It's 3 AM: Do You Know Where Your Data Is?

Patrick M. Hromisin, Esq.

Presented to the Pennsylvania Municipal League
May 13, 2020

SAUL EWING ARNSTEIN & LEHR LLP

Today's Discussion

- What are the dangers?
  - Overall threats
  - COVID-19 pandemic concerns
  - Ransomware attacks on municipalities
- What should you do?
  - Planning and insurance
  - Responding to incidents
  - COVID-19 pandemic areas of emphasis

SAUL EWING ARNSTEIN & LEHR LLP

Terminology

- A **<u>data breach</u>** is a confirmed incident in which sensitive, confidential or otherwise protected data has been accessed and/or disclosed in an unauthorized fashion

- **<u>Data breach</u>** may have different meanings under various state, federal, and international laws
- Distinguish between data breach and **<u>cybersecurity incident</u>**

SAUL EWING ARNSTEIN & LEHR LLP

Broad-Based Dangers

- Malware/Ransomware
- Intrusion via website login systems
- Business email compromise
- Phishing or other social engineering
- Employees/contractors mishandling data
- Human factors/negligence
- Lost/stolen devices

SAUL EWING
ARNSTEIN
& LEHR LLP

Goals of Malicious Actors

- Money
  - Direct theft or ransom
- Theft of personal information
  - Purchase of goods with financial information
  - Filing of fraudulent tax returns
  - Extortion/sale of personal information
- Disgruntled employee(s) use of information
- Espionage, political statement or attack

SAUL EWING ARNSTEIN & LEHR LLP

COVID-19 Concerns

- Remote access platforms
- Personal devices and unsecured home networks
- New/untested vendors and services
- Increased susceptibility to phishing and social engineering
- Remote meeting intrusions ("Zoom-bombing")

SAUL EWING ARNSTEIN & LEHR LLP

Municipal Ransomware Attacks

- The developments
  - Massive move from businesses towards municipal targets
  - Estimates range from 70 to 174 total municipal ransomware attacks in 2019
  - 60% increase over 2018
  - Attackers target city governments and subdivisions (school districts, public works, health department, utilities)

SAUL EWING ARNSTEIN & LEHR LLP

Municipal Ransomware Attacks

- The methods
  - Phishing/social engineering
  - Exploiting un-updated software
  - Exploiting vulnerabilities in municipal contractors or service providers

SAUL EWING ARNSTEIN & LEHR LLP

Municipal Ransomware Attacks

- The causes
  - Resource allocation
  - Criticality of the data under attack
  - Willingness to pay
  - Ease of repeating the attack

SAUL EWING ARNSTEIN & LEHR LLP

Municipal Ransomware Attacks

- The ransom demands
  - Kaspersky reports that demands in 2019 ranged from $5,000 to $5 million, with an average of just over $1 million
  - Ransom often demanded in Bitcoin
  - Demands have increased substantially
  - Some insurance will cover a ransom
  - In July, the United States Conference of Mayors announced its members would not pay ransoms

SAUL EWING ARNSTEIN & LEHR LLP

Municipal Ransomware Attacks

- The remediation costs
  - Some estimates state that the average ransomware incident costs $8.1 million and takes 287 days of work to remediate
  - Atlanta's remediation costs are estimated at over $17 million
  - Baltimore's costs exceed $18 million, including remediation, new hardware, and lost or deferred revenue

SAUL EWING ARNSTEIN & LEHR LLP

SAUL EWING
ARNSTEIN
& LEHR LLP

Plan Ahead

- Threat Assessments
  - A good cyber threat assessment offers security and threat prevention by exposing application vulnerabilities;
  - Detecting malware and botnets;
  - Identifying “at risk” devices; and
  - Indicating preventative measures to take
- Training
  - Decreases susceptibility to phishing and inadvertent losses

SAUL EWING ARNSTEIN & LEHR LLP

Incident Response Plan

- What is an incident response plan?
  - Aims to help you manage a data breach
  - Provides a framework that sets out roles and responsibilities for managing an appropriate response to data breach
  - Describes steps an entity should take to manage a cybersecurity incident , should one occur
- Why do you need one?
  - Provides clarity and mitigates confusion
  - Gives all stakeholders knowledge of how to address an incident
  - Establishes a chain of command and responsibilities of each member
  - Quicker response time

