ECKERT SEAMANS
ATTORNEYS AT LAW

CYBERSECURITY: AN ANALYSIS OF THE LEGAL LANDSCAPE AND BEST PRACTICES

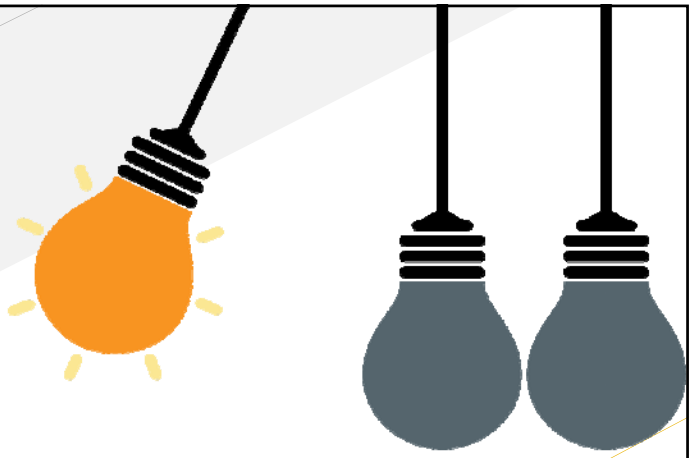
Presented by:

Matthew H. Meade
Member

Eckert Seamans Cherin & Mellott, LLC
600 Grant Street, 44th Floor
Pittsburgh, PA 15219

412.566.6983
mmeade@eckertseamans.com

Cybersecurity: An Analysis of the Legal Landscape and Best Practices



ECKERT SEAMANS
ATTORNEYS AT LAW

MATTHEW H. MEADE

August 9, 2018

What Keeps Us Up at Night?

CYBERSECURITY!

Why are We Up at Night?

Lost productivity

Ransomware

Reputational Damage

EQUIFAX

Fazio Mechanical

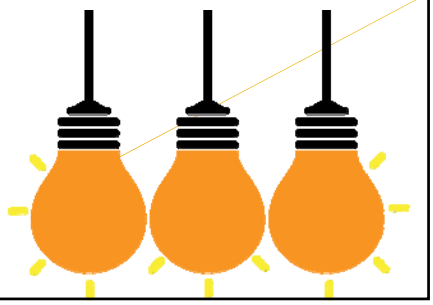
Theft of intellectual property

FINANCIAL COSTS
(response, remediation)

LEGAL ACTIONS

ECKERT SEAMANS
ATTORNEYS AT LAW

What Can You Do?
A Proactive Approach
A Blend of Law and Tech



Understand Sources of Risk

- Failure to heed system alerts and user reports of possible security issues and incidents
- Inadequate policies & procedures for information security
- Failure to monitor for unauthorized systems, applications, access and network connections
- Inadequate security measures with third party providers

Where are the Threats?

Insider threats

- Employee negligence
  - Security failures
  - Lost devices
- Employee ignorance
  - Improper disposal of Personal Information
  - Lack of education and awareness
- Data Hoarding
- Malicious employees

Outside threats

- Hackers
  - Malware
  - Phishing and Spear Phishing
- Thieves (including Social Engineering Tools)
- Vendors
- Commercial Spies
- Foreign Intelligence

What can you do?

- Approach cybersecurity as company-wide risk management issue – not just an IT issue
- Be proactive thru policies and training
- Review and assess third party agreements

What can you do?

- Understand the data life cycle
- Test the incident response plan by participating in a table top breach response exercise
- Make data privacy and security a **regular topic** of discussion at management and board meetings
- Consider cyber liability insurance

Due Diligence Checklist

1. Data Security Policies:
   - Written Information Security Program
   - Password
   - Remote Access
   - International Travel
   - Record destruction/retention
   - Incident response plan

Due Diligence Checklist

2. Conduct an Information Risk Assessment:
   - What is used, collected, and stored
   - Where is it received and stored
   - How is it accessed and tracked
   - How is it disposed of
   - Identify vulnerabilities:
     - Internal
     - External

Best Practices

Risk

You fail to promptly report the loss of a cell phone or laptop, or click on a spear phishing email

Consequence

Increased risk of unauthorized access and possible legal action

Solution

You immediately report a possible security incident

ECKERT SEAMANS

Best Practices

Risk

You have remote access and your password is Password1

Consequence

Anyone can access your network while masquerading as you

Solution

Limit remote access and change your password

… to Password2

ECKERT SEAMANS

Best Practices

Risk

You put Personal Information on a thumb drive/flash drive

Consequence

Increased risk of:

- injecting malware into network and device
- unauthorized access by third parties to information

Solution

Do not use thumb/flash drives to store, share, copy, or transport Personal Information unless encrypted

ECKERT SEAMANS

Best Practices

Risk

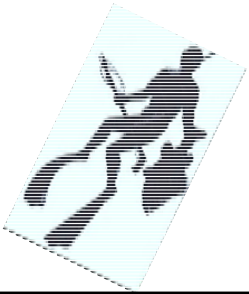
You get an email that tells you to send your SSN to a Nigerian Prince and you do

