NCSL Legislative Summit Preconference | July 31, 2022
Denver, Colorado

Jim Dempsey
Lecturer, UC Berkeley School of Law
Senior Policy Advisor, Stanford Cyber Policy Center
jdempsey@berkeley.edu

Photo by James St. John from https://www.flickr.com/photos/47445767@N05/50493464958/

The relationship between data privacy and cybersecurity

Data security has long been one element of "fair information practices":

- HEW Code (1973)
- OECD Principles (1980, rev. 2013)
- EU Data Protection Directive (1995)
- US Department of Homeland Security (2008)
- EU GDPR (2016):
  - Art. 32: Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk

Evolution of privacy

- Right to be forgotten
- Surveillance capitalism – attention capture
- Algorithmic fairness
- Facial recognition
- Discrimination (pricing; ad delivery for housing, employment)
- Renewed emphasis on data minimization
- Gov surveillance – ALPR, pole cameras, Stingrays
- Gov purchase of commercial data
- Cross-border data flows - Schrems

Evolution of cybersecurity

Evolution of cybersecurity

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

Alerts and Tips Resources

National Cyber Awareness System > Alerts > APT Cyber Tools Targeting ICS/SCADA Devices

Alert (AA22-103A)

APT Cyber Tools Targeting ICS/SCADA Devices

Original release date: April 13, 2022 | Last revised: May 25, 2022

Print Tweet Send Share

Summary

The Department of Energy (DOE), the Cybersecurity and Infrastructure Security Agency (CISA), the National Security Agency (NSA), and the Federal Bureau of Investigation (FBI) are releasing this joint Cybersecurity Advisory (CSA) to warn that certain advanced persistent threat (APT) actors have exhibited the capability to gain full system access to multiple industrial control system (ICS)/supervisory control and data acquisition (SCADA) devices, including:

- Schneider Electric programmable logic controllers (PLCs),
- OMRON Sysmac NEX PLCs, and
- Open Platform Communications Unified Architecture (OPC UA) servers.

Overview of State Cybersecurity Statutes and Regulations

1. 21 states have free-standing statutes requiring businesses to adopt data security practices
   - Most are similar to California – maintain "reasonable" security measures
   - MA, NV, NY have more specific requirements
2. 21 states have adopted the NAIC model law for insurance companies
3. A number of states have other specific laws or regulations on specific industries or specific kinds of data: medical, biometric, IoT, ISPs, data brokers, ed tech.
4. 3 states (OH, UT, CT) have cybersecurity safe harbor or affirmative defense laws. See also KS
5. NC: State and local gov – no ransomware payment (2021)
6. 5 states have comprehensive privacy laws - all also include a cybersecurity provision

21 Free-Standing “Reasonable” Data Security Statutes

21 states have free-standing statutes specifically requiring data security practices for businesses and other covered entities

- Include CA, CO, UT
- Most require covered entities to maintain “reasonable” security measures
- AL, MA, NV, NY have more specific requirements

21 Free-Standing "Reasonable" Data Security Statutes

Alabama
Arkansas
California
Colorado
Delaware
Dist of Columbia
Florida
Illinois
Indiana
Kansas
Louisiana
Maryland
Massachusetts
Nebraska
Nevada
New Mexico
New York
Oregon
Rhode Island
Texas
Utah

21 Free-Standing "Reasonable" Data Security Statutes

"A business that owns, licenses or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure." CA Civil Code § 1798.81.5(b).

"Each covered entity [a sole proprietorship, partnership, corporation, trust, estate, cooperative, association, or other commercial entity that acquires, maintains, stores, or uses personal information], governmental entity, or third-party agent shall take reasonable measures to protect and secure data in electronic form containing personal information." FL Statutes Sec. 501.171(2)

"A holder of personal information shall:

(1) Implement and maintain reasonable procedures and practices appropriate to the nature of the information, and exercise reasonable care to protect the personal information from unauthorized access, use, modification or disclosure." KS 50-6,139b.

21 Free-Standing "Reasonable" Data Security Statutes

Coverage is broad and exceptions are few:

- 15 apply to gov't agencies
- 20 apply to non-profits
- 20 apply to private institutions of higher ed
- Many exempt only data covered by HIPAA and GLBA

21 Free-Standing "Reasonable" Data Security Statutes

Most have narrow definition of "personal information":

"Personal information" is defined as --

(A) an individual's first name or first initial and last name

- in combination with one or more of the following data elements,
- when either the name or the data elements are not encrypted or redacted:
  - Social Security Number;
  - driver's license number other gov't ID number;
  - account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account;
  - medical information;
  - health insurance information;
  - biometric information;
  - genetic information

(B) A username or email address in combination with a password or security question and answer that would permit access to an online account.

CA Civil Code § 1798.81.5(d)(1)

21 Free-Standing "Reasonable" Data Security Statutes

"Personal information" means either of the following:

a. An individual's first name or first initial and last name in combination with any one or more of the following data elements for that individual:

(I) A social security number;

(II) A driver license or identification card number, passport number, military identification number, or other similar number issued on a government document used to verify identity;

(III) A financial account number or credit or debit card number, in combination with any required security code, access code, or password that is necessary to permit access to an individual's financial account;

(IV) Any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional; or

(V) (V) An individual's health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual.

b. A user name or e-mail address, in combination with a password or security question and answer that would permit access to an online account.

