

CYBER SECURITY



A LEGAL PERSPECTIVE

THOMAS G. SCHROETER
ASSOCIATE GENERAL COUNSEL
PORT OF HOUSTON AUTHORITY

DISCLAIMER!



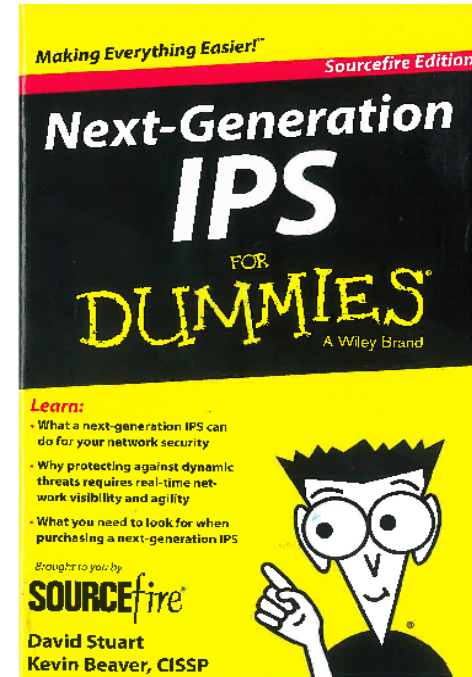
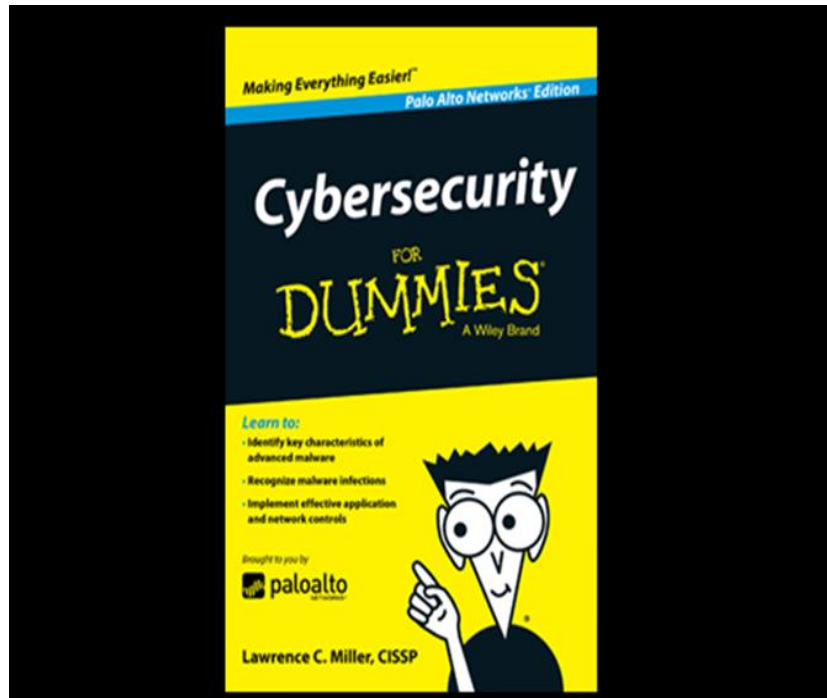
This presentation:

- does **not** include all cyber security laws and regulations
- does **not** constitute the work, conclusions or opinions of AAPA, the Port of Houston Authority or anyone other than the author
- does **not** constitute legal advice or risk management advice
- is for educational purposes only, for use during this session.
- is made without warranties or representations, express or implied, including without limitation, any warranty of fitness for a particular purpose

Consult your counsel & risk manager for specific situations you may encounter!

CYBER SECURITY A LEGAL PERSPECTIVE

Training and Education



CYBER SECURITY A LEGAL PERSPECTIVE

- I. Introduction: What Should Ports Do Now?
- II. Cyber Security Laws, Liabilities, Litigation
- III. Conclusions - Takeaways

CYBER SECURITY A LEGAL PERSPECTIVE


Introduction: What Should Ports Do Now?

Enact a comprehensive **Cyber Security Plan**.




CYBER SECURITY A LEGAL PERSPECTIVE

Cyber Security Plan should include:

- Cyber security assessment
 - Update and implement technical cyber security measures in accordance with assessment results and industry standards (guide: NIST)
 - Incident response plan including a post-incident business resumption plan
 - Insurance review, including General Liability and consideration of Cyber Insurance to reasonably cover your risks
 - Training and education for your IT professionals and all employees and vendors and any others with access to your computer systems
 - Reasonable degree of technical training for Senior Management and Legal Counsel so they can understand IT, ask the right questions and provide appropriate resources
- 

CYBER SECURITY A LEGAL PERSPECTIVE

Form a Port Cyber Security Team with a Quarterback, including:

- IT professionals trained in cyber security
 - FSO or other member of your physical security group familiar with your Facility Security Plans, MTSA and 33 CFR Parts 101 and 105
 - Finance & Administrative Director to whom IT Manager reports (may often be the Quarterback)
 - Outside cyber-security consultant
 - Legal counsel, in-house and specialized outside cyber-security counsel
 - Port Risk Manager and outside insurance consultant
- 

CYBER SECURITY A LEGAL PERSPECTIVE

Port Commission

- **Give your Port Commission periodic reports on Cyber Security at your Port, including**
 - the elements of your Cyber Security Plan,
 - expenses required to achieve your Plan, and
 - notice of reportable data breaches and other breaches that result in harm to individuals and loss or damage to the port and its infrastructure



CYBER SECURITY A LEGAL PERSPECTIVE

The key is to be **pro-active!**



CYBER SECURITY

A LEGAL PERSPECTIVE

Cyber Security Federal and State Criminal Laws

Federal

E.g., The Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030: “Whoever ... intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss.”

