Cyber Security: Identifying and Reducing the Risks

Littler Mendelson, PC
2017 AAPA Port Administration & Legal Issues Seminar

Zoe Argento
Littler Mendelson, P.C.
1900 16th Street, Suite 800
Denver, CO 80202
Phone: 303.362.2876
Email: zargento@littler.com

Agenda

I. Why Should You Worry About Cyber Security?

II. Developing a Security Plan

III. Creating a Culture Of Data Stewardship

IV. When Is an Incident Legally a Breach?

Why Should You Worry About Cyber Security?

The CEO & Board Cares

- **39% of CEOs/Boards involved in data breach preparedness in 2015 vs. 29% in 2014** (Ponemon/Experian 2015)
- **Several CEOs have recently lost their jobs at least partly because of a security breach**
  - HB Gary
  - Ashley Madison
  - Director of OPM

Cost of a Security Breach

Average total cost = $7 million.

– ↑ 8% from $6.5 million in 2015

Average cost breakdown:

– $730K in detection and escalation

– $590K in notification costs

– $1.7M in post-breach costs, *i.e.*, help desk and remediation

– $4M in loss of customers/good will

Average cost per lost or stolen record = $221

– ↑ 2% from $217 in 2015

2016 Cost of Data Breach Study: United States, Ponemon Institute, May 2016

Every Organization Has Sensitive Data

- Social Security numbers of employees
- Health information
- Trade secrets
- Confidential business information
- Credit card numbers
- Bottom line: Would you want all of your emails on Wikileaks?

Sensitive Security Information (SSI)

SSI defined under 49 C.F.R. § 1520.5 includes:

- Security programs and contingency plans
- Vulnerability assessments
- Information circulars on threats to maritime transportation
- Threat information
- Security measures
- Security training materials

Duty to protect SSI and report unauthorized disclosure to TSA

The Cyber Risk to Ports

U.S. Coast Guard, *Cyber Strategy*, June 2015:

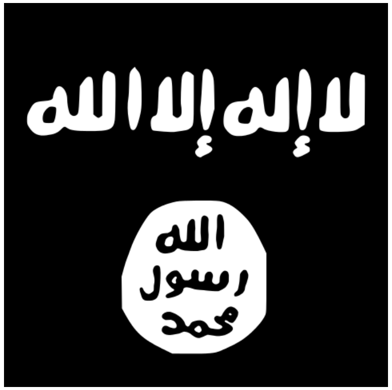
- **"Cyber technology is essential to the operation and efficient functioning of the Nation's maritime critical infrastructure."**
- **Computer systems:**
  - **Operate pumps, machinery, vessel propulsion and navigation systems;**
  - **Monitor and control safety and environmental systems;**
  - **Operate security cameras, gates, and communication systems;**
  - **Track and control container cargo movements…**

Ports Are Critical Infrastructure

- 75% of the nation’s commerce passes through our ports
- A disruption can seriously impact the economy
- 2012 strike at Los Angeles / Long Beach ports was estimated to cost approximately $1 billion / day
- Not just goods: the average cruise ship has 3,000 people on board

Who Would Cyber-Attack a Port?

