Navigating Demands for Ransom and Other Ethical Challenges in Cyber Investigations

October 3, 2017
Business of Ransomware

Global ransomware damage costs predicted to exceed $5 billion in 2017

Who?
• Malicious insider
• Employee mistakes
• Criminal hackers
• Hacktivists
• Cloud or third party compromise

What you are facing?
• Malware
• Phishing
• Ransomware
• Denial of Service
• Loss or Theft of Equipment

Why it is a pandemic?
• Individuals
• Corporations (all sizes)
• Global event

Cyber Triggers by Industry Segment
Ransomware

What is Ransomware
Malicious software designed to either block access to a device/program or encrypt user data. Once the malware executes its function, the victim receives a message demanding payment, usually in Bitcoins, for the key to access the device or data.

Ransomware Types
There are two main types of ransomware:
• Locker
• Crypto
• File Destruction (new wave of attacks)

Commonly Used in Attacks
• WannaCry
• Lockout
• SamSam
• Dark Overload
• XMR Squad

Extortion Threat Landscape
• Engagement
• Automation
Ransom Concerns

• Do you pay the ransom when your organization is hit with ransomware?

• If you decide to pay the ransom, is board approval necessary to set up and fund a bitcoin wallet?

• How do you create a wallet, buy bitcoins and issue payment?

• How to record the acquisition of bitcoin and payment in your books and records?

• What are the ethical issues regarding paying ransom?
When a Breach Occurs

Ten Step Incident Response

- Mobilize incident response team
- Secure infrastructure
- Investigate and validate incident
- Determine scope of issues
- Contain infected hardware and applications
- Alert law enforcement
- Preserve evidence
- Address vulnerabilities
- Comply with legal and regulatory requirements
- Manage distribution of information
# Investigation of an Incident

## Potential Risk Areas

- Laptop / PC security
- Employee furnished mobile devices
- Social media / channel systems
- Enterprise mobile applications
- Cloud-based applications
- Vendor / partner integration points

## Primary Concerns

- How did the ransomware operationalize?
- Exposure
  - Health information
  - Financial information
- Liability
- Disaster Recovery / Business Continuity
- Communications protocol

## Ethical Considerations

- Does accessing employee devices and personal IP addresses help an investigation or infringe on privacy issues?
- Should you notify law enforcement if you identify terrorism indicia or objectionable content?
- After notifying law enforcement officers, they request that you don't share any information about the attack until they complete their investigation - is this ethical?
Business Intelligence

In any industry, although businesses are competitors, it is likely these entities share some of the same critical personal and business information, along with similar vulnerabilities.

**Initiatives:**

- **Cyber Threat Alliance**, a conglomeration of security solution vendors and researchers that have joined forces to collectively share information and protect their customers.

- **Cybersecurity Information Sharing Act (CISA)**, which is meant to ease the way for businesses to join the threat information sharing movement.

Sharing of business intelligence regarding cyber threats should become an essential aspect of any organization’s security program.
The Boardroom Perspective

- Cybersecurity issues are no longer limited to the IT department - board of directors have a fiduciary duty to protect the company’s assets and shareholders’ interests.
- Executives understand cybersecurity is a critical issue, but are unclear who is the enemy and what are the risks to their organization.
- Importance of cyber insurance
Related: ABA Ethics and Professional Responsibility

• Model Rule 1.1 – Competence: “You have a duty to be technologically sophisticated.”

• Model Rule 1.6 – Confidentiality: “A lawyer shall make reasonable efforts to prevent the unintended disclosure of, or unauthorized access to, information relating to the representation of a client.”

• The ABA Standing Committee on Ethics and Professional Responsibility Formal Opinion 477:
  – “Fact-specific” approach to business security obligations requiring a “process” of continual assessments of risks and implementation of commensurate preventive measures.
  – Aims to provide guidance and clarity to lawyers as they consider what level of security to give communications with clients.

• ABA Cybersecurity Resolution: That the American Bar Association encourages all private and public sector organizations to develop, implement, and maintain an appropriate cybersecurity program that complies with applicable ethical and legal obligations and is tailored to the nature and scope of the organization and the data and systems to be protected.
Navigating Demands for Ransom and Other Ethical Challenges in Cyber Investigations

Cyberspace Law Institute and Winter Working Meeting

January 26-27, 2018

Prepared for Ethics CLE Credit
60 Minute Session
10:30-11:30 am
Classroom 331, 3rd FL

Moderator: Cheryl Burtzel, JD
Duggins Wren Mann & Romero, LLP
(cbturzel@dwmrlaw.com)

Panelists: Linda Trickey, JD
Cox Communications
(Linda.Trickey@cox.com)

Louis Scharringhausen, EnCE, GCFA
Charles River Associates
(LouisS@crai.com)

Technical Considerations

• What is ransomware and cyber blackmail? How is it leveraged technically, and what concerns does it bring for exposure of sensitive information.
  o What are the typical options available for remediation or recovery from these incidents?

Ransom Concerns

• Do you pay the ransom when your organization is hit with ransomware?
• If you decide to pay the ransom, is board approval necessary to set up and fund a bitcoin wallet and how do you create it?

Investigation of an Incident

• Can you access the personal email accounts of an individual under investigation? Is this personal or company data?
• Does accessing employee devices and personal IP addresses help an investigation or infringe on privacy issues?
• Should you notify law enforcement if you identify terrorism indicia or objectionable content?
• After notifying law enforcement officers, they request that you don't share any information about the attack until they complete their investigation - is this ethical?

When a Breach Occurs

• Should you notify the parties impacted by a data breach of personally identifiable information if you are not required to do so? What are the ramifications if you decide not to notify them?
• When should you disclose the breach and how much information should you share? As a public company, do you need to disclose the breach in your financial statements?
• If you didn't notify the impacted parties, will your insurer cover a submitted claim?
• When do you notify the board? How do you ensure the board is protected?

Business Intelligence
• Should you notify competitors if you identify any of their breached information on a public forum?

The Board Perspective
• What is the appropriate oversight role for the board?
• When should the board lead the investigation?
• What are the appropriate approval and notification requirements?

Applicable Ethics Rules:
• Model Rule 1.1 – Competence: “You have a duty to be technologically sophisticated.”
• Model Rule 1.6 – Confidentiality: “A lawyer shall make reasonable efforts to prevent the unintended disclosure of, or unauthorized access to, information relating to the representation of a client.”
• The ABA Standing Committee on Ethics and Professional Responsibility Formal Opinion 477:
  “Fact-specific” approach to business security obligations requiring a “process” of continual assessments of risks and implementation of commensurate preventive measures.

Aims to provide guidance and clarity to lawyers as they consider what level of security to give communications with clients.
• ABA Cybersecurity Resolution: “That the American Bar Association encourages all private and public sector organizations to develop, implement, and maintain an appropriate cybersecurity program that complies with applicable ethical and legal obligations and is tailored to the nature and scope of the organization and the data and systems to be protected.”

Proposed Agenda:
• Introduction = 10:30 – 10:35 AM ET
• Applicable Ethics Rules = 10:35 – 10:45 AM ET
• Ransomware and Cyberblackmail and Incident Investigations= 10:45 – 11:00 AM ET
• Breaches, Incident Recovery, and Board Considerations = 11:00 – 11:15 AM ET
• Closing = 11:25 – 11:30 AM ET