SNIA NSF | NETWORKING STORAGE

Storage Networking Security Series: Security & Privacy Regulations

Live Webcast

July 28, 2020

10:00 am PT

Today's Presenters

J Metz

Chair, SNIA Board of Directors

Thomas Rivera, CISSP

Co-Chair, SNIA Data Protection & Privacy Committee
Secretary, IEEE CS Cybersecurity & Privacy Standards Committee
Chair, IEEE Zero Trust Working Group

Eric Hibbard, CISSP, CIPT, CISA

Chair, SNIA Security Technical Work Group
Chair, INCITS TC CS1 Cyber Security
Chair, IEEE CS Cybersecurity & Privacy Standards Committee

SNIA Legal Notice

- The material contained in this presentation 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 containing material from these presentations
- This presentation is a project of the SNIA
- Neither the authors nor the presenters are attorneys and 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 authors' personal opinion and current understanding of the relevant issues involved
  - The authors, the presenters, 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

SNIA-At-A-Glance

SNIA-at-a-Glance

185
industry leading organizations

2,000
active contributing members

50,000
IT end users & storage pros worldwide

Learn more: **snia.org/technical** **@SNIA**

Technologies We Cover

- Ethernet
- iSCSI
- NVMe-oF
- InfiniBand
- Fibre Channel, FCoE
- Hyperconverged (HCI)
- Storage protocols (block, file, object)
- Virtualized storage
- Software-defined storage

SNIA NSF | NETWORKING STORAGE

Learning Objectives

- Understand how privacy and security is characterized
- Data retention and deletion requirements
- Core data protection requirements of sample privacy regulations from around the globe
- The role that security plays with key privacy regulations
- Implications and consequences

Security & Privacy Characterization

Threat Landscape – Security

- Social Engineering
- Advanced Persistent Threat (APT)
- Ransomware/Malware
- Unpatched/Updated Systems
- Security Misconfiguration
- Denial of Service
- Sensitive Data Exposure
- Injection Flaws
- Cryptojacking
- Cyber Physical Attacks
- Broken Authentication
- Broken Access Control
- Third Party (Supplier)
- Insider Theft
- Mobile Malware
- Physical Loss of Devices
- Cross-site Scripting (XSS)
- Man-in-the-Middle Attacks
- IoT Weaponization

Threat Landscape – Privacy

- Information Collection
  - Surveillance
  - Interrogation
- Information Processing
  - Aggregation
  - Identification
  - Insecurity
  - Secondary Use
  - Exclusion
- Information Dissemination
  - Breach of Confidentiality
  - Disclosure
  - Distortion
  - Exposure
  - Increased Accessibility
  - Blackmail
  - Appropriation
- Intrusion & Decisional Interference

Daniel J. Solove, "A Taxonomy of Privacy," University of Pennsylvania Law Review 154

Balance Security and Compliance

Data Security

- Proactive
- Defense-in-depth
- Physical, technical and administrative control areas
- Preventive, detective and corrective control types

Compliance

- Reactive
- Accountability
- Traceability
- Monitoring & Reporting
- Risk Management
- Often the driver for security

ISO/IEC 27001 (Information Security Management)

There are 114 security controls in 14 groups and 35 control categories:

- Information security policies (2 controls)
- Organization of information security (7 controls)
- Human resource security - 6 controls that are applied before, during, or after employment
- Asset management (10 controls)
- Access control (14 controls)
- Cryptography (2 controls)
- Physical & environmental security (15 controls)
- Operations security (14 controls)
- Communications security (7 controls)
- System acquisition, development & maintenance (13 controls)
- Supplier relationships (5 controls)
- Information security incident management (7 controls)
- Information security aspects of business continuity management (4 controls)
- Compliance; with internal requirements, such as policies, and with external requirements, such as laws (8 controls)

ISMS Example – Media Handling

- Management of removable media
- Disposal of media
- Physical media transfer

NOTE: Underlying requirement is to make sensitive data go away

- ISO/IEC 27040 addresses media/data sanitization
  - Sanitization options: clear, purge (include cryptographic erase), destruct
  - Technology specific procedures

Privacy Versus Data Protection

- The rules and safeguards applying under various laws and regulations to ***personal data*** about ***individuals*** that organizations collect, store, use and disclose
- "***Data protection***" is the professional term used in the EU, whereas in the U.S. the concept is generally referred to as "***information privacy***"
- Importantly, data protection is **different** from data security, since data security extends beyond securing information to devising and implementing policies for its fair use

