Cybersecurity and Privacy Risks When Working Remotely

Wednesday, May 27, 2020
JOHN ISAZA, ESQ., FAI

Vice President, Information Governance
Access

Special thanks to Hon. Ron Hedges, who created this slide deck with me
“Although presenter is an attorney admitted to practice law, the contents on this presentation are not to be construed as legal advice.”
Agenda

1. Legal Foundation for Security Mandates
2. Risks of Working Remotely
3. Best Practices Approaches
Issues

• If an employee is ordered to work from home, what precautions has your employer taken to assure the protection of data while working from home?

• How secure is the data if security standards are lowered so the employee can access files from a remote location?

• How can the employer be sure that confidential, privileged or sensitive information will not be seen as others at home walk by the employee’s computer?

• How accountable are employers holding third party service providers for the safety of data, when presumably they are also asking their own employees to work from home?
Laying the Legal Foundation

Regulations Mandating It
Security Standards
Case Law
Agency Opinions
Regulations

- Privacy Laws
- Labor Laws
- Biometric Data Laws
- International Laws
    - Stresses that the protection of personal data remains important.
    - Emphasize GDPR has rules in place that would apply to the processing of personal data in a context like COVID-19, allowing competent public health authorities and employers to process personal data in the context of an epidemic, in accordance with national law and within the conditions set therein.
Any person or business that owns or licenses computerized data which includes private information of a resident of New York shall develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of the private information including, but not limited to, disposal of data.”

(from the NY SHIELD Act)

NIST – System Information Integrity Standards

The National Institute of Standards and Technology is a physical sciences laboratory and a non-regulatory agency of the United States Department of Commerce. Its mission is to promote innovation and industrial competitiveness. NIST’s activities are organized into laboratory programs that include nanoscale science and technology, engineering, information technology, neutron research, material measurement, and physical measurement.

Control Description
The organization handles and retains information within the information system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.

Supplemental Guidance
Information handling and retention requirements cover the full life cycle of information, in some cases extending beyond the disposal of information systems.

The National Archives and Records Administration provides guidance on records retention.

See also Data Minimization Control Standards DM 01 & 02
Case Law – None…Yet!…But…

• Zoom Agrees to Security Measures After NY AG Investigation
• Office Opened an investigation into Zoom Security Practices
• Zoom reached quick agreement to:
  ✓ “enhance encryption protocols by encrypting users’ information”
  ✓ Zoom implemented a “risk-based penetration-testing program” to spot and assess security vulnerabilities
HOWEVER, Heed Related Case Law

- Bear Stearns sought coverage for $140M payment to resolve SEC investigation alleging financial law violations
- Court held $140M was a penalty, and therefore not an insurable “loss”
- By extension, under Shield Act, a penalty for knowing or reckless misconduct could be considered a penalty NOT covered by insurance
- Shield Act penalties could be $250k per instance of failed notification to consumer of a breach
Agency Opinions


• The Department of Health and Human Services (“HHS”) and The Office for Civil Rights

Jointly published guidance, maintaining that the HIPAA covered data should continue to be protected in the same ways it would normally be protected.

The law cannot be set aside because we are in a state of emergency. If the protected health information must be shared, it should be done to the minimum extent necessary.

To ease the burden, HHS has waived sanctions and penalties for HIPAA if you are a hospital, and they have said that they will relax restrictions on sharing data using electronic means.
Agency Opinions (cont’d.)

- Y2K crisis analogy
- DOL issued reminders to employers that it was their “fiduciary duty” to make sure the systems were ready to manage the potential Y2K loss of data when it came to the administration of employee benefits, such as 401(k) plans.
- Employers in turn leaned on their third-party service providers to remind them that they too would be held accountable for services provided to the employee on their behalf, such as 401(k) administration.
- Employer and its third-party service providers would be the ones responsible for managing the crisis, as opposed to passing the buck to the employees for loss of financial data.
Risks of Working Remotely

1. Creation of Data
2. Transmission of Data
3. Storage of Data
Security Assessments

Inventory of Assets
- Physical
- Electronic
- Portable

Vulnerability Tests

Recommendations
Reasonable Security Requirements

Administrative

- Designation of employee to coordinate
- Identification of internal and external risks
- Assessment of sufficiency of safeguards
- Training and managing personnel
- Selecting capable service providers
- Adjusting program as necessary
Reasonable Security Requirements

Technical

- Assess risks in design
- Assess risks in data process, etc.
- Detect, prevent and respond to attacks
- Regularly test and monitor effectiveness
What is a Penetration Test vs. Vulnerability Assessment?

✓ **Pen Test** - An authorized simulated cyberattack on a computer system, performed to evaluate the security of the system. Not to be confused with a vulnerability assessment. The test is performed to identify both weaknesses (also referred to as vulnerabilities), including the potential for unauthorized parties to gain access to the system's features and data, as well as strengths, enabling a full risk assessment to be completed.

✓ **Vulnerability Assessment** - The process of identifying, quantifying, and prioritizing (or ranking) the vulnerabilities in a system. Examples of systems for which vulnerability assessments are performed include, but are not limited to, information technology systems, energy supply systems, water supply systems, transportation systems, and communication systems.
## Reasonable Security Requirements

### Physical

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assess risks of data storage and disposal</td>
<td></td>
</tr>
<tr>
<td>Detect, prevent and respond to intrusions</td>
<td></td>
</tr>
<tr>
<td>Protect against unauthorized access or use</td>
<td></td>
</tr>
<tr>
<td>Dispose after reasonable time</td>
<td></td>
</tr>
</tbody>
</table>
Should Size Matter?

“A small business *** complies with *** this section if *** [it’s] security program contains reasonable administrative, technical and physical safeguards that are appropriate for the size and complexity of the small business, the nature and scope of the small business's activities, and the sensitivity of the personal information the small business collects from about consumers.”

Practical Guidance

FTC has published an article with tips for protecting devices while working from home, including:

• Using passwords and keeping your security software up to date
• Securing your home network
• Securely storing sensitive files
• Deposing of sensitive data securely
• And following the security practices of your employer.
• See: https://www.consumer.ftc.gov/blog/2020/03/online-security-tips-working-home
Plus Lessons from Zoom

✓ Enhance encryption protocols by encrypting users’ information

✓ Implement a risk-based penetration-testing program to spot and assess security vulnerabilities

✓ Includes one “white box” penetration test per year - White Box Testing is a software testing method in which the internal structure/design/implementation of the item being tested is known to the tester. Contrasted with Black Box Testing, where item being tested is NOT known to the tester.
QUESTIONS?
COMMENTS?
THANK YOU!

JOHN ISAZA
John.Isaza@infogovsolutions.com