand increased

- In 2019, average ransom demand was approx. $13,000 (vs. approx. $7,000 in Q1 of 2018)
- Highest known ransom demand in 2019 was $8.5 million

Average cost to recover and rebuild systems impacted by a ransomware incident increased

- In 2019, average cost to a business was $133,000

High-Level Threat Landscape

Unintended Disclosure – Paper / Physical Records

- Shredding, Dumpster Diving, File Cabinets, Natural Disasters, Physical Social Engineering

Unintended Disclosure – Electronic Assets

- Computers, “Non-Computers”, Leased Equipment

Business Email Compromise

- 17% - ‘19 incidents (vs 24% - ‘18 incidents), “Red Letter Alerts”

Unencrypted Portable Devices

- 4% - ‘19 incidents (vs 24% - ‘17 incidents), Encrypt = 49 AGs “Go Away”

Broken Business Practices

- 17% - ’19 incidents

Rogue Employees

- 7% - ‘19 incidents, Disgruntled vs Enticed

Work-From-Home Considerations in the COVID-era

- Shredders
- Home Wi-Fi
- VPNs
- Portable Device Usage (ie Thumb Drives)
- Printers
- BYOD (Bring Your Own Device)
    - Use of MDM (Mobile Device Management)
- Web Conference Services (Zoom / Webex)
- Rogue Employee – Enticed Activity

Forecasting Trends

COVID-19 related phishing attacks, giving rise to malware and ransomware incidents

Issues created by remote work

- Companies may be short staffed and/or have poor communication (Phoenix)
- Poor IT support and infrastructure
  - i.e. open ports, RDP
- Increase in risky behavior on work devices
  - i.e. employees using public wifi, personal business on work device, malicious downloads

Emerging Threats

- RDP / RDG Attack Vector
    - VPN, MFA (VPN and RDP), Patch Frequently, Network Segmentation
- Ransomware
    - SME vs MM, Paying Ransom is on the Table, % that are Breaches is Increasing
- Microsoft Office 365
    - Expensive Forensics Investigation Costs
- CryptoJacking
    - Business Interruption, System Failure, Business Income Loss Liability

Cyber Risk: Potential Costs & Liability

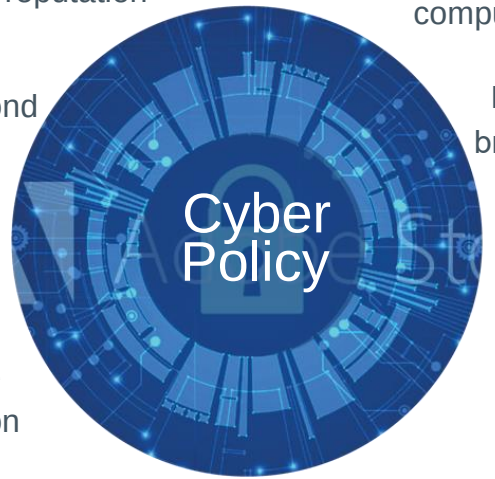
How does a stand-alone cyber policy protect your company?

First Party

Data Breach Response Data Restoration
Network Business Interruption Security and Privacy Liability Cyber Extortion

Third Party

Privacy Liability
Network Security Liability
Privacy Regulatory Defense
Costs Contingent Business Partner
Media Liability
Contingent Injury/Property Damage



Loss or damage to reputation

Extra expense to recover/respond to a computer attack

Loss of revenue due to a computer attack

Loss of damage to data/information

Legal liability to others for computer security breaches

Legal liability to others for privacy breaches of confidential information

Costs to investigate and notify others of a breach

Regulatory actions, fines and scrutiny

Electronic content

Cyber-terrorism

Cyber-extortion

Cyberattack Response Guide: When Reasonable Efforts Aren’t Enough

Why we should be careful with the word "breach"

Using “breach” to describe a data-privacy related incident assumes the incident meets the definition of a security breach which triggers various notification requirements

An “incident” does not always rise to the level of “breach” (i.e., encryption safe harbor)

“Incident” is better received by the public than “breach”

