Cybersecurity and Data Breach Primer for County Attorneys

South Carolina Association of County Attorneys
August 5, 2019

India Vincent

Jim Denning

Burr & Forman, LLP

Session Overview

This presentation will provide an understanding of

- Why cybersecurity is important to you and your client,
- Methods used by criminals and others to compromise data, and
- Examination of how other counties and municipalities have been compromised, and lessons learned from their experiences to help prevent, identify and mitigate data breaches
- Some of the laws that may apply to data breaches

The Bottom Line of Data Breaches

- For local government, including counties and municipalities, there is a cost in real dollars required to identify, stop, and remedy a data breach
- There is also a reputational and political cost incurred by the governmental subdivision and its elected and other leaders
- Applicable state and federal laws require notification and assistance to affected individuals and companies
- The residents and constituents of the subdivision may lose financially and otherwise, through the resulting identity theft or disclosure of personal and financial information, anxiety about possible harm, and a loss of confidence in their elected and appointed leaders, and support staff

South Carolina Is Not Ignored by Cybercriminals

First Three Months of 2019 Analysis of US State Rankings, Exposed Records

Exposed Records Ranking	US State	Total Exposed Records	Number of Breaches	Percentage of Records Exposed in USA
1	NY	235,460,373	26	47.21%
2	CA	212,740,111	60	42.65%
3	WA	19,151,276	10	3.84%
4	TX	9,340,004	52	1.87%
5	OR	8,027,643	6	1.61%
6	KS	4,083,473	6	0.82%
7	FL	2,207,906	19	0.44%
8	GA	375,811	21	0.08%
9	CT	352,237	5	0.07%
10	SC	91,242	4	0.02%

Risk Based Security, Inc.

How the Public Sector Is Breached…

According to VC3, Inc., a Columbia SC-based IT company,

In the Public Sector 98% of attacks fall into 4 categories:

1. Human Error (34%) -
    - Mistakes that compromise security

        (e.g., leaving data unsecure & exposed to Internet)
2. Insider Misuse (24%) -
    - Non-work related, while on the job

        (e.g., malware introduced through accessing questionable websites or through use of unapproved/unscanned USB drives)

How the Public Sector Is Breached (cont.)

3. Crimeware/Outsiders (21%) -
   - Theft via social engineering or technical stealth
     (e.g., via phishing and hacking)

4. Lost/Stolen Assets (19%) -
   - Use of mobile devices without encryption, locking and remote wiping capabilities

Source: VC3 Inc.

Time is Your Enemy

- 84% of breaches required only minutes to execute
- 66% of those took more than a month to be discovered
- 22% took greater than a month to contain the breach, alleviate the problem and recover

Source: VC3, Inc.

Understanding the Risks; Preparing a Strategy

It is critical that you:

- Understand the threats, your client's exposure, and how to promptly and appropriately guide your client in dealing with a data compromise
- Use industry standards and best practices to assess cyber hazards
  - SC Dept. of Administration is statutorily charged with providing guidance and assistance to county government. This is discussed in more detail later in this presentation.

Common cybersecurity threats and attacks

- Hacking
- Network intrusions
- Denial-of-service and distributed denial-of-service (DDoS) attacks
- Data theft (exfiltration)
  - Confidential information
  - Personal information
  - Intellectual property

Common cybersecurity threats and attacks

- Phishing / Spear Phishing
  - Social engineering
  - Uses known relationships and chains of command
- Malicious software (malware)
  - Viruses
  - Worms
  - Trojans
  - Bots
  - Spyware and keystroke loggers
  - Adware

Common cybersecurity threats and attacks

- Ransomware
  - Encryption key traded for $$$
  - Growing in frequency as pre-built toolsets are sold
  - As of June 5, 2019, 22 state and local governments are known to have been hit with ransomware
- Insider threats
  - Systems misuse
  - Fraud
- Sabotage

Some First Steps Toward Readiness and Recovery

- Assess the hardware and software used in the county government's operations is a key part of prevention and mitigation
- Identify the types, criticality, and content of information obtained, retained, and used by the county
- Implement a critical analysis of what equipment and information is actually needed for performance of services,
- Limit information collected to what is actually needed
- Decommission and remove from county networks unused or unneeded equipment, and replace outdated/unsupported devices
- Delete unneeded data and archive (using encryption) unused data

More Steps Toward Readiness and Recovery

- Initiate ongoing training of all county employees about cybersecurity and how emails and other communications can be used to attack the county resources and information
- 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 county operations

South Carolina Laws

- SC Code § 1-11-490 establishes breach notification requirements where computerized data of the county including unencrypted and unredacted personal identifying information of a resident of South Carolina has been, or is reasonably believed to have been, acquired by an unauthorized person and illegal use of the information has or is reasonably likely to occur or create a material risk of harm to the resident.
- See the statute for further details of timing, and type and extent of notice required.

