Cyber Security Data Breach Case Study

Data breach can be defined as an incident in which sensitive. protected, or confidential data has potentially been viewed, stolen, or used by an individual unauthorized to do so. Data breaches may involve payment card information, personal health information, personally identifiable information, trade secrets, or intellectual property.

Data breaches have gained widespread attention as businesses of all sizes become increasingly reliant on digital data, cloud computing, and workforce mobility. With sensitive business data stored on local machines, on enterprise databases, and on cloud servers, breaching a company's data has become as simple or as complex as gaining access to restricted networks. The website below keeps track of the World's Biggest Data Breaches in the last 10 years.

https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

You are required to identify one organization in the last 10 years from the link provided, expand on it and study the report provided for the chosen organization. Ensure that the Organization chosen has sufficient information. Examples of Organizations with sufficient information include:

- Marriot Hotels
- Indian Citizens
- MGM Hotels
- Capital One
- Australian Red Cross
- IRS
- Zomato
- Equifax Bank
- Malaysian Medical Practitioners
- ETC.

You are at liberty to choose any organization of your choice and carry out a thorough investigation.

This case study requires you to demonstrate the ability to conduct an investigation of security risk management issues in corporate organizations based on a real-life case study and answer the questions that follow. Each team should read and understand the case study and provide detailed answers in their own words. In your report. you will be required to follow prescribed procedures to evaluate risk levels and the potential impact of threats and vulnerabilities for a real-life organization and recommend controls. risk decisions and security architecture.

You will be assessed on your ability to analyze the security requirements and objectives of the organization as well as the efficacy of the risk management strategies and controls that have to be implemented.

Cyber Security Data Breach Case Study

1. Introduction to the Case?

2. Identify and explain which of the following data breach type applies to your chosen organization: A. payment card information

B. personal health information

C. personally identifiable information

D. trade secrets

E. intellectual property

F. Others (specify)

3. Recommend five controls from the 20 CSCs to protect it. Please refer to 20 CSC document provided.

4. Assess the impact of the breach on the organization.

5. Identify at least four security issues the organization was facing before the breach.

6. For each security issue identified in the previous question, recommend a suitable control and proper tools. Please refer to 20 CSC document provided.

7. For the previous question, link each tool with proper risk decision (defence, transference, mitigation, acceptance, termination).

8. If you have a very low budget for security, which tools you will use? Explain pros and cons.

9. Explain with an illustration a security architecture that should provide the blueprint and guide the Organization's security program.

10. Individual reflection (Minimum of 200 words): Summarize lessons learned from this incident.

Report Requirements

1. MS Word report with 2000 words.

2. Font: Times New Roman, size 12.

3. APA referencing with in-text references and a "references" page.

4. Max of two students per team.

5. Signed cover sheet

CIS Critical Security Controls

CSC 1
Inventory of Authorized and Unauthorized Devices
Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.

CSC 2
Inventory of Authorized and Unauthorized Software
Actively manage (inventory, track, and correct) all software on the network so that only authorized software is installed and can execute, and unauthorized and unmanaged software is found and prevented from installation or execution

CSC 3
Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
Establish, implement, and actively manage (track, report on, and correct) the security configuration of laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.

CSC 4
Continuous Vulnerability Assessment and Remediation
Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, and to remediate and minimize the window of opportunity for attackers.

CSC 5
Controlled Use of Administrative Privileges
Track, control, prevent, and correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.

CSC 6
Maintenance, Monitoring, and Analysis of Audit Logs
Collect, manage, and analyze audit logs of events that could help detect, understand, or recover from an attack.

CSC 7
Email and Web Browser Protections
Minimize the attack surface and the opportunities for attackers to manipulate human behavior though their interaction with web browsers and e-mail systems.

CSC 8
Malware Defenses
Control the installation, spread, and execution of malicious code at multiple points in the enterprise, while optimizing the use of automation to enable rapid updating of defense, data gathering, and corrective action.

CSC 9
Limitation and Control of Network Ports, Protocols, and Services
Manage (track, control, and correct) the ongoing operational use of ports, protocols, and services on networked devices in order to minimize windows of vulnerability available to attackers.

CSC 10
Data Recovery Capability
Properly back up critical information with a proven methodology for timely recovery.

CSC 11
Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
Establish, implement, and actively manage (track, report on, and correct) the security configuration of network infrastructure devices using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.

CSC 12
Boundary Defense
Detect, prevent, and correct the flow of information transferring networks of different trust levels with a focus on security-damaging data.

CSC 13
Data Protection
Prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information.

CSC 14
Controlled Access Based on the Need to Know
Track, control, prevent, correct, and secure access to critical assets (e.g., information, resources, systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification.

CSC 15
Wireless Access Control
Track, control, prevent, and correct the security use of wireless local area networks (LANS), access points, and wireless client systems.

CSC 16
Account Monitoring and Control
Actively manage the life-cycle of system and application accounts – their creation, use, dormancy, deletion – in order to minimize opportunities for attackers to leverage them.

CSC 17
Security Skills Assessment and Appropriate Training to Fill Gaps
Identify the specific knowledge, skills, and abilities needed to support defense of the enterprise; develop and execute an integrated plan to assess, identify and remediate gaps, through policy, organizational planning, training, and awareness programs for all functional roles in the organization.

CSC 18
Application Software Security
Manage the security life-cycle of all in-house developed and acquired software in order to prevent, detect, and correct security weaknesses.

CSC 19
Incident Response and Management
Protect the organization's information, as well as its reputation, by developing and implementing an incident response infrastructure (e.g., plans, defined roles, training, communications, management oversight).

CSC 20
Penetration Tests and Red Team Exercises
Test the overall strength of an organization's defenses (technology, processes, and people) by simulating the objectives and actions of an attacker.