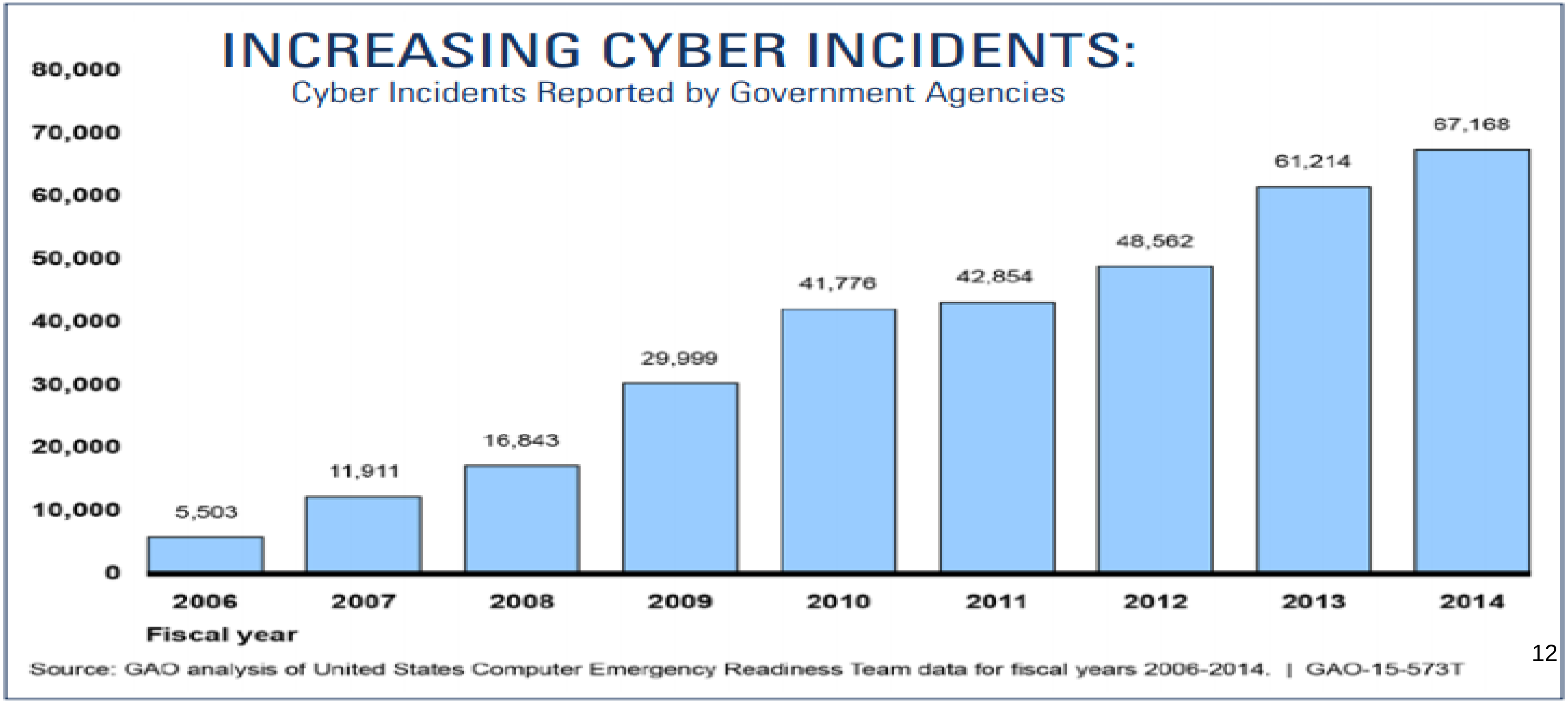
- Nation-States
  - Russia, China, North Korea, Iran, and others



- Terrorist Organizations
- Criminal Organizations
- Hacktivists

Cyber Risks At Ports Are Real

2014: major U.S. port facility suffered a system disruption which shut down multiple ship-to-shore cranes for several hours



Source: GAO analysis of United States Computer Emergency Readiness Team data for fiscal years 2006-2014. | GAO-15-573T

Developing a Security Plan

Facility Security Plans (FSPs)

Required by the Maritime Transportation Security Act; regulations at 33 C.F.R. 105

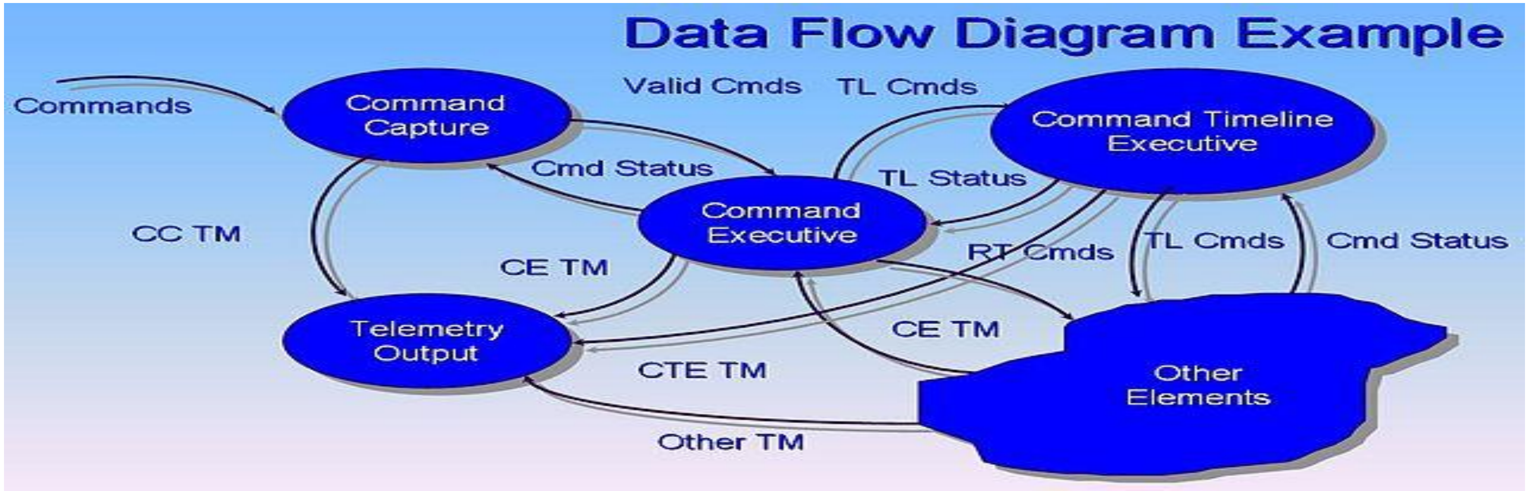
Key points:

