Agenda

- California's SB 327
- California Consumer Privacy Act (CCPA)
- NIST CsF
- HITRUST CSF
- Next Steps
2020 Cybersecurity Readiness in 2019

2020 Cybersecurity Mandates

CCPA Key Facts
- In effect January 1, 2020
- Provides right of action for California residents
- Grants new enforcement power to the Attorney General with high damage recoverable

CCPA Individual Rights
- All personal information is being collected about them
- Whether their personal information is sold or otherwise disclosed and to whom
- To say no to the sale of their personal information
- To access their personal information and request deletion under certain circumstances
- To receive equal service and price

California
- SB 1386
- SB 541
- AB 1950
- SB 24
- AB 1298
- RB 170
- AB 231

SB 327 Key Facts
- In effective January 1, 2020
- Focused on security features of IoT devices to protect personal information
- California attorney general, county counsel, and district attorneys will enforce the bill

HITRUST Cybersecurity Workshop
- Validation & Certification
- Remediation
- Scoping
- Policy & Procedures Development
- Guided Self-Assessment
- Evidence Review

IoT Security

California

SB 327
IoT-driven Internet Wobble on Oct 21, 2016: Why it Matters Now!

- 7:10 AM EST, Friday, October 21, 2016, witnessed a massive cyber assault on the servers.
- DNS is one of the handful of entities on the Internet that provides vital DNS services.
- The DDoS by hundreds of thousands of IoT devices on Dynamic’s DNS servers made the systems inaccessible to all users.
- More than 500,000 IoT devices were earlier compromised by the Mirai malware.
- 10% of compromised IoT devices were associated with the cyber-attack, zombie devices compromised by Mirai formed a botnet army led by cyber-attackers through their command and control servers.

Senate Bill 327 (SB 327)

- SB 327 is a first-of-its kind mandate focused on the security of IoT devices.
- Allows law enforcement agencies to obtain connected device information from a manufacturer as authorized by law or court order.
- Businesses should begin taking steps to build “security by design” into the manufacturing processes for the IoT devices they create.
- Manufacturers need to consider how to deal with post-market security issues, such as patching vulnerabilities with software updates.
Effective January 1, 2020

SB 327 requires manufacturers of connected devices to equip the device with reasonable security features that are 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.

A manufacturer of a connected device shall equip the device with a reasonable security feature or features 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 a LAN, it shall be deemed a reasonable security feature, if either of the following requirements are met:

- The preprogrammed password is unique to each device manufactured
- The device contains 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.
California Consumer Privacy Act (CCPA)

GDPR: European Standard  
CCPA: California Impact
California Consumer Privacy Act (CCPA)

CCPA grants California residents the right:

- To know what personal information is being collected about them.
- To know whether their personal information is sold or otherwise disclosed and to whom.
- To say no to the sale of their personal information.
- To access their personal information and request deletion under certain circumstances.
- To receive equal service and price, even if they exercise their privacy rights.

CCPA: Consumer Ownership

Gives Ownership

- CCPA empowers consumers to find out what information businesses are collecting about them as an individual, devices, and individual’s family, and gives individual the choice to inform them NO.
- If a business collects individual’s personal information, then once a year and free of charge they have to tell what categories of information has been collected, about devices and about children.
- If a business sells personal information, it must inform what categories of personal information they are selling and then inform you to whom they sold the individual’s personal information.
CCPA: Individual Control on Data

**Gives Control**

- If a business is informed to not share or sell an individual's private information, the business cannot charge more, deny an individual’s access to services, or change the quality of the service.
- If someone doesn't want a business to sell their information, you can inform by clicking on a link that says “do not sell my data”
- The business can't hide this in a privacy policy— it must be displayed clearly at the bottom of any page where the individual’s information is collected.

