



ESX

ELECTRONIC SECURITY EXPO
SECURITY CONNECTED.

**The Internet of Litigation:
Security. IoT. Cyber Attacks.**

1



ESXWEB.COM/FEEDBACK

- 1**
Answer 5 Questions About This Session
- 2**
Gain access to the PPT Slides
- 3**
Be Entered to Win a \$100 Gift Card

3 GIFT CARDS (\$100 EACH) AVAILABLE FOR SURVEY RESPONDENT RAFFLES.

WINNERS WILL BE NOTIFIED THROUGH THE ESX APP

2

THE ELECTRONIC SECURITY EXPO IS OWNED BY:

ESA ELECTRONIC SECURITY ASSOCIATION®

3



Anti-Trust

- Neither ESA nor any committee, product group, conference or activity of ESA shall be used for the purpose of bringing about, or attempting to bring about, any understanding or agreement, whether written or oral, formal or informal, express or implied, among competitors with regard to prices, terms or conditions of sale, discounts, distribution, volume of production, territories or customers.

#ESX2022
SECURITY
CONNECTED.

THE INTERNET OF LITIGATION: SECURITY. IOT. CYBER ATTACKS. | ESX 2022

4



ELECTRONIC SECURITY EXPO

COURSE OBJECTIVES

- What product vulnerabilities and litigation exposure does the security industry have?
- What are the responsibilities of the various stakeholders in the delivery of the product or service?
- What are the best practices that mitigate the risk of exposure to litigation from the manufacturer to the installing company?
- Are there any legislation, regulations or protocol solutions that will ensure end users and service providers are not inadvertently or unknowingly adding a connected device that exposes their privacy?

5



ELECTRONIC SECURITY EXPO

MEET THE SPEAKER



Samantha Southall

Buchanan
Ingersoll · Rooney

6



Introduction

#ESX2022
SECURITY
CONNECTED.

THE INTERNET OF LITIGATION: SECURITY. IOT. CYBER ATTACKS. | ESX 2022

7

Internet of Things (IoT)

- A system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers and the ability to transfer data over a network without requiring human to human or human to computer interaction.
 - A person with a heart monitor implant
 - A farm animal with a biochip transponder
 - A car that has built in sensors to alert the driver when tire pressure is low



#ESX2022
SECURITY
CONNECTED.

THE INTERNET OF LITIGATION: SECURITY. IOT. CYBER ATTACKS. | ESX 2022

8

Internet of Things

- IoT is a concept of connecting any device with an on/off switch to the internet and/or each other.
 - Cellphones
 - Washing machines
 - Headphones
 - Wearable Devices
- The dominant consumer IoT device is the Smart TV
 - Between 25-35% of consumers worldwide own a television that can connect to the Internet, according to Deloitte research.

#ESX2022
SECURITY
CONNECTED.

THE INTERNET OF LITIGATION: SECURITY. IOT. CYBER ATTACKS. | ESX 2022

9

IoT Ecosystem

- An IoT ecosystem consists of internet enabled smart devices that use embedded processors, sensors and communication hardware to collect, send and act on data they acquire from their environments
- IoT devices share the sensor data they collect from connecting to an IoT gateway or other device where data is either sent to the cloud to be analyzed or analyzed locally



#ESX2022
SECURITY
CONNECTED.

THE INTERNET OF LITIGATION: SECURITY. IOT. CYBER ATTACKS. | ESX 2022

10

Consumer and Enterprise IoT Applications[®]



#ESX2022
SECURITY
CONNECTED.

THE INTERNET OF LITIGATION: SECURITY. IOT. CYBER ATTACKS. | ESX 2022

11

IoT Challenges

Security, Privacy and Data Sharing Issues

- Because IoT devices are closely connected, all a hacker has to do is exploit one vulnerability to manipulate all the data, rendering it unusable.
- Manufacturers that don't update their devices regularly -- or at all -- leave them vulnerable to cybercriminals.
- Privacy is another major concern for IoT users.
 - Companies that make and distribute consumer IoT devices could use those devices to obtain and sell users' personal data.

#ESX2022
SECURITY
CONNECTED.

THE INTERNET OF LITIGATION: SECURITY. IOT. CYBER ATTACKS. | ESX 2022

12



Legal Landscape

#ESX2022
SECURITY
CONNECTED.

