Security and Compliance for Municipal Government

Greg Bugbee, CISSP, Chief Technology Officer

novusinsight.com
Agenda & Topics

- Introductions
- Common data types in municipalities
  - PII (Personally Identifiable Information)
  - PHI (Personal Health Information) vs. HIPAA
  - FERPA
  - CJIS
  - PCI
- How to identify and locate sensitive data
- Insurance and sensitive data records
- Baseline standards for information system protection
- How to protect sensitive data with readily available tools
- Record retention and discovery
Presenter – Greg Bugbee, Novus Insight

About Novus Insight:

- Based in East Hartford, Connecticut
- Began as IT department of a nonprofit (CT Center for Advanced Technology)
- Technology services provider & consultant
  - Security, compliance, and business process consulting
  - IT managed support
  - Private cloud hosting
  - Application development & data consulting
- Created the Connecticut Municipal Cloud – a hybrid cloud for municipal, education, and nonprofit use
About You

We’d like to get to know you! Please...

1. Introduce yourself and municipality

2. What type of sensitive information do you deal with?
   A. PII
   B. PHI
   C. HIPAA
   D. CJIS
   E. Other
   F. All of the above
Why is sensitive information targeted?

• Information is worth money – a lot of money
• Certain data types are worth more than others
  o Facebook account – $5
  o A single medical record – $1,000
• Goal is to get a complete portfolio of information on a person
• With a complete portfolio, identity theft can take place because the hackers have enough information available to recreate the persona with the fake accounts they have access to.
How Much Is My PII Worth?

$1,200
is all you are worth on the dark web
Hecked accounts of these popular brands and stolen personal info are for sale on the dark web. The Dark Web Market Price Index tracks their average sale price, showing fraudsters can buy up someone’s entire online identity for just $1,200.

<table>
<thead>
<tr>
<th>Category</th>
<th>Online Shopping</th>
<th>Travel</th>
<th>Entertainment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subtotal</td>
<td>$164.65</td>
<td>$45.53</td>
<td>$28.59</td>
</tr>
<tr>
<td>Amazon</td>
<td>Walmart</td>
<td>eBay</td>
<td>Sears</td>
</tr>
<tr>
<td>Coors</td>
<td>Macy's</td>
<td>Expedia</td>
<td>Booking.com</td>
</tr>
<tr>
<td>UBER</td>
<td>Booking.com</td>
<td>Apple</td>
<td>NETFLIX</td>
</tr>
<tr>
<td>Coors</td>
<td>Expedia</td>
<td>Spotify</td>
<td>Netflix</td>
</tr>
<tr>
<td>email</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Category</th>
<th>Personal Finance</th>
<th>Social Media</th>
<th>Proof of Identity</th>
<th>Communication</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subtotal</td>
<td>$710.65</td>
<td>$10.21</td>
<td>$92.20</td>
<td>$72.17</td>
</tr>
<tr>
<td>PayPal</td>
<td>Facebook</td>
<td>LinkedIn</td>
<td>Verizon</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>AT&amp;T</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>T-Mobile</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Category</th>
<th>Delivery</th>
<th>Food Delivery</th>
<th>Email</th>
<th>Dating</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subtotal</td>
<td>$15.59</td>
<td>$12.80</td>
<td>$9.53</td>
<td>$8.82</td>
</tr>
<tr>
<td>DHL</td>
<td>Grubhub</td>
<td>Aol</td>
<td>Yahoo</td>
<td>Match.com</td>
</tr>
<tr>
<td>FedEx</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Source: Dark web market listings collected on 9-10 February, 2016. Markets monitored were Dread, Ps on R, and Wall Street Market. Prices collected in USD as displayed on listings.
1. Complete medical information – up to $1,000
   • Medical information is targeted for prescription fraud, claims fraud, and treatment fraud under an assumed identity
   • Medical records often include a treasure trove of linkable information such as SSN, address, birthday, etc.
   • Unlike credit cards and SSN, medical records can’t be cancelled

2. Online banking accounts and payment services are very attractive - Avg. $250
   • Credit cards are easily cancelled, bank accounts can be drained easily with minimal recourse