- ➢ **Designate Facility Security Officer (FSO)**
- ➢ **Conduct a Facility Security Assessment (FSA)**
- ➢ **Plan to protect communications systems and other security systems**
- ➢ **Training and drills**
- ➢ **Security incident response**
- ➢ **Update every 5 years**

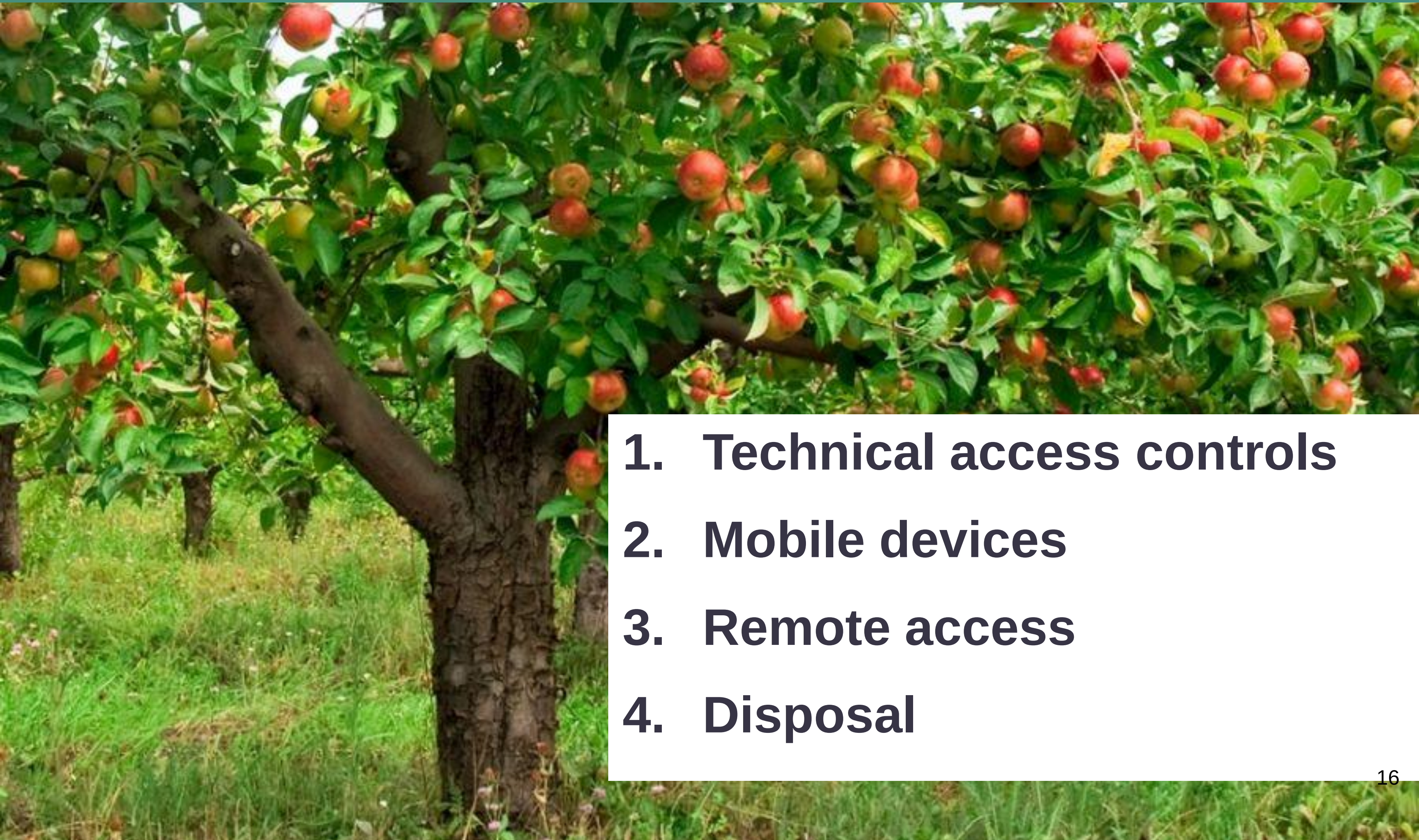
No regulations specifically addressing ports' cyber security … yet

Step 1: Conduct a Risk Assessment

- First step in any security plan
- Update after any significant change in operations or environment
- What are the access points?
- What is the data flow?

