Daphnie Bruno
Instructor: Robin Alarcon
CYB349-O | C202411-02
November 15, 2024

1. **Justify the group's decisions**

The selected cryptography and encryption controls for SnowBe Online that group 5 made are crucial for protecting sensitive customer data and ensuring compliance with industry standards.

IA-5 AUTHENTICATOR MANAGEMENT:
Group 5 picked Authenticator manager because this control is essential for SnowBe Online to properly manage and protect user credentials, especially given their laid-back culture and the need for improved access management. It helps prevent unauthorized access to sensitive systems and data. IA-5(1) AUTHENTICATOR MANAGEMENT | PASSWORD-BASED AUTHENTICATION: This enhancement ensures robust password policies are in place, which is critical for SnowBe Online's e-commerce platform and internal systems to prevent unauthorized access and protect customer data. IA-5(6) AUTHENTICATOR MANAGEMENT | PROTECTION OF AUTHENTICATORS: This enhancement is crucial for safeguarding authentication credentials, particularly important for SnowBe Online's e-commerce platform and internal systems that handle sensitive customer and financial data. IA-5(7) AUTHENTICATOR MANAGEMENT | NO EMBEDDED UNENCRYPTED STATIC AUTHENTICATORS: This enhancement prevents the use of hardcoded or embedded credentials, which is essential for SnowBe Online's security, especially given their recent need to update various systems and software. IA-5(8) AUTHENTICATOR MANAGEMENT | MULTIPLE SYSTEM ACCOUNTS: This enhancement helps manage multiple system accounts securely, which is important for SnowBe Online's diverse IT infrastructure spanning on-premises and AWS environments. IA-5(9) AUTHENTICATOR MANAGEMENT | FEDERATED CREDENTIAL MANAGEMENT: This enhancement supports secure credential management across different systems, which is beneficial for SnowBe Online's multi-location operations and diverse IT infrastructure. IA-5(13) AUTHENTICATOR MANAGEMENT | EXPIRATION OF CACHED AUTHENTICATORS: This enhancement ensures that cached credentials expire after a set time, reducing the risk of unauthorized access, which is important for SnowBe Online's remote access setup. IA-5(18) AUTHENTICATOR MANAGEMENT | PASSWORD MANAGERS: This enhancement promotes the use of password managers, which can help SnowBe Online improve their overall password security across their various systems and applications.

Case study:
"The need to implement more processes into the access management system since most employees had access to almost all the data on each server."
"All credit cards are accepted and stored on the company's website database"
"All customer information and purchase history are stored on the website indefinitely."
"The need to update the firmware of all network devices."
"There are six servers (on-premises and AWS) for access management, storage, customer relations management, order management, accounting, and vendor applications"
"They have multiple storefronts in the U.S. and Europe, which accept checks, cash, or credit cards."
"The thirty laptops are used for sales (retail and wholesale). The laptops use a VPN to log into the office to access company applications."
"As a result of SnowBe's laid-back culture, they neglected to implement technical controls and processes."

SC-13 CRYPTOGRAPHIC PROTECTION:
SC-13 control was picked because it ensures the use of approved cryptographic standards, which is crucial for SnowBe Online to protect sensitive customer and financial data both at rest and in transit. It mandates the implementation of FIPS-validated or NSA-approved cryptography for all systems handling sensitive information, enhancing overall data security and compliance with industry regulations like PCI DSS.

Case study:
"All credit cards are accepted and stored on the company's website database."

SC-28 PROTECTION OF INFORMATION AT REST:
We (group 5) picked SC-28 because this control is vital for SnowBe Online to protect stored customer data and financial information from unauthorized access or tampering. SC-28(1) PROTECTION OF INFORMATION AT REST | CRYPTOGRAPHIC PROTECTION: This enhancement ensures that sensitive data at rest is encrypted, which is crucial for SnowBe Online's customer and financial data stored in their databases. SC-28(2) PROTECTION OF INFORMATION AT REST | OFFLINE STORAGE: This enhancement protects offline or backup data, which is important for SnowBe Online's data retention and disaster recovery practices. SC-28(3) PROTECTION OF INFORMATION AT REST | CRYPTOGRAPHIC KEYS: This enhancement ensures proper management of cryptographic keys, which is essential for maintaining the security of SnowBe Online's encrypted data

Case study:
"All customer information and purchase history are stored on the website indefinitely."
"All credit cards are accepted and stored on the company's website database."
"The need to update their Anti-Virus and backup software."
"The need for PCI compliance before issues occur."