The CIS Critical Security Controls for Effective Cyber Defense Now

The CIS Critical Security Controls are a recommended set of actions for cyber defense that provide **specific and actionable ways to stop today's most pervasive and dangerous attacks.** A principle benefit of the Controls is that they prioritize and focus a smaller number of actions with high pay-off results. The Controls are effective because they are derived from the most common attack patterns highlighted in the leading threat reports and vetted across a very broad community of government and industry practitioners. They were created by the people who know how attacks work – NSA Red and Blue teams, the US Department of Energy nuclear energy labs, law enforcement organizations and some of the nation's top forensics and incident response organizations – to answer the question, "what do we need to do to stop known attacks." That group of experts reached consensus and today we have the most current Controls. The key to the continued value is that the Controls are updated based on new attacks that are identified and analyzed by groups from Verizon to Symantec so the Controls can stop or mitigate those attacks.

In addition to being grounded in current attack data, the Controls align with numerous other frameworks, such as PCI-DSS, ISO 27001, US CERT recommendations, NIST SP 800-53, and the NIST Framework. The Controls don't try to replace these other frameworks, but they are frequently used by enterprises to make sense of other frameworks. The Controls are a highly practical approach to prioritize the overarching security strategy for an enterprise. Further, once a program for cyber security is in place and operational, the Controls can also be used with the Critical Security Controls Measurement Companion to assess the effectiveness of the organization's security efforts.

The Controls take the best-in-class threat data and transform it into actionable guidance to improve individual and collective security in cyberspace. Too often in cybersecurity, it seems the "bad guys" are better organized and collaborate more closely than the "good guys." The Controls provide a means to turn that around.

The CIS Critical Security Controls are the Core of the NIST Cybersecurity Framework

Since its release in February 2014, the NIST *Framework for Securing Critical Infrastructure Cybersecurity* has become a major part of the national conversation about cybersecurity for the critical infrastructure and beyond. (The Center for Internet Security was an active participant in the development of the Cybersecurity Framework, and the CIS Critical Security Controls are called out as one of the "Informative References" that can be used to drive specific implementation).

The Framework provides a way to organize, conduct, and drive planning on security goals and improvements, for individual enterprises and across communities of enterprises. But it does not include any specific risk management process, or specify any priority of action. Those decisions and judgments are left to the adopter to manage for their specific situation and context.

CIS believes that this task is beyond the ability or resources of most enterprises to do effectively and repeatedly. And this approach doesn't recognize the interdependency that every enterprise has with its many vendors, partners, suppliers, and customers. This is why the Controls take a community-first approach by considering attacks that we all face today, translating them into specific actions that are embodied in the Controls, and then creating a community to help enterprises remove barriers to positive action. This approach emphasizes the common threat that we all face, shares the labor and insight needed to identify solutions, and does so in a open way that can be explained and shared no matter the compliance framework, regulatory framework, or demands from the marketplace.

To the right is an example of the working aids that CIS maintains to help our community leverage the Framework. This chart shows the mapping from the CIS Critical Security Controls (Version 6.0) into the most relevant NIST CSF (Version 1.0) Core Functions and Categories.

CIS Critical Security Controls (V6.0)	Cybersecurity Framework (CSF) Core				
	Identify	Protect	Detect	Respond	Recover
1 Inventory of Authorized and Unauthorized Devices	AM				
2 Inventory of Authorized and Unauthorized Software	AM				
3 Secure Configuration of End-User Devices		IP			
4 Continuous Vulnerability Assessment & Remediation	RA		CM	MI	
5 Controlled Use of Administrative Privileges		AC			
6 Maintenance, Monitoring, and Analysis of Audit Logs			AE	AN	
7 Email and Web Browser Protections		PT			
8 Malware Defense		PT	CM		
9 Limitation & Control of Network Ports, Protocols, and Service		IP			
10 Data Recovery Capability					RP
11 Secure Configuration of Network Devices		IP			
12 Boundary Defense			DP		
13 Data Protection		DS			
14 Controlled Access Based on Need to Know		AC			
15 Wireless Access Control		AC			
16 Account Monitoring and Control		AC	CM		
17 Security Skills Assessment and Appropriate Training		AT			
18 Application Software Security		IP			
19 Incident Response and Management			AE	RP	
20 Penetration Tests and Red Team Exercises				IM	IM

A Case Study in Auditing the CIS Critical Controls at the U.S. Federal Reserve

The U.S. Federal Reserve audit community consists of individually chartered audit functions representing each of the 12 regional Reserve Banks. In recognizing the unique and pervasive nature of cybersecurity risk, the collective of Fed internal auditors uses a highly coordinated approach to audit coverage that leverages the CIS Critical Security Controls framework. The approach allows for the prioritization of audit coverage as well as the consideration of control effectiveness as demonstrated in previous audits, organized by the Controls, in business and IT areas across the Fed. The prioritized nature of the Controls is also useful to Fed management, informing cybersecurity and risk management activities.

Cybersecurity risk applies across all business and IT areas, and risks for individual Reserve Banks may vary. Since the Controls are set forth in priority order, they provide a strong starting point for prioritizing audit coverage. The varying levels of control effectiveness in business and IT areas are best known by the local chief audit executives and information security officers. This combination of prioritization and local risk knowledge supports an effective balance of cybersecurity audit coverage applied throughout the Reserve Banks.

As part of management's layered control framework, Fed management assigns an overall maturity score of Fed controls organized by the Controls. Lower assigned maturity scores drive stronger investment and management attention. This aligns the cybersecurity risk focus between management and the internal audit, and improves organizational conversations about relative control effectiveness. It is increasingly apparent that cybersecurity risk isn't just an IT risk – it is an enterprise-wide business risk that requires broad awareness and coordination. The Controls provide a useful framework for both management and auditors for the assessment and management of cybersecurity risk.

