The 10 Commandments of Data Security and Data Management

Presented by:
Mark Cheramie Walz

www.tinyurl.com/BucksOct7

SWEET | STEVENS | KATZ | WILLIAMS

Key Term: Sensitive Data

* Any data that must be kept confidential by law, or that would otherwise be harmful to the IU if released publicly. Includes all sensitive employee records (payroll, disability, workers comp, discipline, etc.) and all FERPA records for students.

Commandment 1 - Nearly All Records Are Subject To Release

- In Litigation - all relevant evidence is subject to discovery, no matter where it is stored or what type of record it is.
- If you work with a public entity, most records must be produced to a request by a citizen under the state Right To Know law.
- HIPAA (healthcare) and FERPA (education) allow patients and students/parents to access records.

More on Record Production

- Doesn't matter
  - Where the record is physically located
  - Why or for what purpose the record was created
  - Who created the record
  - Whether the record is electronic or maintained in hard copy.
  - Whether the record is stored by your employee or by the company

Right To Know Law

- All agency records are public unless the agency can prove that they are exempt.
  - Exceptions such as privilege, security, trade secrets, etc.
- Records in possession of a party with whom the agency contracts to perform a governmental function are not exempt, and therefore are public records.
- Written request must identify the record sought with sufficient specificity to enable the agency to ascertain which records are being sought.

SWEET | STEVENS | KATZ | WILLIAMS

Notes on RTK

* Not required to create records or compile, format, or organize a record.
* Redaction may be required.
* Don't have to provide information that would jeopardize network security.
* Timeline for response is a mere 5 days. (May be extended with written notice to the requestor)
* Record shall be provided in the medium requested if it exists in that medium, otherwise provided in the medium in which it exists.

SWEET | STEVENS | KATZ | WILLIAMS

Litigation: prepare for the unexpected

* There are numerous ways your company could face a lawsuit, regardless of the specific type of business you're in.

* Examples: Breach of contract, employment discrimination, patent infringement, sexual harassment, fraud, patent infringement, etc.

Commandment 2 - All Stored Data Must Be Preservable

* Litigation Hold - means that all data related to that employee, or related to a student, or related to an incident, must be preserved AS IS.

* How to undertake? Who is responsible? How is it "held"?

* Consequences for non-compliance are substantial.

* Here again, doesn't matter where it is stored or by whom it is stored if a contractor is involved.

Spoliation

* AKA - Adverse Inference Instruction
* If records were supposed to be maintained, but we destroyed them of failed to maintain them, the jury is instructed to essentially "assume the worst" about the missing evidence.
* Makes winning very difficult!
* Can be safe harbor for routine deletion so long as it is according to policy and is rigorously adhered to, and there were good faith efforts to preserve the data sought.

E-Discovery Compliance Growing Increasingly Difficult

Melanie Rodier
Senior Editor and Head of Video

See more from Melanie Connect directly with Melanie Bio | Contact

As electronic data proliferates, complying with e-discovery rules becomes more difficult -- and more costly.

Tags: E-discovery, Forrester, Barry Murphy, Patrick Gordon, Michael Everall, FRCP, safe harbor, Morgan Stanley,

AUGUST 17, 2007

Like it or not, every company will almost certainly one day face the daunting task of answering an e-discovery request. And following the revised Federal Rules of Civil Procedure (FRCP), which introduced critical new obligations for any party to a lawsuit in federal court, firms have been scrambling to come to grips with what can be an incredibly costly problem.

"In any e-discovery action, an organization needs to find information no matter where it lives," says Barry Murphy, principal analyst at Forrester Research. "At times, the discovery action will be confined to E-mail, and in such a case, e-discovery can be conducted directly within a message archive. Often, though, e-discovery must extend to other managed and unmanaged repositories, requiring organizations to invest in technologies like search, indexing, extraction and forensic desktop imaging tools."

Commandment 3 - Back Up All Sensitive Data

* Critical in case we need to restore following data breach, loss, outage, etc.

* Individual files stored in unauthorized locations are NOT backed up (e.g. Thumb drive, unauthorized cloud storage, etc.)

* Back-ups play a key role in determining what is lost in the event of a theft or loss of a device.

