MassCyberCenter
at the MassTech Collaborative

Robinson+Cole

Cybersecurity Incident Response Plan Workshops for Municipalities

Workshop 2: Guidance Materials and Tabletop Exercise

20828304v1

2020

Recap from Workshop 1

Cyber risk **impacts** our municipalities, healthcare, politics, economics, professional and personal lives. Because of its impact, cybersecurity risk continues to be **front and center** on the minds of citizens. Are municipalities adequately equipped to know what **questions** to ask, what to do about it or how to become more **knowledgeable** in this critical area?

MassCyberCenter at the MassTech Collaborative

Robinson+Cole

Recap from Workshop 1 (cont'd)

What are the threats to a municipality's operations, infrastructure and/or data?

- Unintended disclosures by employees; employee error
- Hacking/Malware/Ransomware
- Insider Wrong-Doing
- Zero Day Vulnerabilities
- Physical Loss
- Portable Device/Removable Media

- **Technology Intrusions**
  - Phishing/Spear-Phishing Schemes
  - Man-in-the-Middle Attacks
  - Wire Transfer Fraud
  - Skimming Incidents
  - Vendors/Subcontractors –Poor Security Protocols/Standards

Recent Attacks on Municipalities

What makes local governments attractive targets for cyber attacks?

- They house private data
- Security often isn't a top (or well-funded) priority
- Attacks have been successful
- Attacks against local governments are public-facing and attacks can provide a potent outlet, resulting in a variety of disruptive, public consequences

MassCyberCenter at the MassTech Collaborative

Robinson+Cole

Recent Attacks on Municipalities

- City of Hartford, CT
  - Ransomware attack over labor day weekend that caused delay in start of school
  - Still investigating
  - Caused significant disruption
  - Including first response and critical services

Recent Attacks on Municipalities

Alabama City Hit with Ransomware

BY LINN FOSTER FREEDMAN ON JUNE 11, 2020
POSTED IN CYBERSECURITY

On June 5, 2020, Florence, Alabama's information technology systems were hit with ransomware by the DoppelPaymer group demanding a ransom payment of $378,000 in bitcoin. Mayor Steve Holt confirmed that the attack shut down the city's email system, and that the city used an outside firm to negotiate the payment of a lower ransom of close to $300,000 to avoid the publishing of the information of citizens on the internet by the attackers.

Recent Attacks on Municipalities (cont'd)

City of Atlanta

The cyberattack that crippled Atlanta was one of the more noteworthy hacks of a public entity, but the Georgia state capital certainly hasn't been the only city targeted by cyber criminals in recent months – or even the one with the biggest ransom demand.

Recent Attacks on Municipalities (cont'd)

Click2Gov Portal Compromised in Eight Cities

BY LINN FOSTER FREEDMAN ON SEPTEMBER 26, 2019
POSTED IN CYBERSECURITY

Many cities in the United States utilize a self-pay portal for residents to pay bills online, known as Click2Gov. Click2Gov was compromised in 2017 and 2018, when hackers were able to access over 300,000 payment cards and reportedly made more than $2 million in the heist.

It is being reported this week by security researchers that starting sometime in August, Click2Gov systems have been attacked again, compromising the systems in eight cities so far. Six of those cities – Deerfield Beach, Florida, Palm Bay, Florida, Milton, Florida, Bakersfield, California, Coral Springs, Florida, and Ames, Iowa – also were hit in the previous attack.

Recent Attacks on Municipalities (cont'd)

Twenty-three Texas Municipalities Crushed by Coordinated Ransomware Attack

BY LINN FOSTER FREEDMAN ON AUGUST 22, 2019
POSTED IN CYBERSECURITY

We have definitely seen an uptick in the number of ransomware attacks against municipalities around the country. Thus far, the attacks have been against single cities, towns, and court systems, and recently against a Louisiana school system. The pace and coordination of these attacks have magnified, as evidenced by the coordinated and simultaneous ransomware attacks this … Continue Reading

Recent Attacks on Municipalities (cont'd)

City of Baltimore Shuts Down Servers Following Ransomware Attack

BY LINN FOSTER FREEDMAN ON MAY 9, 2019
POSTED IN CYBERSECURITY

Another city, another ransomware attack. Cities and municipalities continue to be targeted with ransomware campaigns. Fortunately, in this case, essential services such as fire, police, Emergency Medical Services and 311 service were still operational despite the attack. According to a tweet by Mayor Bernard Young, Baltimore shut down its servers in response to the ransomware … Continue Reading