Florida Statutes Sec. 501.171(2)

Comprehensive Privacy Laws with Cybersecurity Provisions

A controller shall take reasonable measures to secure personal data during both storage and use from unauthorized acquisition. The data security practices must be appropriate to the volume, scope, and nature of the personal data processed and the nature of the business. CO

A controller shall … "establish, implement and maintain reasonable administrative, technical and physical data security practices to protect the confidentiality, integrity and accessibility of personal data appropriate to the volume and nature of the personal data at issue;" CT

Comprehensive Privacy Laws with Cybersecurity Provisions

Broader definitions of personal information:

- Colorado: “’Personal Data’ (a) means information that is linked or reasonably linkable to an identified or identifiable individual” and does not include de-identified data or publicly available info
- Connecticut: "Personal data" means any information that is linked or reasonably linkable to an identified or identifiable individual. "Personal data" does not include de-identified data or publicly available information.

Comprehensive Privacy Laws with Cybersecurity Provisions

But many more exceptions. See CT law:

Sec. 3. (NEW) (*Effective July 1, 2023*) (a) The provisions of sections 1 to 11, inclusive, of this act do not apply to any: (1) Body, authority, board, bureau, commission, district or agency of this state or of any political subdivision of this state; (2) nonprofit organization; (3) institution of higher education; (4) national securities association that is registered under 15 USC 78o-3 of the Securities Exchange Act of 1934, as amended from time to time; (5) financial institution or data subject to Title V of the Gramm-Leach-Bliley Act, 15 USC 6801 et seq.; or (6) covered entity or business associate, as defined in 45 CFR 160.103.

(b) The following information and data is exempt from the provisions of sections 1 to 11, inclusive, of this act: (1) Protected health information under HIPAA; (2) patient-identifying information for purposes of 42 USC 290dd-2; (3) identifiable private information for purposes of the federal policy for the protection of human subjects under 45 CFR 46; (4) identifiable private information that is otherwise information collected as part of human subjects research pursuant to the good clinical practice guidelines issued by the International Council for Harmonization of Technical Requirements for Pharmaceuticals for Human Use; (5) the protection of human subjects under 21 CFR Parts 6, 50 and 56, or personal data used or shared in research, as defined in 45 CFR 164.501,

that is conducted in accordance with the standards set forth in this subdivision and subdivisions (3) and (4) of this subsection, or other research conducted in accordance with applicable law; (6) information and documents created for purposes of the Health Care Quality Improvement Act of 1986, 42 USC 11101 et seq.; (7) patient safety work product for purposes of section 19a-127o of the general statutes and the Patient Safety and Quality Improvement Act, 42 USC 299b-21 et seq., as amended from time to time; (8) information derived from any of the health care related information listed in this subsection that is de-identified in accordance with the requirements for de-identification pursuant to HIPAA; (9) information originating from and intermingled to be indistinguishable with, or information treated in the same manner as, information exempt under this subsection that is maintained by a covered entity or business associate, program or qualified service organization, as specified in 42 USC 290dd-2, as amended from time to time; (10) information used for public health activities and purposes as authorized by HIPAA, community health activities and population

health activities; (11) the collection, maintenance, disclosure, sale, communication or use of any personal information bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics or mode of living by a consumer reporting agency, furnisher or user that provides information for use in a consumer report, and by a user of a consumer report, but only to the extent that such activity is regulated by and authorized under the Fair Credit Reporting Act, 15 USC 1681 et seq., as amended from time to time; (12) personal data collected, processed, sold or disclosed in compliance with the Driver's Privacy Protection Act of 1994, 18 USC 2721 et seq., as amended from time to time; (13) personal data regulated by the Family Educational Rights and Privacy Act, 20 USC 1232g et seq., as amended from time to time; (14) personal data collected, processed, sold or disclosed in compliance with the Farm Credit Act, 12 USC 2001 et seq., as amended from time to time; (15) data processed or maintained (A) in the course of an individual applying to, employed by

Possible Responses

- If you are one of 21 states with free-standing cybersecurity and no privacy law, consider updating/expanding definition of pers info.
- If you are one of 30+ states that do not have cybersecurity provision, consider adopting one with more modern broad definition and only narrow exceptions.
- If you are one of the 30+ that do not have a comprehensive privacy law and do not have a free-standing cybersecurity law and are considering the VA/UT model, pay close attention to the exceptions.

