Cybersecurity Risks and Cities

Strategies to Address Escalating Threats
Thursday, September 23, 2021, 1:15 p.m.

BBK | **Best Best & Krieger**
ATTORNEYS AT LAW

- ## Leeann Habte
- Leeann counsels clients on privacy and security issues, including security incident response plans, breach notification and investigations, security risk assessments, security frameworks, vendor management practices, privacy laws, policies, and data-sharing, and related issues. Leeann is a certified information privacy professional, chair of the American Health Lawyer's Association digital health workgroup, and co-chair of BBK's new Privacy & Cybersecurity practice group.

-

BBK | **www.bbklaw.com**
© 2021 BEST BEST & KRIEGER LLP

Agenda

- Cybersecurity Threats 2021
- Security Risk Management Strategies
- Security Incident Response Plans
- Breach Reporting

Cybersecurity Threats

- Ransomware fastest growing threat since 2016
- 400 cities/counties attacked since 2016
- 300% increase in complaints during COVID-19 pandemic

Colonial Pipeline CEO Tells Why He Paid Hackers a $4.4 Million Ransom

Joseph Blount says he needed to quickly restore service after cyberattack threatened East Coast supply

By Collin Eaton and Dustin Volz
Updated May 19, 2021 4:01 pm ET

The operator of the Colonial Pipeline learned it was in trouble at daybreak on May 7, when an employee found a ransom note from hackers on a control-room computer. By that night, the company's chief executive officer came to a difficult conclusion: He had to pay.

Joseph Blount, CEO of Colonial Pipeline Co., told The Wall Street Journal that he authorized the ransom payment of $4.4 million because executives were unsure how badly the cyberattack had breached its systems, and consequently, how long it would take to bring the pipeline back.

Mr. Blount acknowledged publicly for the first time that the company had paid the ransom, saying it was an option he felt he had to exercise, given the stakes involved in a shutdown of such critical energy infrastructure. The Colonial Pipeline provides roughly 45% of the fuel for the East Coast, according to the company.

"I know that's a highly controversial decision," Mr. Blount said in his first public remarks

Notable Ransomware Attacks on Cities - 2021

- **Feb. 2021 - Oldsmar, Florida**
  - Water treatment plant was hacked by an unknown party who then ***attempted to poison the water supply*** by raising the levels of sodium hydroxide.
    - **Automatic Funds Transfer Services (AFTS)**
  - Attack on payment processing and address verification system utilized by many U.S. state and local government agencies.
- **May 2021 – Washington D.C**. – Babuk hacked into and stole police department data. When ransomware not paid, data dumped on the dark net.
- **July 2021 – Tulsa, Oklahoma –** Attackers targeted utilities and police records. When ransomware not paid, released 18,000 records on dark web.

Common Cybersecurity Threats

Cybersecurity Risks

- Network infrastructure
- Human error
- Third party software
- Cloud computing vulnerabilities

Additional challenges with remote work

Cybersecurity Threats: Phishing, Ransomware, Viruses & Worms, Key-Logging, Trojans, Internal Data Theft, Direct Access Attack, Click Jacking, Denial of Service, Spoofing

Safeguarding Your Data/Risk Mitigation

- Implement Robust Security Framework
  - Identify levels of protection which are necessary to protect your systems and data based on data sensitivity, operational impact (critical infrastructure) and regulatory requirements
- Conduct Appropriate Due Diligence of Vendors
- Train Your Employees
- Implement Network Monitoring
- Routinely Backup Your Data and Maintain Offsite
- Conduct Business Continuity Planning/Review Vendor Business Continuity Plans

Protecting Your Data – Implementing Best Practices

Make use of government and industry resources:

- The FBI has a list of best practices to prevent ransomware (https://www.ic3.gov/Media/Y2019/PSA191002) as well as resources for agencies that have a law enforcement role or function in terms of protecting sensitive data and information.
- The National Institute of Standards and Technology has extensive materials on best practices, evaluating technology risks and training employees (https://www.nist.gov/cybersecurity)
- The Cybersecurity and Infrastructure Security Agency has resources on protecting critical infrastructure: https://www.cisa.gov/water-and-wastewater-systems-sector