Recent Attacks on Municipalities (cont'd)

Orange County, NC Hit with Ransomware Attack

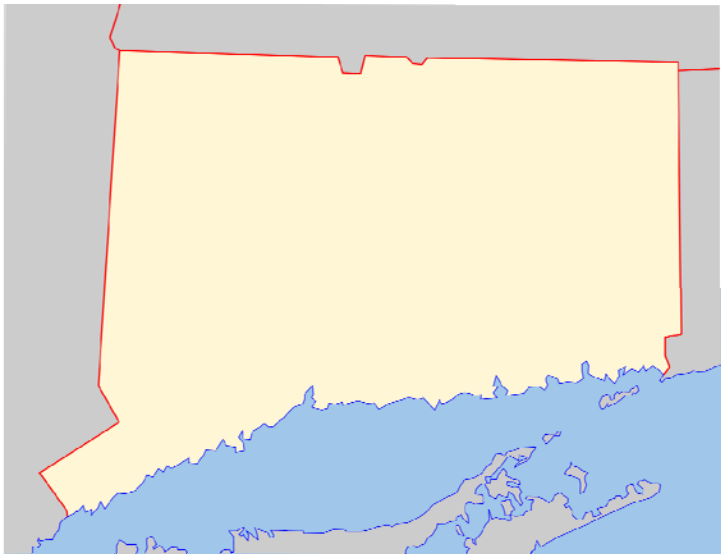
BY LINN FOSTER FREEDMAN ON MARCH 21, 2019
POSTED IN CYBERSECURITY

The headlines of hacking incidents against counties, cities and towns are racking up like the retail space was several years ago. The hackers have targeted state and municipalities to wreak their havoc. This week, Orange County, NC was hit with a ransomware attack that brought it to its knees. As a result of the attack, … Continue Reading

Recent Attacks on Municipalities (cont'd)

$2 Million Stolen from Town of Farmington, Connecticut Accounts

- A network originating in China had targeted municipal customers and diverted online payments.



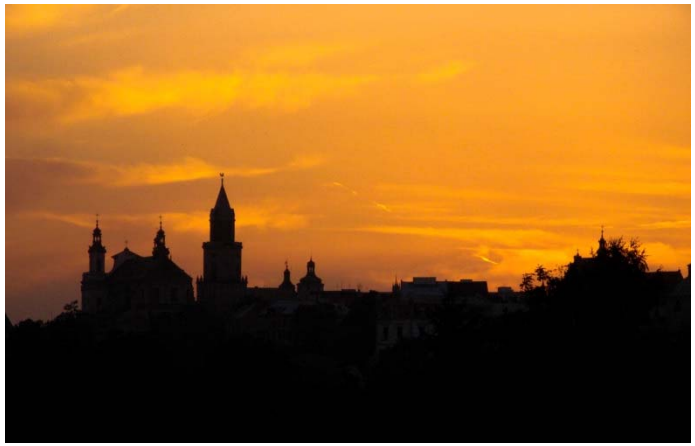
Recent Attacks on Municipalities (cont'd)

City of Leeds, Alabama

- Paid ransomware criminals $12,000 in Bitcoin to regain control of their systems

