SNIA STORAGE SECURITY SUMMIT
Wednesday, May 11, 2022 • Virtual

# Secure Your Storage or We'll See You in Court!

## Is Your Storage Security "Reasonable Security"?

,

Lucy L. Thomson, Esq. CISSP, CIPP/US
Livingston PLLC, Washington, D.C.

A SNIA Event

# SNIA Legal Notice

- The material contained in this tutorial is copyrighted by the SNIA unless otherwise noted.
- Member companies and individual members may use this material in presentations and literature under the following conditions:
  - Any slide or slides used must be reproduced in their entirety without modification
  - The SNIA must be acknowledged as the source of any material used in the body of any document containin material from these presentations.
- This presentation is a project of the SNIA.
- Nothing in this presentation is intended to be or should be construed as legal advice or an opinion of counsel. If you need legal advice or a legal opinion please contact your attorney.
- The information presented herein represents the author's personal opinion and current understanding of the relevant issues involved. The author, the presenter, and the SNIA do not assume any responsibility or liability for damages arising out of any reliance on or use of this information.

  NO WARRANTIES, EXPRESS OR IMPLIED. USE AT YOUR OWN RISK.

# CYBER THREAT LANDSCAPE

"Cyber threats from nation states and their surrogates will **remain acute**. Foreign states use cyber operations to **steal information, influence populations, and damage industry**, including physical and digital critical infrastructure."

**Annual Threat Assessment of the US Intelligence Community**, April 8, 2021

"The United States faces persistent and increasingly sophisticated malicious cyber campaigns that **threaten the public sector, the private sector, and ultimately the American people's security and privacy.**"

**Executive Order on Improving the Nation's Cybersecurity, EO 14028: (May 12, 2021)**

## Massive IoT Cyber Breaches Attack Vectors

Fish tank thermometer

Photo credit:
Mirko_Rosenau l Getty Images

Xiaomi Mijia
Smart IP Camera

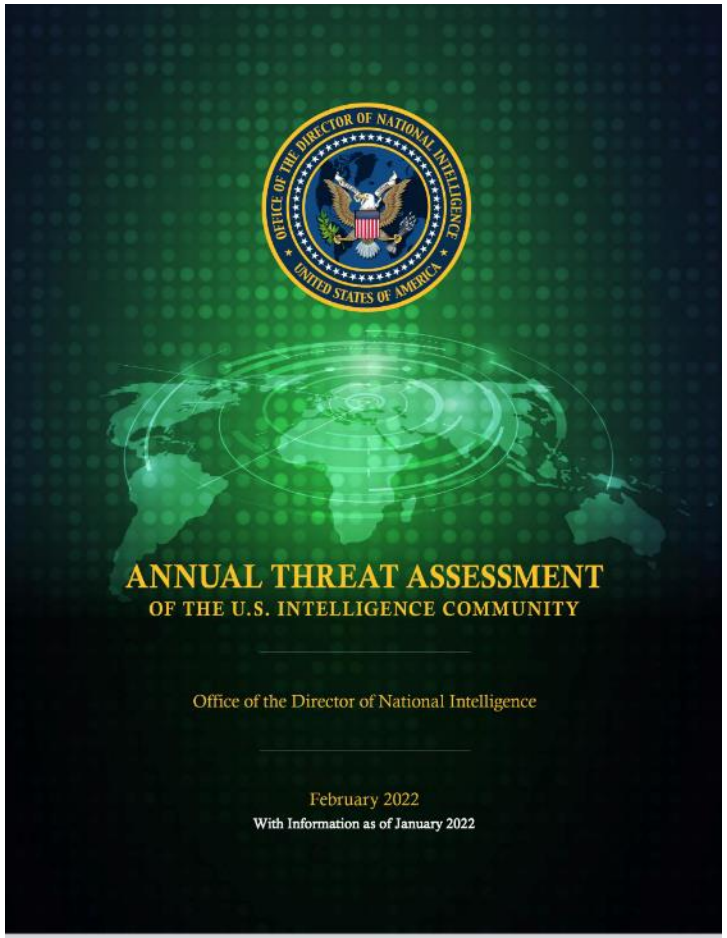
 

# THE THREAT LANDSCAPE

## 2018 – CYBER

"The potential for surprise in the cyber realm will increase in the next year and beyond **as billions more digital devices are connected – with relatively little built-in security –** and both nation states and malign actors become more emboldened and better equipped in the use of increasingly widespread cyber toolkits. . . .