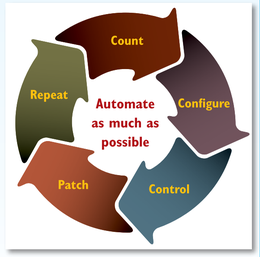
The National Campaign for Cyber Hygiene

The National Campaign for Cyber Hygiene was developed to provide a plain-language, accessible, and low-cost foundation for implementation of the CIS Critical Security Controls. Although the Controls already simplify the daunting challenges of cyber defense by creating community priorities and action, many enterprises are starting from a very basic level of security.

The Campaign starts with a few basic questions that every corporate and government leader ought to be able to answer:

- Do we know what is connected to our systems and networks? (CSC 1)
- Do we know what software is running (or trying to run) on our systems and networks? (CSC 2)
- Are we continuously managing our systems using "known good" configurations? (CSC 3)
- Are we continuously looking for and managing "known bad" software? (CSC 4)
- Do we limit and track the people who have the administrative privileges to change, bypass, or over-ride our security settings? (CSC 5)

These questions, and the actions required to answer them, are represented in plain language by the Top 5 Priorities of the Campaign: "**Count, Configure, Control, Patch, Repeat**." To support the Campaign, volunteers have created documentation and toolkits to guide implementation.



Although the language is simple and catchy, behind the scenes each of these questions is associated with a primary CIS Critical Security Control that provides an action plan. The Campaign is also designed to align with the first five of the CIS Critical Security Controls, the Australian Signals Directorate's Top Four Strategies to Mitigate Targeted Intrusions, and the DHS Continuous Diagnostic and Mitigation Program. This provides a strong and defendable basis for the Campaign Priorities, a growth path for maturity beyond these basic actions, and the benefits of a large community of experts, users, and vendors.

The National Campaign for Cyber Hygiene has been jointly adopted by the Center for Internet Security (home of the Multi-State Information Sharing and Analysis Center) and the National Governor's Association Homeland Security Advisory Council as a foundational cybersecurity program across many state, local, tribal, and territorial governments.

The CIS Critical Security Controls as the Basis for Cybersecurity Audits

Daily headlines of significant cyber intrusions with their associated effects on consumers and citizens have generated an outcry from the public and lawmakers to demand better performance in cybersecurity for enterprises in every sphere. Executives and board directors have become sensitized to the problem but are, for the most part, still largely unaware of how best to protect their IT and sensitive data.

Jane Holl Lute, Chief Executive Officer of the Center for Internet Security (CIS), frequently meets with CEOs and CIOs of major companies and government organizations who are grappling with the cybersecurity problem. As the former Deputy Secretary and Chief Operating Officer for the Department of Homeland Security, Jane understands the challenges facing leaders who must make tough choices about how to allocate resources to cybersecurity. The problem has shifted from a traditional technology and product view of security to also include the executive's view of the risk to the business. Therefore our solutions (both as individual enterprises and as communities) must bridge this gap in a manner that can be openly described, assessed, shared, and negotiated.

The CIS Critical Security Controls provide a highly practical and useful framework for every organization to use for both implementation and assessment. Because the Controls are developed by the community and based on actual threat data, they are an authoritative, industry-friendly, and vendor-neutral approach to assessment and auditing of security.

Getting Started: Ask and Answer Key Questions

- **What am I trying to protect?** Create a prioritized list of business- or mission-critical processes and inventory the computing assets that map to those processes. This information will be crucial for creating a baseline of your current capabilities against the CIS Critical Security Controls.
- **Where are my gaps?** For each business- or mission-critical asset, compare existing security controls against the CIS Critical Security Controls, indicating the sub-controls that the existing controls already meet and those they do not meet.
- **What are my priorities?** Based on your identified gaps and specific business risks and concerns, take immediate tactical steps to implement the Top 5 Controls and develop a strategic plan to implement the other Controls.
- **Where can I automate?** As you plan your implementation of the Controls, focus on opportunities to create security processes that can be integrated and automated using tools that relieve skilled security and administrative staff of grunt work. The Controls were specifically created to enable automation. The goal is to more rapidly and efficiently deliver accurate, timely, and actionable information to the system administrators and others who can take proactive steps to deter threats.
- **How can my vendor partners help?** Some vendor solutions significantly improve and automate implementation for the Critical Controls, especially in terms of continuous monitoring and mitigation. Contact your current vendors to see how they can support your implementation of the CIS Critical Security Controls and compare their capabilities with other vendor products.

The Configuration Benchmarks Community

The Center for Internet Security (CIS) develops and distributes secure configuration benchmarks and automated configuration assessment tools, and certifies security software products designed to help organizations improve their security posture. The internationally recognized benchmarks are developed through an open, consensus-based process and are aligned with the CIS Critical Security Controls. Cybersecurity and industry professionals from around the world volunteer to participate in CIS's open security benchmark development community. New and updated benchmark development efforts are continually launched for a wide array of system, network and device technologies. The CIS Configuration Assessment Tool (CIS-CAT) enables organizations to identify system vulnerabilities, assess configurations against the benchmarks, and monitor security improvement over time. For more information on CIS-CAT or CIS Benchmark membership, visit **cisecurity.org**.

Security through Collaboration

The Center for Internet Security (CIS) is a not-for-profit organization that is dedicated to enhancing the cybersecurity readiness and response among public and private sector entities. Utilizing its strong industry and government partnerships, CIS combats evolving cybersecurity challenges on a global scale and helps organizations adopt key best practices to achieve immediate and effective defenses against cyber attacks. CIS is home to the Multi-State Information Sharing and Analysis Center, CIS Benchmarks, and CIS Critical Security Controls. To learn more, please visit **cisecurity.org** or follow us at **@CISecurity**.

Where to Learn More

Here are some additional resources for effective planning and implementation of the CIS Critical Security Controls

1) SANS courses on planning and implementing the CIS Critical Security Controls include:

TWO-DAY COURSE

SEC440: Critical Security Controls: Planning, Implementing and Auditing

This course helps you master specific, proven techniques and tools needed to implement and audit the Critical Security Controls as documented by the Center for Internet Security.