CCPA: Getting Prepared

- Assign responsibility
- Acquire deeper understanding of the regulation
- Update policies
- Engage in a data mapping activity that provides information on who in your organization collects, uses and shares what personal information for what purposes, and that tells you where and how that data is stored and accessed
- Adopt and follow a cybersecurity framework
- Encrypt or redact consumers’ personal information when collected, stored, and transmitted
- Update written contracts with service providers and vendors with which you share consumers’ personal information to ensure the requirements of CCPA are addressed.
Bottomline with CCPA

- CCPA goes into effect in 2020, and grants California residents new privacy rights
- Enforcement is with the Attorney General

Gives Ownership
Gives Security
Gives Control

NIST CsF
NIST CsF: Fundamentals

Framework Core Structure

<table>
<thead>
<tr>
<th>Functions</th>
<th>Categories</th>
<th>Subcategories</th>
<th>Informative References</th>
</tr>
</thead>
<tbody>
<tr>
<td>IDENTIFY</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PROTECT</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DETECT</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RESPOND</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RECOVER</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Function and Category Unique Identifiers

<table>
<thead>
<tr>
<th>Function Unique Identifier</th>
<th>Function</th>
<th>Category Unique Identifier</th>
<th>Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>Identify</td>
<td>ID.AM</td>
<td>Asset Management</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.BE</td>
<td>Business Environment</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.GV</td>
<td>Governance</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.RA</td>
<td>Risk Assessment</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.RM</td>
<td>Risk Management Strategy</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.SC</td>
<td>Supply Chain Risk Management</td>
</tr>
<tr>
<td>ID</td>
<td>Protect</td>
<td>PR.AC</td>
<td>Identify Management and Access Control</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PR.AT</td>
<td>Awareness and Training</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PR.DS</td>
<td>Data Security</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PR.IP</td>
<td>Information Protection Processes and Procedures</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PR.MA</td>
<td>Maintenance</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PR.PT</td>
<td>Protective Technology</td>
</tr>
<tr>
<td>DE</td>
<td>Detect</td>
<td>DE.AE</td>
<td>Anomalies and Events</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DE.CM</td>
<td>Security Continuous Monitoring</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DE.DP</td>
<td>Detection Processes</td>
</tr>
<tr>
<td>RS</td>
<td>Respond</td>
<td>RS.RP</td>
<td>Response Planning</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RS.CO</td>
<td>Communications</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RS.AN</td>
<td>Analysis</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RS.MI</td>
<td>Mitigation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RS.JM</td>
<td>Improvements</td>
</tr>
<tr>
<td>RC</td>
<td>Recover</td>
<td>RC.JP</td>
<td>Recovery Planning</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RC.JM</td>
<td>Improvements</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RC.CO</td>
<td>Communications</td>
</tr>
</tbody>
</table>
Why HITRUST Certification?

- **Efficient** for managing security requirements inherent in HIPAA, NIST, and other regulations.
- **Maps** many industry regulation requirements into an actionable roadmap, cross-referenced to many other security and data privacy regulations such as GDPR and State laws.
- **Prescriptive** controls across a broad range of regulatory requirements.
- **Reduces** complexity, risk and cost while protecting sensitive information.
- **Brand** protection, brand confidence.

HITRUST: At Its Core

- **Comprehensive, industry-level overlay of the NIST RMF**
  - Structured on ISO 27001
  - Built on NIST SP 800-53
  - Integrates many other relevant sources
- **Designed to address:**
  - Risk management requirements
  - Security requirements
  - Compliance needs
- **Ensures information and cybersecurity-related risks are managed smartly and consistent with business, risk and compliance objectives**
Control Categories & Objectives