Ransomware and malware attacks have spread globally. . . . "




## 2022 – CYBER

- **CHINA** China is almost certainly capable of launching cyber attacks that would **disrupt critical infrastructure services**, including against **oil and gas pipelines and rail systems**.
- **RUSSIA** Russia is particularly focused on improving its ability to **target critical infrastructure**, including **underwater cables and industrial control systems.**
- **IRAN** Iran's growing expertise and willingness to conduct **aggressive cyber operations** make it a major threat to the security of U.S. and allied networks and data.
- **NORTH KOREA**. Cyber actors linked to North Korea have conducted espionage against **media, academia, defense companies, and governments**, in multiple countries.
- **TRANSNATIONAL CYBER CRIMINALS** are increasing the number, scale, and sophistication of **ransomware attacks**, fueling a virtual ecosystem that threatens to cause greater disruptions of **critical services worldwide**.
- Attackers are focusing on **victims whose business operations lack resilience or whose consumer base cannot sustain service disruptions**, driving ransomware payouts up.

# THE THREAT LANDSCAPE – Use Case = CHINA

THE UNITED STATES DEPARTMENT of JUSTICE

ABOUT OUR AGENCY TOPICS NEWS RESOURCES CAREERS

Home » Office of Public Affairs » News

JUSTICE NEWS

Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE Wednesday, September 16, 2020

**Seven International Cyber Defendants, Including "Apt41" Actors, Charged In Connection With Computer Intrusion Campaigns Against More Than 100 Victims Globally**

**Two Defendants Arrested in Malaysia; Remaining Five Defendants, One of Whom Allegedly Boasted of Connections to the Chinese Ministry of State Security, are Fugitives in China**

- May 2021 – Feb 2022 – Chinese hacking group successfully compromised the computer networks of at least **six U.S. state governments.**
- September 2020 – The Justice Department indicted five Chinese nationals for cyber attacks that **facilitated the theft of source code, software code signing certificates, customer account data, and valuable business information.**
- The intrusions also facilitated **other criminal schemes**, including **ransomware** and **"crypto-jacking" schemes** (unauthorized use of victim computers to "mine" cryptocurrency).

## THE FALLOUT FROM NATION STATE ATTACKS CAN LAND YOU IN COURT!

Computer intrusions affected over **100 victim companies in the U.S. and abroad** – including:

- software development companies,
- computer hardware manufacturers,
- telecommunications providers,
- social media companies,
- video game companies,
- non-profit organizations,
- universities,
- think tanks, and
- foreign governments, as well as pro-democracy politicians and activists in Hong Kong.

# Warning! Storage Security Standards Provide *Notice* of Threats/Risks and Potential Liability

## COMMON COMPLIANCE ISSUES – STORAGE SYSTEMS AND INFRASTRUCTURE

- Unauthorized access and disclosure
- Theft or accidental loss of storage media
- Breach of country-specific **privacy** requirements
- Unlawful **transfer of data** (e.g. moving restricted data out of particular jurisdiction)
- Unauthorized usage of storage resources
- Non-conformance with **policies** (e.g. sanitization)
- Inadequate **data retention and protection**
- Insufficient **evidence of security** (e.g. audit logs and proof of encryption/sanitization).
- Integrity – Corruption/modification and destruction of data, including backup or recovery copies
- Malware (e.g. ransomware) & DDoS attacks on storage systems

"For storage systems and infrastructure the risks associated with data breaches, data corruption or destruction, temporary or permanent loss of access/ availability, and failure to meet statutory, regulatory, or legal requirements are the **major concerns**."

Organizations can incur **significant liabilities and penalties for non-compliance =** costly sanctions and remediation (e.g. breach notifications).