Consequence

Your identity is stolen, passwords compromised and systems accessed

Solution

Add a strong mail filter, add multi-factor authentication, and don't give your SSN to a Nigerian Prince



ECKERT SEAMANS

Best Practices

Risk

Failure to encrypt laptops and data at rest

Consequence

Increased risk of unauthorized access by third parties to sensitive information and regulatory fines

Solution

Mandatory laptop and data encryption and/or eliminate need to store documents on laptop

ECKERT SEAMANS

Best Practices

Risk

Agreements with vendors who have access to Personal Information

Consequence

Increased risk of unauthorized access

Solution

Require vendors to maintain appropriate security measures

ECKERT SEAMANS

Best Practices

Risk

Lack of an incident response plan and adequate training

Consequence

Loss of valuable time and data because of lack of preparedness and failure to have a coordinated response

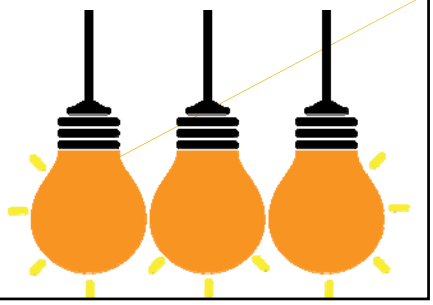
Solution

Implement and test plan

ECKERT SEAMANS

ECKERT SEAMANS
ATTORNEYS AT LAW

GDPR - DOES IT EFFECT OUR BUSINESS?



How Does GDPR Impact American Companies?

- Regulates "processing" of personal data by controllers or processors with an **establishment in the EU** (even if the regulated activity takes place outside the EU)
- Also regulates controllers or processors **not established in the EU** where processing relates to:
  - Offering of goods or services to data subjects in the EU
  - Monitoring the behavior of data subjects in the EU

What is "Offering Goods or Services" in the EU?

- Targeting **data subjects** in the EU:
  - Website available in EU languages (other than English)
  - Accept payment in euros or other EEA currency
  - Features EU residents in marketing
- Offering goods or services B2B is not offering to data subjects

What is "Monitoring Behavior"?

- Includes tracking EU residents on the internet, i.e. using cookies:
  - To make decisions about the person; or
  - To analyze or predict personal preferences, behaviors, and attitudes
- How are cookies (and other tracking tools) used?
  - Website usage statistics only (session cookies)
  - IP addresses plus profiling to send personalized marketing to EU residents
  - Third parties can place ads
  - Cookies to allow targeted ads on others' websites

Controller's Duties for Breach Notification

- Notice required if breach is "likely to result in high risk to the rights and freedoms of natural persons"
- Notify supervisory authority without undue delay and—where feasible—not later than 72 hours after becoming "aware" of breach
- Notify affected data subjects without undue delay unless:
  - Breached data is unreadable (i.e. encrypted), or
  - Measures in place to ensure no high risk to rights and freedoms of data subjects
- Document all breaches to verify compliance
- Be prepared to justify a decision that notification is not required


Cyber
Scenario


Your personal files are encrypted.
Your personal files are encrypted.
Your documents, photos, databases and other important files have been encrypted with strongest encryption and unique key, generated for this computer.
Private decryption key is stored on a secret Internet server and nobody can decrypt your files until you pay and obtain the private key.
You only have 72 hours to submit the payment. If you do not send money within provided time, all your files will be permanently crypted and no one will be able to recover them.
Press 'View' to view the list of files that have been encrypted.
Press 'Next' to connect to the secret server and follow instructions.
WARNING! DO NOT TRY TO GET RID OF THE PROGRAM YOURSELF. ANY ACTION TAKEN WILL RESULT IN DECRYPTION KEY BEING DESTROYED. YOU WILL LOSE YOUR FILES FOREVER. ONLY WAY TO KEEP YOUR FILES IS TO FOLLOW THE INSTRUCTION.
View
71:59:07
Next >>
can open it and use copy-paste for address and key.
ECKERT SEAMANS

If data is encrypted

- What is the recovery time if restoring from backup? (1 hr, 1 day, 1 week, 2 weeks - never)
- What is the recovery time if purchasing a decryption key? (1 hr, 1 day, 1 week, 2 weeks – never)

Other Considerations

- Does your insurance cover payment of a ransom?
- Would you hire a forensic investigator?
- Working with law enforcement?
- Is there a data breach?

ECKERT SEAMANS
ATTORNEYS AT LAW

Thank You.

Matthew H. Meade
412.566.6983
mmeade@eckertseamans.com
eckertseamans.com

Matthew H. Meade

MEMBER

Matt Meade concentrates his practice in the area of data security providing advice to clients regarding data breaches, information and records management, and other areas concerning data security. Matt helps clients identify business risks associated with the use and storage of sensitive information. He regularly guides clients through security incident investigations, analysis, communications, and, if necessary, responding to regulatory inquiries and litigation. He advises clients on security breach notification laws and other U.S. state and federal data security requirements (including laws regarding disposal of records). Matt drafts agreements addressing issues related to data use, privacy, and security. He also prepares document retention and management policies and develops associated training programs.