SEC440 does not contain any labs. If the student is looking for hands-on labs involving the Critical Controls, they should take SEC566.

sans.org/course/critical-security-controls-planning-implementing-auditing

FIVE-DAY COURSE

SEC566: Implementing and Auditing the Critical Security Controls – In-Depth

The course shows security professionals how to implement the controls in an existing network through cost-effective automation. For auditors, CIOs, and risk officers, the course is the best way to understand how you will measure whether the Controls are effectively implemented.

sans.org/course/implementing-auditing-critical-security-controls

2) The SANS Solution Directory posts case studies of organizations that have successfully implemented the Controls and seen immediate benefits.
sans.org/critical-security-controls/vendor-solutions

3) Summits where managers from user organizations and strategists from vendor companies share lessons learned and plan for future improvements.
sans.org/summit

4) The Center for Internet Security delivers world-class cybersecurity solutions and best practices in order to prevent and rapidly respond to cyber incidents to enable an environment of trust in cyberspace.
cisecurity.org

SANS

PRESENTS

CIS Critical Security Controls

POSTER

41ST EDITION

CSC-P-v1-10-15

MAPPINGS TO THE

CIS Critical Security Controls

CIS CRITICAL SECURITY CONTROL	NIST 800-53 rev4*	NIST Core Framework	DHS CDM Program	ISO 27002:2013	ISO 27002:2005	NSA MNP	Au Top 35	NSA Top 10	GCHQ 10 Steps	UK Cyber Essentials	UK ICO Protecting Data	PCI DSS 3.0	HIPAA	FFIEC Examiners Handbook	COBIT 5	NERC CIP v5	NERC CIP v4	NERC CIP v3	Cloud Security Alliance	FY15 FISMA Metrics	ITIL 2011 KPIs
1 Inventory of Authorized & Unauthorized Devices	CA-7 IA-3: SI-4 CM-8 SA-4 PM-5 SC-17	ID.AM-1 ID.AM-3 PR.DS-3	• HWAM: Hardware Asset Management	A.8.1.1 A.9.1.2 A.13.1.1	A.7.1.1 A.10.6.2 A.10.6.1 A.11.4.6	• Map Your Network • Baseline Management • Document Your Network • Personal Electronic Device Management • Network Access Control • Log Management					• Inappropriate Locations for Processing Data	2.4	• 164.310(b): Workstation Use - R • 164.310(c): Workstation Security - R	• Host Security • User Equipment Security (Workstation, Laptop, Handheld)	• APO13: Manage Security • DSS05: Manage Security Services • BAI09: Manage Assets	CIP-002-5 R1 CIP-002-5 R2	CIP-002-4 R1 CIP-004-4 R4 CIP-002-4 R2 CIP-005-4 R2 CIP-002-4 R3 CIP-006-4 R3 CIP-003-4 R5	CIP-002-3 R1 CIP-003-3 R5 CIP-002-3 R2 CIP-004-3 R4 CIP-002-3 R3 CIP-005-3 R2 CIP-002-3 R4 CIP-006-3 R3	DCS-01 MOS-09 MOS-15	1: System Inventory 2: Continuous Monitoring	Information Security Management
2 Inventory of Authorized & Unauthorized Software	CA-7 CM-8 SA-4 SI-4 CM-2 CM-10 SC-18 PM-5 CM-11 SC-34	ID.AM-2 PR.DS-6	• HWAM: Hardware Asset Managementt • SWAM: Software Asset Management	A.12.5.1 A.12.6.2		• Baseline Management • Executable Content Restrictions • Configuration and Change Management	1 14 17	• Application Whitelisting			• Decommissioning of Software or Services		• 164.310(b): Workstation Use - R • 164.310(c): Workstation Security - R	• Host Security • User Equipment Security (Workstation, Laptop, Handheld)	• APO13: Manage Security • DSS05: Manage Security Services				CCC-04 MOS-3 MOS-04 MOS-15	1: System Inventory 2: Continuous Monitoring	Information Security Management
3 Secure Configurations for Hardware & Software	CA-7 CM-6 CM-11 SC-15 CM-2 CM-7 MA-4 SC-34 CM-3 CM-8 RA-5 SI-2 CM-5 CM-9 SA-4 SI-4	PR.IP-1	• CSM: Configuration Settings Management	A.14.2.4 A.14.2.8 A.18.2.3	A.15.2.2	• Patch Management • Baseline Management • Data-at-Rest Protection • Configuration and Change Management	2-5 21	• Control Administrative Privileges • Set a Secure Baseline Configuration • Take Advantage of Software Improvements	• Secure Configuration	• Secure Configuration • Patch Management		2.2 2.3 6.2 11.5	• 164.310(b): Workstation Use - R • 164.310(c): Workstation Security - R	• Host Security • User Equipment Security (Workstation, Laptop, Handheld)	• APO13: Manage Security • DSS05: Manage Security Services • BAI10: Manage Configuration	CIP-007-5 R2 CIP-010-5 R2	CIP-003-4 R6 CIP-007-4 R3	CIP-003-3 R6 CIP-007-3 R3	IVS-07 MOS-15 MOS-19 TVM-02	2: Continuous Monitoring	Information Security Management