SAUL EWING ARNSTEIN & LEHR LLP

Incident Response Plan

- The Incident Response Plan should contain:
  - The actions to be taken if a breach is suspected, discovered or reported by a staff member, including when it is to be escalated to the response team
  - The Members of your incident response team
  - The actions the response team is expected to take and the sequence in which to take them
  - A clear explanation of what constitutes a data breach
  - The reporting line if staff do suspect a data breach

SAUL EWING ARNSTEIN & LEHR LLP

Incident Response Plan

- The Incident Response Plan should contain (cont'd):
  - The circumstances in which the incident can be handled by a front-line manager or when it should be escalated
  - A policy for recording data concerning incidents
  - A strategy to identify and address any weaknesses that contributed to the incident
  - A system for a post-incident review and assessment of your organization's response and the effectiveness of the incident response plan itself

SAUL EWING ARNSTEIN & LEHR LLP

Incident Response Team

- Every organization is different, but an incident response team should usually include:
  - IT staff
  - Forensic consultants
  - Security/law enforcement
  - Legal counsel
  - Human resources
  - Public Relations
  - Insurance contacts

SAUL EWING ARNSTEIN & LEHR LLP

Privilege and Confidentiality

- In general, the more confidentiality you have, the better investigation you get
- Public investigations may be subject to second-guessing, compromise of leads, and confirmation bias
- Pennsylvania's Right-to-Know Law (65 P.S. § 67.708(b)(4)) exempts from disclosure:
  - "A record regarding computer hardware, software and networks, including administrative or technical records, which, if disclosed, would be reasonably likely to jeopardize computer security."

SAUL EWING ARNSTEIN & LEHR LLP

Insurance

- "Traditional" policies almost never cover harm from cyber incidents
- First-party cyber coverage typically does cover:
  - Cyber extortion/ransom
  - Data restoration
  - Forensic costs
  - Crisis management
  - Legal costs
  - Notification, call center, credit monitoring/identity restoration
- Distinguish between cyber incident and crime theft policy

SAUL EWING ARNSTEIN & LEHR LLP

Insurance

- To qualify for a cyber policy, an organization might have to conduct a detailed assessment and review of its security posture
- Being aligned with best practices makes an organization safer *and* more insurable
- Cyber insurance providers often assist in non-financial ways, both in preventative measures and in incident response

SAUL EWING ARNSTEIN & LEHR LLP

Incident Response

1. Identify
2. Contain
3. Investigate
4. Notify
5. Remediate

SAUL EWING ARNSTEIN & LEHR LLP

Identify

- Determine whether your system is under attack, there has been a data breach, or there are other security concerns
- Network monitoring software can help by noting introduction of new software, unexpected IP addresses, unusual traffic patterns, etc.
- Draw on input from IT or forensic consultants if situation is unclear
- Follow Incident Response Plan procedures for reporting internally

SAUL EWING ARNSTEIN & LEHR LLP

Contain

- Record the date and time when the breach or incident was discovered & response efforts begin
- Alert and activate relevant members of the response team
- If possible, secure the premises around affected equipment to help preserve evidence
- Stop additional data loss
  - Take devices offline but DO NOT turn off
- Assess priorities and risks

SAUL EWING ARNSTEIN & LEHR LLP

Contain

- Work with forensic experts
  - Encryption enabled
  - Analyze backup or preserved data
  - Review the type of information compromised
- Determine if network segmentation is effective
- Develop a communication plan
  - Develop comprehensive plan to communicate internally, then to external stakeholders
- Alert law enforcement if appropriate

SAUL EWING ARNSTEIN & LEHR LLP

Investigate

- Identify and record relevant evidence
- Inside or outside threat?
- Conduct interviews
- Analyze compromised systems
- Identify malware employed, if applicable
- Reconstruct the incident

SAUL EWING ARNSTEIN & LEHR LLP

Investigate

- Key Questions
  - What information was improperly disclosed or encrypted?
  - Was the information recovered?
  - When and how did the incident happen?
  - How many individuals were affected?
  - Does the incident involve residents of multiple states?
- Document the investigation findings, conclusion and rationale

SAUL EWING ARNSTEIN & LEHR LLP

Notify

- Determine notification obligations
  - 73 P.S. § 2303(a) states that "an entity that maintains, stores or manages computerized data that includes personal information shall provide notice of any breach of the security of the system following discovery of the breach of the security of the system to any resident of this Commonwealth whose unencrypted and unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person."
  - 73 P.S. § 2302 defines "entity" as a "State agency, a political subdivision of the Commonwealth or an individual or a business doing business in this Commonwealth."