3. Anything with a photo ID and proof of address: $15 – $65
   • Stolen passports are not typically used for travel purposes
   • Passports and driver’s licenses are often stolen and used for money laundering and setup of online accounts
   • Very few mechanisms to alert people if a copy of their passport has been stolen
   • A real, physical passport – $13,500
Attorney/Client communications
Life Safety/Critical Infrastructure
HIPAA/PHI
PCI
PII, PHI
SCADA/Critical Infrastructure
Banking
SSN/PII PHI, CJIS
Personal finance
Employment records
FOIA Record Retention/Discovery

Town of Winthrop
Pop. 18,688

Novus Insight, Inc.
222 Pitkin Street, East Hartford, CT 06108
860.282.4200
novusinsight.com
Personally Identifiable Information (PII)

PII is a broad term that encompasses two main categories:

- **PII**
  - PII means information that can be used to distinguish or trace an individual’s identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual.
  - Anything that can be used to identify a person - name with a combination of address, phone number, etc.
  - Not all PII needs to be protected. In fact, much of it is public information.

- **Protected PII**
  - Protected PII means an individual’s first name or first initial and last name in combination with any one or more types of information, including, but not limited to:
    - Social security number, passport number, credit card numbers, clearances, bank numbers, biometrics, date and place of birth, mother’s maiden name, criminal, medical and financial records, educational transcripts.
    - This does not include PII that is required by law to be disclosed.
18 identifiers that make health information PHI are:

- Names
- Dates, except year
- Telephone numbers
- Geographic data
- FAX numbers
- Social Security numbers
- Email addresses
- Medical record numbers
- Account numbers
- Health plan beneficiary numbers
- Certificate / license numbers
- Vehicle identifiers and serial numbers including license plates
- Web URLs
- Device identifiers and serial numbers
- Internet protocol addresses
- Full face photos and comparable images
- Biometric identifiers (i.e. – retinal scan, fingerprints)
- Any unique identifying number or code
HIPAA vs. PHI

• HIPAA applies to “Covered Entities,” including:
  o Health plans
  o Health care clearinghouses
  o Health care providers who conduct certain financial and administrative transactions electronically. These electronic transactions are those for which standards have been adopted by the Secretary under HIPAA, such as electronic billing and fund transfers.
  o Business associates of the above organizations who store, process, or transmit PHI (technology providers, processors, etc.)

• HIPAA does not apply to employers except for HR instances related to insurance. HR asks insurance or healthcare provider about employee, or self-insuring organizations.

• Workers’ compensation, sick leave documentation, etc. may be PHI but not covered under HIPAA.

• Public agencies that deliver social security or welfare benefits are also exempt under HIPAA.
PHI Laws

Each state has their own laws regarding patient access to records, record retention, and security handling.

At a minimum, PHI requires the same handling and reporting requirements as PII, but always check state laws.
• Not all ambulance services are covered entities and subject to HIPAA. If the service does not engage in any HIPAA-covered electronic transactions (the most common one being electronic billing of Medicare, Medicaid, or other insurance companies, either in-house or through a third-party) then the service is not a covered entity and the requirements of HIPAA do not apply.

• Ambulance services will typically fall under HIPAA. This introduces a major compliance program if the municipality sponsors an ambulance service, or if fire department EMT services bill insurance for services.
FERPA – Family Education Rights and Privacy Act

- Protects the privacy of student education records. It is important to note that when a child is in school, behavior, school nurse records, grades, etc., all fall under FERPA.
- Schools must receive funds under an applicable program of the Department of Education.
- Gives parents rights to their children’s educational records. When the student reaches 18, the rights transfer to the student.
- Protects student information from disclosure.
- Parents also have the right to request that records be corrected if inaccurate.
- Schools must be careful as to ensure 3rd parties are properly handling FERPA data on their behalf.
Massachusetts specific law that builds upon FERPA
Provides clarity and definition related to:
- Authorized school personnel
- Responsible party for security and privacy
- Destruction of records – 60 years
- Access logging
- Noncustodial parent access
- Third party access
• Criminal Justice Purposes
  o includes criminal identification activities and the collection, storage, and dissemination of criminal history record information
  o applies to law enforcement and justice-related agencies
  ❖ Detection
  ❖ Apprehension
  ❖ Prosecution
  ❖ Adjudication
  ❖ Detention

  ❖ Correctional supervision
  ❖ Pre/Post trial release
  ❖ Rehabilitation of accused persons