4 Continuous Vulnerability Assessment & Remediation	CA-2 RA-5 SI-4 CA-7 SC-34 SI-7	ID.RA-1 DE.CM-8 ID.RA-2 RS.MI-3 PR.IP-12	• VUL: Vulnerability Management	A.12.6.1 A.14.2.8	A.12.6.1 A.13.1.2 A.15.2.2	• Patch Management • Log Management • Configuration and Change Management	2 3	• Take Advantage of Software Improvements		• Patch Management	• Software Updates	6.1 6.2 11.2	• 164.310(b): Workstation Use - R • 164.310(c): Workstation Security - R	• Host Security • User Equipment Security (Workstation, Laptop, Handheld)	• APO13: Manage Security • DSS05: Manage Security Services	CIP-007-5 R2 CIP-010-5 R3	CIP-005-4 R4 CIP-007-4 R3 CIP-007-4 R8	CIP-005-3 R4 CIP-007-3 R3 CIP-007-3 R8	IVS-05 MOS-15 MOS-19 TVM-02	2: Continuous Monitoring	Information Security Management
5 Controlled Use of Administrative Privileges	AC-2 AC-19 IA-5 AC-6 CA-7 SI-4 AC-17 IA-4	PR.AC-4 PR.MA-2 PR.AT-2 PR.PT-3		A.9.1.1 A.9.2.2 - A.9.2.6 A.9.3.1 A.9.4.1 - A.9.4.4	A.10.4.4 A.11.5.1 - A.11.5.3	• User Access • Baseline Management • Log Management	4 9 11 25	• Control Administrative Privileges	• Monitoring	• Access Control	• Configuration of SSL and TLS • Default Credentials	2.1 7.1 - 7.3 8.1 - 8.3 8.7	• 164.310(b): Workstation Use - R • 164.310(c): Workstation Security - R	• Authentication and Access Controls	• APO13: Manage Security • DSS05: Manage Security Services	CIP-004-5 R4 CIP-004-5 R5 CIP-007-5 R5	CIP-003-4 R5 CIP-005-4 R3 CIP-004-4 R4 CIP-006-4 R3 CIP-005-4 R2 CIP-007-4 R3	CIP-003-3 R5 CIP-005-3 R3 CIP-004-3 R4 CIP-006-3 R3 CIP-005-3 R2 CIP-007-3 R3	IAM-09 - IAM-13 MOS-16 MOS-20	3: Identity Credential & Access Management	Information Security Management
6 Maintenance, Monitoring, & Analysis of Audit Logs	AC-23 AU-6 AU-11 IA-10 AU-2 AU-7 AU-12 SI-4 AU-3 AU-8 AU-13 AU-4 AU-9 AU-14 AU-5 AU-10 CA-7	PR.PT-1 DE.DP-3 DE.AE-3 DE.DP-4 DE.DP-1 DE.DP-5 DE.DP-2	• Generic Audit Monitoring	A.12.4.1 - A.12.4.4 A.12.7.1	A.10.10.1 - A.10.10.3 A.10.10.6	• Log Management	15-16 35		• Monitoring			10.1 - 10.7	• 164.308(a)(1): Security Management Process - Information System Activity Review R • 164.308(a)(5): Security Awareness and Training - Log-in Monitoring A	• Security Monitoring	• APO13: Manage Security • DSS05: Manage Security Services	CIP-007-5 R4	CIP-005-4 R3 CIP-007-4 R6	CIP-005-3 R3 CIP-007-3 R6	IVS-01 IVS-03		Information Security Management
7 Email & Web Browser Protections	CA-7 CM-6 CM-11 SC-15 CM-2 CM-7 MA-4 SC-34 CM-3 CM-8 RA-5 SI-2 CM-5 CM-9 SA-4 SI-4	PR.IP-1	• CSM: Configuration Settings Management	A.14.2.4 A.14.2.8 A.18.2.3	A.15.2.2	• Patch Management • Baseline Management • Data-at-Rest Protection • Configuration and Change Management	2-5 21	• Control Administrative Privileges • Set a Secure Baseline Configuration • Take Advantage of Software Improvements	• Secure Configuration	• Secure Configuration • Patch Management		2.2 2.3 6.2 11.5	• 164.310(b): Workstation Use - R • 164.310(c): Workstation Security - R	• Host Security • User Equipment Security (Workstation, Laptop, Handheld)	• APO13: Manage Security • DSS05: Manage Security Services • BAI10: Manage Configuration	CIP-007-5 R2 CIP-010-5 R2	CIP-003-4 R6 CIP-007-4 R3	CIP-003-3 R6 CIP-007-3 R3	IVS-07 MOS-15 MOS-19 TVM-02	2: Continuous Monitoring	Information Security Management
8 Malware Defenses	CA-7 SC-44 SI-4 SC-39 SI-3 SI-8	PR.PT-2 DE.CM-4 DE.CM-5		A.8.3.1 A.12.2.1 A.13.2.3	A.10.4.1 - A.10.4.2 A.10.7.1	• Device Accessibility • Virus Scanners & Host Intrusion Prevention Systems • Security Gateways, Proxies, & Firewalls • Network Security Monitoring • Log Management	7 26 17 30 22	• Use Anti-Virus File Reputation Services • Enable Anti-Exploitation Features	• Removable Media Controls • Malware Protection	• Malware Protection		5.1 - 5.4	• 164.308(a)(5): Security Awareness and Training - Protection from Malicious Software A • 164.310(d)(1): Device and Media Controls - Accountability A • 164.310(b): Workstation Use - R • 164.310(c): Workstation Security - R	• Host Security • User Equipment Security (Workstation, Laptop, Handheld)	• APO13: Manage Security • DSS05: Manage Security Services	CIP-007-5 R3	CIP-007-4 R4	CIP-007-3 R4	MOS-01 MOS-15 TVM-01 TVM-03	4: Anti-Phishing & Malware Defense	Information Security Management
9 Limitation & Control of Network Ports	AT-1 AT-4 PM-13 AT-2 SA-11 PM-14 AT-3 SA-16 PM-16	PR.AC-5 DE.AE-1	• Boundary Protection	A.9.1.2 A.13.1.1 A.13.1.2 A.14.1.2	A.10.6.1 - A.10.6.2 A.11.4.4	• Baseline Management • Configuration and Change Management	2 13 3 27 12	• Limit Workstation-to-Workstation Communication	• Network Security		• Decommissioning of Software or Services • Unnecessary Services	1.4	• 164.310(b): Workstation Use - R • 164.310(c): Workstation Security - R	• Network Security	• APO13: Manage Security • DSS05: Manage Security Services	CIP-007-5 R1	CIP-007-4 R2	CIP-007-3 R2	DSI-02 IVS-06 IPT-04		Information Security Management