THE INTERNET OF LITIGATION: SECURITY. IOT. CYBER ATTACKS. | ESX 2022

13

Legal Requirements for Protecting Personal Data

- Federal laws:
 - Health and consumer credit records
 - Consumer protection (unfair trade practices and deceptive advertising)
 - Government contractors required to secure government data
- State laws:
 - Data breach notification laws for breach of personally identifiable information
 - Duty to implement “reasonable” data security measures
 - Consumer protection laws
 - Emerging: state privacy laws
- International privacy laws: EU General Data Protection Regulation and many other countries’ data protection laws (including Brazil)
- Private contracts—confidentiality and, increasingly, security
- Industry standards for payment cards and ACH funds transfer

#ESX2022
SECURITY
CONNECTED.

THE INTERNET OF LITIGATION: SECURITY. IOT. CYBER ATTACKS. | ESX 2022

14

Thrust of U.S. Data Protection Laws

PROTECT:

- Security
- Confidentiality
- Integrity
- Availability
- Privacy

AGAINST:

- Unauthorized disclosure
- Unauthorized access
- Unauthorized acquisition
- Unauthorized use
- Alteration
- Destruction
- Loss

#ESX2022
**SECURITY
CONNECTED.**

Cybersecurity v. Privacy

Cybersecurity Risks

Loss of :

- Confidentiality
- Integrity
- Availability

**SECURITY
BREACH**

Privacy risks:

- Embarrassment
- Stigma
- Discrimination
- Economic loss
- Physical harm
- Sanctity of personal space

#ESX2022
**SECURITY
CONNECTED.**

Common Features of State Breach Notification Laws

- Each state protects its own residents regardless of where the responsible party is located
- Each state requires notification to individuals affected by a data breach
- Not industry specific
- **Laws are covering more categories of personal information and requiring shorter periods before notification must be given**

#ESX2022
SECURITY
CONNECTED.

THE INTERNET OF LITIGATION: SECURITY. IOT. CYBER ATTACKS. | ESX 2022

17

But, State Breach Notification Laws Vary Significantly:

- What types of personal information are protected
- What is a “breach of security” (unauthorized access or acquisition)
- Whether notice is required only if there is a “reasonable likelihood of harm”
- Timing of notice: how long after breach is “discovered” or “determined”
- Method and content of required notice
- Whether notice to state Attorney General is required
- Whether notice to Attorney General is published online
- Whether paper records are covered
- What penalties are imposed
- Whether consumers have a private right of action (at least 18 states)

#ESX2022
SECURITY
CONNECTED.

THE INTERNET OF LITIGATION: SECURITY. IOT. CYBER ATTACKS. | ESX 2022

18

New and Pending Cybersecurity Regulation

- Executive Order: Federal agencies to adopt regulations requiring cybersecurity standards and breach notification for critical infrastructure (16 industry sectors)
- IoT Cybersecurity Improvement Act of 2020:
 - NIST to develop standards managing and disclosing security vulnerabilities in IoT devices
 - Enforcement begins December 5, 2022

#ESX2022
SECURITY
CONNECTED.

THE INTERNET OF LITIGATION: SECURITY. IOT. CYBER ATTACKS. | ESX 2022

19

New and Pending Cybersecurity Regulation

- Legislative action on consumer privacy protection:
 - California at the forefront with California Privacy Rights Act effective January 1, 2023
 - Colorado, Virginia, Utah, Connecticut
 - Other states expected to follow this year or next—New York, Washington, others
 - Federal legislation introduced—again
 - Consumer class actions containing more privacy-based claims
- Tightening scrutiny of third-party risk management practices:
 - Contract obligations
 - Access restrictions
 - Security assessments
 - Formal third-party risk management programs

#ESX2022
SECURITY
CONNECTED.

THE INTERNET OF LITIGATION: SECURITY. IOT. CYBER ATTACKS. | ESX 2022

20

Allegations in Data Breach in Enforcement Actions and Private Litigation

- Defendant failed to reasonably safeguard information:
 - Failed to encrypt sensitive information
 - Failed to have adequate technical controls
 - Failed to train personnel
 - Failed to have adequate data security program
 - Failed to monitor vendor security
- Failed to respond timely or adequately to the breach
- Material disparity between security promised and security delivered

#ESX2022
SECURITY
CONNECTED.

THE INTERNET OF LITIGATION: SECURITY. IOT. CYBER ATTACKS. | ESX 2022

21

Private Litigation

- Claims based on negligence, breach of contract, breach of fiduciary duty, invasion of privacy, breach of a duty of confidentiality and conversion
- Plaintiffs face difficult issues of standing, injury, causation, and class certification
- Defense is expensive, even if cases are dismissed
- Some states provide some form of private right of action for failure to use reasonable measures to protect PII

#ESX2022
SECURITY
CONNECTED.

THE INTERNET OF LITIGATION: SECURITY. IOT. CYBER ATTACKS. | ESX 2022

22



Ways to Mitigate Challenges Posed by IoT

#ESX2022
SECURITY
CONNECTED.