State


E.g. Texas Penal Code, Title 7, Chapter 33: “ A person commits an offense if the person knowingly accesses a computer, computer network, or computer system without the effective consent of the owner.”



CYBER SECURITY A LEGAL PERSPECTIVE

State Notice Laws

Some 47 states have cyber security laws requiring that **notice** of cyber breaches be given to individuals and/or Attorney Generals of data breaches resulting in loss or theft of Personal Identifiable Information (PII).



CYBER SECURITY

A LEGAL PERSPECTIVE

State Laws

Protected Personal Identifiable Information (“PII”) varies from state to state; typically includes:

- Individuals’ names including maiden names
- Date of birth
- Social security numbers
- Health and medical data
- Passwords and PINS
- Bank account numbers

CYBER SECURITY

A LEGAL PERSPECTIVE

State Laws

- Exemption often given for encrypted data
- But not if the person accessing the data has the encryption key to decrypt the data
- Exemption sometimes given where no significant risk of identity theft (Rhode Island)



CYBER SECURITY


A LEGAL PERSPECTIVE

State Laws

Enforcement rights vary:

- Enforcement by Attorney General
- Private Right of Action

Penalties vary:

- Virginia: up to \$150,000 per security breach
 - Texas: up to \$250,000 for failure to timely notify
 - Louisiana: up to \$5,000 per violation; each day w/o notifying is a separate violation
 - Tennessee: Private action to collect damages, seek injunctive relief
- 

CYBER SECURITY A LEGAL PERSPECTIVE

Federal Laws

Bottom Line:

- No *comprehensive* federal cyber security legislation



CYBER SECURITY

A LEGAL PERSPECTIVE

Federal Laws - What's Likely to Be Included in the Next Wave?

Borrowing from:

- State Laws: Required Notification of Data Breaches
- The **Federal Information Security Management Act (FISMA)** enacted in 2002, updated in 2015). Applies to all federal agencies
 - Requires an **assessment** of each agencies computer systems
 - Requires **risk-based plans**
 - **NIST** (National Institute of Standards and Technology) publishes **standards and guidelines** and works closely with federal agencies to implement FISMA and to protect the agencies' information and information systems

CYBER SECURITY

A LEGAL PERSPECTIVE

Federal Laws

Borrowing from:

- Two Executive Orders signed by President Obama:
No. 13636 (February, 12, 2013), and
No. 13691 (February 13, 2015)
- Centers much of federal cyber security efforts in the **Department of Homeland Security (DHS)**
- Call for the creation of voluntary standards to boost the security of computer networks in **critical industries**
- Promote voluntary **exchange of information**
- Create a framework for the **protection of critical infrastructure, including maritime transportation sector**
- Calls on **NIST** (National Institute of Standards and Technology) to publish **standards and guidelines** and to work closely with federal agencies to implement FISMA and to protect the agencies' information and information systems

CYBER SECURITY A LEGAL PERSPECTIVE

Federal Laws

Borrowing from:

- Maritime Transportation Security Act of 2002 (MTSA) and 33 CFR Parts 101 and 105
 - **Assessments**
 - **Plans**, based on vulnerabilities found in assessments, approved by USCG
- Pending **Critical Infrastructure Protection Act (HR 3696)** – **SAFETY ACT** concept

CYBER SECURITY

A LEGAL PERSPECTIVE

So, comprehensive federal legislation may contain:

- **Notification** requirements for data breaches
- Incentives, including immunity from liability, for **information sharing** with federal agencies
- Required cyber security **assessments**
- **Cyber Security Plans** as part of (or in addition to) Facility Security Plans
- **SAFETY ACT** type provisions including:
 - **certifications** of Cyber Security Plans and
 - **Immunity from liability** over approved amount of Cyber Security Insurance carried

CYBER SECURITY

A LEGAL PERSPECTIVE

What Happens after a Significant Data Breach:

- Litigation -- various theories pleaded, including:
 - Failure to timely notify under state statutes and HIPAA
 - Negligence – duty owed to individuals whose PII is lost or stolen
 - What is foreseeable?
 - Contract, express and/or implied
 - Fraud, misrepresentation
- Investigations
 - FBI, DOJ (federal criminal laws)
 - HHS (HIPAA)
 - FTC (unreasonable and unfair data security practices)
 - State Attorney Generals (state criminal laws; state notification laws)
- Media Exposure (reputation and trust at stake)
- In the case of Target, CEO Job Loss (someone has to take the blame)


CYBER SECURITY A LEGAL PERSPECTIVE

Is the maritime industry truly at risk?



CYBER SECURITY A LEGAL PERSPECTIVE

Final Takeaways:

- Conduct a Cyber Security Assessment & Assess Your Risks
 - Review Insurance Policies; look into Cyber Insurance
 - Draft and Implement a Cyber Security Plan
 - Include Appropriate Training for IT, Senior Management, All Employees, Vendors
 - Form a Port Cyber Security Team
 - Periodic Reports to Port Commissioners
- 

CYBER SECURITY A LEGAL PERSPECTIVE

Role of Port Commissions

As a general rule, Port Commissions set the *policy* for ports and communicate with the Port's stakeholders; they do not do the work of port staff in developing and implementing standards and procedures.

For Cyber Security, Port Commissions should:

- be advised as to port staffs putting a Cyber Security Plan in place
- receive information adequate to perform their role of setting port policy
- be prepared to communicate with port stakeholders
- receive periodic reports from port staff on the state of cyber security at the port
- authorize expenditure and other port resources to manage cyber security at the port.

**CYBER SECURITY
A LEGAL PERSPECTIVE**



QUESTIONS?



THANKS FOR YOUR TIME!