SC-8 TRANSMISSION CONFIDENTIALITY AND INTEGRITY:
This control was picked because it protects data in transit, which is crucial for SnowBe Online's e-commerce operations and remote access setup. SC-8(1) TRANSMISSION CONFIDENTIALITY AND INTEGRITY | CRYPTOGRAPHIC PROTECTION: This enhancement ensures that data transmitted over networks is encrypted, which is vital for SnowBe Online's e-commerce transactions and remote access. SC-8(2) TRANSMISSION CONFIDENTIALITY AND INTEGRITY | PRE- AND POST-TRANSMISSION HANDLING: This enhancement protects data before and after transmission, which is important for SnowBe Online's overall data security strategy. SC-8(3) TRANSMISSION CONFIDENTIALITY AND INTEGRITY | CRYPTOGRAPHIC PROTECTION FOR MESSAGE EXTERNAL: This enhancement ensures that external messages are cryptographically protected, which is crucial for SnowBe Online's communication with customers and partners. SC-8(4) TRANSMISSION CONFIDENTIALITY AND INTEGRITY | CONCEAL OR RANDOMIZE COMMUNICATIONS: This enhancement helps protect against traffic analysis, which is important for SnowBe Online's overall network security. SC-8(5) TRANSMISSION CONFIDENTIALITY AND INTEGRITY | PROTECTED DISTRIBUTION SYSTEM: This enhancement provides additional protection for sensitive data transmission, which is crucial for SnowBe Online's financial transactions and customer data.

Case study:
"The majority of their sales are processed online through their website, housed on the AWS platform."
"The laptops use a VPN to log into the office to access company applications."
"The need for PCI compliance before issues occur."
"Although, there had been a few attempts that did not cause any harm or alerts to worry anyone."
"The credit card transactions are processed using bank-provided credit card terminals in each store."

SC-12 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT:
We (group 5) chose this control ensures proper management of cryptographic keys, which is essential for maintaining the security of SnowBe Online's encrypted data and communications. SC-12(1) CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | AVAILABILITY: This enhancement ensures the availability of cryptographic keys, which is crucial for SnowBe Online's continuous operations and data access. SC-12(2) CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | SYMMETRIC KEYS: This enhancement manages symmetric cryptographic keys, which is important for SnowBe Online's data encryption practices. SC-12(3) CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | ASYMMETRIC KEYS: This enhancement manages asymmetric cryptographic keys, which is crucial for SnowBe Online's secure communications and authentication processes. SC-12(6) CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | PHYSICAL CONTROL OF KEYS: This enhancement ensures physical control of cryptographic keys, which is important for SnowBe Online's overall key management strategy.

Case study:
"The need for PCI compliance before issues occur."
"There are six servers (on-premises and AWS) for access management, storage, customer relations management, order management, accounting, and vendor applications."
"All credit cards are accepted and stored on the company's website database."
"The laptops use a VPN to log into the office to access company applications."
"The need to lock the servers in a secured area of the office."

IA-7 CRYPTOGRAPHIC MODULE AUTHENTICATION:
Group 5 decided SnowBe Online needed this control because it ensures that cryptographic modules are properly authenticated, which is crucial for overall cryptographic security. It mandates the use of NSA-approved authentication mechanisms for cryptographic modules, enhancing the protection of sensitive data and encryption keys. This is particularly important for SnowBe Online's e-commerce platform, where secure transactions and data protection are vital. Implementing this control helps maintain compliance with industry standards like PCI DSS and strengthens the company's defense.

Case study:
"The need for PCI compliance before issues occur."

SC-17 PUBLIC KEY INFRASTRUCTURE CERTIFICATES:
Group 5 picked this control because it manages PKI certificates, which is important for SnowBe Online's secure communications and e-commerce operations. It ensures the proper issuance, validation, and management of digital certificates, providing a strong framework for authenticating users, devices, and services across the company's digital infrastructure and protecting against potential security breaches.

Case study:
"The majority of their sales are processed online through their website, housed on the AWS platform."

MP-5 MEDIA TRANSPORT:
SnowBe Online need MP-5 Media Support control in order to protects media during transport, which is important for SnowBe Online's data handling practices across multiple locations. MP-5(3) MEDIA TRANSPORT | CUSTODIANS: This enhancement was picked because it is needed to ensure proper custody of transported media, which is crucial for SnowBe Online's data protection during physical transport

Case study:
"They have multiple storefronts in the U.S. and Europe, which accept checks, cash, or credit cards."

MP-6 MEDIA SANITIZATION:
Group 5 picked this control because it will ensure a proper sanitization of media, which is important for SnowBe Online's data protection and compliance efforts. MP-6(1) MEDIA SANITIZATION | REVIEW, APPROVE, TRACK, DOCUMENT, AND VERIFY: This enhancement ensures thorough media sanitization processes, which is crucial for SnowBe Online's data protection and compliance efforts. MP-6(3) MEDIA SANITIZATION | NONDESTRUCTIVE TECHNIQUES: This enhancement uses nondestructive sanitization techniques, which is important for SnowBe Online's data management practices. MP-6(4) MEDIA SANITIZATION | DUAL AUTHORIZATION: This enhancement requires dual authorization for media sanitization, which adds an extra layer of security for SnowBe Online's sensitive data handling. MP-6(5) MEDIA SANITIZATION | REMOTE PURGING OR WIPING OF INFORMATION: This enhancement allows remote purging of data, which is important for SnowBe Online's mobile device management and data protection

Case study:
"The need for PCI compliance before issues occur."
"All customer information and purchase history are stored on the website indefinitely."
"The need to implement more processes into the access management system since most employees had access to almost all of the data on each server."
"The thirty laptops are used for sales (retail and wholesale). The laptops use a VPN to log into the office to access company applications."