• Non-Criminal Justice Purposes
  o related to the administration of criminal justice, including employment suitability, licensing determinations, immigration, and naturalization matters, and national security clearances
  o applies to many agencies/organizations – HR departments, schools, municipalities, etc.
Municipal departments potentially subject to CJIS audit:

- Police departments
- HR departments (fingerprints, background checks)
- School departments (background checks, fingerprints)
- Youth services/Parks and Rec (background checks)

Note:

- Background checks do not always qualify as CJIS.
- Viewing a pass/fail background check from a provider is not CJIS.
- Printing a full criminal history would be subject to CJIS.
• **Information Exchange Agreements** – If you’re sharing CJIS-protected data with another organization, you must have a written agreement between the organizations that you will both comply with CJIS security standards.

• **Security Awareness Training** – Any employees handling CJIS data must have security training within the first six months of being assigned to their role and additional training every other year moving forward.

• **Incident Response** – You must have safeguards in place to detect and contain any data breaches. You also need data recovery measures in place. Any data breach must be reported to the appropriate authorities.

• **Auditing and Accountability** – You should implement audit controls to monitor who is accessing data, when they are accessing it, and for what purpose they are accessing it. This information should be logged for any future audits.

• **Access Control** – Under CJIS policy area 5, you must have the ability to control who can access your data. This can include controlling who can access, upload, download, transfer, and delete secure data. It also impacts your login management systems, remote access controls, and more.

• **Identification and Authentication** – To access CJIS data, users must align with CJIS login credential standards, meet password requirements, and use advanced authentication methods like one-time passwords and multi-factor authentication.
CJIS – Requirements (cont.)

- **Configuration Management** – Per area 7, only authorized users can make configuration adjustments, like upgrading systems or initiating modifications.

- **Media Protection** – CJIS-related data must be protected in all forms, digital & physical, both in transit and at rest. Equipment that is no longer being used by your organization must be sanitized and disposed according to CJIS policies.

- **Physical Protection** – The physical location for stored CJIS data must be secured at all times, preventing access from unauthorized persons.

- **System and Communications Protection and Information Integrity** – Your organization’s systems and communications need to be protected just like your data. This policy section outlines the steps you must take to protect your systems, like encryption, network security, data breach detection measures, and more.

- **Formal Audits** – If you use and manage CJIS data, you are subject to audits a minimum every three years by either the CJIS Audit Unit (CAU) or the CJIS Systems Agency (CSA) for your state.

- **Personnel Security** – Everyone associated with your organization – from employees to contractors and subcontractors – must submit to security screenings and national fingerprint-based record checks.

- **Mobile Devices** – Even your employees’ mobile devices (like smartphones and tablets) are subject to CJIS oversight. You must establish usage restrictions, and authorize, monitor, and control access to your systems via these devices.
Many municipalities think because they outsource credit card processing that they are exempt from PCI compliance. This is not true.

PCI compliance applies to any organization, regardless of size or number of transactions, that accepts, transmits, or stores any cardholder data.

You are responsible if you have card readers or manually enter credit card data on behalf of constituents.
Municipalities accepting credit cards are required to complete a self assessment on how they manage credit card data.

If required, municipalities must complete a vulnerability scan.

For a fully outsourced organization, a 14-question self attestation is necessary.

If cards are taken, questions increase up to 139.

https://www.pcicomplianceguide.org/category/pci-101/
5 Minute Break
Identifying Sensitive Data

So, you think you have one or more of the data types mentioned in this presentation. How should you inventory it?

Options for sensitive information discovery:

1. Microsoft 365 - E5 license or EMS E5 license required
   - Microsoft Cloud Access Security/Defender for Cloud Apps
   - Azure Information Protection
   - Azure Information Protection Scanner (scans on-premises file servers)

2. Google Workspaces
   - Cloud DLP (available in Enterprise plans)

3. CU Spider
   - Open source PII Scanning Application
   - Free to use
   - No support
   - Will not scan cloud storage

4. Varonis
   - Cloud and on-premises data discovery, tracking, and auditing tool
   - Can be expensive compared to other tools
   - Requires server hardware
Maintaining an accurate inventory of sensitive data records is critical to rightsizing insurance polices:

• Insurance providers will ask, “How many unique sensitive records do you have?”

• They use this data to calculate premiums and understand how many individuals would require identity protection in the event of a breach.