10 Data Recovery Capability	CP-9 CP-10 MP-4	PR.IP-4		A.10.1.1 A.12.3.1	A.10.5.1 A.10.8.3	• Backup Strategy						4.3 9.5 - 9.7	• 164.308(a)(7): Contingency Plan - Data Backup Plan R • 164.308(a)(7): Contingency Plan - Disaster Recovery Plan R • 164.308(a)(7): Contingency Plan - Testing & Revision Procedure A • 164.310(d)(1): Device & Media Controls - Data Backup & Storage A	• Encryption	• APO13: Manage Security • DSS05: Manage Security Services		CIP-009-4 R4 CIP-009-4 R5	CIP-009-3 R4 CIP-009-3 R5	MOS-11		Information Security Management
11 Secure Configurations for Network Devices	AC-4 CA-9 CM-5 MA-4 CA-3 CM-2 CM-6 SC-24 CA-7 CM-3 CM-8 SI-4	PR.AC-5 PR.IP-1 PR.PT-4	• CSM: Configuration Settings Management • Boundary Protection	A.9.1.2 A.13.1.1 A.13.1.3	A.10.6.1 - A.10.6.2 A.11.4.5 A.11.4.7 A.11.5.1 - A.11.5.3	• Map Your Network • Patch Management • Baseline Management • Document Your Network • Security Gateways, Proxies, and Firewalls • Configuration and Change Management	2 3 10	• Set a Secure Baseline Configuration • Segregate Networks and Functions	• Secure Configuration • Network Security	• Boundary Firewalls & Internet Gateways • Secure Configuration • Patch Management	• Software Updates • Inappropriate Locations for Processing Data	1.1 - 1.2 2.2 6.2		• Network Security	• APO13: Manage Security • DSS05: Manage Security Services • BAI10: Manage Configuration	CIP-005-5 R1 CIP-007-5 R2	CIP-003-4 R6 CIP-006-4 R3 CIP-004-4 R4 CIP-007-4 R3 CIP-005-4 R2	CIP-003-3 R6 CIP-006-3 R3 CIP-004-3 R4 CIP-007-3 R3 CIP-005-3 R2	DSI-02 IVS-09 IAM-03 MOS-19 IVS-06 TVM-02	3: Identity Credential & Access Management	Information Security Management
12 Boundary Defense	AC-4 CA-7 SC-7 AC-17 CA-9 SC-8 AC-20 CM-2 SI-4 CA-3 SA-9	PR.AC-3 PR.AC-5 PR.MA-2 DE.AE-1	• Boundary Protection	A.9.1.2 A.12.4.1 A.13.1.3 A.12.7.1 A.13.2.3 A.13.1.1	A.10.6.1 - A.10.6.2 A.11.5.1 - A.11.5.3 A.11.7.1 - A.11.7.2 A.10.10.2 A.11.4.2 A.11.4.5 A.11.4.7	• Map Your Network • Network Architecture • Baseline Management • Document Your Network • Personal Electronic Device Management • Security Gateways, Proxies, and Firewalls • Remote Access Security • Network Security Monitoring • Log Management	10-11 18-20 23 32-34	• Segregate Networks and Functions	• Home and Mobile Working • Monitoring • Network Security	• Boundary Firewalls & Internet Gateways	• Configuration of SSL and TLS • Inappropriate Locations for Processing Data	1.1 - 1.3 8.3 10.8 11.4		• Network Security • Security Monitoring	• APO13: Manage Security • DSS05: Manage Security Services	CIP-005-5 R1 CIP-005-5 R2 CIP-007-5 R4	CIP-005-4 R3 CIP-007-4 R6	CIP-005-3 R3 CIP-007-3 R6	DSI-02 IVS-01 IVS-06 IVS-09 MOS-16	3: Identity Credential & Access Management 6: Network Defense 7: Boundary Protection	Information Security Management
13 Data Protection	AC-3 CA-9 SC-8 SI-4 AC-4 IR-9 SC-28 AC-23 MP-5 SC-31 CA-7 SA-18 SC-41	PR.AC-5 PR.DS-2 PR.DS-5 PR.PT-2		A.8.3.1 A.10.1.1 - A.10.1.2 A.13.2.3 A.18.1.5	A.10.7.1 A.12.3.1 - A.12.3.2 A.12.5.4 A.15.1.6	• Network Architecture • Device Accessibility • Security Gateways, Proxies, and Firewalls • Network Security Monitoring	26		• Removable Media Controls			3.6 4.1 - 4.3	• 164.308(a)(4): Information Access Management - Isolating Health Care Clearinghouse Function R • 164.310(d)(1): Device and Media Controls - Accountability A • 164.312(a)(1): Access Control - Encryption and Decryption A • 164.312(e)(1): Transmission Security - Integrity Controls A • 164.312(e)(1): Transmission Security - Encryption A	• Encryption • Data Security	• APO13: Manage Security • DSS05: Manage Security Services	CIP-011-5 R1			DSI-02 DSI-05 EKM-01 - EKM-04 MOS-11	5: Data Protection	Information Security Management
14 Controlled Access Based on the Need to Know	AC-1: AC-6 RA-2 AC-2: AC-24 SC-16 AC-3 CA-7 SI-4 MP-3	PR.AC-4 PR.DS-2 PR.AC-5 PR.PT-2 PR.DS-1 PR.PT-3	• TRUST: Access Control Management • PRIV: Privileges	A.8.3.1 A.9.1.1 A.10.1.1	A.10.7.1 A.10.10.1 - A.10.10.3 A.11.4.5 A.11.4.7 A.11.6.1 - A.11.6.2 A.12.5.4	• Network Architecture • Device Accessibility • User Access • Data-at-Rest Protection • Log Management	26	• Segregate Networks and Functions	• Managing User Privileges • Network Security	• Access Control	• Inappropriate Locations for Processing Data	1.3 - 1.4 4.3 7.1 - 7.3 8.7	• 164.308(a)(1): Security Management Process - Information System Activity Review R • 164.308(a)(4): Information Access Management - Isolating Health Care Clearinghouse Function R • 164.308(a)(4): Information Access Management - Access Authorization A • 164.312(a)(1): Access Control - Encryption and Decryption A • 164.312(c)(1): Integrity - Mechanism to Authenticate Electronic Protected Health Information A • 164.312(a)(1): Access Control - Automatic Logoff A • 164.312(d): Person or Entity Authentication - R • 164.312(e)(1): Transmission Security - Integrity Controls A • 164.312(e)(1): Transmission Security - Encryption A	• Authentication and Access Controls • Encryption • Data Security	• APO13: Manage Security • DSS05: Manage Security Services	CIP-005-5 R1 CIP-005-5 R2 CIP-007-5 R4 CIP-011-5 R1	CIP-003-4 R5 CIP-004-4 R4 CIP-005-4 R2 CIP-006-4 R3	CIP-003-3 R5 CIP-004-3 R4 CIP-005-3 R2 CIP-006-3 R3	DSI-02 IVS-09 MOS-11		Information Security Management