SAUL EWING ARNSTEIN & LEHR LLP

Remediate

- Generally long and thorough and requires looking at other potential flaws in security infrastructure
- Develop a remediation plan that is tailored to the breach incident to prevent it from happening again
- Remediation costs can be costly and time-consuming but are necessary after a flaw has been exposed

SAUL EWING ARNSTEIN & LEHR LLP

Remediate

- Remediation practices can include
  - Developing an internal and external communications plan
  - Strengthen data security policies
  - Planning to prevent reoccurrence
  - Providing additional training to employees on data security
  - Maintaining documentation of actions
  - Insurance considerations

SAUL EWING ARNSTEIN & LEHR LLP

COVID-19 Areas of Emphasis

- VPNs for remote access
- Special training/refreshers for personnel
- Determine appropriate levels of access for users
- Flag external emails to prevent phishing
- Discourage use of personal devices if possible
- Implement multi-factor authentication

SAUL EWING ARNSTEIN & LEHR LLP

COVID-19 Areas of Emphasis

- Zoom and other telepresence apps
  - Require meeting passwords
  - Turn off recording of meetings
  - If recording is necessary, ensure it's stored securely
  - Designate a meeting host who can pay attention to settings and attendees

SAUL EWING ARNSTEIN & LEHR LLP

Questions?

Patrick M. Hromisin
Saul Ewing Arnstein & Lehr LLP
Philadelphia, Pennsylvania
215-972-8396
Patrick.Hromisin@saul.com

SAUL EWING
ARNSTEIN
& LEHR LLP

Baltimore
Lockwood Place
500 East Pratt Street, Suite 900
Baltimore, MD 21202-3171
T: 410.332.8600 • F: 410.332.8862

Boston
131 Dartmouth Street
Suite 501
Boston, MA 02116
T: 617.723.3300 • F:617. 723.4151

Chesterbrook
1200 Liberty Ridge Drive
Suite 200
Wayne, PA 19087-5569
T: 610.251.5050 • F:610.651.5930

Chicago
161 North Clark
Suite 4200
Chicago, IL 60601
T: 312.876.7100 • F: 312.876.0288

Fort Lauderdale
200 E. Las Olas Blvd.
Suite 1000
Fort Lauderdale, FL 33301
T: 954.713.7600 • F: 954.713.7700

Harrisburg
Penn National Insurance Plaza
2 North Second Street, 7th Floor
Harrisburg, PA 17101-1619
T: 717.257.7500 • F: 717.238.4622

Miami
701 Brickell Avenue
17th Floor
Miami, FL 33131
T: 305.428.4500 • F: 305.374.4744

Minneapolis
33 South Sixth Street, Suite 4750
Minneapolis, MN 55402
T: 612.217.7130 • F: 612.677.3844

New York
1270 Avenue of the Americas,
Suite 2005
New York, NY 10020
T: 212.980.7200 • F: 212.980.7209

Newark
One Riverfront Plaza
Newark, NJ 07102
T: 973.286.6700 • F: 973.286.6800

Philadelphia
Centre Square West
1500 Market Street, 38th Floor
Philadelphia, PA 19102-2186
T: 215.972.7777 • F: 215.972.7725

Pittsburgh
One PPG Place
30th Floor
Pittsburgh, PA 15222
T: 412.209.2500 • F:412.209.2570

Princeton
650 College Road East, Suite 4000
Princeton, NJ 08540-6603
T: 609.452.3100 • F: 609.452.3122

Washington
1919 Pennsylvania Avenue, N.W.
Suite 550
Washington, DC 20006-3434
T: 202.333.8800 • F: 202.337.6065

West Palm Beach
515 N. Flagler Drive
Suite 1400
West Palm Beach, FL 33401
T: 561.833.9800 • F: 561.655.5551

Wilmington
1201 North Market Street
Suite 2300 • P.O. Box 1266
Wilmington, DE 19899
T: 302.421.6800 • F: 302.421.6813

SAUL EWING
ARNSTEIN
& LEHR LLP