• It is important to include not only the data stored by the municipality but also the data given to 3rd parties on behalf of the municipality. If you enter data into a system, you are responsible for the security of that data. If you have a login, you are a data owner/operator; the third party is simply a custodian. They have responsibility, but in a breach, everyone is investigated.

• For premium calculation, $170-$220 per record is a good rule to follow.

• Remember to include archival data, sensitive information related to vendors and contractors, etc.
You’ve discovered sensitive data; how should you protect it?

• **Limit access** – Make sure only authorized parties are allowed to handle sensitive data.

• **Provide training** – Each security requirement we discussed today has training associated with it. If people handling credit cards are not trained, they need go through PCI handling training.

• **Create procedures** – When left to their own devices, people will take the easy route. A simple modification to a process such as the use of a dry erase board for jotting credit cards vs. a notebook or Excel file will make all the difference.

• **Audit everything** – Make sure there is an audit trail for all transactions. Audit trails must be traced back to a person. That means no generic accounts.

• **Protect the information system** – Patch and scan for vulnerabilities.

• **Keep tabs on where sensitive data goes** – Are there systems in place to prevent sensitive data from being downloaded to unauthorized devices? Would you know if a user copied sensitive data to their personal email or cloud account?

• **Encrypt** – Encryption makes it so that sensitive data can’t be read by someone without the key to unlock the data. Sensitive data should never be transmitted without encryption. Regular email is not adequate for transmitting sensitive data. Data must be encrypted at rest - when stored on computers, in backup files, and on servers.
Encryption requires an investment in technology.

**Transmission Technology:**
- Most email platforms have some type of email encryption system available. Both Microsoft 365 and Google Workspaces allow for encrypted emails to be sent. Users need to be trained to work with encrypted messages. The recipient signs into a message viewer to view the messages, creating an audit trail.
- Secure links can also be used to share files with trusted and verified external parties.
- Wireless connections must be encrypted – WPA2/3.
- Always look for the lock icon on websites to make sure they are encrypted.

**Drive Encryption:**
- Hard drives of workstations and laptops should be encrypted using BitLocker. BitLocker is included with Microsoft Windows. If a computer is lost, stolen, or improperly disposed of, the data on the hard drive can’t be read.
- USB drives should also be encrypted using BitLocker to Go or built-in encryption.

**Services** – Validate the type of encryption used for backup, cloud, and other 3rd party services.

**Backup** – Disk and external backup drives must be encrypted.

If CJIS data is present, all encryption must be FIPS 140-2 validated. FIPS encryption requires special configuration and technology to implement.
Data Loss Prevention (DLP):

- Scans files and emails for PII or other patterns that match sensitive data
- Prevents information from being moved, copied, transmitted, etc., without proper authorization and encryption
- Included with select Microsoft 365, Google Workspace, and through 3rd party services/software
- Endpoint DLP prevents files from being copied to external storage or cloud platforms
- Modern DLP platforms can even look at PDF forms and based on image patterns determine if it is a W2 or other type of form with/without sensitive data
- Requires configuration, training, and tuning to reduce false positives
- Provides alerting on file transfers and attempts by users to transmit sensitive information
Information Rights Management (IRM):

- Allows files to be classified and protected
- Can scan files to detect sensitive information, label them as such, and encrypt them
- When IRM is used, encryption applies to the file, “wrapping” it and requiring those accessing it to unlock it with a username, password, and MFA.
- Protection follows the file - if it is copied to a USB drive, it is protected even if the drive isn’t encrypted
- Access can be revoked, even remotely. Once access is revoked, the file is useless.
- Requires data classification, end user training, and appropriate licensing. Included with Microsoft 365 and 3rd party software/services.
- Files can be automatically classified based on data types, folder they reside in, and other factors.
Baseline Standards

• Even with fancy encryption tools, we still need to make sure our information system is secure.  
  *Remember: Users hold the keys to unlocking encrypted data – we need to still protect the keys and keyholders.*

• Baseline standards can help secure systems and ensure systems are configured in a consistent manner.

• The Mass Cyber Center has developed a 4-goal minimum baseline for municipal information systems.

• The four goals include:
  - Training
  - Regional awareness and threat sharing
  - Incident response planning
  - Secure technology environment and best practices
Authoritative source for baseline configurations and critical security controls is CIS.