Source: International Association of Privacy Professionals (IAPP) Glossary

Main Areas of Privacy

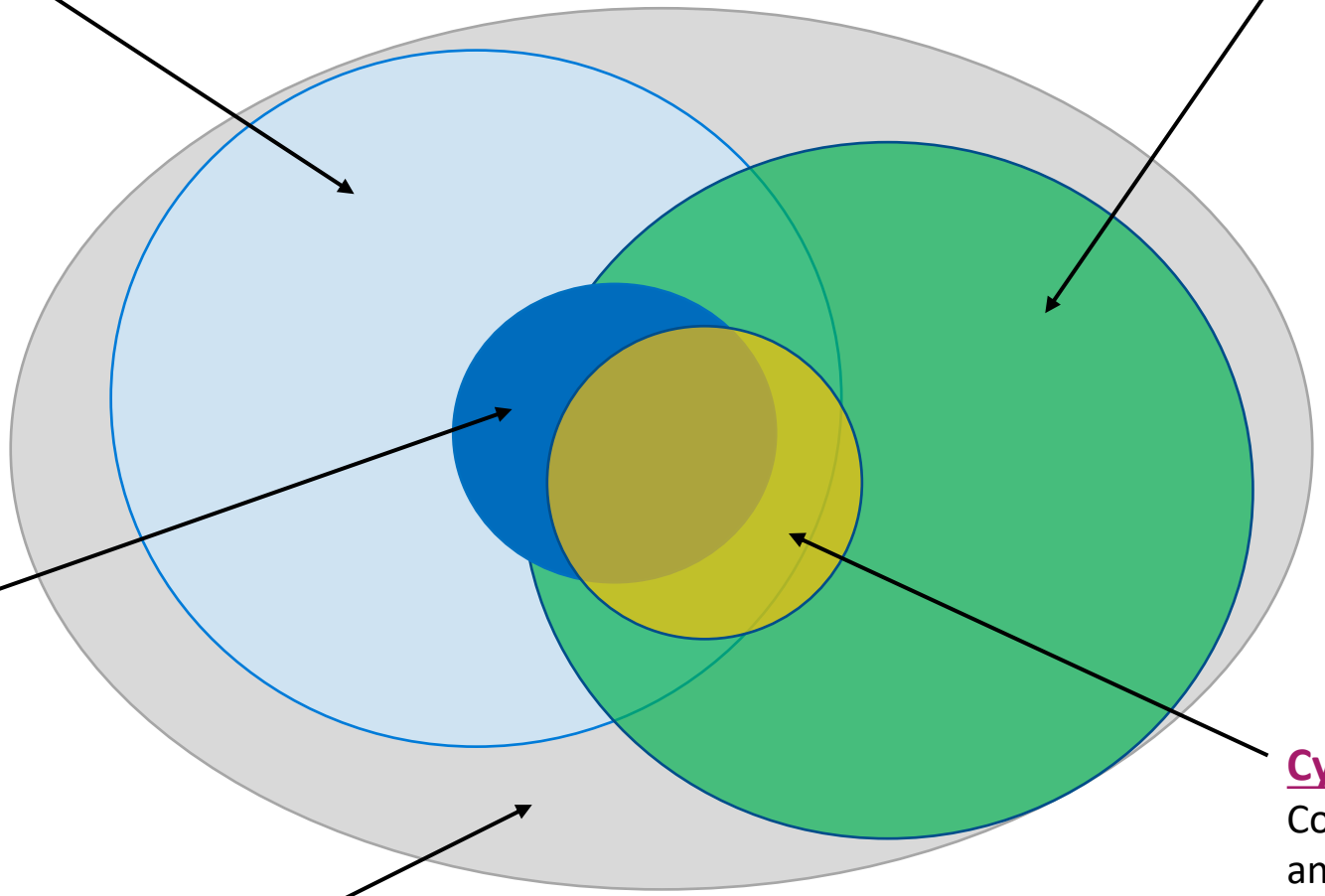
- **Information Privacy** – The claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others
- **Bodily Privacy** – It focuses on a person's physical being and any invasion thereof (e.g., genetic testing, drug testing or body cavity searches)
- **Territorial Privacy** – It is concerned with placing limitations on the ability of one to intrude into another individual's environment (not limited to the home; it may be defined as the workplace or public space and environmental considerations can be extended to an international level)
- **Communications Privacy** – It encompasses protection of the means of correspondence, including postal mail, telephone conversations, electronic e-mail and other forms of communicative behavior and apparatus

Common Privacy Principles

- Collection Limitations
- Data Quality
- Purpose Specification
- Use Limitation
- Security Safeguards
- Openness
- Individual Participation
- Accountability