South Carolina Laws

- Part 1B § 93.21 D500 (Dept. of Administration) of the 2017-2018 Appropriations Act calls for counties to be capable of submitting, upon the request of the SC Dept. of Administration, sufficient evidence to establish that their cybersecurity policies, guidelines and standards meet or exceed those adopted and implemented by the Dept. § 93.21 also sets forth requirements relating to breach notification, including a requirement that the Dept. be informed of all cybersecurity breaches and is authorized to oversee incident responses. See the text of § 93.21 for further details.
- See full current Dept. of Administration Plan at https://www.admin.sc.gov/files/SC%20Dept%20of%Admin_Statewide%20Strategic%20IT%20Plan_Final%20Version_121708_New%20Fo.pdf

US Federal Laws - HIPAA

Health Insurance Portability and Accountability Act of 1996 – HIPAA

(Codified at 42 U.S.C. § 300gg and 29 U.S.C. § 1181 et seq. and 42 USC 1320d et seq.)

- Many local governments, especially counties, are HIPAA covered entities because they offer services or have staff that (1) meet the definition of "health care provider" under HIPAA and (2) transmit health information in electronic form in connection with a HIPAA-covered transaction. (those that meet both (1) and (2) are referred to as "a HIPAA-covered health care providers.") Most key HIPAA definitions are found in 45 C.F.R. 160.103.
- A "health care provider" includes a person or organization who furnishes, bills, or is paid for health care in the normal course of business. A county may, for example, operate a clinic in the health department that meets the definition of health care provider.
- Since, in order for this provider to be a HIPAA-covered health care provider, the county must also transmit health information electronically in connection with a HIPAA-covered transaction. The list of HIPAA-covered transactions is limited to certain types of communications including submission of health care claims, querying eligibility for a health plan, enrolling someone in a health plan, and coordinating benefits across plans. These are described in more detail in 45 C.F.R. Part 162.
- If the county is a HIPAA-covered health care provider, all individually identifiable health information maintained by the county would be subject to the HIPAA regulations, including the privacy rule and the security rule.

General Data Protection Regulation (EU)

- General Data Protection Regulation (of the European Union) - generally speaking, the GDPR would apply to a county only if the county is soliciting EU residents to use a service or purchase goods. An example of triggering conduct might be a tourism campaign targeting residents living in Europe to induce residents to visit the county; in which case any Personally Identifiable Information (PII) collected on those European citizens by the county would likely fall under GDPR data protection and disclosure requirements.
- Consider that each situation is fact and circumstance specific and the outcome of the analysis might be different.

Recent Breaches – Case Studies

Lake City, Florida (June 2019)

- In May-June 2019 Baltimore, MD and two cities in Florida fell victim to ransomware attacks
- Both Florida cities, including Lake City, paid six-figure ransoms via Bitcoin to obtain the key to retrieve use of systems and access to data
- Baltimore refused to pay and as of early June only 1/3 of its employees had access restored

Lake City, Florida (June 2019) – p. 2

- Baltimore estimated its costs related to the ransomware at over $18 million in early June, with no certainty of the total cost to remediate the lost data
- Lake City agreed to a $500,000 ransom but was insured against cyberdamages by the Florida League of Cities who paid most of the ransom amount; Lake City was only responsible for a $10,000 deductible
- Upon payment of the ransom, the encryption key was delivered to Lake City and the town was able to reassess its equipment and data fully within a few days

Lake City, Florida (June 2019) – p. 3

Lessons and Takeaways

1. Ransomware attacks are increasingly targeting local government
2. This increased focus on local government is due in part to willingness to pay ransom (as evidenced by the Lake City incident)
3. Bitcoin (a type of cryptocurrency) has helped enable cybercriminals to attack with anonymity, thus promoting ransomware attacks

Lake City, Florida (June 2019) – p. 4

4. Ransom demands are growing, from low-six figures initially for Baltimore to mid-six figures for the two smaller Florida victims
5. Although ransom demands may seem large, the costs associated with not paying can dwarf the ransom amount
6. Data breach / cyber insurance should be considered by local government as a part of the cost of its risk management program

Lake City, Florida (June 2019) – p. 5

7. Ransomware can be initiated by a hack of existing vulnerability (e.g., in an external facing web app), but is often installed using a spear phishing attack
8. Effects of ransomware may be reduced by using data back-ups - that actually work, and by using segmented networks
9. Segmented networks are built so that parts of the overall network can be cordoned off from the wider network in the event of an attack

Click2Gov Data Breach (2017 – 2019)

- Widely used online payment software application used by 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

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.

