GLOBAL cyber risk LLC

THE COUNCIL

The Council of Insurance Agents & Brokers

CIAB: The Council Academy

The Current Threat Environment & Actions to Take

Jody R. Westby

CEO, Global Cyber Risk LLC

July 20, 2021

Council Academy: Exploring the Cyber Risk Environment

- 7/20/21 The Current Cyber Threat Environment & Actions to Take
- 7/21/21 Countering Cyber Attacks: What Good Incident Response Looks Like
- 7/27/21 Managing Cyber Risks Associated With The “New Work”
- 7/28/21 Cyber Compliance: Here Come The Regulators And Lawsuits
- 7/29/21 Director & Officer Liability: The Role of Cyber Governance

Mofenda

Cyber Threat Environment

- Although most of us think in terms of 'breach', events actually involve
  - Ransomware & botnet activities - # 1
  - Targeted attacks & sophisticated malware & use of AI
  - Hacktivism and cyber espionage
  - Nation states
  - Insider actions
- Many forms of assets are under siege
  - Confidential and proprietary data; trade secrets & IP; customer information, internal communications
  - Personal/medical data
  - Payment systems and data
  - Critical infrastructure
- Multi-pronged attacks signal new era in cybercrime
- Defenses are mounting, but the bad guys are winning
- The objective is to mitigate; it is not possible to eliminate

Drivers of Cyber Risk: Operational Factors

- Today's operating environment:
  - Globalization
  - 24/7 connectivity
  - Complex IT architectures, clouds, outsourcing, and mobile
  - Blending of personal/ professional lives & home working environments
  - Highly sophisticated threat environment
- Privacy & Cybersecurity compliance requirements, inconsistent cybercrime laws
- Lack of integrating privacy compliance requirements in security programs
- Inadequate security programs & incident response planning
- Difficulties in attribution and prosecuting cybercrimes
- Management awareness lags behind threats
  - Little understanding of operational impact of cyber events
  - No data on cyber business interruption & loss exposures
  - Lack of governance structure
  - No defined roles & responsibilities for governance

Potential Impacts of Cyber Attacks

- Malware infests operating systems, workstations, removable media
- Software vulnerabilities are exploited to gain system access
- Malware changes system configuration, turns off anti-virus, alters settings
- Data is encrypted for ransom
- Data is stolen and/or disclosed
- Extortion payment is demanded
- Data is zeroed out or corrupted
- Confidential and proprietary information is disclosed; sold to competitors, used for fraudulent or nefarious purposes
- Personal data, medical info, classified, or defense data is involved and triggers laws and contractual clauses
- Web site is infected; web application vulnerability is exploited
- Denial of service shuts down system
- System is used by botnet to attack other systems or store stolen data
- These can cause Operational, Financial, Legal, & Reputational Impacts

Common Forms of Cyber Attacks & Examples

- Socially engineered malware (ransomware, trojans, worms, etc.) – Trick someone into running a program for a website, install an update, ignore security warnings, social media "friend" or request to install an application
- Password phishing attacks – Trick person into revealing login credentials
- "Clickless" attacks through unpatched software
- Advanced Persistent Threats (APT) – Unknown attacks for which no patch has been developed

Examples

- Critical infrastructure attacks (attempt to poison FL water system by increasing the amount of sodium hydroxide , JBS meat plant, Colonial Pipeline)
- Microsoft Exchange Attack: 4 zero day attacks, impacted millions of Microsoft email customers
- CNA insurance ransomware attack
- Bombardier – confidential supplier data, customers, employee data posted online by exploiting vulnerability in third-party file transfer application
- Managed security service provider Kaseya by leveraging vulnerability in its VSA software
- Houston Rockets – Hackers stole 500 GB data, including NDAs and contracts

Ransomware Attacks by Industry

Coveware analyzed ransomware attacks by industry per Q4 2020:

- Healthcare 17.9%
- Professional Services 16.3%
- Consumer Services 11.9%
- Public Sector 9.5%
- Other sectors

