ALSTON & BIRD

Life After Lock Up: After Your Data is Taken and Your Systems Encrypted

Privacy + Security Forum

May 10, 2024

Speaker Introductions

Kate Hanniford
Partner,
Alston & Bird

Sara Sendek
Managing Director,
Cybersecurity & Data Privacy,
FTI Consulting

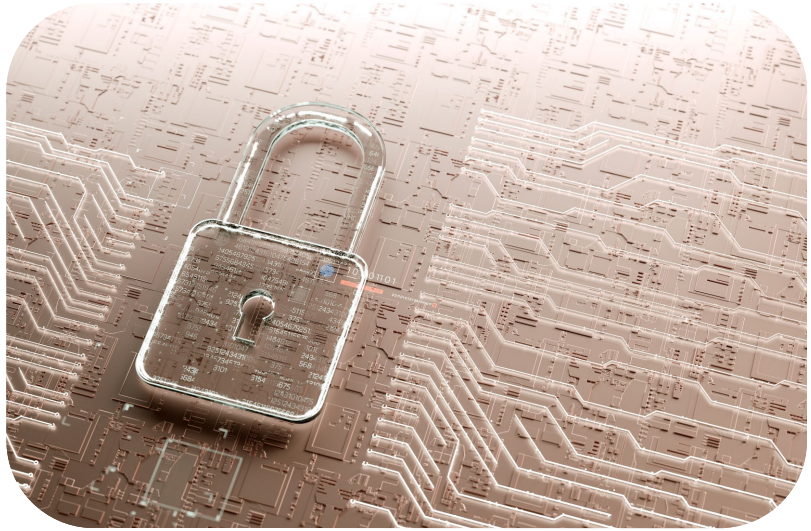
Jon Knight
Sr. Corporate Counsel,
Deltek

Sam Kaplan
Assistant General Counsel, Public Policy & Government Affairs
Palo Alto Networks

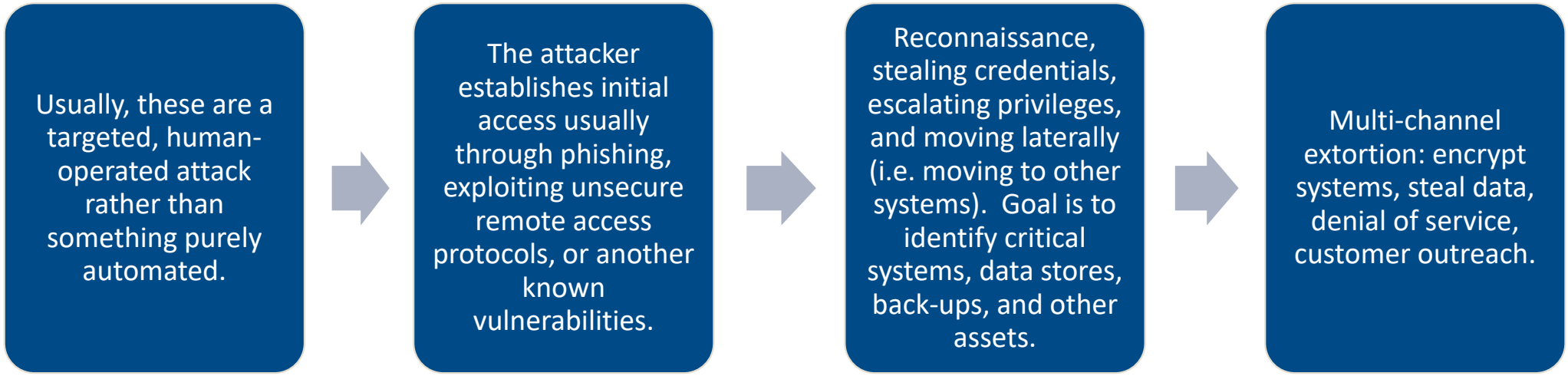
Ransomware Background and Trends

Ransomware Landscape – Trends

- In 2023:
  - 37% increase in ransomware attacks YoY (driven largely by RaaS.
  - Q4 – Average ransom payment = $568,705.
  - Ransom payments in 2023 total over $ 1 billion.
  - Average Ransom in 2023 – $1.54 million.
  - 24% of organizations took between 1-6 months to recover.
  - 97% of organizations recovered their encrypted data.
  - Average total cost of a ransomware attack *excluding the ransom* is $5.13 million.



A Typical Ransomware Attack – Multi-Faceted Extortion



- Remember: Initial compromise can occur weeks or even months prior to ransomware deployment.

