Lessons Learned From Data Breaches

South Carolina School Boards Association
2020 Annual Convention
February 22, 2020

Jim Denning

Burr Forman McNair

Session Overview

This presentation will provide an understanding of

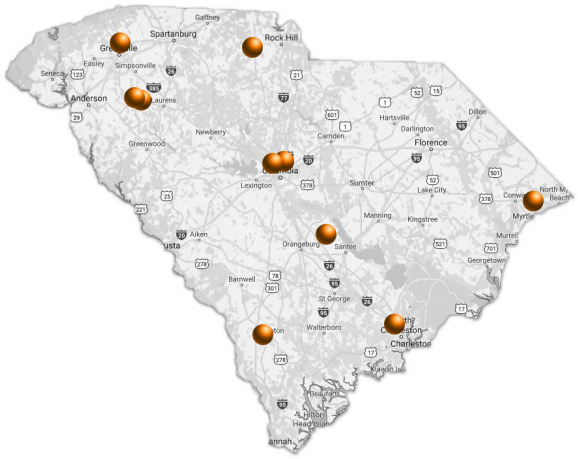
- Why cybersecurity is important to you;
- Methods used by criminals and insiders to access and steal your organization's data and money;
- Some ways to avoid or mitigate data loss and the related costs; and
- How school districts and others have been compromised, and what can be learned from their experiences to help prevent and mitigate the damage.

The Bottom Line of Data Breaches

- For any organization, there is a **cost in real dollars** required **to identify, stop, and remedy** a data breach
- There is **also a reputational and political cost** to the district, its board and leadership
- State and federal laws require notification and assistance to affected individuals and companies
- **Stakeholders** may **lose** financially and otherwise, through the resulting identity theft or disclosure of **personal and financial information**, **lose access** to services or information, **suffer anxiety** about possible harm, and **feel a loss of confidence** in their elected and appointed leaders and support staff

BURR FORMAN MCNAIR

School District Breaches (2016 -2019)



BURR FORMAN MCNAIR

Understanding the Risks; Preparing a Strategy

It is critical that you understand:

- the threats – who the bad actors are and the tools they use
- your organzation's exposure, and
- how to promptly and appropriately guide your employees and other stakeholders in dealing with a data compromise

Understanding the Risks; Preparing a Strategy

- To help understand the risks and have an effective strategy,
  - Use industry standards and best practices to assess cyber hazards, including from
    - Industry and professional associations
    - SC Dept. of Administration (formerly Budget Control Board) offers resources for planning and responding.
    - Cyber security consultants, and response firms

Common cybersecurity threats and attacks

- Malware (viruses, ransomware, spyware, etc.)
- Hacking (via zero-day exploit, malware, etc.)
- Network intrusions
- Denial-of-service and distributed denial-of-service (DDoS) attacks
- Data theft (exfiltration)
  - Confidential Information
  - Personally identifiable information
  - Intellectual property & proprietary information

Common cybersecurity threats and attacks

- Social Engineering Scams
  - **Phishing** – uses email to trick recipient into taking action requested by cybercrook; often use bank/credit card company or other vendor impersonation to create impression of urgency
  - **Spear phishing** – phishing that targets a specific individual or small group by disquising cybercrook as trustworthy friend or co-worker/boss; uses details about recipient to provide added authenticity
  - **Vishing** – phishing-like activities using video chat
  - **Smishing** – phishing-like activities using texting
  - **Whaling** – high-level executives are targeted

Common cybersecurity threats and attacks

- Insider threats
  - Disgruntled employees
  - Nonresponders
  - Insider collusion
  - Insider profiteers
- Systems misuse
- Fraud/embezzlement
- Sabotage
- User mistake or error

Ransomware – The Basics

- Ransomware based on the principal of extortion.
- Either prevents you from accessing / using your data OR copies your data and threatens to make it public
- Most frequently seen model is encryption (locking out)
- A growing pattern of encryption followed by threat of release (double-dipping)
- Recently no encryption (Maze), crooks just exfiltrate the data and extort with threat of public release
- Encryption key / return of data traded for $$ in bitcoin
- Growing in frequency as pre-built toolsets are sold
- Since ransomware attacks are generally initiated via email attachments or links, the incidence of spear phishing is also on the rise. (but vishing & smishing)

Ransomware Attacks Continue to Grow

- 23 Texas cities were targeted in August 2019 in what authorities are calling a “coordinated ransomware attack”.
- According to IT security firm Barracuda Networks in a late-2019 report, “from 2018 to 2019, there was a 235% increase in ransomware attacks on K-12 and higher education.”
- Even if target organization doesn’t pay the ransom, the press coverage of the attack may encourage other crooks to take aim at similar organizations to obtain notoriety or due to perceived wealth

Ransomware (cont.) – p. 2

- Cybersecurity firm Armor tracks school district ransomware incidents. Armor reported in December 2019 that from January through November, ransomware infections hit at least 72 US school districts, potentially impacting 1,039 US schools. 11 districts were hit in November 2019.
- A report issued on December 31, 2019 by antivirus software maker Emsisoft says 89 ransomware incidents occurred during 2019 at US school districts and other educational establishments, impacting the operations of 1,233 schools and colleges.

