DORSEY™
always ahead

Implementing the CIS Critical Security Controls for the CCPA and Other Laws

Brock Rutter, CISSP, CIPP, Focal Point

Cody Wamsley, CISSP, Dorsey & Whitney

Bill Dixon, CISSP, CISM, Kroll

Soleil Dolce, CISSP, CISM, CTPRP, Wells Fargo

Reasonable Security

Failure to implement "reasonable security procedures and practices" results in statutory damages of:

$100-750 PER CONSUMER PER INCIDENT

Reasonable Security

"The 20 controls in the Center for Internet Security's Critical Security Controls identify a minimum level of information security that all organizations that collect or maintain personal information should meet. The failure to implement all the Controls that apply to an organization's environment constitutes a lack of reasonable security."

- Kamala Harris, as California Attorney General in 2016

CSC 20

1) Inventory and Control of Hardware Assets
2) Inventory and Control of Software Assets
3) Continuous Vulnerability Management
4) Controlled Use of Administrative Privileges
5) Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
6) Maintenance, Monitoring and Analysis of Audit Logs
7) Email and Web Browser Protections
8) Malware Defenses
9) Limitation and Control of Network Ports, Protocols and Services
10) Data Recovery Capabilities
11) Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
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) Implement a Security Awareness and Training Program
18) Application Software Security
19) Incident Response and Management
20) Penetration Tests and Red Team Exercises

DORSEY™
always ahead

CSC 20

- **Basic 1-6**
- **Foundational 7-16**
- **Organizational 17-20**

- **171 total subcontrols**

- **Implementation Groups (new)**
  IG1 - A family-owned business with ~10 employees
  IG2 - A regional organization providing a service
  IG3 - A large corporation with thousands of employees

How to Implement?

- **Self-assess risks to prioritize**
  - Identification of risks (informed vs. uninformed)
  - Impact vs. Likelihood
  - Maturity
  - Cover percentages
  - Cost
- **Control Effectiveness**
  - Testing
  - Audit findings
  - Issues
  - Exceptions
- **Control Governance**
  - Documentation
  - Oversight
- **Think like a plaintiff's attorney**

1. Inventory and Control of Hardware Assets

- **Maintain Detailed Asset Inventory**
- **Address Unauthorized Assets**

2. Inventory and Control of Software Assets

- **Maintain inventory of Authorized Software**
- **Ensure Software is Supported by Vendor**
- **Address Unapproved Software**

3. Continuous Vulnerability Management

- **Deploy Automated System Operating System Patch Management Tools**
- **Deploy Automated Software Patch Management Tools**

4. Controlled Use of Administrative Privileges

- **Change Default Passwords**
- **Ensure the Use of Dedicated Administrative Accounts**

5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers

- **Establish Secure Configurations**

6. Maintenance, Monitoring, and Analysis of Audit Logs

- **Activate Audit Logging**

7. Email and Web Browser Protections

- **Ensure Use of Only Fully Supported Browsers and Email Clients**
- **Use of DNS Filtering Services**

8. Malware Defenses

- **Ensure Anti-Malware Software and Signatures Are Updated**
- **Configure Anti-Malware Scanning of Removable Media**
- **Configure Devices to Not Auto-Run Content**

9. Limitation and Control of Network Ports, Protocols, and Services

- **Apply Host-Based Firewalls or Port-Filtering**

10. Data Recovery Capabilities

- **Ensure Regular Automated Backups**
- **Perform Complete System Backups**
- **Protect Backups**
- **Ensure All Backups Have at Least One Offline Backup Destination**

11. Secure Configuration for Network Devices, such as Firewalls, Routers, and Switches

- **Install the Latest Stable Version of Any Security-Related Updates on All Network Devices**

12. Boundary Defense

- **Maintain an Inventory of Network Boundaries**
- **Deny Communication over Unauthorized Ports**

13. Data Protection

- **Maintain an Inventory of Sensitive Information**
- **Remove Sensitive Data or Systems Not Regularly Accessed by Organization**
- **Encrypt Mobile Device Data**

14. Controlled Access Based on Need to Know

- **Protect Information Through Access Control Lists**

15. Wireless Access Control

- **Leverage the Advanced Encryption Standard (AES) to Encrypt Wireless Data**
- **Create Separate Wireless Network for Personal and Untrusted Devices**

16. Account Monitoring and Control

- **Disable Any Unassociated Accounts**
- **Disable Dormant Accounts**
- **Lock Workstation Sessions After Inactivity**

17. Implement a Security Awareness and Training Program

- **Implement a Security Awareness Program**
- **Train Workforce on Secure Authentication**
- **Train Workforce on Identifying Social Engineering Attacks**
- **Train Workforce on Sensitive Data Handling**
- **Train Workforce on Causes of Unintentional Data Exposure**
- **Train Workforce Members on Identifying and Reporting Incidents**

18. Application Software Security

- **None!**

19. Incident Response and Management

- **Document Incident Response Procedures**
- **Designate Management Personnel to Support Incident Handling**
- **Maintain Contact Information for Reporting Security Incidents**
- **Publish Information Regarding Reporting Computer Anomalies and Incidents**

20. Penetration Tests and Red Team Exercises

- **None!**

Reasonable Security, generally

- Written Information Security Policy
  - Segregation of duties & least privilege
  - Retention policies for logs, audits, etc.
  - Consequences for violating WISP
  - Patch management
  - Data disposal/deletion policies
- Follow industry standards (ISO 27001, NIST 800-53, etc.)
- Incident Response Plan
- Change Management Controls
- Encryption Standards
- Vulnerability Management
- Audit/Certification Processes (SOC2)
- Security Awareness Training
- Vendor Management

Bonus: Diligence Spectrum