The Next Frontier of Cybersecurity Law

- Protection of critical infrastructure:
  - Water (fresh and waste water treatment)
  - Power
  - Dams
  - Transportation
  - Financial services (including insurance)
  - Health care
  - Food processing and supply chain
  - Police, emergency services, other public safety

What is “Reasonable” Security

1. Legislative standards
2. Enforcement-based – case-by-case
3. Private litigation – case-by-case
4. Administrative guidelines (non-binding)
5. Administrative regulations
6. Industry or other private sector standards
7. Regulator endorsement of private sector standards

1. Legislative (statutory) standards

"A data collector that maintains records which contain personal information of a resident of this State shall implement and maintain reasonable security measures to protect those records … ." Nevada Revised Statutes 603A.210

"A data collector doing business in this State … shall not:

a) Transfer any personal information through an electronic, nonvoice transmission other than a facsimile to a person outside of the secure system of the data collector unless the data collector uses encryption to ensure the security of electronic transmission … ."

Nevada Revised Statutes 603A.215.

2. Case-by-case enforcement: FTC Settlement with Equifax (2019)

Carried Forward from Eli Lilly	Plus: The New Generation of Requirements
Comp. written info sec program designed to protect personal info	Assess risks and sufficiency of safeguards following any Security Incident
Designate qualified employee to coord and be responsible	Provide program and evaluations to Board
Assess risks at least once every 12 months	Internal complaint process
Design & implement safeguards to control risks identified	Patch management
Training at least once every 12 months	Timely remediation of critical or high risk vulnerabilities
	Asset inventory
	Protections such as network intrusion protection, host intrusion protection, and file integrity monitoring
	Access measures such as segmentation
	Access controls, such as MFA
	Limit employee and contractor access – business need to access
	Test and monitor effectiveness at least once a year
Obtain biennial assessment from qualified, objective, independent 3rd party pro.	Protections such as encryption if feasible
Select and retain service providers capable of safeguarding personal info	Secure development practices and test externally developed apps
Evaluate and adjust	Vulnerability testing once every 4 months
	Bug bounty
Order remains in effect 20 years	Notice to FTC of all breaches

3. Case-by-case - private litigation

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

In re: Equifax Inc. Customer Data Security Breach Litigation	MDL Docket No. 2800 No. 1:17-md-2800-TWT CONSUMER ACTIONS Chief Judge Thomas W. Thrash, Jr.

SETTLEMENT AGREEMENT AND RELEASE

4. Administrative guidelines (non- binding)

Framework for Improving Critical Infrastructure Cybersecurity

Version 1.1

National Institute of Standards and Technology

April 16, 2018

https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Table 1: Function and Category Unique Identifiers

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
		RS.RP	Response Planning

5. Administrative Regulations

NY State Department of Financial Services, 23 NYCRR 500 (3/1/17)

- Process: Requires policy, which must address 14 areas "to the extent applicable," including:
  - asset inventory
  - business continuity
  - systems and network monitoring
- Specific Technology: Requires
  - continuous monitoring or periodic pen testing and vulnerability assessments
  - audit trails designed to detect and respond to attacks
  - limits on user access privileges
  - secure dev practices for in-house developed apps
  - due diligence and/or contractual protections related to 3rd party service providers

5. Administrative Regs

- Massachusetts
  - Data on portable devices must be encrypted
  - Must assign unique IDs and passwords
  - Blocking access to user identification after multiple unsuccessful attempts
  - Regulatory humility: “to the extent technically feasible”

201 C.M.R. 17.

7. Government Endorsement of Private Sector Standards

"If a data collector doing business in this State accepts a payment card in connection with a sale of goods or services, the data collector shall comply with the current version of the Payment Card Industry (PCI) Data Security Standard, as adopted by the PCI Security Standards Council or its successor organization, with respect to those transactions, … ."

Nevada Revised Statutes, 603A.15

7. Government Endorsement of Private Sector Standards

Affirmative defense to tort action if security program "reasonably conforms to an industry recognized cybersecurity framework" –

- NIST Framework
- NIST special publications 800-171 or 800-53 and 800-53a
- FedRAMP security assessment framework
- CIS controls
- International Organization for Standardization (ISO)/International Electrotechnical Commission(IEC) 27000 family

Ohio Code, Title XIII, Secs 1354.01-1354.03

CIS Controls

First 5 CIS Controls
Eliminate the vast majority of your organisation's vulnerabilities

Secure Your Organization

All 20 CIS Controls
Secure your entire organization against today's most pervasive threats

1: **Inventory of Authorized and Unauthorized Devices**
2: **Inventory of Authorized and Unauthorized Software**
3: **Secure Configurations for Hardware and Software**
4: **Continuous Vulnerability Assessment and Remediation**
5: **Controlled Use of Administrative Privileges**
6: **Maintenance, Monitoring, and Analysis of Audit Logs**
7: **Email and Web Browser Protections**
8: **Malware Defenses**
9: **Limitation and Control of Network Ports**
10: **Data Recovery Capability**
11: **Secure Configurations for Network Devices**
12: **Boundary Defense**
13: **Data Protection**
14: **Controlled Access Based on the Need to Know**
15: **Wireless Access Control**
16: **Account Monitoring and Control**
17: **Security Skills Assessment and Appropriate Training to Fill Gaps**
18: **Application Software Security**
19: **Incident Response and Management**
20: **Penetration Tests and Red Team Exercises**