California: Hospital Pays Bitcoin Ransom to Hackers

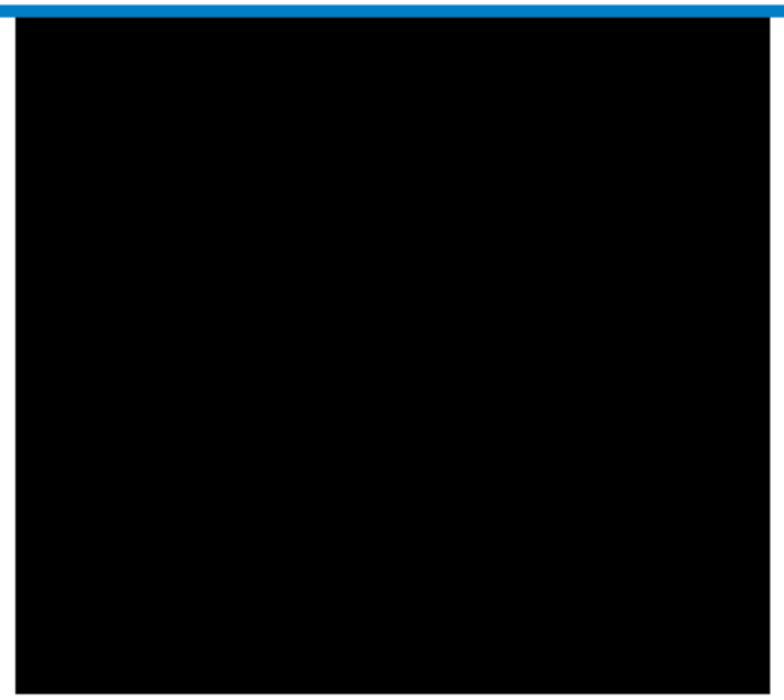
By THE ASSOCIATED PRESS FEB. 17, 2016

Hollywood Presbyterian Medical Center paid a ransom in bitcoins equivalent to about $17,000 to hackers who infiltrated and disabled its computer network, the hospital's chief executive said Wednesday. It was in the hospital's best interest to pay the ransom of 40 bitcoins after the hacking that began Feb. 5, the C.E.O., Allen Stefanek said. The F.B.I. is investigating the attack, often called "ransomware," in which hackers encrypt a computer network's data to hold it hostage, providing a digital decryption key to unlock it for a price. "The quickest and most efficient way to restore our systems and administrative functions was to pay the ransom and obtain the decryption key," Mr. Stefanek said. Bitcoins, an online currency, are hard to trace. The Los Angeles hospital network was operating fully again Monday, and patient care was not affected by the hacking, Mr. Stefanek said. Neither law enforcement officials nor the hospital gave any indication of who might have been behind the attack or whether there were any suspects.

A version of this brief appears in print on February 18, 2016, on page A17 of the New York edition with the headline: California: Hospital Pays Bitcoin Ransom to Hackers.

A New Jersey school district was hit with crypto-ransomware, bringing out the feds to investigate and holding up the computerized PARCC exams. Oddly, reported ransom amounts range from $500 in bitcoins to 500 bitcoins worth about $124,000.

Network World | Mar 25, 2015 10:53 AM PT



New Jersey school district Swedesboro-Woolwich is a victim of crypto-ransomware.

When Swedesboro-Woolwich school district, which has four elementary schools with a total of about 2,000 students, was hit with crypto-ransomware, big guns showed up to investigate. After the district's network was locked up due to ransomware on March 22, the local Woolwich Police, the New Jersey State Police Cyber Crimes Unit, the FBI and Homeland Security are all investigating.

In an announcement about the malware, the school district said:

> Forensic analysis is being performed by the NJ State police. At this point there appears to be no data breach. The files affected were mainly Word documents, Excel spreadsheets and .pdf files created by staff members. Data for the student information system as well as other applications is [sic] stored offsite on hosted servers and was not affected by the virus.

It's also thrown a kink in the school district's scheduled Partnership for Assessment of

Commandment 4 - Must Vet All Contractors Storing Sensitive Data

* Ensure that contractors utilize appropriate data security precautions and backups.

* Review contracts to ensure legal compliance.

* Seek provisions assuring confidentiality where data involved.

* Ensure contractor is obligated to notify your company in event of a data breach.

SWEET | STEVENS | KATZ | WILLIAMS

Commandment 5 - Have Data Breach Response Plan

* Common Data Breaches
    * Lost laptop
    * Lost mobile device
    * Lost thumb drive, or other portable media
    * Content mistakenly posted publicly
    * Contractor data breach
    * Errant e-mail sent to wrong party

SWEET | STEVENS | KATZ | WILLIAMS

Less Common Data Breaches

* Firewall failure

* Hacking (whether from internal or external sources)

* Rogue employee data dump

Hacker strikes Cumberland Valley computers; district and law enforcement accessing damage

Cumberland Valley School District officials say a hacker gained access to its computer network but it is still trying to determine whether any data was stolen.

By **David Wenner | dwenner@pennlive.com**
Email the author | Follow on Twitter
on August 22, 2014 at 2:20 PM, updated August 22, 2014 at 7:14 PM

Security Breach at Lewisburg Area School District

POSTED 5:26 PM, OCTOBER 30, 2014, BY NIKKI KRIZE

LEWISBURG – Lewisburg Area School District officials discovered this

What are you required to do in light of a data breach?

SWEET | STEVENS | KATZ | WILLIAMS

PA Data Breach Law

* Breach of Personal Information Notification Act(73 P.S. § 2301)

* “Entity.” A State agency, a political subdivision of the Commonwealth or an individual or a business doing business in this Commonwealth.

SWEET | STEVENS | KATZ | WILLIAMS

Notification of Breach

* (a) General rule.--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.