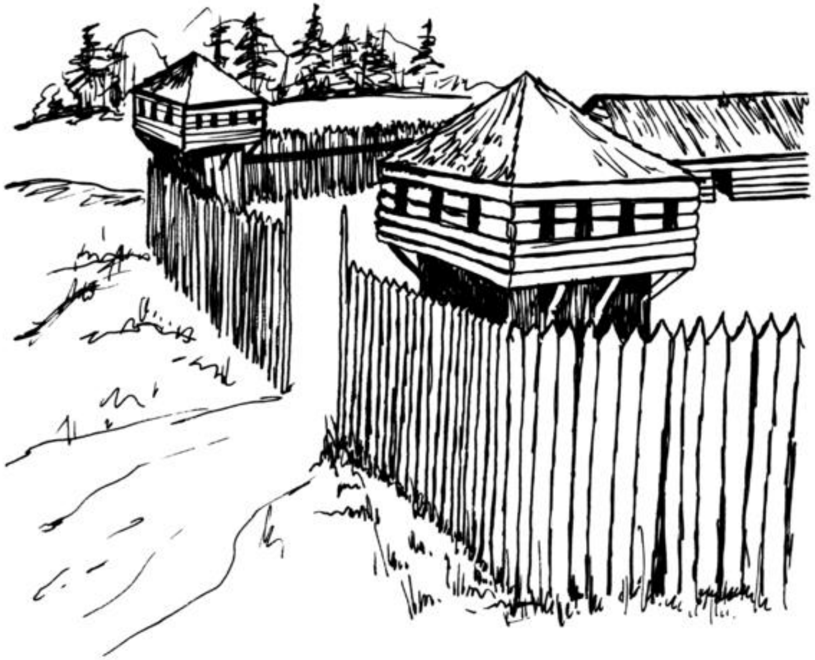


The Low Hanging Fruit of Data Security



1. Technical access controls
2. Mobile devices
3. Remote access
4. Disposal

Technical Access Controls: Perimeter defense is good



- Firewall (turned on)
- Anti-Virus / Anti-Malware
- Patch updates
- Access controlled:
  - Strong passwords
  - Passwords changed every 90 days
  - Passwords encrypted if stored
- Penetration testing
- Inventory of devices with access

Technical Access Controls: Defense in depth is better

Technical Access Controls: Defense in Depth

1. Only employees who need access to sensitive information to perform job responsibilities have authorized access
2. Activity and access logs and audits
3. Authorized access restricted by “minimum necessary” principle
4. Access rights are modified when job duties change
5. Terminate access promptly upon termination of employment

Mobile Devices

Do not store sensitive information on portable devices without a strong business need

Key Security Controls For Mobile Devices

1. Encryption
2. Password protection
3. Automatic lock down after brief period of inactivity
4. Automatic wipe or lock-out after ten failed attempts
5. Remote deletion of data on lost or stolen devices

Remote Work Environment

- Select a work location that is isolated from general household traffic
- Don’t let household members use the workstation
- Beware of strangers (e.g., cleaners, repair technicians, service providers)
- Follow same procedures for workstation security as if in the workplace