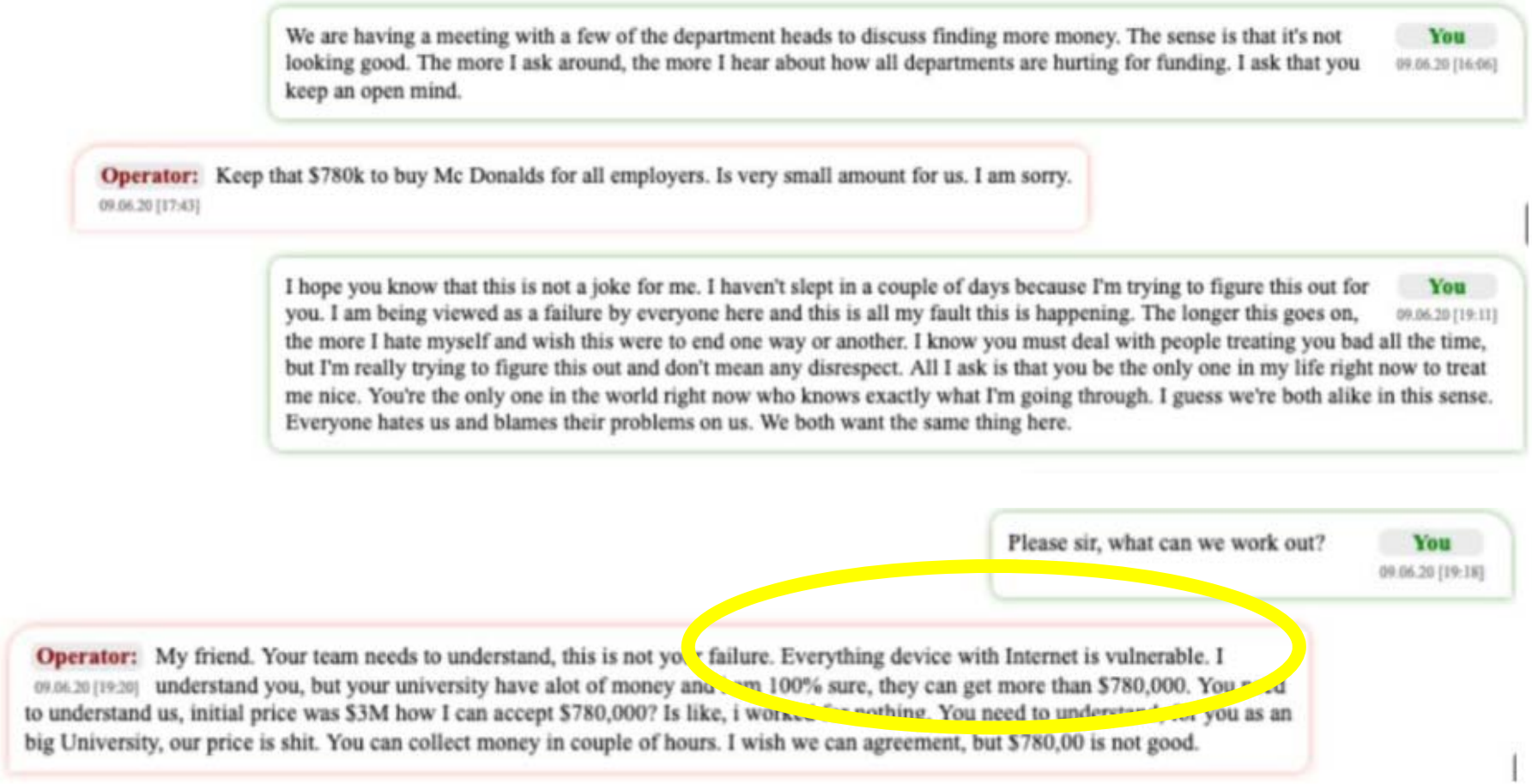
City of Leominster, Massachusetts

- Paid $10,000 following a ransomware attack on the city's school district



Recent Example of Ransomware Attack and Negotiation

University of California at San Francisco's COVID-19 Research Center -118 Bitcoins (about $1.35 million)



Are there any new threats to consider during the pandemic with your employees working from home?

Security Challenges Related to COVID-19 Pandemic

- Telework – more exposed systems and data;
- Unpatched and out-of-date systems, and IoT (Internet of Things) devices at home enabled and listening (e.g., home security cameras, Alexa, etc.)
- Increased use of (insecure) personal mobile devices;
- Unprotected wireless networks used to join VPNs and remotely access corporate networks and sensitive data;
- Increase in social engineering & phishing attempts using COVID19-themed phishing messages to conduct ransomware attacks or implant malware;
- Large-scale stimulus fraud and stimulus-themed spear-phishing campaigns;
- Violations of confidentiality – who's listening? IoT concerns;
- Is your data properly and regularly backed up?;
- Increased collection of health information from employees (e.g., temperature checks, answers to screening questions, contact tracing apps).

Internet of Things – vulnerable to hackers…

Why would people hack IoT devices?

- It's a way into your network….
  - Is Alexa listening in on your confidential work conversations?
  - Can your IoT devices such as your smart doorbell & camera security system be hacked? Yes
  - Other smart devices also vulnerable – smart TVs, beds, doorbells, thermostats, dog feeders, garage door openers, refrigerators….