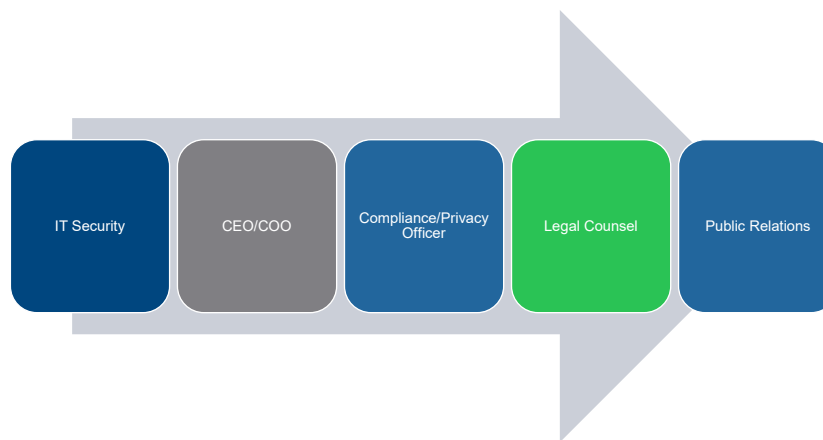# Security Incident Response Plans

Have a detailed and tested security incident response plan, which includes

- Chain of command for all individuals involved.
- Key steps to isolate, eradicate, recover, investigate, and report incident.
- A robust disaster recovery and business continuity plan.
- An internal and external communications plan.
- Identification of computer forensic contractors and other consultants and contract arrangements for immediate activation.
- A policy regarding reporting to law enforcement and payment of ransom.
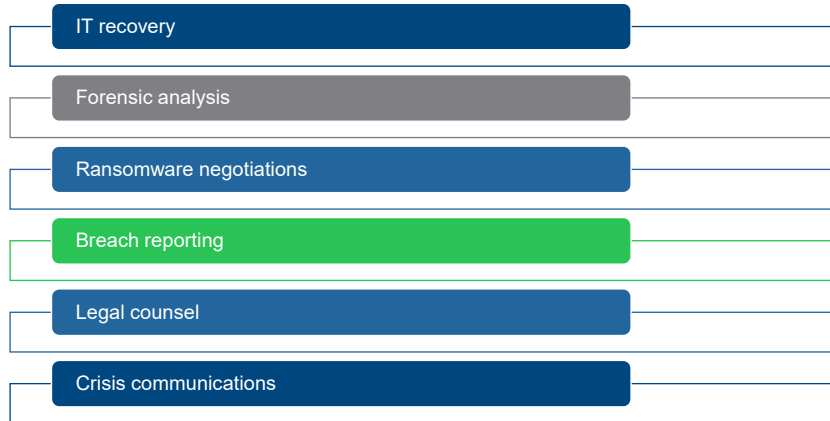- Prompt communication with cyberinsurance carrier.

Chain of Command

| IT Security | CEO/COO | Compliance/Privacy Officer | Legal Counsel | Public Relations |

Contractors

- IT recovery
- Forensic analysis
- Ransomware negotiations
- Breach reporting
- Legal counsel
- Crisis communications

Incident Response

- Standup incident response team and initiate disaster recovery
- Isolate
- Investigate
- Disinfect
- Prevent
- Train
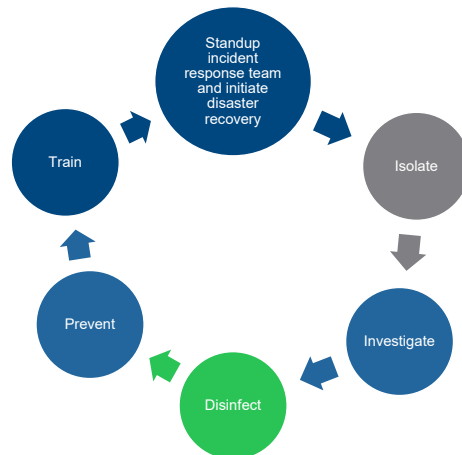
Cyber Insurance

Review of Cyber Insurance Policies Exclusions and Limitations

- Consider limits on amounts of coverage by category, and ensure that they are adequate.
- Consider whether policy requires use of preferred vendors or caps costs at a lower amount for non-insurance vendors.
- Beware of clauses that could impact indemnity.

Breach Assessment and Reporting

Whether the security incident involved unencrypted Personal Information.

Whether the information was acquired by threat actor.

Need good forensic analysis to guide your determination.

Breach Reporting

- Consider whether "breach of the security of the system" involves "Personal Information." (Cal. Civil Code 1798.29.)
  - Personal information means "any information that is maintained by an agency that identifies or describes an individual, including, but not limited to, his or her name, social security number, physical description, home address, home telephone number, education, financial matters, and medical or employment history. It includes statements made by, or attributed to, the individual."

- If Fire Department is a covered entity under the Health Insurance Portability and Accountability Act,
  - Evaluate whether Protected Heath Information (PHI) has been compromised.

Breach Reporting

Notification to Individuals

"Notice of Data Breach"	"What Happened,"	"What Information Was Involved,"	"What We Are Doing,"	"What You Can Do," and	"For More Information."	Additional information may be provided as a supplement to the notice.

Breach Reporting

Notification to State Attorney General if 500+ affected individuals/Office for Civil Rights if PHI → Notification must include submission of template Notice of Breach → Notification to other state agencies for residents of other states, as required by state law

---

Contact Information

Leeann Habte
(213) 787-2572
leeann.habte@bbklaw.com