Ransomware (cont.) – p. 3

- In October 2019 alone at least 15 school districts across the US were hit, affecting over 100 K-12 schools.
- While it is true that ransomware operators and affiliates have not typically followed through with their threats to release data, this may be changing….
- On November 21, the operators of the Maze Ransomware publicly released 10% of the data that was stolen from a security staffing firm after they did not pay the ransom demanded. The criminals state that they will release the rest of the data if an increased ransom payment is not made.

What's Ahead in 2020?

- Continued escalation of spear phishing and ransomware attacks with increasing sophistication as ransom demands increase and increasingly succeed
  - "Double" Ransom to remove encryption PLUS additional ransom to prevent public disclosure or sale of information
  - Disclosure Ransom to prevent (maybe) publication of data
- Introduction of Deepfake attacks into the mainstream:
  - Deepfake is artificial intelligence technology that is used to create audio and video that appear credible but are not
  - One threat: convincing fakes of voices of executives to trick workers into transferring money into criminal's account
  - Likely to further advance into convincing fake video of an executive asking for emergency transfer of funds
- 5G network (5^{th} generation cellular wireless) will introduce new vulnerabilities as the technology matures and expands

Fundamental Rules of Data Security

- Know what (software/hardware/data) you have.
- Know what (software/hardware/data) you need.
- Get rid of what (software/hardware/data) you have but don't need.
- Maintain and protect what (software/hardware/data) you keep.
- Only keep it (software/hardware/data) for so long as you need it; weigh the risk of keeping it.
- When you get rid of it (software/hardware/data), do so in a responsible, safe, and secure way.
- Assess mobile and laptop configuration/security.
- Continually re-evaluate each step.

Some First Steps Toward Readiness and Recovery

- Perform a pre-incident inventory and understand the hardware and software used in the district's and individual school's operations -- this is a key part of prevention and mitigation
- Identify the types, criticality, and content of data obtained, retained, and used by the district and individual schools
- Implement a critical analysis of what equipment and information is actually needed for performance of services

More Steps Toward Readiness and Recovery

- Limit information collected to what is actually needed
- Decommission and remove from internal networks unused or unneeded equipment, and replace outdated/unsupported devices
- Delete unneeded data and archive (using encryption) unused but useful data
- Initiate ongoing training of all employees about cybersecurity and how emails and other communications can be used to attack the district's / schools' resources and information

More Steps Toward Readiness and Recovery

- Be familiar with South Carolina law and regulations relating to cybersecurity policies and breach notification requirements
- Identify federal data security and breach (including notification) laws applicable to your operations
- Be aware that the data privacy and breach notification of other states may apply if your district has non-resident students from other states
- Form an Incident Response Planning Team
- Prepare a Comprehensive Incident Response Plan
- Identify and Obtain Cybersecurity Monitoring Tools

More Steps Toward Readiness and Recovery

- Form an Incident Response Team with internal and external members
  - Staff with incident response executive, security analyst, IT engineer, public relations, human resources, finance, risk management, one or two high level executives, internal (if applicable) and external legal counsel, and external security forensic experts.
- Have prior retainer relationships with legal counsel and security forensics experts for expedited response

Cyber Insurance – Key Elements

- Cyber insurance generally contain some combination of these policies:
  - Network Security
  - Privacy Liability
  - Network Business Interruption
  - Media Liability
  - Error and Omissions (E&O)
- Be mindful of coverage overlaps or gaps with your existing policies

Cyber Insurance -- Coverage

- First Party Coverage – covers your network
  - Cyber extortion payments
  - Cyber forensic services
  - Legal counsel assistance in evaluating regulatory and legal requirements
  - Notification of affected individuals (victims)
  - Effects of and extra resources required due to business interruption
  - Regulatory fines and penalties
  - Public Relations services
  - *Credit monitoring / ID theft repair services

Cyber Insurance -- Coverage

- Third Party Coverage – defense of claims made against your organization by others
  - Attorneys' fees and other legal defense costs
  - Settlements
  - Expert witnesses
  - Court costs
  - Judgments
  - *Credit monitoring / ID theft repair services

Cyber Insurance – Cost of Coverage

- The premium cost to your organization reflects, among other things:
  - The amount of sensitive information handled by your organization
  - The type of industry
  - The number of employees in the organization
  - Vendor contracts with cybersecurity and indemnification of your organization
  - Types of coverage sought & exclusions
  - Coverage limits and sublimits
  - Existence and amount of deductible / self-insured retention

Cyber Insurance – What is Covered?