**Country-specific legislation** has an important influence on information security requirements for multi-national organizations.

*Information technology – Security techniques – Storage security,* ISO/IED DIS 27040 § 6.4

*See* NIST SP 800-209 Security Guidelines for Storage Infrastructure (Oct. 2020) § 3

# Is Your Storage Security Reasonable Security? Requirements in State Laws

- **DATA BREACH NOTIFICATION – All 50 states**, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have laws requiring private businesses, and in most states, governmental entities, to **notify individuals of security breaches** of personally identifiable information (PII).
- **DATA SECURITY – At least 25 states** have laws that address data security practices of private sector entities.
- Requirements can vary significantly between different jurisdictions.

## "REASONABLE SECURITY"

- Most of the state data security laws require businesses that own, license, or maintain personal information about a resident of that state to **implement and maintain "reasonable security procedures and practices" appropriate to the nature of the information and to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.**

# Overview: Patchwork of Privacy & Security Laws

## Healthcare

Health Insurance Portability and Accountability Act (HIPAA), 42 U.S.C. § 1306, Privacy and Security Rules; Breach Notification

Genetic Nondiscrimination Act, 42 U.S.C. § 2000ff

## Financial

Right to Financial Privacy Act, 12 U.S.C. § 3402

Gramm-Leach-Bliley Act, 15 U.S.C. § 6801-09

Fair Credit Reporting Act, 15 U.S.C. § 1681

## Telecom

Cable Communications Privacy Act, 47 U.S.C. § 551

Telephone Consumer Protection Act, 47 U.S.C. § 227

Electronic Communications Privacy Act, 18 U.S.C. §§ 2510-21, 2701-11

## Children

Online Privacy Protection Act (COPPA), 15 U.S.C. § 6501

## International

EU General Data Protection Regulation (GDPR)

EU Data Breach Notification

## U.S. States

California Consumer Privacy Act of 2018 (CCPA),

BOTS: Disclosure, Connected Devices

State Data Breach Notification Laws

State Data Disposal Laws

# Financial Institutions – New Security Safeguard Rules Are Prescriptive

## Gramm-Leach-Bliley Act Sections 501 and 505(b)(2)

Requires **banks** to develop, implement, and maintain ***reasonable administrative, technical, and physical safeguards*** to protect the security, confidentiality, and integrity of **customer information.**

## *New* FTC Standards for Safeguarding Customer Information – Safeguards Rule (2021)

Security requirements for **non-bank financial institutions**

- **Written Information Security Program (**comprehensive program for safeguarding customer information)
- **Designation of a Qualified Individual**
- **Periodic Risk Assessments**
- **Program Design Based on Risk Assessment Outcomes**
- **Access and Authentication Controls**
- **Encryption of Customer Information at Rest and in Transit**
- **Multifactor Authentication**
- **Oversight of Service Providers**
- **Penetration Testing and Vulnerability Scanning**
- **Data Retention and Disposal**
- **Incident Response Plan**

# WHAT IS "REASONABLE SECURITY"?

## Reasonable Security Requires A *PROCESS*

- **Assign responsibility for security**
- **Identify the information assets to be protected**
  - Data and information systems (i) under company control and (ii) outsourced
- **Conduct a risk assessment**
  - Identify and evaluate threats, vulnerabilities, and damages (including if you are the manufacturer/ producer/processor OR relying on a 3rd party)
- **Leverage an appropriate security framework** (e.g., ISO/IEC 2700x, CIS 20, NIST 800)
- **Select, develop and implement security controls**
  - Responsive to the risk assessment
  - Address the required "categories" of controls
- **Address third party vendor issues**
- **Educate and train employees and business partners**
- **Continually monitor, and regularly review, reassess, and adjust the program**

*The information security risk management process presented in **ISO/IEC 27005** consists of: context establishment, risk assessment, risk treatment, risk acceptance, risk communication, and risk monitoring and review.*

# NIST CYBER FRAMEWORK – MITIGATE RISKS & STAY OUT OF COURT

## RISK MANAGEMENT = PROCESS

Adopt a **risk management program** that focuses on protection, detection, and response.