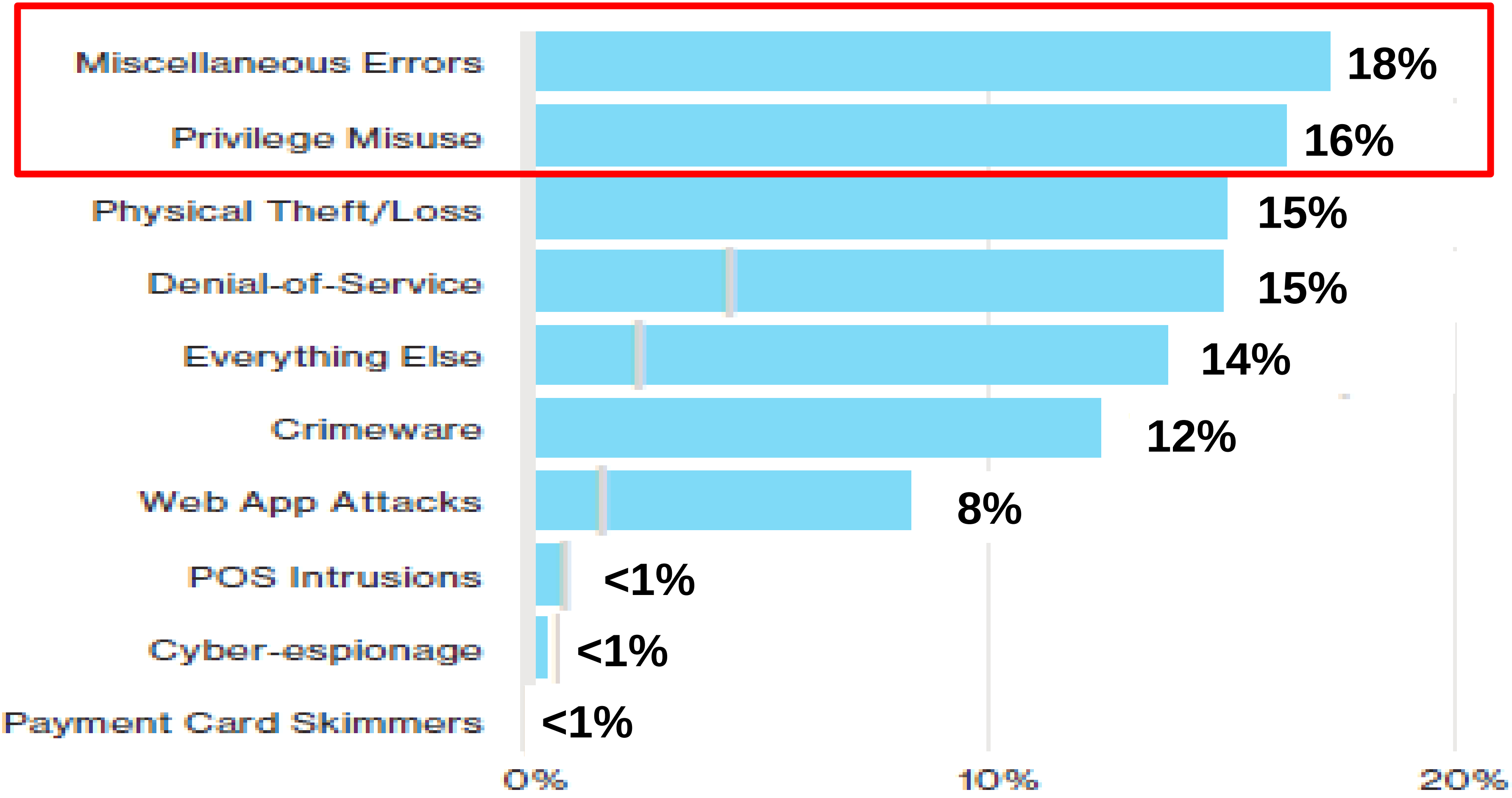
Proper Disposal

- Consult with IT department before discarding any computer or storage device (e.g., thumb drive, CD)

- Shred paper documents before discarding

Creating a Culture of Data Stewardship

People Are #1 Cause of Breaches



2016 Verizon Data Breach Investigations Report

Confidentiality Agreements

- **During the on-boarding process**
- **Key Terms**:

1. “Confidential Information” should cover sensitive personal information, trade secrets, business information, and facility information
2. Require return of all confidential information upon request or at termination of employment relationship

Information Security Training

- **Every employee should receive data privacy training at orientation**
  - Only 44% provided training at orientation (Ponemon/Experian 2015)
- **Employees with access to trade secrets, confidential information, or personal data should have more in-depth training**
  - Training can vary based on job functions and sensitivity of data that is accessed
- **Periodically send reminders, updates, and notices**
  - 71% of companies that provide training do so only once or sporadically (Ponemon/Experian 2015)

Big Picture Points

1. **Employer’s legal and/or contractual obligations to safeguard sensitive data**
2. **Types of information falling within scope of legal duty**
3. **Potential consequences for employer of noncompliance**
4. **Steps employees can take to safeguard sensitive data**

Training On Safeguards

1. **Importance of protecting log-in credentials**
   - In 2015, 63% of confirmed data breaches involved weak, default or stolen passwords (2016 Verizon Data Breach Report)
2. **How to create a strong password**
3. **Screen security**
4. **How to recognize a “phishing” e-mail**
   - Sanctioned phishing tests conducted in 2015 revealed that 30% of phishing messages are opened and 12% click on the malicious attachment (2016 Verizon Data Breach Report)

Strong Passwords

I changed all my passwords to "incorrect." So whenever I forget, it will tell me my password is "incorrect."