15 Wireless Access Control	AC-18 CM-2 SC-40 AC-19 IA-3 SI-4 CA-3 SC-8 CA-7 SC-17			A.10.1.1 A.12.4.1 A.12.7.1		• Map Your Network • Baseline Management • Document Your Network • Personal Electronic Device Management • Network Access Control			• Monitoring • Network Security			4.3 11.1		• Network Security • Encryption • Security Monitoring	• APO13: Manage Security • DSS05: Manage Security Services	CIP-007-5 R4	CIP-005-4 R3 CIP-007-4 R6	CIP-005-3 R3 CIP-007-3 R6	IVS-01 IVS-06 IVS-12 MOS-11		Information Security Management
16 Account Monitoring & Control	AC-2 CA-7 AC-3 IA-5 AC-7 IA-10 AC-11 SC-17 AC-12 SC-23	PR.AC-1 PR.AC-4 PR.PT-3	• CRED: Credentials and Authentication Management	A.9.1.1 A.9.2.1 - A.9.2.6 A.9.3.1 A.9.4.1 - A.9.4.3 A.11.2.8	A.8.3.3 A.11.2.1 A.11.2.3 - A.11.2.4 A.11.3.1 - A.11.3.3 A.11.5.1 - A.11.5.3	• User Access • Baseline Management • Log Management	25		• Managing User Privileges	• Access Control	• Configuration of SSL and TLS	7.1 - 7.3 8.7 - 8.8	• 164.308(a)(1): Security Management Process - Information System Activity Review R • 164.308(a)(4): Information Access Management - Access Authorization A • 164.308(a)(4): Information Access Management - Access Establishment and Modification A • 164.308(a)(5): Security Awareness and Training - Password Management A • 164.312(a)(1): Access Control - Unique User Identification A • 164.312(a)(1): Access Control - Automatic Logoff A • 164.312(d): Person or Entity Authentication - R • 164.312(e)(1): Transmission Security - Integrity Controls A • 164.312(e)(1): Transmission Security - Encryption A	• Authentication and Access Controls	• APO13: Manage Security • DSS05: Manage Security Services	CIP-005-5 R1 CIP-005-5 R2 CIP-007-5 R4	CIP-005-4 R3 CIP-007-4 R5 CIP-007-4 R6	CIP-005-3 R3 CIP-007-3 R5 CIP-007-3 R6	IAM-02 IAM-09 - IAM-12 MOS-14 MOS-16 MOS-20	3: Identity Credential & Access Management	Information Security Management
17 Security Skills Assessment and Appropriate Training to Fill Gaps	AT-1 AT-4 PM-13 AT-2 SA-11 PM-14 AT-3 SA-16 PM-16	PR.AT-1 PR.AT-4 PR.AT-2 PR.AT-5 PR.AT-3	• BEHV: Security-Related Behavior Management	A.7.2.2	A.8.2.2	• Training	28		• User Education & Awareness			12.6	• 164.308(a)(5): Security Awareness and Training - Security Reminders A • 164.308(a)(5): Security Awareness and Training - Protection from Malicious Software A • 164.308(a)(5): Security Awareness and Training - Log-in Monitoring A • 164.308(a)(5): Security Awareness and Training - Password Management A	• Personnel Security	• APO13: Manage Security • DSS05: Manage Security Services	CIP-004-5 R1 CIP-004-5 R2	CIP-004-4 R1 CIP-004-4 R2	CIP-004-3 R1 CIP-004-3 R2	HRS-10 MOS-05	8: Training and Education	Information Security Management
18 Application Software Security	SA-13 SA-20 SI-11 SA-15 SA-21 SI-15 SA-16 SC-39 SI-16 SA-17 SI-10	PR.DS-7	• VUL: Vulnerability Management	A.9.4.5 A.12.1.4 A.14.2.1 A.14.2.6 - A.14.2.8	A.10.1.4 A.12.5.2 A.12.2.1 A.12.5.5 A.12.2.4	• Training	24				• SQL Injection	6.3 6.5 - 6.7		• Application Security • Software Development & Acquisition	• APO13: Manage Security • DSS05: Manage Security Services				AIS-01 CCC-02 AIS-03 CCC-03 AIS-04 IVS-08 CCC-01		Information Security Management
19 Incident Response & Management	IR-1 IR-4 IR-7 IR-2 IR-5 IR-8 IR-3 IR-6 IR-10	PR.IP-10 RS.AN-1-4 DE.AE-2 RS.MI-1-2 DE.AE-4 RS.IM-1-2 DE.AE-5 RC.RP-1 DE.CM-1-7 RC.IM-1-2 RS.RP-1 RC.CO-1-3 RS.CO-1-5		• Plan for Events • Respond to Events	A.6.1.3 A.7.2.1 A.16.1.2 A.16.1.4 - A.16.1.7	A.6.1.6 A.8.2.1 A.13.1.1 A.13.2.1 - A.13.2.2	• Incident Response and Disaster Recovery Plans			• Incident Management			12.10	• 164.308(a)(6): Security Incident Procedures - Response and Reporting R		• APO13: Manage Security • DSS05: Manage Security Services • DSS02: Manage Service Requests and Incidents	CIP-008-5 R1 CIP-008-5 R2 CIP-008-5 R3	CIP-008-4 R1 CIP-008-4 R2	CIP-008-3 R1 CIP-008-3 R2	SEF-01 - SEF-05	9: Incident Response	Information Security Management
20 Penetration Tests & Red Team Exercises	CA-2 CA-8 PM-6 CA-5 RA-6 PM-14 CA-6 SI-6			A.14.2.8 A.18.2.1 A.18.2.3	A.6.1.8 A.15.2.2 A.15.3.1	• Audit Strategy						11.3			• APO13: Manage Security • DSS05: Manage Security Services • MEA02: Monitor, Evaluate and Assess the System of Internal Control						Information Security Management