Matt speaks and writes regularly on data security matters and serves on The Sedona Conference Working Group Series Leadership Council, after previously serving on the Steering Committee for Working Group II on Data Security and Privacy, through which lawyers, judges, policy makers, security experts, technologists, and business leaders work together to identify and develop principles and best practices to constructively resolve issues surrounding data security and privacy liability. Matt has served as a Co-Chair of the ABA's First, Second, and Third Annual National Cybersecurity Institute (2016-2018).

REPRESENTATIVE MATTERS

- Advised numerous entitles, including healthcare providers, manufacturers, retailers, schools, financial services companies, county governments and collection agency on information security breach notification procedures and development of post breach corrective action plans.
- Coordinated response to multi-state security breaches, ransomware, and hacking incidents with local and federal law enforcement, and United States Attorney.
- Performed comprehensive review and subsequent revisions of all security policies for leading hospitality provider and then provided data security training to managers and executives on subjects covered in policies.
- On behalf of a healthcare automation solutions provider, obtained dismissal of claims arising from the theft of an employee's laptop computer containing protected health information, on grounds that court lacked subject matter jurisdiction because plaintiff failed to adequately allege injury-in-fact.
- Conducted employee cyber training sessions in hospitality, education, healthcare, manufacturing, insurance, and financial sectors.
- Organized, ran, and oversaw tabletop mock data breach scenarios for multiple organizations including universities, energy companies, banks, insurance companies, and healthcare organizations.

ECKERT SEAMANS
ATTORNEYS AT LAW

PITTSBURGH, PENNSYLVANIA

600 Grant St.
44th Floor
Pittsburgh, PA 15219

P: 412.566.6983

F: 412.566.6099

mmeade@eckertseamans.com

PRACTICE AREAS:

Data Security & Privacy

Business Counseling

STATE ADMISSIONS:

Pennsylvania

New York

New Jersey

EDUCATION:

J.D., Fordham University School of Law, 1992; Editor-in-Chief, Fordham Moot Court Board

B.A., Yale College, 1987; Casner Prize for Outstanding Achievement; Moriarty Prize; Kiphuth Scholar

- Developed cyber training for board of directors of community bank and manufacturing company.
- Conducted comprehensive review of security implications of agent agreements for provider of homeowner's insurance.
- Prepared and reviewed company security policies including Written Information Security Programs, document management, and incident response plans.
- Coordinated internal investigations of healthcare data breaches, subsequent patient notice, communication with the Department of Health & Human Services Office of Civil Rights ("OCR") and development of corrective steps. OCR closed the case taking no further action and noting the voluntary compliance efforts of the entity.
- Prepared and reviewed company policies including Written Information Security Programs, document management, social networking and incident response.
- Conducted internal investigation of processes and procedures of professional sports league, including analysis of discipline by league of teams, coaches and players, and of document management policy.
- Conducted an internal investigation of a large-scale data leak of personnel information at a Fortune 100 Corporation; interviewing relevant employees and preparing a report and recommendations for the Executive Board.
- Advised clients on proper security measures in connection with employee and customer personal information.

PROFESSIONAL AFFILIATIONS

- Pennsylvania Bar Association
- New York Bar Association
- American Bar Association National Institute on Cybersecurity, Co-Chair
- The Sedona Conference Working Group Series Leadership Council, Member
- The Sedona Conference Working Group 11 on Cyber Liability, Former Steering Committee Member
- Carnegie Mellon University CISO-Executive Program, Faculty Member

COMMUNITY INVOLVEMENT

- Children's Museum of Pittsburgh, Board Member
- Chuck Cooper Foundation, Vice President and Board Member

AWARDS AND RECOGNITION

- Selected for inclusion in *The Best Lawyers in America* list for 2017 and 2018 in the Privacy and Data Security Law category.

NEWS AND INSIGHTS

MEDIA COVERAGE

- "Lessons and Trends from FTC's 2017 Privacy and Data Security Update: Workshops and Guidance (Part Two of Two)," *The Cybersecurity Law Report*, February 2018.
- "Lessons and Trends from FTC's 2017 Privacy and Data Security Update: Enforcement Actions (Part One of Two)," *The Cybersecurity Law Report*, January 2018.

SPEAKING ENGAGEMENTS

- "Interactive Breach Scenarios," presented at the NetDiligence Cyber Risk Summit, June 2018.
- "Practice Makes Perfect: A Proactive Approach to Cybersecurity in an Interconnected Hotel Industry" presented at the Hotel & Lodging Legal Summit at Georgetown University Law Center, October 2017.
- "Cybersecurity: There ARE Things Lawyers Can and Should Do," CLE presentation, October 2017.
- "You've Got Hacked: How to protect yourself against campaign data security dangers and liabilities," panel presentation at the American Association of Political Consultants' 2017 Annual Pollie Awards & Conference, March 2017.