This means:

(1) identify key assets,

(2) assess threats to those assets,

(3) mitigate those threats,

(4) deploy detection mechanisms,

(5) build and test a cyber incident response and recovery plan (including public relations), and

(6) provide education and training.


**NIST Cybersecurity Framework**

is a good starting point.

https://www.nist.gov/cyberframework

# THE REGULATORS (there are others)
# Will they come after you?







# “Reasonable Security” Defined by FTC Cases

*FTC brings charges of **unfair and deceptive practices for security failures.***

**SANCTIONS** – Required companies to implement **comprehensive security and privacy programs “reasonably designed to address security risks.”** Imposed fines, *e.g*. Equifax $575 million (2019)

- ***HTC America***—Millions of HTC **smartphone**s were manufactured with insufficient security controls. (2013)
- ***TaxSlayer***—Hackers **accessed thousands of financial accounts** and engaged in tax identity theft. FTC found violations of Gramm Leach Bliley Act. (2017)
- ***ASUSTeK Computer***—Critical security flaws in **routers** put the home networks of hundreds of thousands of consumers at risk. (2016)
- ***D-Link***—Misrepresentations that the company took reasonable steps to secure its **wireless routers and Internet-connected cameras**. (2019)
- ***Tapplock***—Falsely claimed its Internet-connected **smart locks** were designed to be “unbreakable” and secure. (2020
- ***BLU Products***—Cell phone company **software installed on consumers’ devices** transmitted personal information to third parties without their knowledge. (2018)
- ***LightYear Dealer Technologies***—Auto dealer **software** provider failed to take reasonable steps to secure consumers' data (2019)

# *New* SEC Proposes Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies

"Today, cybersecurity is an emerging risk with which public issuers increasingly must contend. Investors want to know more about how issuers are managing those growing risks."

SEC Chair Gary Gensler (draft for comment March 9, 2022)

The proposed amendments would require, among other things:

- Current reporting about **material cybersecurity incidents** and periodic reporting to provide updates about previously reported cybersecurity incidents.
- Periodic reporting about a registrant's **policies and procedures to identify and manage cybersecurity risks**; the registrant's board of directors' oversight of cybersecurity risk; and management's role and expertise in **assessing and managing cybersecurity risk and implementing cybersecurity policies and procedures.**
- Annual reporting or certain proxy disclosure about the **board of directors' cybersecurity expertise**, if any.

# IoT Cybersecurity Improvement Act
## *New* federal law/ new industry standard?

**1)** NIST *Recommendations for Security of IoT Devices* (purchased by the federal government)

NIST SP 800-213 (Nov. 29, 2021), includes:

- Secure development
- Identity management
- Patching
- Configuration management
- Vulnerability Management

**2)** NIST Guidelines on *Vulnerability Disclosure and Remediation,* NIST 800-216 (draft)

**3)** Contractors and Vendors to publish *Coordinated Vulnerability Disclosure Policies*

# *New* State Laws Define IoT "Reasonable Security Features"

## California and Oregon

State IoT laws are intended to create ***minimum security requirements*** **for Internet-connected devices.**

"**Reasonable security features**" should be:

- appropriate for the ***nature and function of the device***;
- appropriate for the ***information*** the device collects, contains, or transmits; and
- designed to ***protect the device and any information contained*** therein from unauthorized access, destruction, use, modification, or disclosure.

Laws are *vague* about *what this means*.

# Updated Storage Security Standards – ISO, NIST, PCI *New Standards of Care* for Cyber Litigation?

## HOW A DATA BREACH CASE IS WON/LOST IN COURT

**Failure to exercise reasonable care** may lead to **liability**, if such a **failure caused an injury.** Four conditions (elements) must be met:

1) **Duty** – The **level of care that a reasonable person would exercise** in the circumstances – Industry standards?
2) **Breach of duty = data breach**
3) **Harm/ damage/ injury**
4) **Causation**

### Causation: Liability Exposure?

**Who is responsible for a breach** when security vulnerabilities are found on an (1) **IoT device**, in the (2) **network** (including supply chain), or in the (3) **IoT infrastructure**?