Ransomware Demands

- 3/21 Broward County Schools $40 million

What to Do To Prepare For Ransomware & Malware

- Have a data inventory with assigned data owners, classification of data, and criticality
- Refresh training internally to help prevent phishing attacks
- Ensure all equipment and software is within vendor support & install MFA
- Ensure all software – including antivirus software – has current patches
- Monitor logs and security tools; keep an eye out for anomalous behavior; use MSSP
- Conduct regular vulnerability scanning and remediate vulnerabilities
- Have a well-developed incident response plan; test it
- Disable or block Server Message Block (SMB) protocol outbound & restrict PowerShell
- Maintain regularly updated "gold images" of critical systems in the event they need to be rebuilt.
- Have off-site backups with hash integrity checks, source code & executables available
- Have a tested backup/recovery plan
- Have access to a continuity environment
- Have a good cyber insurance policy that will cover ransom payments
- Join an Information Sharing & Analysis Center (ISAC)

What to Do To Respond To Ransomware Attack

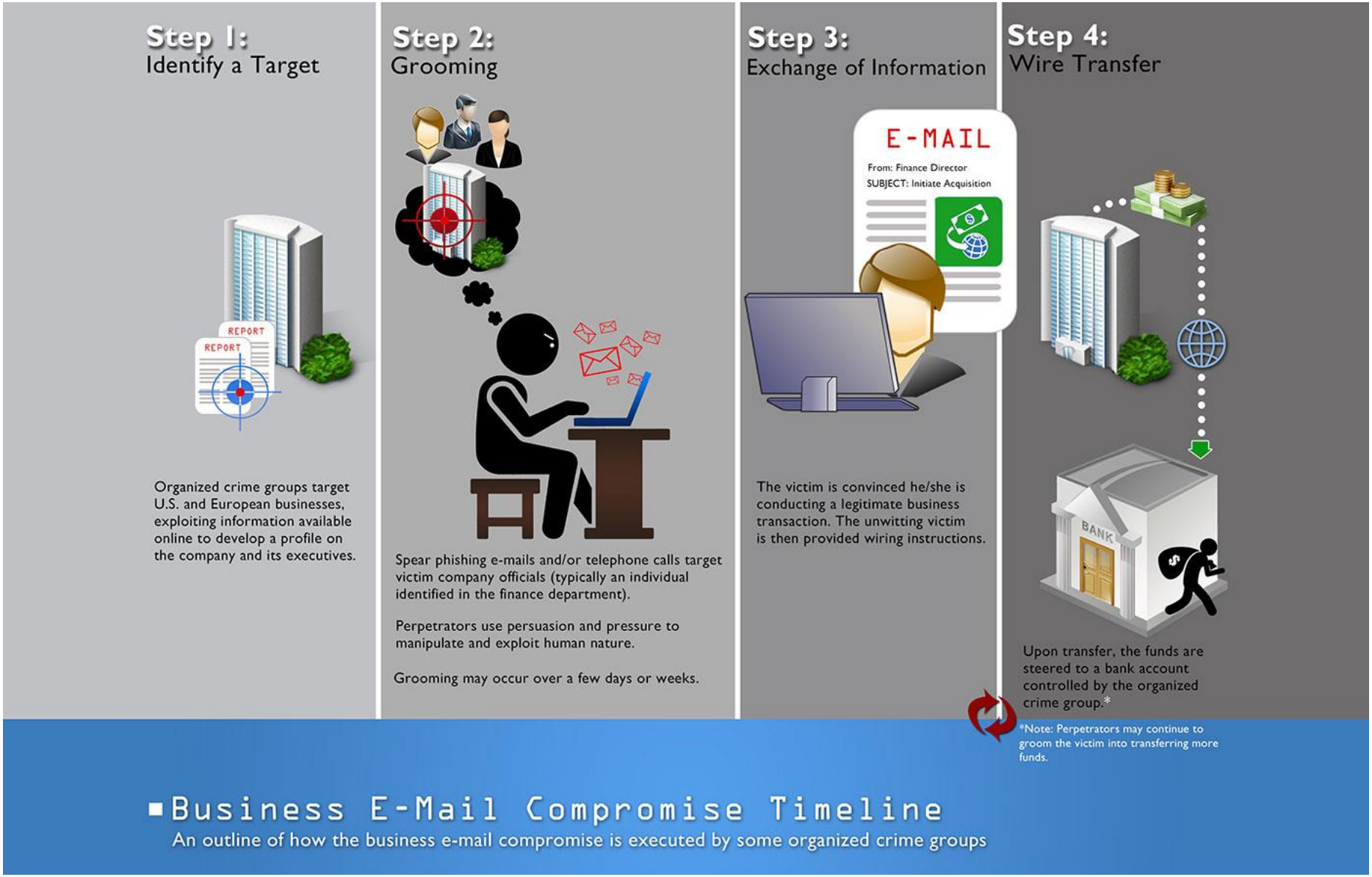
- Take a photo of the ransom message
- Remove from the network or turn off network; if unable to disconnect devices from the network, power them down to avoid further spread of the ransomware infection
- Use out-of-band communication methods, such as phones, so attackers are not aware you are on to them
- Contact your forensic investigation firm
- DO NOT try to take actions on the computer; you will destroy evidence
- See if a free key is available to unlock data from Nomoreransom.org or your anti-malware provider
- Contact your cyber insurance broker or carrier
- Stop replication and online backup activities
- Contact local FBI office
- Run anti-malware program to detect and uninstall malware
- Check hash integrity of most recent backup files and restore on clean machine if good
- Obtain latest guidance from DHS Critical Infrastructure and Information Security Agency:2020 Ransomware Guide is helpful:

