2024 Verizon DBIR Report

CIS Controls Mapped to Incident Classification Patterns

CIS CONTROL 3: DATA PROTECTION

- [ ] Establish and Maintain a Data Management Process [3.1] (Misc. Errors)
- [ ] Establish and Maintain a Data Inventory [3.2] (Misc. Errors)
- [ ] Configure Data Access Control Lists [3.3] (Misc. Errors)
- [ ] Enforce Data Retention [3.4] (Misc. Errors)
- [ ] Securely Dispose of Data [3.5] (Misc. Errors)
- [ ] Encrypt Data on End-User Devices [3.6] (Lost and Stolen Assets)
- [ ] Encrypt Data on Removable Media [3.9] (Lost and Stolen Assets)
- [ ] Segment Data Processing and Storage Based on Sensitivity [3.12] (Misc. Errors)
- [ ] Deploy a Data Loss Prevention Solution [3.13] (Miscellaneous Errors)

CIS CONTROL 4: SECURE CONFIGURATION OF ENTERPRISE ASSETS AND SOFTWARE

- [ ] Establish and Maintain a Secure Configuration Process [4.1] (System Intrusion) (Privilege Misuse)
- [ ] Establish and Maintain a Secure Configuration Process for Network Infrastructure [4.2] (System Intrusion)
- [ ] Implement and Manage a Firewall on Servers [4.4] (System Intrusion)
- [ ] Implement and Manage a Firewall on End-User Devices [4.5] (System Intrusion)
- [ ] **Manage Default Accounts on Enterprise Assets and Software [4.7] (Privilege Misuse)**
- [ ] Enforce Automatic Device Lockout on Portable End-User Devices [4.10] (Lost and Stolen Assets)
- [ ] Enforce Remote Wipe Capability on Portable End-User Devices [4.11] (Lost and Stolen Assets)

CIS CONTROL 5: ACCOUNT MANAGEMENT

- [ ] Establish and Maintain an Inventory of Accounts [5.1] (System Intrusion) (Social Engineering) (Basic Web Application Attacks)
- [ ] Disable Dormant Accounts [5.3] (System Intrusion) (Social Engineering) (Basic Web Application Attacks)
- [ ] **Restrict Administrator Privileges to Dedicated Administrator Accounts [5.4]**

CIS CONTROL 6: ACCESS CONTROL MANAGEMENT

- [ ] Establish an Access Granting Process [6.1] (System Intrusion) (Social Engineering) (Basic Web Application Attacks) (Privilege Misuse)
- [ ] Establish an Access Revoking Process [6.2] (System Intrusion) (Social Engineering) (Basic Web Application Attacks) (Privilege Misuse)
- [ ] Require MFA for Externally Exposed Applications [6.3] (System Intrusion) (Social Engineering) (Basic Web Application Attacks)
- [ ] Require MFA for Remote Network Access [6.4] (System Intrusion) (Social Engineering) (Basic Web Application Attacks)

CIS CONTROL 7: CONTINUOUS VULNERABILITY MANAGEMENT

- [ ] Establish and Maintain a Vulnerability Management Process [7.1] (System Intrusion) (Basic Web Application Attacks)
- [ ] Establish and Maintain a Remediation Process [7.2] (System Intrusion) (Basic Web Application Attacks)
- [ ] Perform Automated Operating System Patch Management [7.3] (Basic Web Application Attacks)
- [ ] Perform Automated Application Patch Management [7.4] (Basic Web Application Attacks)
- [ ] Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets [7.6] (Miscellaneous Errors)

CIS CONTROL 9: EMAIL AND WEB BROWSER PROTECTIONS

- [ ] Use DNS Filtering Services [9.2] (System Intrusion)

CIS CONTROL 10: MALWARE DEFENSES

- [ ] Deploy and Maintain Anti-Malware Software [10.1] (System Intrusion)
- [ ] Configure Automatic Anti-Malware Signature Updates 10.2] (System Intrusion)

CIS CONTROL 11: DATA RECOVERY

- [ ] Establish and Maintain a Data Recovery Process [11.1] (System Intrusion)
- [ ] Perform Automated Backups [11.2] (System Intrusion)
- [ ] Protect Recovery Data [11.3] (System Intrusion)
- [ ] Establish and Maintain an Isolated Instance of Recovery Data [11.4] (System Intrusion)

CIS CONTROL 14: SECURITY AWARENESS TRAINING

- [ ] Train Workforce on Data Handling Best Practices [14.4] (Miscellaneous Errors)
- [ ] Train Workforce Members on Causes of Unintentional Data Exposure [14.5] (Miscellaneous Errors)

CIS CONTROL 16: APPLICATION SOFTWARE SECURITY

- [ ] Use Standard Hardening Configuration Templates for Application Infrastructure [16.7] (Miscellaneous Errors)
- [ ] Train Developers in Application Security Concepts and Secure Coding [16.9] (Miscellaneous Errors)
- [ ] Apply Secure Design Principles in Application Architectures [16.10] (Miscellaneous Errors)

CIS CONTROL 17: INCIDENT RESPONSE MANAGEMENT

- [ ] Establish and Maintain Contact Information for Reporting Security Incidents [17.2] (Social Engineering)
- [ ] Establish and Maintain an Enterprise Process for Reporting Incidents [17.3] (Social Engineering)

- [ ] Although not part of the CIS Controls, a special focus should be placed on BEC and processes associated with updating bank accounts. (Security awareness programs) (Social Engineering)

Verizon's annual DBIR report maps incident classification patterns to the Center for Internet Security's (CIS) Critical Security Controls. This one-pager offers visibility into these controls for security practitioners, enabling them to focus on the highest priority controls most frequently involved in data breaches. The controls in **red highlights** indicate controls added in 2024 that were not present in the 2023 DBIR report.

Source: 2024 Verizon Data Breach Investigations Report