Privacy: Collection Limitations, Data Quality, Purpose Specification, Use Limitation, Security Safeguards, Openness, Individual Participation, Accountability

Information Security: Ensures Confidentiality, Integrity, and Availability (CIA) of information



Personal Data Protection: Safeguards applying under various laws and regulations to personal data (PII, PHI, etc.) about individuals that organizations collect, store, use and disclose

Ethics: Moral principles that govern a person's behavior or the conducting of an activity

Cybersecurity: Ensures Confidentiality, Integrity, and Availability of data; Identify, Protect, Detect, Respond, Recover

Privacy & Security Summarized

What is Privacy?

- In some parts of the world, privacy has often been regarded as an element of liberty, the right to be free from intrusions government
- Privacy is realized through legal means – not through technology
- Data Protection deals with the technical framework

What is Security? (As it relates to data)

- Measures taken to guard against loss of or unauthorized access, destruction, use, modification, or disclosure of data
- Core elements are confidentiality, integrity, and availability of data
- Frameworks focus on identify, protect, detect, respond, recover

Privacy* is dependent upon *Security*; however *Security* is not dependent upon *Privacy

Data Protection Regulation Sampler

(The Good, The Bad, and The Ugly)

Personally Identifiable Information (PII)

Different definitions in each country

ISO/IEC 29100:2011 (Privacy Framework) defines:

> *PII: "any information that:*
> *(a) can be used to identify the PII principal to whom such information relates, or*
> *(b) is or might be directly or indirectly linked to a PII principal*
> *NOTE: To determine whether a PII principal is identifiable, account should be taken of all the means which can reasonably be used by the privacy stakeholder holding the data, or by any other party, to identify that natural person."*
>
> *PII principal: Natural person to whom the personally identifiable information (PII) relates*
> *NOTE: Depending on the jurisdiction and the particular data protection and privacy legislation, the synonym "data subject" can also be used instead of the term "PII principal".*

Example:

- A user's IP address is not classified as PII on its own, but is classified as a linked PII
  - However, in the GDPR, the IP address of an Internet subscriber may be classed as personal data

Sample Privacy Regulations

- EU General Data Protection Regulation (GDPR):
  - Enforcement went into effect on May 25, 2018
  - GDPR mandates a baseline set of standards for companies that handle EU citizens' data to better safeguard the processing and movement of citizens' personal data

- California Consumer Protection Act (CCPA):
  - Went into effect on January 1, 2020
  - CCPA provides enhanced privacy rights & consumer protection for CA residents

- California IoT Law (S.B. 327):
  - Went into effect on January 1, 2020
  - This privacy law regulates Internet of Things (IoT) connected devices

EU “Data Protection” Described

Data Protection as defined by the EU

- Data protection is about protecting any information relating to an identified or identifiable natural (living) person (“data subject”), including names, dates of birth, photographs, video footage, email addresses and telephone numbers
- Data protection has precise aims to ensure the fair processing (collection, use, storage) of personal data by both the public and private sectors

Data Protection Regulation

- EU law entitles individuals to exercise specific data protection rights and requires (public or private sector) organisations that process their data to permit the exercise of these rights
- In April 2016, the EU adopted a new privacy framework - the General Data Protection Regulation (GDPR), including additional directives for the areas of law enforcement & police

GDPR & PII

- GDPR requirements apply to each member state of the European Union, aiming to create more consistent protection of consumer and personal data across EU nations

- Some of the key privacy and data protection requirements of the GDPR include:
  - Requiring the consent of subjects for data processing
  - Anonymizing collected data to protect privacy
  - Providing data breach notifications
  - Safely handling the transfer of data across borders
  - Requiring certain companies to appoint a data protection officer to oversee GDPR compliance
  - Right to be forgotten

- GDPR mandates a baseline set of standards for companies that handle EU citizens' data to better safeguard the processing and movement of citizens' personal data

CCPA: Personal Information (PI)

- CCPA aims to provide enhanced privacy rights & consumer protection for CA residents and under CCPA businesses must:
  - Disclose the PI collected, sold, or disclosed for a business purpose, and inform consumers of the categories of PI collected and purposes of their PI usage
  - Not discriminate against any consumer who exercises their rights under CCPA
  - Provide the consumer with access to their data
  - On request, delete the PI of the consumer - including if the data has been shared with a 3rd-party
  - Provide the consumer with the capability to opt-out
- CCPA applies to for-profit businesses that collect the PI of CA consumers