https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C.pdf

What to Do: Business Email Compromise (BEC)

- 95% of attacks leverage email (Mimecast); “Email is still the most common channel for opportunistic and targeted attacks, as well as a significant source of data loss.” Gartner
- BEC is one of the most financially damaging cybercrimes. FBI
- Train employees; hover over email addresses, be alert for suspicious emails; verify
- Maintain documentation on email rules
- Restrict privileged admin: have two people involved, one-time passwords, multifactor authentication, restrictions on remote desktop protocol
- Monitor admin activity daily and logs for exfiltration
- Do not ever allow admins to share passwords
- Restrict executions of Powershell
- Implement administrative controls over financial transfers, transfers of sensitive data
- Have offsite backups of emails
- Contact your financial institution asap
- Contact the local FBI office
- File a complaint with the Internet Crime Complaint Center (IC3)

What to Do: Business Email Compromise (BEC)



https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/business-email-compromise

Truth: Cybercrime Costs More Than Maturity

- Cybercriminals are making billions off companies that are not prepared and have weak security controls.
- The job market for cybersecurity professionals is tight; not enough personnel.
- All companies are being targeted; no one is too small.
- Incident response plans are necessary no matter how small a company is.
- Vendors can provide security services and absorb many tasks that an internal person would have to do and usually for less money
- Having ”reasonable cybersecurity practices and procedures” is common language in state laws; failure to have them is cause of private right of action in California
- Regulators and legislators are getting fed up with companies ignoring their cybersecurity programs
- It will always cost more to respond to an attack than it will to implement and maintain a strong cybersecurity program.
- Cybersecurity insurance can no longer be the “hedge” against cyber attacks.

CIAB Resources from Leader's Edge

- Ripple Effects of Cyber Attacks, June 1, 2021, https://www.leadersedge.com/p-c/ripple-effects-of-cyber-attacks
- Ransomware Continues to Lead Cyber Attacks, Mar. 26, 2021, https://www.leadersedge.com/p-c/ransomware-continues-to-lead-cyber-attacks
- Put Incident Response Front and Center, Feb. 28, 2021, https://www.leadersedge.com/p-c/put-incident-response-front-and-center
- Forgiveness After An Attack, Jan. 14, 2021, https://www.leadersedge.com/p-c/forgiveness-after-an-attack
- 2020 vs. 2021, Nov. 30, 2020, https://www.leadersedge.com/p-c/2020-vs-2021
- 20 for 2020, Jan. 14, 2020, https://www.leadersedge.com/p-c/pay-now-or-pay-later
- Ransomware: It Doesn't Have to be This Hard, Nov. 21, 2019, https://www.leadersedge.com/p-c/ransomwareit-doesnt-have-to-be-this-hard
- Pay Now or Pay Later, July 11, 2019, https://www.leadersedge.com/p-c/pay-now-or-pay-later

Thank You!

Jody R. Westby, Esq.

westby@globalcyberrisk.com

202.255.2700