Double Extortion: Exfiltration and Encryption

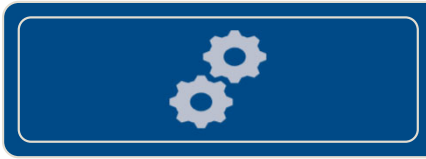
The criminals first steal or exfiltrate your data.

Then they use a scripted deployment of ransomware to encrypt the systems.

This gives them multiple points of leverage to pressure for a ransom payment.

Pay us in order to decrypt your systems.

Pay us or we will publicly leak your data on the dark web or sell it to the highest bidder.



Attackers now try multiple avenues for extortion. They demand payment for decryption and threaten DDOS attacks, posting of data taken, or contacting customers if payment is not made.

Why do you need to be prepared?

Within 48 hours of an incident, you may need to consider or initiate the following steps:

- Engage outside counsel, forensics firm, ransomware intermediary, data recovery and public relations firm.
- Assess the need for 8-K reporting and other SEC considerations.
- Report to the Board of Directors.
- Institute any insider trading restrictions.
- Make contact with the criminal actor and initiate a negotiation strategy.
- Establish a working containment strategy.
- Identify timeline for restoration and any available backups.
- Assess any data exfiltration or unauthorized access to personal information.
- Begin to formulate a communications strategy – media, holding statement, legal reporting, and contractual reporting obligations.

SEC Cyber Disclosure Rules

New Cybersecurity Disclosures in Form 8-K

SEC's Newest Reporting Requirements	Considerations
▪ Materiality determination made "without unreasonable delay." ▪ Must report a material cybersecurity incident on Form 8-K within four business days after determining that such incident is material. ▪ Need to describe incident's nature, scope, timing and impact (actual or likely) – less granular information than originally proposed and amend as appropriate. ▪ Law enforcement waiver possible (but not likely). ▪ Effective December 18, 2023	▪ Multiple existing 8-K approaches – expected changes? ▪ Create a materiality framework in conjunction with incident response plan (identify escalation points). ▪ Document materiality considerations and decision process. ▪ Solidify relationship between information security team and legal. ▪ Note: The SEC is active in gathering information from companies' incidents to verify whether companies are making 8-Ks.

New Cybersecurity Disclosures in Form 10-K

New Disclosures

- Describe processes for assessing, identifying and managing material risks from cybersecurity threats.
- Describe the Board and Audit and Risk Committee's oversight of cybersecurity risks and risk management.
- Describe management's role in assessing and managing material risks from cybersecurity threats.
- Responsibility for risk assessment and managing risks (and relevant expertise).
- How information flows within the company regarding cybersecurity threats and incidents.
- The SEC did NOT adopt a requirement for the Board to disclose if there was a cybersecurity expert on the Board.
- Effective December 15, 2023.

Considerations

- Internal and external disclosure counsel need to gain knowledge and understanding of the information security program.
- Identify existing disclosures (including in 10-K/20-F, Proxy Statement, Website, Sustainability Report); analyze gaps with new disclosure requirements.
- Establish verification process to ensure that disclosure matches with actual processes/procedures.
- Wide range in approach – will be a few years of growing pains under the new rules.

Delay Requests

DOJ

Clarified that its primary inquiry in deciding whether to approve a delay request will be "***whether the public disclosure of a cybersecurity incident threatens public safety or national security, not whether the incident itself poses a substantial risk to public safety and national security***." DOJ provides the following examples:

- Incidents resulting from exploitation of a technique for which there is not yet well-known mitigation and when disclosure could lead to more incidents.
- Incidents primarily impacting a system containing sensitive U.S. government information and public disclosure could lead to further cyber exploitation.
- When a company is conducting remediation efforts for any critical infrastructure or critical system and disclosure of the incident could undermine those efforts.
- When a government agency has made the company aware of circumstances that require delaying disclosure, such as law enforcement operations to disrupt criminal activity or the potential compromise of confidential sources.

Delay Requests (cont'd)

FBI

- On December 6, 2023, FBI issued guidance for companies seeking delays in reporting material cybersecurity incidents, explaining it is tasked with processing delay requests on behalf of DOJ.
- Companies are encouraged to engage local FBI field office as soon as possible.
- Delay requests that fail to disclose the date, time, and time zone of the company's materiality determination – or not filed with the FBI "immediately" upon making that materiality determination – will be automatically denied.

- Analysis: minimal benefit to seeking delay request, and minimal chance it will be granted.

Final Thoughts and Questions

Thank you!