California Internet of Things (IoT) Security Law

- The law applies to manufacturers and requires all “connected devices” sold or offered for sale in California to have “reasonable security” measures
- “Connected device” means any device, or other physical object that is capable of connecting to the Internet, directly or indirectly, and that is assigned an Internet Protocol address or Bluetooth address
  - Medical devices, copy machines, headsets, automobile entertainment centers, smart watches, smart appliances, etc.
- Device required to be equipped with a reasonable security feature(s) that are all of the following:
  - Appropriate to the nature and function of the device
  - Appropriate to the information it may collect, contain, or transmit
  - Designed to protect the device and any information contained therein from unauthorized access, destruction, use, modification, or disclosure
- If a connected device is equipped with a means for authentication outside of a LAN, either a preprogrammed password that is unique to each device manufactured or a security feature that requires a user to generate a new means of authentication before access is granted to the device for the first time is required
- Commentary: The use of “reasonable security” is sufficiently vague that it may be left to the lawyers to determine whether the requirements have been met

EU Lot 9EU ErP Regulations – Lot 9

- ErPis DIRECTIVE 2009/125/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 21 October 2009 establishing a framework for the setting of ecodesign requirements for energy-related products
- Applies to enterprise servers, data storage and ancillary equipment
- From 1 March 2020, a functionality for secure data deletion shall be made available for the deletion of data contained in all data storage devices of the product
- Secure data deletion means the effective erasure of all traces of existing data from a data storage device, overwriting the data completely in such a way that access to the original data, or parts of them, becomes infeasible for a given level of effort

- Commentary: The overwriting requirement for storage may not actually eliminate data and if used, could result in a data breach [Explicit and not adequate!]

Security Failures

Implications

- Ransomware
- Data Breaches
- Advanced persistent threats
- Unfulfilled contractual obligations
- Supply chain insecurity
  - Counterfeits
  - Disruptions

Consequences

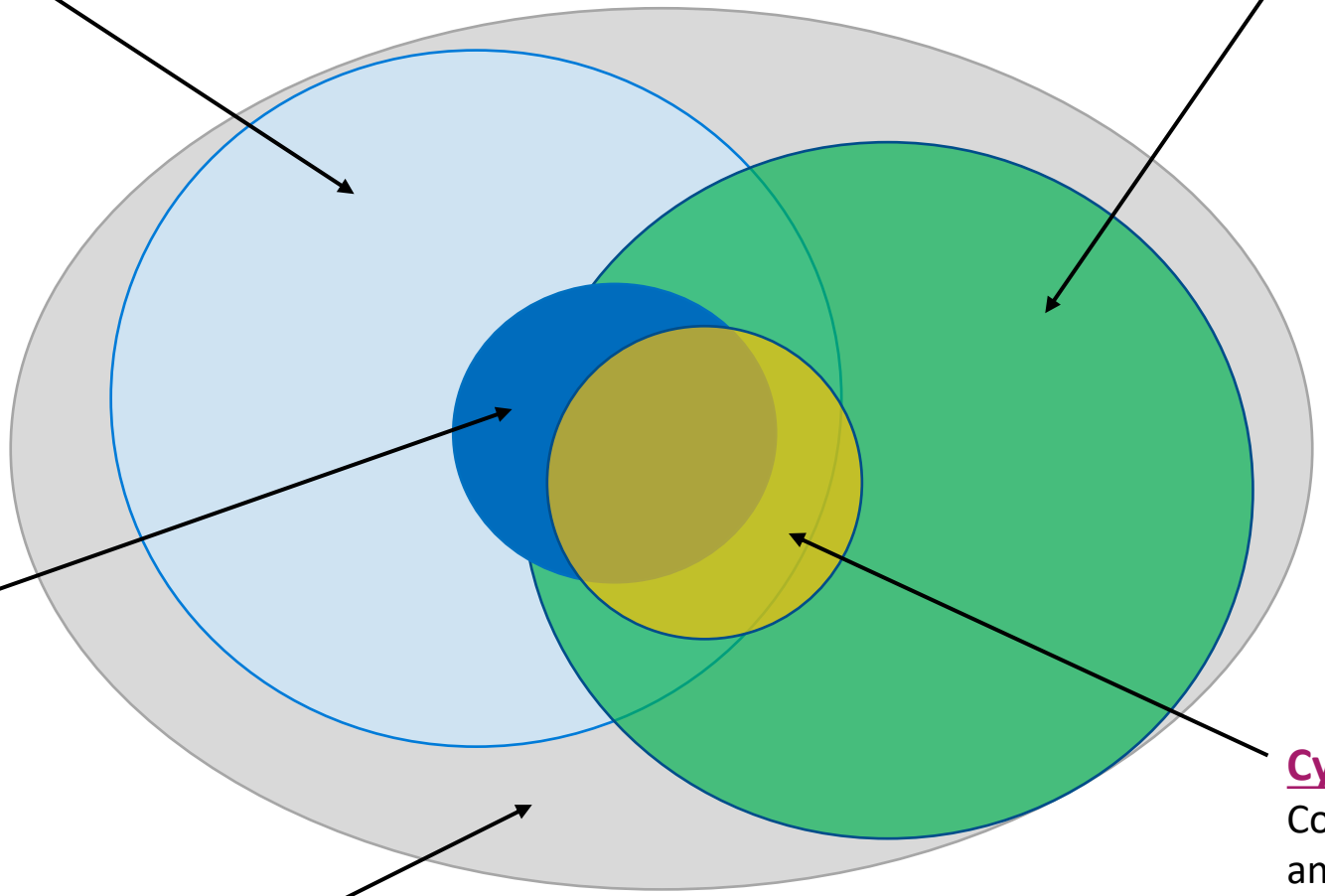
- Liabilities
- Incident response costs
- Loss of intellectual property
- Cyber extortion costs
- Business interruption
- Legal and regulatory fines & penalties
- Contractual fines & penalties
- Loss of reputation
- Systems damage

