Cyber – Post-Attack and Claim Services

Dawn Simmons – Moderator
Vice President, Cyber Underwriting

Melissa K. Ventrone, CIPP/US
Partner – Thompson Coburn LLP

Adam J. DeMonaco, CISSP
Senior Director, Chief Security Officer – Kivu Consulting, Inc.

AEGIS 2017 PHC

Cyber – Post-Attack and Claim Services

Melissa K. Ventrone, CIPP/US
Partner – Thompson Coburn LLP

AEGIS 2017 PHC

You've Been Breached!

Now what?


AEGIS *2017* PHC

Agenda

- Assumptions for this presentation
- Lifecycle of a data breach
- Identifying a security incident
- Containment and remediation
- Notification and response

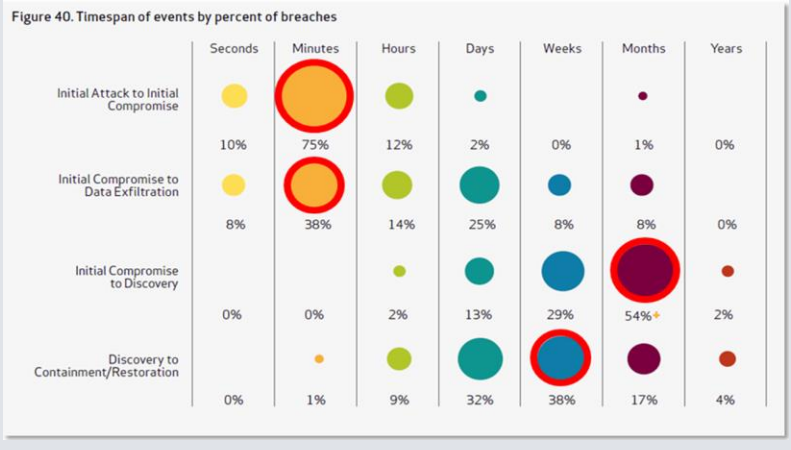
AEGIS *2017* PHC

Assumptions

- Understand the definition of personally identifiable information
- Background on laws applicable to collection, retention, transmission, access, use, and destruction of data
- Basic understanding of what constitutes a "data breach"

Life Cycle of a Data Breach

Identification: time to impact vs. time to discover



AEGIS 2017 PHC

Lifecycle of a Data Breach

- Identification and triggering the incident response team
- Containment
- Remediation
- Notification

AEGIS *2017* PHC

What Happens First?

- Identification of a security incident
  - What is a “security incident”?
  - How do you recognize a “security incident”?
  - The intersection of technology, processes, and people
  - Training and education

AEGIS *2017* PHC

And What's Next?

- Triggering the incident response team
  - Who is on the team – and have you told them?
  - How do you trigger the incident response process?
  - Members identified for this specific incident?
  - What are their roles and responsibilities?

AEGIS *2017* PHC

And Then What?

It depends, but the order can vary

- Containment
  - Have you stopped the bleeding?
- Remediation
  - Implementing corrective measures to prevent a similar event from occurring in the future
- Notification
  - Who do I tell, what do I say, and when do I say it?

AEGIS *2017* PHC

Let's Practice!
Subject

- On Monday, a customer calls customer service and reports that he was conducting online research for a class and happened to find a website with his email address, username and password on a public website called www.$ecrtysks.com. According to the customer, the website contained a number of other email addresses. You learned about this today (Wednesday), when the CIO informed you of the event at your 3:30 p.m. staff meeting.
  - What do you do?

Things to Consider
Remember the following

- What do I know, what don't I know, who needs to be involved in making decisions, and who needs to be informed?
- Establish a communication protocol
- Set reasonable expectations internally and externally

AEGIS 2017 PHC

Forensic Findings

- Through outside counsel, you engaged a computer security forensic company that are onsite and beginning their investigation. According to this company, they see malicious activity on a server containing the database for your online payment platform. This database contains names, addresses, email addresses, usernames, and passwords of all customers with online accounts.
  - What does this mean? What concerns are raised by this fact?

A Momentary Pause...

- Plan for the worst, hope for the best
  - Make sure the right people are involved in the investigation
  - Remember, "facts" change as the investigation proceeds
  - Trust your instincts, you know your systems best
  - Ask questions of the investigators

What If…

- The CEO contacts you and informs you he just received an email from an unknown person claiming to have hacked into your systems and taken the personal information for all customers. He threatens to sell the information unless your company pays him what he calls a "fee". If the company pays the "fee", he will provide a contract stating that he obtained the data as part of his job as an independent contractor hired to identify vulnerabilities in your company's network.
  - Now what?

Or What If…

- An employee in HR contacts IT complaining that he can't access any files. Further research determines that the files are infected with ransomware, and contain a screen that demands three bitcoins in exchange for the decryption key
  - When IT checked the backups, it turns out they were not available because of a recent system update that inadvertently changed the configuration on the backups. The last backup was completed three months ago
  - The files contain, at a minimum, data such as employee evaluations, background checks, benefit information, and other similar data
  - What do you do?

A Momentary Pause…
Let's talk about law enforcement

- To notify law enforcement
- Or not...?
- What if it isn't an extortion attempt?

Back to the "Breach"

- 3:00 p.m.: Your public relations department receives a call from a local reporter who wants to obtain information about a breach impacting the entire customer database. She intends to "go live" with the story tomorrow on the 8:00 a.m. news segment. Could someone give her a call to discuss?