Strong Passwords

K*&Lkd7

Strong Passwords

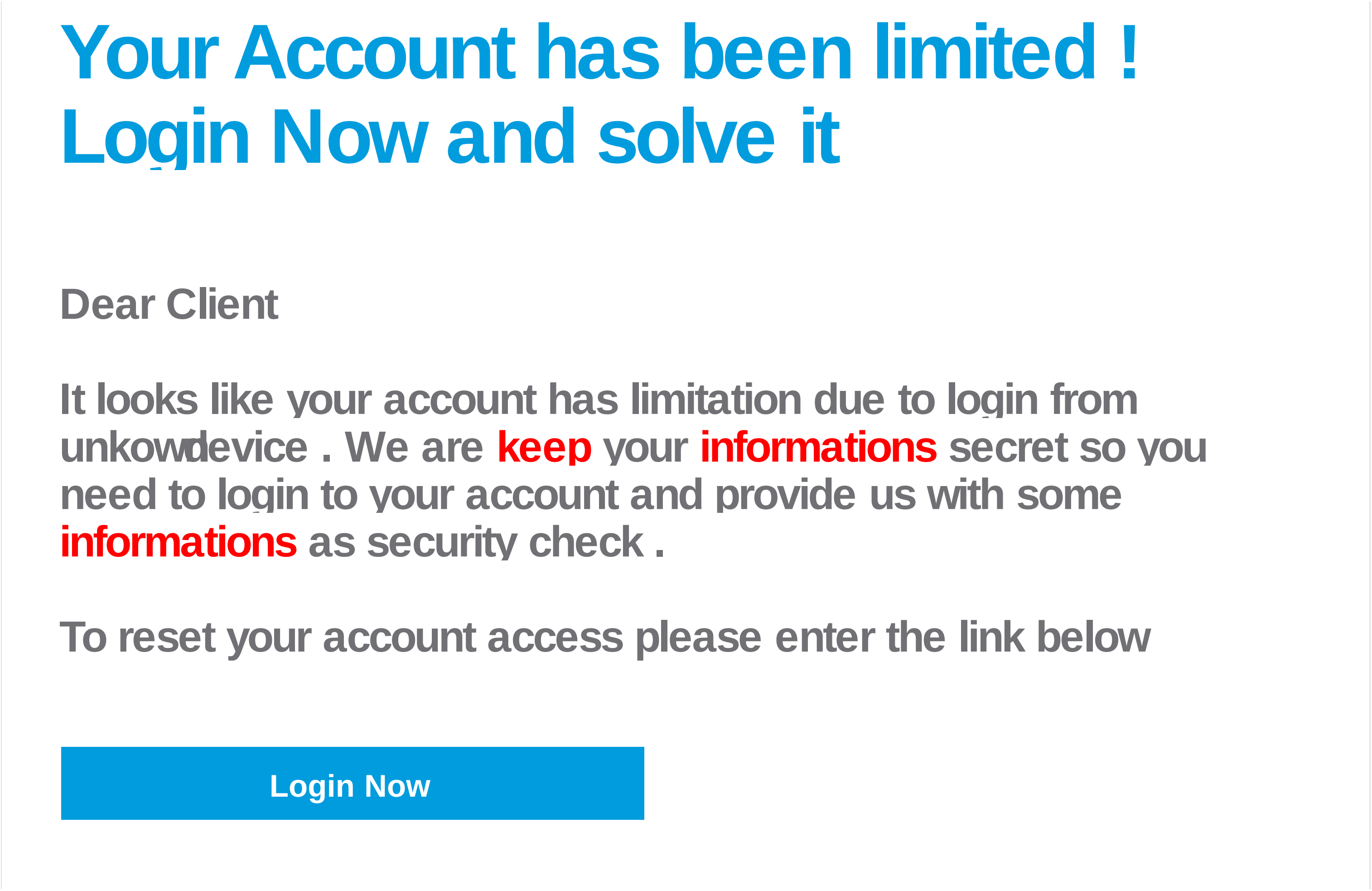
My first car was a Toyota Corolla, which I bought for $2000

MfcwaTC,wIbf$2000

Training On Safeguards

1. **Importance of protecting log-in credentials**
   - In 2015, 63% of confirmed data breaches involved weak, default or stolen passwords (2016 Verizon Data Breach Report)
2. **How to create a strong password**
3. **Screen security**
4. **How to recognize a “phishing” e-mail**
   - Sanctioned phishing tests conducted in 2015 revealed that 30% of phishing messages are opened and 12% click on the malicious attachment (2016 Verizon Data Breach Report)