Security & Privacy Regulations: Summary

- Regulations that focus on risk as opposed to specific security features are essentially future-proofed
  - Organizations need to pay attention to their risk situation and tolerance
- Privacy/data protection requirements may change security prioritizations
- Requirements can be introduced as part of unrelated regulations
- Operating in multiple jurisdictions can result in complicated compliance scenarios

Privacy: Collection Limitations, Data Quality, Purpose Specification, Use Limitation, Security Safeguards, Openness, Individual Participation, Accountability

Information Security: Ensures Confidentiality, Integrity, and Availability (CIA) of information



Personal Data Protection: Safeguards applying under various laws and regulations to personal data (PII, PHI, etc.) about individuals that organizations collect, store, use and disclose

Ethics: Moral principles that govern a person's behavior or the conducting of an activity

Cybersecurity: Ensures Confidentiality, Integrity, and Availability of data; Identify, Protect, Detect, Respond, Recover

Key Takeaways

- Privacy is dependent upon Security; however, Security is not dependent upon Privacy
- Jurisdictional variance can be significant for privacy
- Imprecise language in regulations can complicate compliance or undermine the original objective of the regulation
- Data indiscretions involving personal data appear to get more coverage in recent regulations than other types of data (e.g., intellectual property)

A Few Words from the Panel

Q&A Panel Discussion

J Metz

Chair, SNIA Board of Directors

Thomas Rivera, CISSP

Co-Chair, SNIA Data Protection & Privacy Committee
Secretary, IEEE Cybersecurity & Privacy Standards Committee
Chair, IEEE Zero Trust Working Group

Eric Hibbard, CISSP, CIPT, CISA

Chair, SNIA Security Technical Work Group
Chair, INCITS TC CS1 Cyber Security
Chair, IEEE CS Cybersecurity & Privacy Standards Committee

Our Next Storage Networking Security Webcast

Applied Cryptography

August 5, 2020

Register at:

https://www.brighttalk.com/webcast/663/424155

More SNIA Security Resources

- Storage Networking Security Webcast Series: On-demand at the SNIA Educational Library: snia.org/educational-library
  - Understanding Storage Security and Threats
  - Protecting Data at Rest
  - Encryption 101
  - Key Management 101
- Follow us on Twitter @SNIANSF for dates and times of others planned:
  - Protecting Data in Transit
  - Securing the Protocol
  - Securing the System: Hardening Methods

Additional SNIA Resources

- Learn more about SNIA:
  - https://www.snia.org
- The Networking Storage Forum (NSF):
  - https://www.snia.org/forums/nsf/technology
- The Security Technical Working Group within SNIA:
  - https://www.snia.org/securitytwg
- The Data Protection & Privacy Committee (DPPC):
  - https://www.snia.org/dppc

After this Webcast

- Please rate this webcast and provide us with your feedback
- This webcast and a copy of the slides will be available at the SNIA Educational Library https://www.snia.org/educational-library
- A Q&A from this webcast, including answers to questions we couldn't get to today, will be posted on our blog at https://sniansfblog.org/
- Follow us on Twitter @SNIANSF

Thank you for Attending!