* The notice shall be made without unreasonable delay.*

SWEET | STEVENS | KATZ | WILLIAMS

* “Breach of the security of the system.” The unauthorized access and acquisition of computerized data that materially compromises the security or confidentiality of personal information maintained by the entity as part of a database of personal information regarding multiple individuals and that causes or the entity reasonably believes has caused or will cause loss or injury to any resident of this Commonwealth.

* maintained by the entity as part of a database of personal information regarding multiple individuals and that causes or the entity reasonably believes has caused or will cause loss or injury

* Personal Information:

    * (1) An individual's first name or first initial and last name in combination with and linked to any one or more of the following data elements when the data elements are not encrypted or redacted:

        * (i) Social Security number.

        * (ii) Driver's license number or a State identification card number issued in lieu of a driver's license.

        * (iii) Financial account number, credit or debit card number, in combination with any required security code, access code or password that would permit access to an individual's financial account.

Other details

* Must provide notice of the breach if encrypted information is accessed and acquired in an unencrypted form OR if the security breach is linked to a breach of the security of the encryption, OR if the security breach involves a person with access to the encryption key.

* Contractor/Vendor - required to notify the entity. It is then the duty of the entity to make the notification required by the law.

* If more than 1000 notified, must also notify credit reporting agencies.

SWEET | STEVENS | KATZ | WILLIAMS

Summary of PA Data Breach Law

* Applies in a narrow instance to very specific and highly sensitive information.

* Definitely does not apply to most minor data breaches.

* Requires timely and specific response

* May be costly response for large-scale breach, of breach whose scale is unknown.

SWEET | STEVENS | KATZ | WILLIAMS

If not required, then what are best practices?

SWEET | STEVENS | KATZ | WILLIAMS

Planning Ahead

* Set backup frequency to better plan data breach response.
* Plan for remote tracking or lost devices and securing authority to remotely wipe the contents of lost devices without other approval.
* Train staff to utilize approved cloud based storage instead of thumb drives for transferring files.
* Plan clean-up of downloaded files and other cached data at regular intervals.
* Password protect and/or encrypt data on company owned devices.
* Adopt policies and procedures for safeguarding data on employee owned devices.

SWEET | STEVENS | KATZ | WILLIAMS

Commandment 6 - Destroy Irrelevant And Outdated Records

* Should have a records retention and destruction policy and all employees should be trained to follow it.

* Tech department and administration need to work together to establish parameters for each department that everyone is capable of following.

* This ensures that data that is not longer relevant is destroyed, freeing up space and resources, but importantly removing any risk associated with data security.

SWEET | STEVENS | KATZ | WILLIAMS

Related: Destroy Temporary Data

* Examples: Chat logs, video surveillance, voicemails, text messages, fax cover sheets, post-it notes, etc.

* Define "records" to exclude these temporary data sources in record retention policy.

* Even in litigation - if the data doesn't exist anymore, it can't be subject to discovery.

Commandment 7 - Mind The Meta Data

* The internal data on files can tell who created the file, when it was edited, what changes were made, who sent a document, etc.

* This may become relevant in litigation. It can also be key to a RTK request.

* Under RTK, must provide document in the form requested if it exists in the form requested. (e.g. Can't turn MS Word file into PDF prior to sending if request is for the MS Word file).

* When sending files outside the organization, use metadata tools to clean meta data from the file prior to sending.

Commandment 8 - Adopt and Enforce A Mobile Device Policy

* Require all employees to utilize data security standards on their personal devices.

* These include passwords on devices, and ensuring that sensitive data is never stored locally on a personal device.

* Also includes provisions for the termination of access upon retirement or separation to ensure data integrity.

SWEET | STEVENS | KATZ | WILLIAMS

More on Mobile Devices

* Data belonging to the organization that is stored on a personal mobile device is still subject to RTK, if you work with the government.

* Data stored on personal mobile phones is subject to discovery in the event of litigation.

* Need to utilize approved resources only to ensure that the data needed can be quickly recovered, preserved, and produced.

Commandment 9 - Emails Are A Record of Operations

* Always use business/organization account, not personal account, to conduct business (including board members).

* Utilize an email archiver to retain a searchable record of all messages into and out of the organization.

* Staff MUST be trained on the level of professionalism needed over email. Don't write anything you wouldn't want to see in litigation.

* Work with staff on when to speak on the phone, or in person, instead of utilizing email.

SWEET | STEVENS | KATZ | WILLIAMS

Commandment 10 - Establish a Culture of Data Security

* Establish a culture where security matters - from passwords, to encryption, to data back-ups.

* Don't just turn the other way when you find out that an employee is storing data in an unapproved resource.

* The only way data stays secure in large organizations is with team buy-in, where all employees are aware of expectations and policies.

SWEET | STEVENS | KATZ | WILLIAMS

The 10 Commandments of Data Security and Data Management

Presented by:
Mark Cheramie Walz

www.tinyurl.com/BucksOct7

SWEET | STEVENS | KATZ | WILLIAMS