Phishing E-mail: Exhibit #1



Your Account has been limited ! Login Now and solve it

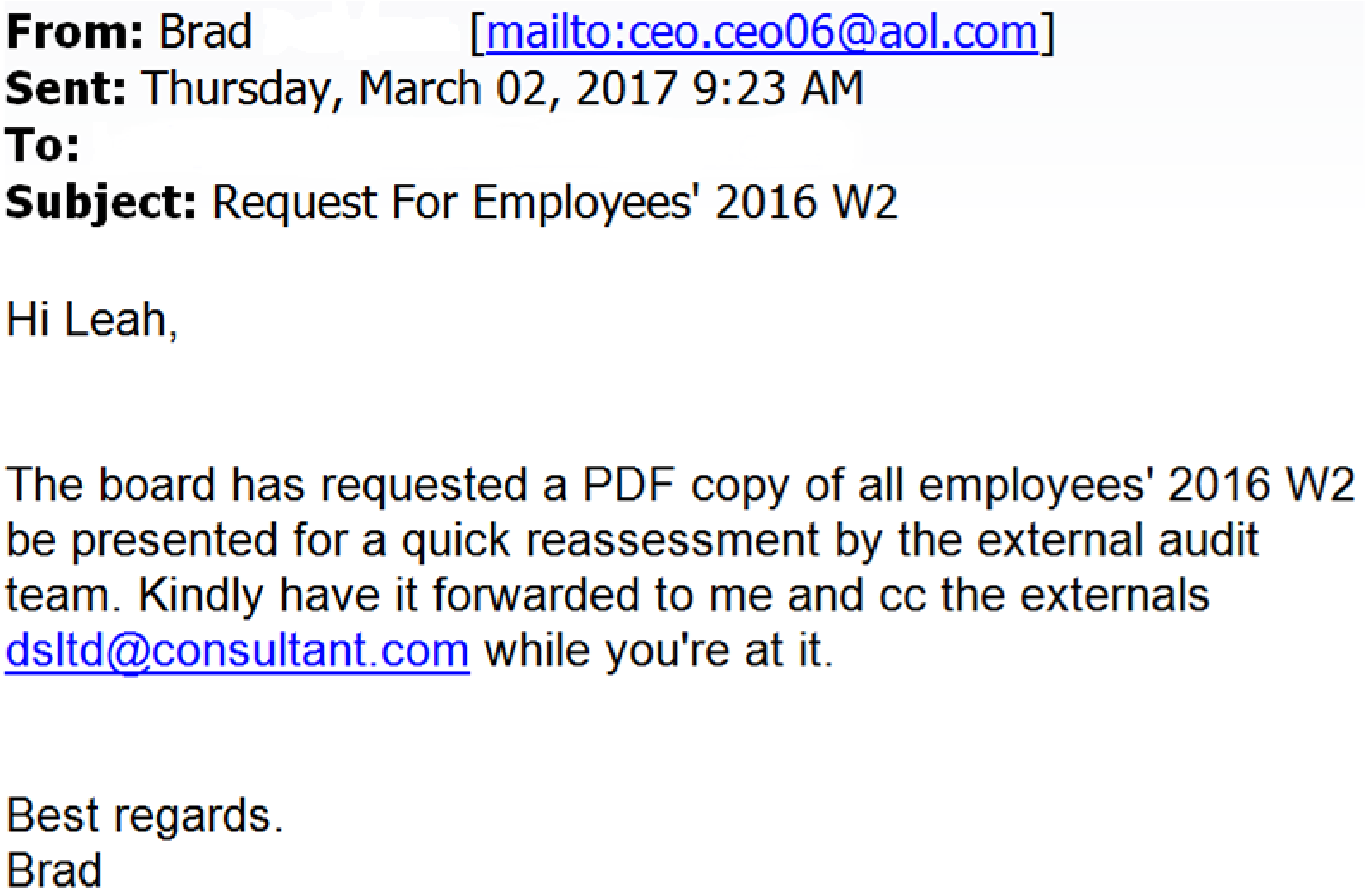
Dear Client

It looks like your account has limitation due to login from unkowdevice . We are keep your informations secret so you need to login to your account and provide us with some informations as security check .

To reset your account access please enter the link below

Login Now

Phishing E-mail: Exhibit #2



From: Brad [redacted] [mailto:ceo.ceo06@aol.com]
Sent: Thursday, March 02, 2017 9:23 AM
To: [redacted]
Subject: Request For Employees' 2016 W2

Hi Leah,

The board has requested a PDF copy of all employees' 2016 W2 be presented for a quick reassessment by the external audit team. Kindly have it forwarded to me and cc the externals dsltd@consultant.com while you're at it.

Best regards.
Brad

Exit Interviews

1. Provide departing employee with copy of executed confidentiality agreement
2. Remind employee of ongoing obligation to keep information confidential
3. Ensure return of all employer-owned computers, mobile devices and portable storage media
4. Ensure return of all paper documents containing confidential information

Exit Interviews

5. **Coordinate removal of confidential business information from any “BYOD device”**
   - Only 38% of organizations do this (Blanco Tech Group 2016)
   - Only 34% securely wipe departing employees’ BYOD 100% of the time (Blanco Tech Group 2016)
6. **Coordinate removal of confidential information from all personal accounts and media**

Cyber Insurance

Types:

- Network security
- Privacy

Coverage:

- Average cost of a breach notification/remediation: ~$2.5M
- Factors to consider:
    - Amount / type of data stored;
    - Technology infrastructure and practices;
    - Use of mobile devices; and
    - Number of third-party contractors with access to sensitive data

Key Questions To Ask About Cyber Insurance

1. What are the minimum technology security requirements?
2. Quick wins to reduce premiums?
3. What are the audit requirements?
4. How does a breach affect premiums?
5. What is the time frame in which a breach must be reported to benefit from the policy?