***NIST 800-53 LISTINGS**

AC-1: Access Control Policy and Procedures
AC-2: Account Management
AC-3: Access Enforcement
AC-4: Information Flow Enforcement
AC-6: Least Privilege
AC-7: Unsuccessful Logon Attempts
AC-11: Session Lock
AC-12: Session Termination
AC-17: Remote Access
AC-18: Wireless Access
AC-19: Access Control for Mobile Devices
AC-20: Use of External Information Systems
AC-23: Data Mining Protection
AC-24: Access Control Decisions
AT-1: Security Awareness and Training Policy and Procedures
AT-2: Security Awareness Training
AT-3: Role-Based Security Training
AT-4: Security Training Records
AU-2: Audit Events
AU-3: Content of Audit Records
AU-4: Audit Storage Capacity
AU-5: Response to Audit Processing Failures
AU-6: Audit Review, Analysis, and Reporting
AU-7: Audit Reduction and Report Generation
AU-8: Time Stamps
AU-9: Protection of Audit Information
AU-10: Non-repudiation
AU-11: Audit Record Retention
AU-12: Audit Generation
AU-13: Monitoring for Information Disclosure
AU-14: Session Audit
CA-2: Security Assessments
CA-3: System Interconnections
CA-5: Plan of Action and Milestones
CA-6: Security Authorization
CA-7 Continuous Monitoring
CA-8: Penetration Testing
CA-9: Internal System Connections
CM-2: Baseline Configuration
CM-3: Configuration Change Control
CM-5: Access Restrictions for Change
CM-6: Configuration Settings
CM-7: Least Functionality
CM-8: Information System Component Inventory
CM-9: Configuration Management Plan
CM-10: Software Usage Restrictions
CM-11: User-Installed Software
CP-9: Information System Backup
CP-10: Information System Recovery and Reconstitution
IA-3: Device Identification and Authentication
IA-5: Authenticator Management
IA-10: Adaptive Identification and Authentication
IR-1: Incident Response Policy and Procedures
IR-2: Incident Response Training
IR-3: Incident Response Testing
IR-4: Incident Handling
IR-5: Incident Monitoring
IR-6: Incident Reporting
IR-7: Incident Response Assistance
IR-8: Incident Response Plan
IR-9: Information Spillage Response
IR-10: Integrated Information Security Analysis Team
MA-4: Nonlocal Maintenance
MP-3: Media Marking
MP-4: Media Storage
MP-5: Media Transport
PM-5: Information System Inventory
PM-6: Information Security Measures of Performance
PM-13: Information Security Workforce
PM-14: Testing, Training, & Monitoring
PM-16: Threat Awareness Program
RA-2: Security Categorization
RA-5: Vulnerability Scanning
RA-6: Technical Surveillance Countermeasures Survey
SA-4: Acquisition Process
SA-9: External Information System Services
SA-11: Developer Security Testing and Evaluation
SA-13: Trustworthiness
SA-15: Development Process, Standards, and Tools
SA-16: Developer-Provided Training
SA-17: Developer Security Architecture and Design
SA-18: Tamper Resistance and Detection
SA-20: Customized Development of Critical Components
SA-21: Developer Screening
SC-7: Boundary Protection
SC-8: Transmission Confidentiality and Integrity
SC-15: Collaborative Computing Devices
SC-16: Transmission of Security Attributes
SC-17: Public Key Infrastructure Certificates
SC-18: Mobile Code
SC-20: Secure Name/Address Resolution Service (Authoritative Source)
SC-21: Secure Name/Address Resolution Service (Recursive or Caching Resolver)
SC-22: Architecture and Provisioning for Name/Address Resolution Service
SC-23: Session Authenticity
SC-24: Fail in Known State
SC-28: Protection of Information at Rest
SC-31: Covert Channel Analysis
SC-34: Non-Modifiable Executable Programs
SC-39: Process Isolation
SC-40: Wireless Link Protection
SC-41: Port and I/O Device Access
SC-44: Detonation Chambers
SI-2: Flaw Remediation
SI-3: Malicious Code Protection
SI-4: Information System Monitoring
SI-6: Security Function Verification
SI-7: Software, Firmware, and Information Integrity
SI-8: Spam Protection
SI-10: Information Input Validation
SI-11: Error Handling
SI-15: Information Output Filtering
SI-16: Memory Protection

CIS Critical Security Controls