Aligning with the CIS 18 Critical Security Controls is highly recommended for all municipalities.

CIS also provides detailed secure baseline configuration guides for many of the technology platforms in use at your municipality – Microsoft 365, Window 10, Windows Server, SQL, Linux, and firewall platforms. These are known as CIS Benchmarks.

https://www.cisecurity.org/controls/cis-controls-list/
• Simple checklist of basic cyber activities designed for leadership and IT professionals

• Use the essentials to guide and track progress of your cyber program

• More information: https://www.cisa.gov/cyber-essentials
Record Retention

- Massachusetts requires municipal governments to retain records for prescribed periods of time.
- The “Quick Guide” is 128 pages long and available here: https://www.sec.state.ma.us/arc/arcpdf/Municipal_Retention_Schedule_20200406.pdf
- With the amount of electronic information floating around municipalities, it is a challenge to keep track of it all.
- Using tools like retention tags can help automate the retention process.
- Similar to sensitive data, data that needs to be kept can be tagged with retention tags.
- Once tags have been applied, the data cannot be deleted until the time period expires, or the tag is removed.
- Microsoft 365 features retention tags, retention reporting and record management tools for addressing complicated record structures.
- Retention tags can apply to emails, documents, folders, or any files that need preserving.
- Requires Microsoft 365 subscription and files must be in the cloud.
Massachusetts public records laws requires every municipality to designate a Records Access Officer to assist requesters in obtaining public records.

Public records requests are happening more frequently and are becoming more time consuming for RAOs to manage.

E-Discovery tools can ease this burden by providing search capacity across email, files, and chat messages.

Manually going from machine to machine to search email accounts is time consuming and not effective. E-Discovery needs to take place at the server level, not the endpoint.

Both Google and Microsoft offer robust e-Discovery tools with their enterprise platforms.

When coupled with record retention, e-discovery becomes a powerful tool for providing requesters with information and an audit trail of how the search was conducted.

E-Discovery allows for external users such as attorneys to review the export and redact privileged information before final distribution to the requester.
Key Takeaways

• Sensitive information is targeted by hackers because it is worth a lot of money. With a complete portfolio, hackers can steal a person’s identity because they have enough information available to recreate a persona.

• PII encompasses two main categories: PII & protected PII. Protected PII means an individual’s first name or first initial and last name in combination with any one or more of certain types of information.

• PHI typically requires at least the same handling and reporting requirements as PII, though each state has their own laws regarding patient access to records, record retention, and security handling.

• HIPAA does not apply to employers except for HR instances related to insurance. HR asks insurance or healthcare provider about employee, or self-insuring organizations.

• Massachusetts state law 603 CMR 23.00 provides additional clarity and definition related to FERPA data handling.

• CJIS data can be for criminal justice purposes or non-criminal just purposes. Handling requirements vary accordingly. Municipal departments potentially subjected to CJIS include Police, Schools, HR, Youth Services.

• Municipalities are not exempt from PCI compliance just because they outsource credit card processing.

• Maintaining an accurate inventory of sensitive data records is critical to right sizing insurance polices.

• Protect sensitive data by limiting access, providing training, creating procedures, auditing everything, and via encryption.

• Massachusetts requires municipal governments to retain records for a prescribed period of time.
Q & A

Thank you!

Greg Bugbee, CISSP
gbugbee@novusinsight.com
860.282.4200
Next workshop will focus on:

Resources available to Massachusetts municipalities
Resources

- MS-ISAC- Cyber resources for local government - [https://www.cisecurity.org/ms-isac/](https://www.cisecurity.org/ms-isac/)
- CISA- Cybersecurity & Infrastructure Security Agency - [https://www.cisa.gov/](https://www.cisa.gov/)
- DOL Cyber guidelines - [Cyber Recommendations](#)
- Minimum Cyber Baselines - [Minimum Baseline of Cybersecurity for Municipalities | Mass Cyber Center](#)
- KnowBe4 Free Tools - [https://www.knowbe4.com/free-it-security-tools](https://www.knowbe4.com/free-it-security-tools) (see ransomware and USB security test for incident response scenarios)
- Secure File Sharing – Answers to Common Questions: [Answers to Common Secure File Sharing Questions (ftptoday.com)](#)
- PCI Compliance Guide Blog: [PCI 101 Archives - PCI Compliance Guide](#)