When Is An Incident Legally A Breach?

Events That Ports Must Report

Transportation Security Incident (TSI)

- Incidents that can lead to loss of life, environmental damage, transportation system disruption, or economic disruption to a particular area
- Concern is cyber security not necessarily data security
- Use best judgment

Breach of Security (BoS)

- An incident that has not resulted in a TSI, in which security measures have been circumvented, eluded, or violated.

Suspicious Activity (SA)

- Activities that may result in a TSI

Ports' Reporting Obligations

Must report:

- Suspicious Activities and Breaches of Security to National Response Center
- Transportation Security Incident to Captain of the Port (COTP) and to cognizant District Commander

Content: to the extent possible:

- Name and contact information
- Name and contact information of suspicious party
- Location of incident
- Description of incident

Timing: "Without delay"

Is The Incident A Breach?: Sources of Law

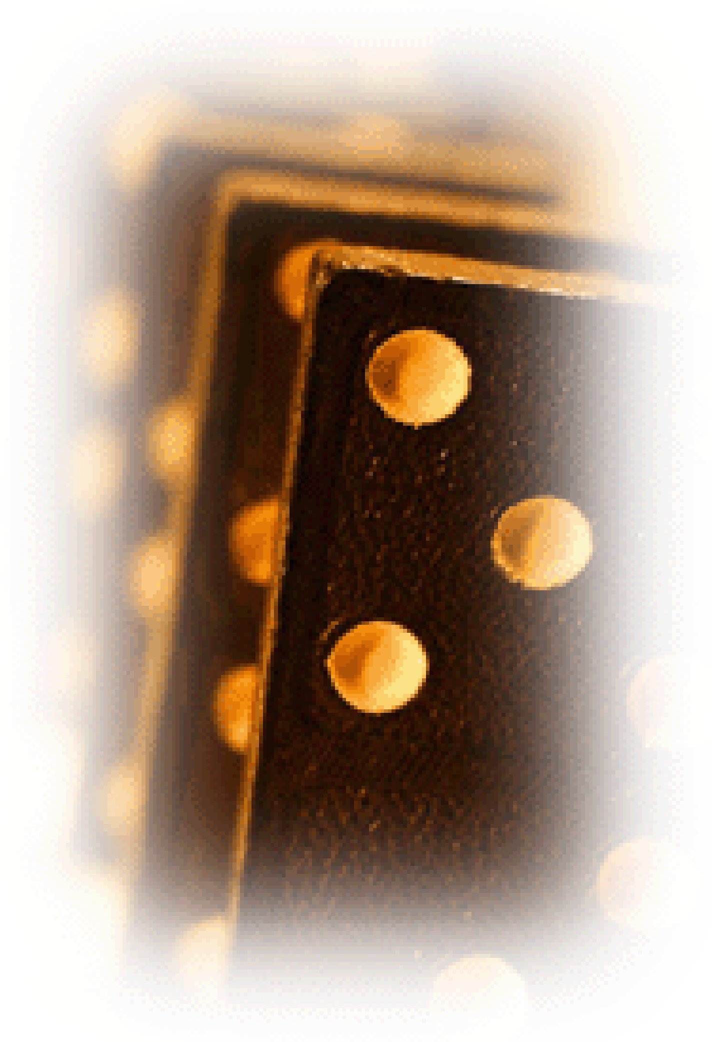
- ➢ **State Law**
- ➢ **HIPAA**
- ➢ **Payment Card Industry Data Security Standard**

State Breach Notification Laws

47 states D.C., Puerto Rico, USVI, and Guam now mandate notice of security breach

Only the following states do not have notice statutes: AL, NM, and SD

Trigger Event



1. Unauthorized acquisition
2. Unencrypted
3. Computerized
4. Personal information
5. A material risk of harm

Personal Information Defined

First name or initial <u>plus</u> last name <u>plus:</u>

- SSN
- Driver's license number and/or state-issued ID number
- Credit or debit card number or financial account number in combination with any required password

<u>Other information included</u>:

AK, AR, CA, CO, DC, FL, GA, IL, IN, IA, KY, ME, MD, MO, MT, NC, ND, NE, NJ, NV, OR, PR, RI, SC, TX, VA, WI, WY

HIPAA Trigger Event

- Notification must be provided when there is a “breach” of “unsecured PHI”
- Unsecured = unencrypted
- “Breach” = any unauthorized access to, or acquisition, use, or disclosure of, PHI subject to four exceptions

Questions?

Littler

Thank You