Security Challenges Related to COVID-19 Pandemic (cont'd)

- Corporate cybersecurity leaders are concerned that it may be easier for employees to expose data or create openings for hackers while working remotely during the pandemic
- Companies have limited capabilities to monitor certain violations of data policies
- Distracted workers also may be more likely to fall for common scams
- Employees can pose cybersecurity risks through mistakes or deliberate attempts to cause harm to a company
  - 45% of people working remotely said their companies provided no special training on securing devices at home, according to a survey from International Business Machines Corp
  - 42% said they handle personal identifiable information such as Social Security numbers or financial data in their job

COVID-19 Cyber Threats

Pandemic Lessons Learned

1. **Coronavirus Phishing Activity**: Most organizations reported a mass flooding (600%) of COVID Phishing Email campaigns & Business Email Compromise – Stimulus Check Scams
2. **Fake Websites & Infection Tracking Sites:** Numerous fake & fraudulent domains and Website immediately stood up including fake infection tracking sites to instill fear.
3. **Remote Access & Virtual Collaboration platforms being targeted**: As agencies worked to increase VPN and remote collaboration tools malicious cyber actors worked to exploit misconfigurations or vulnerabilities. Zoom Bombing
4. **Increase in Coronavirus-related Cyberattacks:** Malware (COVIDLock, Emotet, AZORult, Qbot, Trickbot, FormBook, Nanocore RAT,Ransomware, DDOS, Malspam) and credential harvesting malware. Criminal to Nation-state Activity
5. **Insider Threats:** Primarily from the non-malicious insider who inadvertently exposed the agency to a breach or leaked agency credentials to malicious actors

Actions Items from Workshop 1

Develop an Incident Response Plan

- Determine who the stakeholders are
- Determine what decisions need to be made
- Establish an Incident Response Team
  - Determine roles and responsibilities
- Obtain and select insurance approved vendors
- Distribute the Plan and review it at least once annually

WHAT'S NEXT… conduct a tabletop exercise!

Tabletop Exercise

Here's the scenario:

8:32 a.m. You receive a phone call from an employee who has arrived at the office and attempted to log into the city's systems. However, the employee says that the system appears "locked" and they are unable to access the network or any city data.

8:35 a.m. IT staff confirms that the system has been attacked by ransomware.

Two days later: IT staff migrates to the City's backup system and does not pay the ransom. However, the hackers provide proof of life that all of your HR data has been copied and will be published on the Internet unless you pay them $500,000.

What do you do?

Now What?

What can you do to protect your municipality?

Determine where your high-risk data is, where it is going, and the overall ***data flow*** so that you know how to protect it (and ***who*** to protect it from)

Identifying and Protecting High-Risk Data

- **Personally Identifiable Information**
  - Includes SS #, state-issued ID #, mother's maiden name, driver's license #, passport #, credit history, criminal history
- **Name & Contact Information**
  - Includes initials, address, telephone number, e-mail address, mobile number, date of birth
- **Personal Characteristics**
  - Includes age, gender, marital status, nationality, sexual orientation, race, ethnicity, religious beliefs

Identifying and Protecting High-Risk Data (cont'd)

- **Financial Data**
  - Includes credit, ATM, debit card #s, bank accounts, payment card information, PINs, magnetic stripe data, security codes, access codes, passwords
- **Health & Insurance Account Information**
  - Includes health status and history, disease status, medical treatment, diagnoses, prescriptions, insurance account #, Medicare and Medicaid information
- **Employment Information**
  - Includes income, salary, service fees, compensation information, background check information

Implementing an Enterprise-Wide Data Privacy & Security Plan

- **Map your high-risk data**
- **Conduct a security risk assessment**
- **Protect your data**
    - Paper records
    - Stored in locked areas
    - Retain only as necessary
    - Electronic records
    - Segregate highly sensitive data
    - Access controls & user authentication
- **Data retention and destruction program**

Implementing an Enterprise-Wide Data Privacy & Security Plan (cont'd)

- **Policies and procedures as legally required to address**
    - Privacy
    - Security
- **Technology to secure it**
    - Encryption
    - Firewalls
- **Educate users and employees**
- **Designate Privacy & Security Team**
- **Designate Incident Response Team**

Implementing an Enterprise-Wide Data Privacy & Security Plan (cont'd) – Vendor Management

- **Map all vendors who have access to PI**
  - Follow the data

- **Put vendor confidentiality agreements in place with each**
  - Payroll/HR
  - Benefits/insurance
  - Website hosting provider
  - Cloud service provider
  - IT service providers
  - CPAs/Legal

Implementing an Enterprise-Wide Data Privacy & Security Plan (cont'd) – Education & Training