THE INTERNET OF LITIGATION: SECURITY. IOT. CYBER ATTACKS. | ESX 2022

23

Understand Your Business

- Where do you operate?
 - Europe
 - United States
- Federal requirements are often industry specific
 - Financial services
 - Healthcare
 - Government Contractors
- With whom do you work (or with whom do they work)?

Understand Your Data

- To whom does the data relate?
 - State laws often protect PII relating to state residents
- What type of data do you have
 - Personal v. pseudonymous v. anonymous
 - Biometrics
- What entity is the controller?
- How long do you need to retain the data?

#ESX2022
SECURITY
CONNECTED.

THE INTERNET OF LITIGATION: SECURITY. IOT. CYBER ATTACKS. | ESX 2022

24

Understand Where Your Data is Processed or Stored

- What is processing?
- Where is the data processed?
 - Increased importance of cloud storage
- How does the data travel?



Understand How Your Data Is Used

- What do you say about processing?
 - Privacy Policy
 - Privacy Notice
 - Other Public Statements
- Do you obtain consent?
 - Scope of the consent
 - Was consent "freely given?"
- Data maps and flows
- Privacy by design

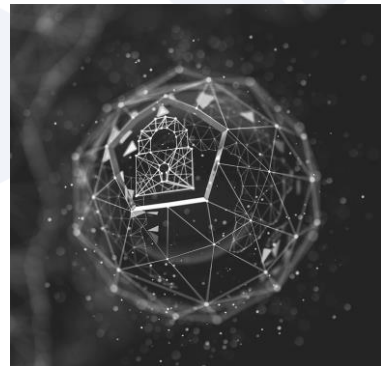
#ESX2022
**SECURITY
CONNECTED.**

THE INTERNET OF LITIGATION: SECURITY. IOT. CYBER ATTACKS. | ESX 2022

25

Understand Your Collection Points

- Notice and Consent
- Notice at Collection Requirements
 - CCPA
 - BIPA
- What must be in the notice
- Conspicuousness requirements
- GLBA requirements
 - Customer
 - Consumer



#ESX2022
**SECURITY
CONNECTED.**

THE INTERNET OF LITIGATION: SECURITY. IOT. CYBER ATTACKS. | ESX 2022

26

Understand Your Contracts

- Contractual requirements often go beyond legal or regulatory ones
- Representations and warranties
- Indemnification
- CPRA liability exemption

Understand Your Vendor Relationships and Practices

- What entities perform services related to personal data?
- Risk rating relationships
- Oversight requirements
 - Standards as a tool to simplify selection and oversight

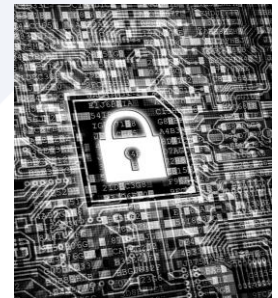
#ESX2022
**SECURITY
CONNECTED.**

THE INTERNET OF LITIGATION: SECURITY. IOT. CYBER ATTACKS. | ESX 2022

27

Understand Security Breach (and Incident) Risks and Requirement's

- What is an incident and what is a breach?
- Notice obligations
 - Owners
 - Consumer
 - Attorneys General (or other governmental entities)
 - Non-owners
 - Owner
 - Contracts
- Common attacks and litigation risks



#ESX2022
**SECURITY
CONNECTED.**

THE INTERNET OF LITIGATION: SECURITY. IOT. CYBER ATTACKS. | ESX 2022

28

Understand the Applicable Law

- What law applies?
 - Overlapping requirements
- Who can sue?
 - Private rights of action
 - Actions by Attorneys and the Federal Trade Commission
- Developing Case Law
- Developing Statutory Frameworks
- Difficult Issues of Privilege

Understand Your Insurance Coverage

- Rise of cyber insurance
- Lack of standardization
- Importance of brokers
- Coverage disputes
- Issues to address before an incident

#ESX2022
SECURITY
CONNECTED.

THE INTERNET OF LITIGATION: SECURITY. IOT. CYBER ATTACKS. | ESX 2022

Thank you

Samantha Southall



- Phone: 215 665 3884
- Email: samantha.southall@bipc.com

#ESX2022
SECURITY
CONNECTED.

THE INTERNET OF LITIGATION: SECURITY. IOT. CYBER ATTACKS. | ESX 2022

ELECTRONIC SECURITY EXPO

RATE THIS SESSION
ESXWEB.COM/FEEDBACK

★★★★★

31

ELECTRONIC SECURITY EXPO

JOIN US

ESX 2023 | JUNE 5-8 | LOUISVILLE, KY

ESX2022
SECURITY PROTECTED.

32