- Developer?
- Manufacturer?
- Seller?
- Tech integrator?
- Data Owner?

# Is Your Storage Security "Reasonable Security"?

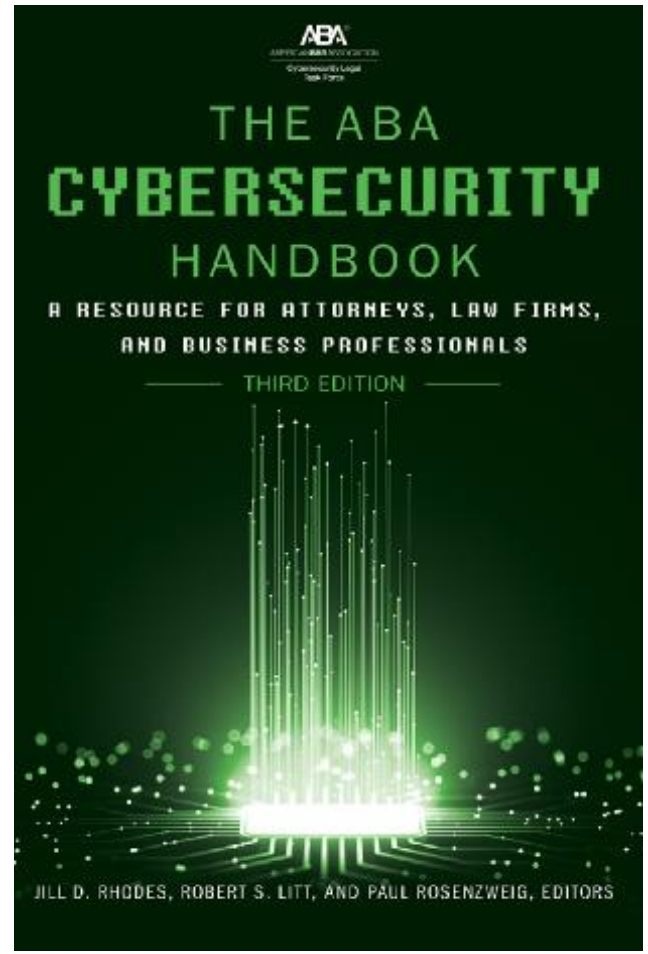
## ACTION STEPS

- ✓**Understand the cyber threats and risks** and address them in your storage security architecture, systems and infrastructure
- ✓**Follow security and privacy-by-design –** build into your storage security business model and storage systems and infrastructure
- ✓Develop plans to **comply with the most restrictive** laws and security standards
- ✓Follow the **well-accepted process for "reasonable security"**
- ✓Conduct a **risk assessment**
- ✓Assess security of **business partners** and **3P vendors**
- ✓Secure the **supply chain**; follow EO 14028 SBOM; information sharing; zero trust architecture
- ✓**Continually monitor** the legal and threat landscape and security of storage systems and infrastructure

# RESOURCES


- NIST Cybersecurity Framework v 1.1
- ISO/IEC 27002:2022 (3rd Ed.) (Feb. 2022) Information security, cybersecurity and privacy protection — Information security controls
- ISO/IEC 27040:2015 – Information technology - Security techniques - Storage security
- NIST SP 800-53A Rev. 5, Assessing Security and Privacy Controls in Information Systems and Organizations (Jan. 2022)
- NIST SP 800-209, Security Guidelines for Storage Infrastructure (Oct. 2020)
- Payment Card Industry (PCI) Data Security Standard (DSS) (2022)



Lucy L. Thomson
lucythomson1@mindspring.com

## SPEAKER

**Lucy L. Thomson,** Esq. CISSP CIPP/US
Founding Principal, Livingston PLLC
Washington, D.C.

- *ABA Internet of Things: Legal Issues, Policy, and Practical Strategies,* Co-editor
- *Data Breach and Encryption Handbook,* Editor


# Please take a moment to rate this session.

Your feedback is important to us.