<table>
<thead>
<tr>
<th>#</th>
<th>Control Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0</td>
<td>Information Security Management Program</td>
</tr>
<tr>
<td>1.0</td>
<td>Access Control</td>
</tr>
<tr>
<td>2.0</td>
<td>Human Resources Security</td>
</tr>
<tr>
<td>3.0</td>
<td>Risk Management</td>
</tr>
<tr>
<td>4.0</td>
<td>Security Policy</td>
</tr>
<tr>
<td>5.0</td>
<td>Organization of Information Security</td>
</tr>
<tr>
<td>6.0</td>
<td>Compliance</td>
</tr>
<tr>
<td>7.0</td>
<td>Asset Management</td>
</tr>
<tr>
<td>8.0</td>
<td>Physical &amp; Environmental Security</td>
</tr>
<tr>
<td>9.0</td>
<td>Communications &amp; Operations Management</td>
</tr>
<tr>
<td>10.0</td>
<td>Information Systems Acquisition, Development &amp; Maintenance</td>
</tr>
<tr>
<td>11.0</td>
<td>Information Security Incident Management</td>
</tr>
<tr>
<td>12.0</td>
<td>Business Continuity Management</td>
</tr>
<tr>
<td>13.0</td>
<td>Privacy Practices</td>
</tr>
</tbody>
</table>

What are the CSF Domains?

01 Information Protection Program
02 Endpoint Protection
03 Portable Media Security
04 Mobile Device Security
05 Wireless Security
06 Configuration Management
07 Vulnerability Management
08 Network Protection
09 Transmission Protection
10 Password Management
11 Access Control
12 Audit Logging & Monitoring
13 Education, Training, & Awareness
14 Third Party Assurance
15 Incident Management
16 Business Continuity & Disaster Recovery
17 Risk Management
18 Physical & Environmental Security
19 Data Protection & Privacy
**HITRUST Maturity Levels**

- Maturity levels:
  - Non-compliant
  - Somewhat compliant
  - Partially compliant
  - Mostly compliant
  - Fully compliant

- Maturity levels are ranked

---

**HITRUST: Getting Started**

<table>
<thead>
<tr>
<th>Rating (Score)</th>
<th>Policy</th>
<th>Procedure</th>
<th>Implemented</th>
<th>Measured</th>
<th>Managed</th>
</tr>
</thead>
<tbody>
<tr>
<td>NC (0%)</td>
<td>No CSF requirements</td>
<td>None of the CSF requirements</td>
<td>None of the CSF requirements</td>
<td>No measure or metric in place</td>
<td>No management action taken</td>
</tr>
<tr>
<td>SC (25%)</td>
<td>Some CSF requirements and ad hoc</td>
<td>Some CSF requirements supported by ad hoc procedures</td>
<td>Some CSF requirements are supported by ad hoc procedures</td>
<td>Operational OR independent measure</td>
<td>Measure or metric and management actions sometimes taken on ad hoc basis</td>
</tr>
<tr>
<td>PC (50%)</td>
<td>All CSF requirements and ad hoc</td>
<td>All CSF requirements supported by ad hoc procedures</td>
<td>Some CSF requirements and full scope</td>
<td>Operational and independent measure</td>
<td>Measure or metric and management actions sometimes taken and formal action management process exists</td>
</tr>
<tr>
<td>MC (75%)</td>
<td>Some CSF requirements written/signed and remainder ad hoc</td>
<td>Some CSF requirements supported by written and/or automated procedures, and remaining CSF requirements addressed by ad hoc procedures</td>
<td>All CSF requirements and partial scope</td>
<td>Operational OR independent metric</td>
<td>Metric only and corrective actions always taken and on ad hoc basis</td>
</tr>
<tr>
<td>FC (100%)</td>
<td>All CSF requirements written/signed</td>
<td>ALL CSF requirements supported by written procedures and/or automated</td>
<td>All CSF requirements and full scope</td>
<td>Operational metric and independent measure or metric</td>
<td>Metric only and corrective actions always taken and formal remediation management process exists</td>
</tr>
</tbody>
</table>
The following table captures some key numbers/metrics associated with the HITRUST CSF framework. We summarize key numbers-related facts about the HITRUST CSF.