Logistics of a Security Incident

- People underestimate the amount of time it takes to respond to an event
  - Forensics
  - Communication plan
  - Notification
  - Remediation

AEGIS *2017* PHC

What About Notification

- Statutory notification requirements
- Contractual notification requirements
- Other considerations
  - Business reasons
  - Public and community relations

AEGIS *2017* PHC

30 / 60 / 90 Day Considerations

- Don't forget to plan for the future
- What impact with the breach have on plans 30/60/90 days in the future?
  - On contractual relationships / obligations?
  - What about the community?
  - And the customer and employee population?
  - Are there other considerations?

AEGIS *2017* PHC

In Summary

- No two security incidents are alike
- Training and education are key
- Practice, practice, and practice

AEGIS *2017* PHC

Questions?

AEGIS *2017* PHC

Contact Information

Melissa K. Ventrone

Chair, Data Privacy and Security

Thompson Coburn, LLC

T 312.580.2219

C 312.485.0540

mventrone@thompsoncoburn.com

AEGIS *2017* PHC

Cyber – Post-Attack and Claim Services

Adam J. DeMonaco, CISSP
Senior Director, Chief Security Officer
Kivu Consulting, Inc.

AEGIS Insurance Services, Inc.

AEGIS *2017* PHC

You've Identified a Compromise, Now What?

- Don't panic
- Refer to your incident response plan
- Identify the key stake-holders
- Collect any and all evidence for preservation
- Build a timeline of events as you know it

AEGIS *2017* PHC

You've Identified a Compromise, Now What?

- Reference your cyber insurance policy
- Contact someone
  - Insurer
  - Breach coach
  - Incident response firm

Incident Response Process

- Initial triage call with client
- Coordinate collection
  - Evidence preservation
    - Network and host-based logs
    - Malware sample
    - Forensic images

Incident Response Process

- Centralize analysis
  - Indicator of compromise
  - Vector of compromise
  - Scope of compromise
  - Data exfiltration

AEGIS *2017* PHC

Incident Response Process

- Formulate response
  - Remediation
  - Mitigation
  - Notification
  - Litigation

AEGIS *2017* PHC

Ransomware / Extortion Process

Much like incident response process

- Collection of evidence
  - Sample of encrypted files
  - Copy of ransom note with contact information
- Key differences
  - Contact with attacker
  - Sample of decryption tool
  - Negotiation of BitCoin ransom
  - Malware analysis on decryption tool
  - Document decryption process

AEGIS *2017* PHC

Computer Forensic Process

- Collect evidence of compromise for preservation and future analysis
- Confirm compromise

AEGIS *2017* PHC

Computer Forensic Process

- Analysis helps identify extent of compromise
  - Was malware resident?
  - Did malware spread?
  - Did malware collect data?
    - PII
    - PHI
    - PCI
  - Did malware exfiltrate data?

AEGIS *2017* PHC

Data Breach Analysis Goals

- Quantify and qualify the scope of affected individuals
  - Leveraging best practices in identifying
    - Protected Health Information (PHI)
    - Personally Identifiable Information (PII)
    - Payment Card Industry (PCI)
    - etc.
- Identify the jurisdictions and regulatory compliance drivers
- Assist in the preparation of data and coordinate logistics of notification

AEGIS *2017* PHC

Obstacles to Successful Response

- Lack of functional incident response plan
  - The right people need access to the right information to properly remediate risk
  - Boardroom paralysis / incorrect assumptions

AEGIS *2017* PHC

Obstacles to Successful Response

- Slow to react to indicators of compromise
  - Inadvertent destruction / failure to collect evidence
  - IT resources are not empowered
  - Monitoring is not in place to detect compromise
- Organizations rely on technology not people to detect / respond
  - Antivirus is not silver bullet

AEGIS *2017* PHC

Obstacles to Successful Response

- Lack of proper information management lifecyle
  - Inability to truly identify data according to data classification
    - Public – website, press release
    - Internal use – project plans, budgets
    - Confidential – employee and customer data
    - Sensitive / restricted – encryption keys, passwords
- No clear understanding of cyber threats
  - If you get threat intel from CNN, Fox, USA Today
    - Its too late

AEGIS *2017* PHC

Keys to Risk Reduction

- Use regulatory compliance to your advantage
- Partner with third party for annual risk assessments
  - The concussion test
- Identify externally facing systems
  - External pen testing
- Develop patch management program
  - Internally scan to identify vulnerable systems
  - Assess risk of not patching known vulnerabilities

AEGIS *2017* PHC

Keys to Risk Reduction

- Know the data and where it resides
  - Data classification paired with control standards can be powerful and actionable
- Employee awareness
  - Tap into employees egos

Cyber Risk Management / Mitigation

- Security risk assessment
- Penetration testing / vulnerability scanning
- Incident response plan
  - Development
  - Analysis
  - Table top exercises
- Application code review

Contact Information

Contact for AEGIS members
T 855.548.8767
incidentresponse@kivuconsulting.com
Adam DeMonaco
Senior Director, Chief Security Officer
Kivu Consulting, Inc.
T 415.524.7471
C 415.517.7550
ademonaco@kivuconsulting.com

Kivu Background

Kivu combines both technical and legal expertise to deliver industry leading Incident Response, Ransomware / Extortion, Cyber Forensics and Cyber Risk Management services.

With offices through the United States, Canada and Europe, the team is made up of experienced legal counsel, law enforcement, security operations, and C-Suite leaders to provide efficient and effective risk mitigation strategies for our clients.

Kivu's resources are certified experts in incident response and computer forensics including GIAC GCIH, CISA, CISSP, and EnCE.


AEGIS
AEGIS 2017 PHC