- Be attentive to What is Covered – and Not.
- Watch coverage gaps with other policies
- Does the policy cover
  - Employee negligence?
  - Social engineering (e.g., spear phishing) and network attacks (DDOS, intrusions, hacks)?
  - Any attack your organization falls victim to OR ONLY those targeted specifically against your organization? (e.g., phishing vs spear phishing)
  - Breaches that begin with a vendor and infiltrate your network via vendor credentials, etc.?
  - Outages of cloud and remote network systems?

Recent Breaches – Case Studies

Recent Incidents & Breaches

- South Carolina municipality – Late last year, an employee's credentials were compromised by successful phishing attack, after which the hackers used the compromised account to send phishing emails to the employee's contact list. Municipality says the scam was detected and its network was not breached beyond the employee's account
- On December 6, 2019 an employee of the Katy (TX) ISD mistakenly included birth dates and SSNs of all district employees in a response to a "routine request for an employee list". Katy ISD says the data was destroyed upon discovery.

Other Recent Incidents and Breaches

- The Allegheny Intermediate Unit, a Penn. countywide taxpayer-funded education agency, recently suffered a ransomware attack. Malware encrypted parts of its network and the cybercrook demanded a ransom payment to unencrypt the data. The school had backups and restored access to the vast majority of impacted files without engaging or paying the intruder.
- Analysis of the servers is continuing, to determine whether personal or protected information may have been impacted. Because of uncertainty, employees are being cautioned to monitor their personal financial accounts.

San Diego Unified School District

- No school district wants to start a notice to parents and children – much less its own employees – with:

  "This notice is in regard to an incident at (San Diego Unified School District) involving the security of personal data on the district's information systems."

- The breach began through a successful spear phishing attack in late December 2017, and access was gained to the accounts in January 2018
- SDUSD estimated that about 50 district employees had their login credentials stolen during the initial attack.

San Diego Unified SD – p. 2

- The compromise went undetected until October 2018, when staff reported suspicious emails to IT personnel
- Although the breach was discovered in October 2018, potential victims (and the press) were not notified of the breach until the end of December 2018
- The reason given for the delay was that silence was necessary so as to allow gathering of information about the hack and the hackers before tipping them off with public disclosure
- SDUSD says that over 11 months the hackers accessed the personal data of over 500,000 going as far back as the 2008-2009 school year.

San Diego Unified SD – p. 3

- Names, dates of birth, SSNs, mailing & home addresses, phone numbers, health information, disciplinary records, and other information of students and staff members was accessed
- Some staff payroll and financial information was also viewed, as was health insurance and other staff benefits information
- SDUSD said that “all individuals affected by the date breach have been notified directly” by a representative of the district.

San Diego Unified SD – p. 4

Lessons and Takeaways

1. A spear phishing attack that nets 50 employees means that it was an extremely well researched and executed attack and/or that there was inadequate training of employees about phishing attacks or the employees had forgotten the training points

   => ongoing training and top-down emphasis is an important tool for fighting spear phishing attacks

2. It wasn't until 11 months after the initial compromise that IT became aware of the hack

   => shows importance of training of employees as well as need for intrusion detection equipment and protocols

San Diego Unified SD – p. 5

Lessons and Takeaways

3. Notice that public notification (even of affected individuals) was not made until the investigation had gotten to the point of identifying not only the types of breached data and victims, but the alleged hacker too

   => many state data breach notification laws allow for delay due to legitimate need of law enforcement

4. None of the data from the current academic year or any of the previous 9 years had been encrypted

   => if the district had encrypted prior year data (or archived it outside the district network or destroyed it), there could have been a much smaller victim pool

San Diego Unified SD – p. 6

Lessons and Takeaways

5. Notice that each affected individual – those who the district reasonably determined had likely been compromised by the hack – was "directly" notified by the district

   => it isn't known whether the contact was made in person, by phone, email, or letter, but strongly consider having an authorized employee (who has been adequately prepared) reach out personally to each victim to express regret and discuss what can be done to mitigate any potential harm

Pearson AIMSweb platform (2019)