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 subdivisions 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

Oregon Dept. of Human Services (Jan 2019)

- Data breach occurred in January 2019
- Result of successful phishing email opened by 9 ORDHS employees
- Hacker had access for 20 days
- Access to the 9 email accounts allowed viewing and possible use of names, addresses, dates of birth, Social Security numbers, case number, personal health information and other personal details

Oregon Dept. of Human Services (Jan. 2019) p.2

- ORDHS is notifying 645,000 people of possible compromise of their personal information
- ORDHS is providing ID theft monitoring and recovery services, as well as, $1 million insurance reimbursement policy to those affected

Oregon Dept. of Human Services (Jan. 2019) p.3

Lessons & Takeaways

1. Phishing (particularly Spear Phishing) Attacks are alive and well – and often successful – and aimed increasingly at local and state government agencies and departments
2. Spear Phishing is particularly effective because the criminal spends time in advance of the attack researching the individuals and the organization so as to make the email appear more believable and legitimate

Oregon Dept. of Human Services (Jan. 2019) p.4

3. It is becoming increasingly common for compromised agencies and governments to provide individual victims with ID theft monitoring service for a specified period (1 – 3 years)
4. Many compromised agencies and governments also provide some level of ID theft insurance to victims
5. Ongoing training of personnel on email security and phishing can be an important step toward preventing successful phishing attacks

Whistler, British Columbia (Dec 2018)

- Municipality's website hacked via an "obscure vulnerability that was not protected by regular updates, security patches, and ongoing monitoring"
- Attack re-directed users to different (unauthorized) website when they tried to visit the town's official website
- Staff detected the hack on Dec. 28, 2018

Whistler, British Columbia (Dec 2018) – p.2

- Staff believed breach had been removed, but found on Jan. 3, 2019, that forms on the official website had been compromised, so webforms were removed
- Cybercriminals often take advantage of access to create additional entrances or install other malware; don't assume the pathway initially identified is the sole threat

Whistler, British Columbia (Dec 2018) – p.3

Lessons and Takeaways

1. It appears that this is a case of old hardware (or software) that is no longer supported and for which patches and security updates are no longer issued
2. An example of the foregoing involves legacy systems using Microsoft products that are no longer supported, such as the Windows XP operating system and Windows Server 2003, both of which were widely used by business and government

Whistler, British Columbia (Dec 2018) – p.4

3. Another possible vulnerability arises from proprietary (privately developed) software or software that has been highly customized
4. Firmware for aging devices and peripheral equipment (e.g., routers, copiers, printers, etc.) may also be unpatched and unsupported due to manufacturer phase outs
5. It is important for the county to identify and audit all equipment that is regularly or may be from time to time connected to its network, and then patch or retire/replace the equipment

Questions?

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

India E. Vincent
(205) 458-5284
ivincent@burr.com

Jim Denning

Practice Areas
Data Privacy and Cybersecurity
Data Breach Response
International Trade Law
Licensing
Corporate

Practice Description

Jim counsels domestic and foreign businesses, local governments and school districts, universities, and individuals, helping with cybersecurity and data privacy issues, 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. In addition to project-based engagements, he provides outside general counsel services.

BURR FORMAN McNAIR

India E. Vincent

Practice Areas
Data Privacy and Cybersecurity
Data Breach Response
Trademark Protection and Enforcement
Licensing

Practice Description

India's practice includes data privacy, cybersecurity, technology & software licensing, and intellectual property protection & monetization. She regularly counsels clients on complying with GDPR, CCPA, and other privacy laws, developing and implementing policies and procedures to secure their data, and responding to data incidents as they occur. She also assist clients in the preparation and implementation of appropriate strategies for clearing, protecting, licensing and enforcing intellectual property rights, and advises clients regarding contractual relationships with customers and vendors. India works with clients in all industries, including the software, technology, biotechnology, entertainment, health care, hospitality, aerospace and manufacturing industries.

360 Attorneys.

19 Offices

1 Firm.

Southeastern Strong.

BURR FORMAN McNAIR

Get Connected

linkedin.com/company/burrforman

@burrforman

www.burr.com

Thank you for your participation.