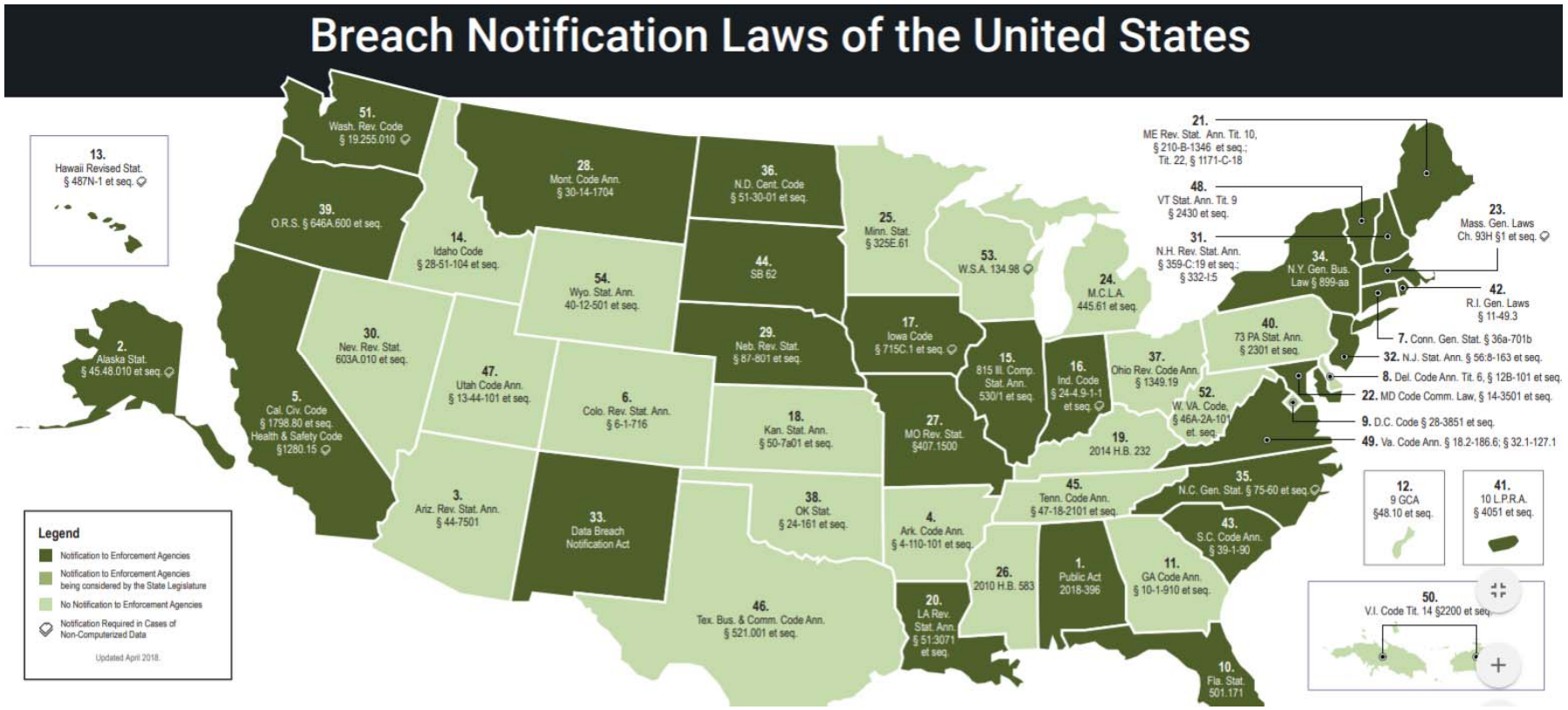
- Conduct employee and user education and training at least yearly on data privacy and security, risks and how to protect your organization
- Keep records of the training
- Each employee/user should sign an acknowledgement form after attending the training

What should you do if your municipality is a victim of one of these attacks?
What are your legal obligations?

MassCyberCenter at the MassTech Collaborative

Robinson+Cole

50 State Data Breach Notification Laws



MassCyberCenter at the MassTech Collaborative

Robinson+Cole

How Do You Engage the Leadership of your municipality?

As a leader in your municipality's IT or Security organization, you can help protect against cyber threats by asking the 'right' questions:

- How is our executive leadership informed about the current impact of cyber risks to the municipality?
- What is the business impact of cyber risks to our municipality?
- What is our plan to address identified risks?
- How does our cybersecurity program apply industry standards and best practices?
- How many and what types of cyber incidents do we detect in a normal week?
- What is our threshold for notifying our executive leadership of a cyber incident?
- How comprehensive is our cyber incident response plan?
  - How often is it tested?
- Does our municipality have adequate cybersecurity insurance?