- Pearson's AIMSweb 1.0 platform is a reading and math monitoring and assessment program for pre-school through high school students
- Pearson was notified by the FBI in March 2019 that its platform had been hacked in November 2018
- The hackers exploited a vulnerability in the platform to gain unauthorized access to 13,000 school and university accounts
- Personal data exposed included first and last name of students and, in some cases, date of birth and email addresses – no SSNs, credit card numbers or other financial data were exposed

Pearson AIMSweb platform (2019) – p. 2

- Pearson says there is no evidence that any of the exposed information was misused
- The exact number of students affected is unknown but is estimated to be in the hundreds of thousands, and included data from as far back as 2001
- Pearson is in the process of phasing out the 1.0 system and has replaced it with AIMSweb Plus
- A class action was filed against Pearson in September 2019 in Illinois federal court claiming that Pearson filed to maintain adequate security measures and had no system in place to detect intrusions and breaches

Pearson AIMSweb platform (2019) – p. 3

Lessons and Takeaways

1. Pearson waited 5 months after becoming aware of the breach (March) to notify victims (July) and offered victims one year of free credit monitoring => there's no indication that the delay was needed or justified (if it was, Pearson should have made that known) – unnecessary delay in notifying individuals whose personal information is thought to have been viewed, removed or used is not only a bad idea, it violates the breach notification laws of most states and several potentially applicable (depending on type of data) federal laws
2. Pearson would have benefited from a skilled public relations firm

Click2Gov Data Breach (2017 – 2019)

- Widely used online self-service bill-payment software application used by utilities, municipalities and county governments to collect fines, fees and taxes
- Vulnerabilities first reported in 2017; confirmed as nationwide problem in September 2018
- As of December 2018, estimated 295,000 payment card records (card number, verification number, expiration date, etc., stolen from 46 US municipalities
- In August 2019 a new round of attacks surfaced, hitting systems in 8 cities (6 of those were hit in the first round of breaches).

Click2Gov Data Breach (2017 – 2019) – p. 2

- Data has been posted for sale on Dark Web
- Over $1.7 million received by hackers from sales of the data
- Average cost of purchase on Dark Web is $10 per record
- Costs to victims (the individuals, the municipality, and the bank or credit card company) can be in hundreds of thousands of dollars (and untold time and anxiety)

Click2Gov Data Breach (2017 – 2019) – p. 3

- C2G's provider, Superion, claimed all affected systems were locally hosted by the compromised local government (or its host), and that its cloud-based system was not compromised
- In June 2018, Superion deployed a patch to the affected third party software, thought by experts to be Oracle WebLogic.
- The August 2019 hacks seem to incidate that even an up-to-date and fully patched system is still vulnerable to being compromised

Click2Gov Data Breach (2017 – 2019) – p. 4

- Experts blame a "systematic problem across organizations with a lack of or poorly documented and executed patch management strategies for critical servers, especially Web application servers where patching requires downtime or the potential for failed upgrades
- Compromised organizations blame Superion for failing to give prompt notice of vulnerabilities once reports began coming in during mid-2017

Click2Gov Data Breach (2017 – 2019) – p. 5

Lessons & Takeaways

1. Hacking remains a danger
2. Even the best patch protocol can fail if one-off or aging devices are not manually updated
3. Software application vendors must be required to vigilantly seek out vulnerabilities of their software and companion software, and timely provide patches and upgrades

Click2Gov Data Breach (2017 – 2019) – p. 6

4. Software application vendors often try to push blame and liability to customer, claiming failure to follow protocol
5. Consider including a requirement in the county contract with software application vendors calling for prompt notice of vulnerabilities of their software and companion software; also require regular or periodic patches and upgrades

Questions?

Jim Denning
(864) 271-4940
jdenning@burr.com

Jim Denning

Practice Areas
Data Privacy and Cybersecurity
Data Breach Response
Advertising and Promotions
International Trade Law and Import Issues
Licensing and Intellectual Property
Corporate

Practice Description

Jim counsels domestic and foreign businesses, local governments and school districts, universities, and individuals, helping with cybersecurity and data privacy issues, advertising clearance, import, tariff, and customs matters, and operational and strategic relationships and transactions. He also assists clients with protection and monetization of intellectual property and technology services and products, using licenses and other commercialization and development agreements. He addresses software, web and mobile app opportunities and issues.

360 Attorneys.
19 Offices
1 Firm.
Southeastern Strong.

BURR FORMAN MCNAIR

BURR FORMAN MCNAIR

Get Connected

linkedin.com/company/burrforman

@burrforman

www.burr.com

Thank you for your participation