| 14 | Security control categories (domains) |
| 46 | Control objectives |
| 149 | Controls |
| 75 | Controls required for HITRUST CSF certification |
| 3 | Levels of implementation requirements may be associated with each control |
| 5 | Maturity levels (Policy, Procedure, Implementation, Measured, Managed) |
| 5 | Point compliance scale (Not Compliant (0%), Somewhat Compliant (25%), Partially Compliant (50%), Mostly Compliant (75%), Fully Compliant (100%)) |
| 15 | Maturity ratings (Level -1, 1, 1+ to Level -5, 5, 5+) |
| 37 | Major information security standards, regulations and frameworks integrated with HITRUST CSF |
| 3 | Risk factors (Organizational, System, Regulatory) |
| 233 - 1153 | Possible Requirement Statements for CSF Security Assessment |
| 326 – 1336 | Possible Requirement Statements for CSF Security & Privacy Assessment |
| 353 – 1536 | Possible Requirement Statements for CSF Comprehensive Security Assessment |
| 446 - 1719 | Possible Requirement Statements for CSF Comprehensive Security & Privacy Assessment |
| 186 | Possible Requirement Statements for NIST Cyber Security Assessment |

HITRUST Certification Roadmap

- **Step 1:** Self-Assessment
  - Can be done by you or a Third Party
- **Step 2:** Validation
  - Performed by an Authorized Assessor
- **Step 3:** Certification
  - Performed by an Authorized Assessor and HITRUST

**Types of Reports**

- CSF Security Assessment
- CSF Privacy and Security Assessment
- CSF Comprehensive Security Assessment
- CSF Comprehensive Privacy and Security Assessment
- All Incorporate NIST CsF
- **Part of the Scoping Process**
HITRUST Methodology

1. Scoping
2. Policy & Procedure Development
3. Guided Self-Assessment
4. Evidence Review
5. Remediation
6. Validated Assessment
7. HITRUST Review & Certification

HITRUST Cybersecurity Workshop

Improve Certification Time-line!

Next Steps
Cybersecurity Program: Five Dimensions Aligned

1. Policy
2. Procedure
3. Implementation
4. Measured
5. Managed

Cyber Immune Defense

1. Assign Responsibility
2. Security Assessment
3. Evidence-based Program
4. Encrypt Everywhere
5. Active Control Management
6. Cyber Secure Supply Chain
7. Cyber Literate Workforce

Credible & Evidence-based Cybersecurity Program
2020 Cybersecurity Readiness in 2019

Cyber Action Required Annually!

1. Develop a credible cybersecurity strategy
2. Conduct a comprehensive security risk assessment
3. Ensure a technical vulnerability assessment is performed quarterly, and a pen test annually
4. Perform a Business Impact Analysis (BIA)
5. Develop a detailed Disaster Recovery Plan (DRP)
6. Create a cyber incident response plan
7. Implement a cybersecurity framework (e.g., HITRUST, NIST CSF)

Lifecycle approach

Cyber Risk Assessment & Management

- Risk Assessment: The organization understands the cybersecurity risk to organizational operations (including assets, functions, image, or reputation), organizational assets, and individuals.
- Risk Management: The organization prioritizes, constructs, risk tolerance, and assumptions are established and used to support operational risk decisions.

2019

Cyber Facts:
- No business is 100% secure.
- Security is only as strong as your weakest link.
- A comprehensive and thorough risk assessment establishes the state of your cybersecurity program and identifies compliance gaps and security vulnerabilities.

Vulnerability Assessment
- External
- Internal
- Discovering Vulnerabilities
- Firewall/DMZ
- Wireless
- Conduct a VI
- Conduct a VA
- Validate & Remediate Findings
- Pen Test
Certification Training

- Certified HIPAA Professional
- Certified Security Compliance Specialist™
- Certified Cyber Security Architect℠
- HITRUST Cybersecurity Strategy Workshop
- GDPR Cybersecurity 1-Day Workshop