Key cyber risk management concepts that all municipalities need to know

- Incorporate cyber risks into existing risk management and governance process
- Elevate cyber risk management discussions to the Municipality leadership –cybersecurity is not only an IT issue
- Implement industry standards and best practices
- Evaluate and manage the municipality's specific cyber risks
- Provide oversight and review
- Coordinate cyber incident response planning and implement the incident response plan
- Maintain situational awareness of cyber threats, particularly threats to municipalities

Basic Cyber Hygiene

Tips for Protecting and Securing Data

- Employees should be wary of transmitting personal, health or confidential data over public Wi-Fi networks—use encryption
- If you are going to be away from your workstation for more than a few minutes, Ctrl+Alt+Del to lock your computer
- Encrypt laptops
- Limit use of USBs

Tips for Protecting and Securing Data (cont'd)

On your mobile devices…

- Install and enable security software
- Keep your security software up to date
- Research mobile applications/software BEFORE downloading
- Maintain physical control over the device
- Use complex password
- Delete/destroy all stored data before discarding or reusing a mobile device

Tips for Protecting and Securing Data (cont'd)

- On your mobile devices (cont'd)…
  - PRIVACY SETTINGS
    - Location, microphone

Tips for Protecting and Securing Data (cont'd)

When using e-mail…

- Encryption
- Verify Selected Recipients
- Use Standard Confidentiality Disclaimers
- Do not send data to personal e-mail account

Tips for Protecting and Securing Data (cont'd)

- Use of Gmail to communicate or transmit data leaves the information open to vulnerabilities, as well as potential enforcement and/or consequences for non-compliance with certain laws and regulations
- Data sent via standard Gmail is not protected
- Gmail terms state Google has access to all data transmitted through Gmail account
- Google mines all data

Tips for Protecting and Securing Data (cont'd)

- Passwords –
  - Use of complex passphrases
  - Change password as required
  - Use of passphrases

Additional Resources for Cybersecurity

- **The Sys-Admin, Audit, Network and Security Institute (SANS)**
  https://www.sans.org/security-resources/blogs
  SANS maintain a wide variety of blogs aimed at all subcategories of IT and IT Security. They also maintain one of the largest archives of webcasts featuring the who's who in Cybersecurity and Digital Forensics. Great information for folks new to the industry and expert and access to the vast majority of the content is free.

- **Global Information Assurance Certification (GIAC)**
  https://www.giac.org/
  GIAC maintains a reading room full of security white papers on numerous topics.

- **United States Computer Emergency Readiness Team**
  https://www.us-cert.gov/bsi/copyright/carnegie-mellon-university
  An online library from Carnegie Mellon's collaboration with the US Department of Homeland Security, containing loads of top-quality publications on all manner of security-related information.

Additional Resources for Cybersecurity

- **Cybrary**
  https://cybrary.it/
  Cybrary is possibly one of the best IT Security education sites on the internet. It contains full-length college course videos for everything from basic networking up to and including training for certifications, explanations of secure coding, penetration testing and everything else security related.

- **National Institute of Standards and Technology (NIST)**
  http://www.nist.gov/
  In particular, the **Computer Security Resource Center (CSRC)** (http://csrc.nist.gov)holds a collection of papers that describe security best practices, called NIST Special Publications (SPs). They also create security assessment tools.

Additional Resources for Cybersecurity

- **Robinson + Cole Blog - Data Privacy Security Insider**
  www.dataprivacyandsecurityinsider.com
  Weekly posts on cybersecurity and risk management

- **Security Now! Podcast**
  https://www.grc.com/securitynow.htm
  A weekly security-focused podcast that covers all topics from law, current events, to conference reviews and explanations of specific exploits as they are discovered in the world.

- **Krebs on Security**
  https://krebsonsecurity.com/about/
  Brian Krebs, author of Spam Nation is also one of the better-known security bloggers in the world, having written over a thousand articles on security.

- **Udemy**
  https://www.udemy.com/
  Possibly one of the biggest and least expensive resources for cybersecurity learning there is.

Linn Foster Freedman

lfreedman@rc.com

Robinson + Cole
One Financial Plaza

Suite 1430

Providence, RI 02903

401-709-3353

www.dataprivacyandsecurityinsider.com

Thank you

QUESTIONS?