Best Practices

Recommend that insured immediately contact broker and/or insurance company

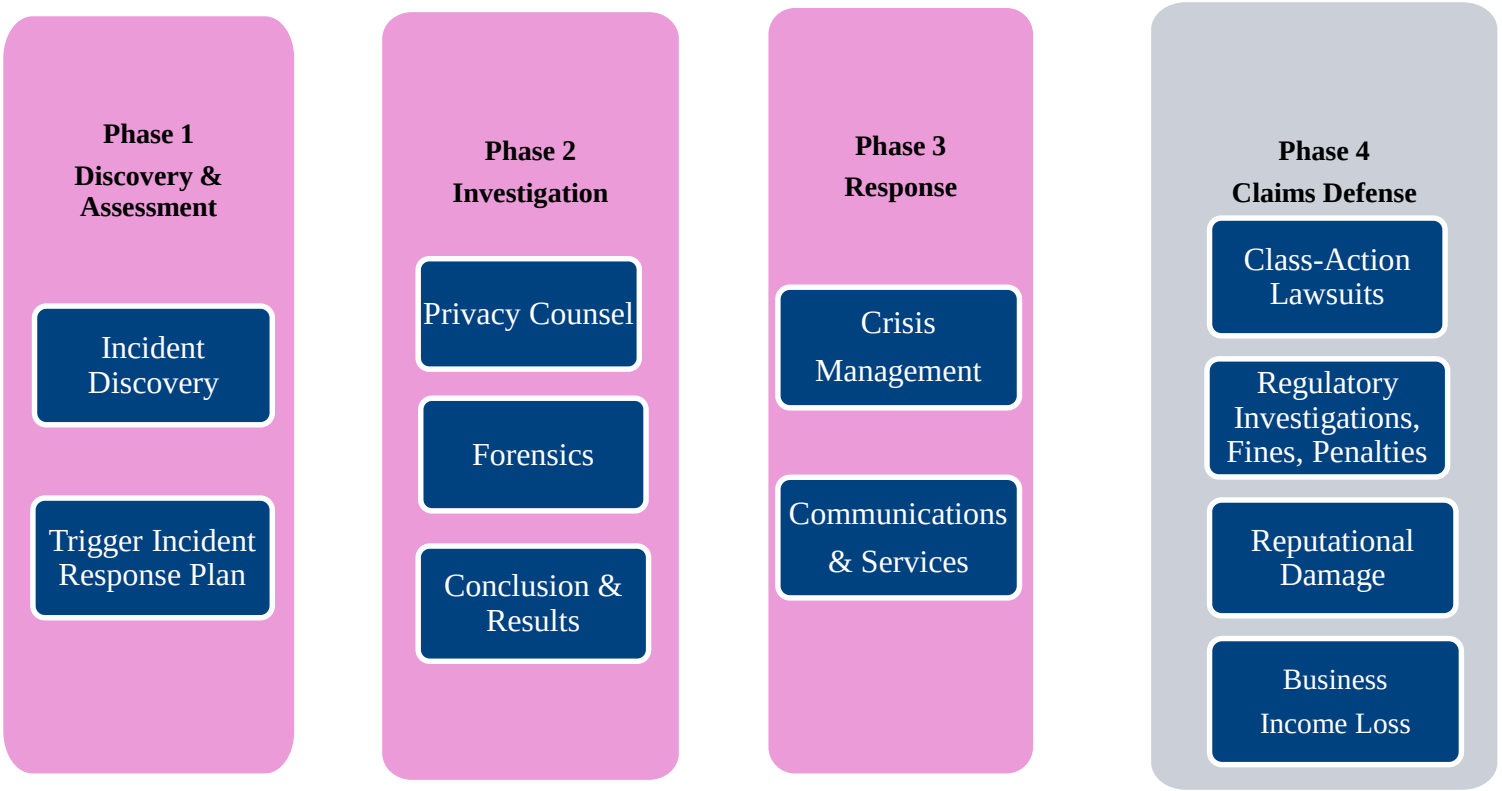
Insured SHOULD NOT destroy forensic evidence or reach out directly to threat actor, but should wait for forensics engagement

Appropriate experts should be brought in immediately:

- Broker/Insurance
- Legal
- Forensics

Coordination with Your Cyber Carrier

The Privacy/Cyber Response Methodology



Risk Can Still Be Managed

"Cannot Un-Ring the Bell"

Importance of Legal

"Quarterback" forensic investigation

Analyze event and contractual/regulatory requirements for any notification obligations

As attacks become more sophisticated, increase in need for legal to be involved from the beginning

- i.e. increase in exfiltrating ransomware variants results in earlier legal obligations

Importance of Forensics

Knowledge of data recovery/remediation beyond most IT vendors/in house IT

- Most forensic firms assist on thousands of ransomware incidents per year

Providers have familiarity with ransomware variants and threat actors that allows them to negotiate better deals for insured

- Some providers collect data that reveals how long negotiations are necessary for a good price, the best price that can be expected, etc.

Response to a Security Incident: Immediate Response and Containment

Don’t panic, don’t overcommunicate

Alert your cybersecurity insurance carrier

Terminate any authorized access into your system

Work with IT/external forensics to ensure no malware remains on your system, and no access continues in your network, and threat has been contained

Response to a Security Incident: Immediate Response and Containment

In a ransomware incident:

- Assess the viability of back-ups
- Work with IT and/or external forensics to restore from back-ups or determine how to move forward
- Do not communicate with attackers from an identifying or business email address

Response to a Security Incident: After Containment

Work with IT and/or forensics to determine whether information was accessed or acquired from your system or network

- PII, “confidential information,” “material client information”

Assess security of confidential client information

Update security, protections for sensitive information

Fulfilling Your Notification Duty

If sensitive information was accessed or acquired, work with a breach coach to determine required notifications

- Could include notification to clients, other individuals, or regulators
- Be aware of potential timing requirements

QUESTIONS?

Jim Giszczak: 248-220-1354 jgiszczak@mcdonaldhopkins.com

Alex Ricardo: 917-344-3311 alex.ricardo@Beazley.com

Mario Paez: 763-746-8246 mario.paez@marshmma.com

McDonald Hopkins 24/7 Hotline: 855-643-2821

Beazley Breach Response 24/7 Hotline: 866-567-8570

MarshMMA.com