CYBERSECURITY AND PRIVACY LAW ISSUES

Presented for American Association of Port Authorities By:

Aldo Leiva, Esq.
Fort Lauderdale, FL
(954) 768-1622
aleiva@bakerdonelson.com

DISCLOSURE

- These materials should not be considered legal advice and are not intended to nor do they create an attorney-client relationship
- The materials are general and may not apply to particular individual legal or factual circumstances

Objectives

- Develop a general understanding of Cybersecurity and Privacy Law issues faced by Port Authorities
- Overview of GDPR and the California Consumer Privacy Act (CCPA)
- Considerations for In House Counsel

Cybersecurity vs. Privacy

- Cybersecurity - Safeguarding Data (of any type- financial, health, proprietary, confidential, sensitive, etc.)

- Privacy- Safeguarding User Identity

U.S. Data Security and Privacy Laws

- No comprehensive federal legislation
- NIST is guidance, NOT law
- Sector-based approach
- Federal vs. State laws and regulations
- Common law
- Contracts (Vendors, Supply Chain)

- Laws do not propose specific technical standards
- Laws lag behind real-time threats (Moore's Law effect)

U.S. Federal Laws that relate to Data Security and/or Privacy

- Federal Trade Commission Act (FTC)
- Gramm-Leach-Bliley Act (GLBA)- financial institutions
- Health Insurance Portability and Privacy Act (HIPAA)
- Telephone Consumer Protection Act (TCPA)
- Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM)- commercial email
- Children's Online Privacy Protection Act (COPPA)
- Computer Fraud and Abuse Act – unauthorized computer use and tampering
- SEC Disclosure

State Laws that relate to Data Security and/or Privacy

- Hundreds of them
- “Baby” FTC Acts
- GLBA and HIPAA add-ons
- SSN Laws
- Records retention/destruction laws
- Breach Notification laws (50+)
- Data Security Laws (California, Massachusetts, New York)

Cross Border/International Laws

- GDPR
- US Privacy Shield

Maritime Issues

- Complex and increasingly automated
- Cyber attacks don’t just impact data, buy can cause physical damage (Stuxnet)
- Industrial Control Systems
- IT vs. OT
- Docking ships can spread viruses/malware onto port systems via Wifi or other data networks
- Internet of Things (IOT)
- Critical Infrastructure- context of cyberwar

What is the GDPR?

- **G**eneral **D**ata **P**rotection **R**egulation
- Regulation (EU) 2016/679 of the European Parliament- 99 Articles to read through
- Applies to all EU member states
- Replaces the 1995 Data Directive and is intended to simplify compliance
- Extends EU requirements that personal data be kept securely
- Organizations are accountable for data security
- Enforceable as of May 25, 2018

Key Aspects

- Defines measures that data holders must take to protect data
- Emphasizes enforcement
- Authorizes large fines and penalties
- Imposes disclosure requirements for data breaches

Scope/Applicability

- Applies to organizations located in EU Member States OR
- Applies to ANY ORGANIZATION OUTSIDE THE EU MEMBER STATES that:

(1) **offers** goods or services to EU citizens (even if no payment is received)

(2) **monitors** the behavior of EU citizens

Maximum Penalties

- GDPR can cost up to $ 24M OR 4% of the violator's annual global revenue, **WHICHEVER IS HIGHER**

Assessing whether GDPR Applies

- **Present in EU and are a Data Controller ? YES**
- **Present in EU and are a Data Processor ? YES**
- **Subsidiary controls or processes data in EU? YES**
- **Online Presence? MAYBE**
- **Advertising to EU residents? YES**
- **(i.e. offering terms in Euros or Pounds? YES)**
- **Dropping Cookies or otherwise tracking behavior of EU residents? YES**
- **EU Business Customer transfers data to you? If you sign GDPR Compliance Agreement, YES**

New EU Data Breach Notification Requirements

- Controllers must report data breaches to authority without undue delay and, where feasible, within **72** hours of becoming aware of breach, **unless** breach is unlikely to result in risk for rights and freedoms
- Must document/justify why notifications was not made within 72 hours
- Affected data subjects must be notified without undue delay if high risk for rights or freedoms
- **Consider**: Breach preparedness with guidelines, policies, plans, and lists of who to notify; training

Key Points

- May 25, 2018 was the compliance deadline
- **GDPR establishes only a floor – individual countries may expand on it (must still looks at individual laws- 18 have been passed so far)**
- Demonstrating reasonable cybersecurity goes beyond the legal department (which is sometimes last to know)
- Investigations are underway- first fines

California Consumer Privacy Act (CCPA)

- Similar framework to GDPR
- Will impact more US companies than GDPR
- Effective date January 1, 2020
- Fine- $ 7,500.00 for each intentional violation

California Consumer Privacy Act (CCPA)

- Definition of Personal Information is similar to GDPR but also includes info linked to a “household,” which would include a physical address that is not directly linked to an individual
- Must inform consumers what type of data will be collected and how it will be used
- Must disclose categories of PII that have been collected, sold, or disclosed in past 12 months
- “Clear and conspicuous” opt out link on website
- Requires appropriate security protocols
- Right to be “forgotten” (all copies purged)

In House Counsel Considerations

- Communicate with Chief Compliance Officer, Chief Information Officer, Chief Information Security Officer, Chief Privacy Officer, or Data Protection Officer.
- Not just an IT issue- you have a vital role
- Understand information assets and risks
- Perform Risk Assessments
- Identify Legal Obligations - Federal, State, International, Contractual, etc.
- Develop, Implement and Maintain WISP
- Industry Standards/Best Practices

In House Counsel Considerations

- Involve Senior Management
- Develop and Enforce Cybersecurity and Privacy Policies (including breach assessment)
- Ensure Training of Employees
- Manage Vendor Risks
- Manage Maritime Risks
- Pre-engagement Due Diligence
- Develop and test Cybersecurity response (including key law enforcement and military contacts/resources)
- Assess Cyber Insurance
- Cybersecurity Information Sharing Programs

Trends to Monitor

- Internet of Things (IOT)-
- Cyber insurance Coverage Litigation (Mondelez v. Zurich - 2018-L-011008)
- Autonomous Machines and Vessels
- National and International Legislation
- Cybersecurity Grants (over 30 ports have received grants totaling $ 100M)

THANK YOU

Presented for American Association of Port Authorities By :

Aldo Leiva, Esq.
Fort Lauderdale, FL
(954) 768-1622
aleiva@bakerdonelson.com