SI-7 SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY:

This control ensures the integrity of software, firmware, and information, which is crucial for SnowBe Online's overall system security. SI-7(1) SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | INTEGRITY CHECKS: This enhancement performs integrity checks, which is important for SnowBe Online's system and data security. SI-7(2) SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | AUTOMATED NOTIFICATIONS OF INTEGRITY VIOLATIONS: This enhancement provides automated notifications of integrity violations, which is crucial for SnowBe Online's prompt response to security issues. SI-7(5) SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | AUTOMATED RESPONSE TO INTEGRITY VIOLATIONS: This enhancement provides automated responses to integrity violations, which is crucial for SnowBe Online's prompt and consistent handling of security issues. SI-7(6) SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | CRYPTOGRAPHIC PROTECTION: This enhancement uses cryptographic protection for software, firmware, and information integrity, which is important for SnowBe Online's overall data security. SI-7(9) SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | VERIFY BOOT PROCESS: This enhancement verifies the boot process, which is crucial for SnowBe Online's system security from startup. SI-7(10) SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | PROTECTION OF BOOT FIRMWARE: This enhancement protects boot firmware, which is important for SnowBe Online's system security at the hardware level. SI-7(12) SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | INTEGRITY VERIFICATION: This enhancement performs integrity verification, which is crucial for SnowBe Online's overall system and data integrity. SI-7(15) SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | CODE AUTHENTICATION: This enhancement performs code authentication, which is important for SnowBe Online's software security and integrity. SI-7(17) SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | RUNTIME APPLICATION SELF-PROTECTION: This enhancement provides runtime application self-protection, which is crucial for SnowBe Online's application security, especially for their e-commerce platform.

Case study:

"The need to update the firmware of all network devices."

"The need to update the patches for all PCs and Windows servers to ensure they are on the latest Windows version."

"Although, there had been a few attempts that did not cause any harm or alerts to worry anyone."

"There are six servers (on-premises and AWS) for access management, storage, customer relations management, order management, accounting, and vendor applications."

"All credit cards are accepted and stored on the company's website database."

"The need to update their Anti-Virus and backup software."

"The need to update the company's WordPress shopping cart."

"The majority of their sales are processed online through their website, housed on the AWS platform."

SC-7 BOUNDARY PROTECTION

SC-7 was the last control that group 5 decided was needed. This is because C-7 provides boundary protection, which is essential for SnowBe Online's network security and data protection. SC-7(3) BOUNDARY PROTECTION | ACCESS POINTS: This enhancement limits the number of access points, which is important for SnowBe Online's network security management. SC-7(4) BOUNDARY PROTECTION | EXTERNAL TELECOMMUNICATIONS SERVICES: This enhancement manages external telecommunications services, which is crucial for SnowBe Online's

secure communication with external entities. SC-7(5) BOUNDARY PROTECTION | DENY BY DEFAULT — ALLOW BY EXCEPTION: This enhancement implements a deny-by-default policy, which is important for SnowBe Online's overall network security posture. SC-7(7) BOUNDARY PROTECTION | SPLIT TUNNELING FOR REMOTE DEVICES: This enhancement prevents split tunneling for remote devices, which is crucial for SnowBe Online's secure remote access setup. SC-7(9) BOUNDARY PROTECTION | RESTRICT THREATENING OUTGOING COMMUNICATIONS TRAFFIC: This enhancement restricts outgoing traffic that may be threatening, which is crucial for SnowBe Online's network security and data protection. SC-7(10) BOUNDARY PROTECTION | PREVENT EXFILTRATION: This enhancement is crucial for SnowBe Online to prevent unauthorized data exfiltration, protecting sensitive customer and financial information stored in their databases and systems. It helps safeguard against data breaches and maintains compliance with data protection regulations. SC-7(11) BOUNDARY PROTECTION | RESTRICT INCOMING COMMUNICATIONS TRAFFIC: This enhancement is important for SnowBe Online to control and limit incoming network traffic, reducing the attack surface and protecting against potential threats. It's especially critical given their e-commerce operations and multiple locations. SC-7(12) BOUNDARY PROTECTION | HOST-BASED PROTECTION: This enhancement is necessary for SnowBe Online to implement host-based security measures on individual systems, providing an additional layer of protection beyond network-level controls. This is particularly important for their diverse IT infrastructure. SC-7(14) BOUNDARY PROTECTION | PROTECT AGAINST UNAUTHORIZED PHYSICAL CONNECTIONS: This enhancement is crucial for SnowBe Online to prevent unauthorized physical access to their network infrastructure, especially important given their multiple physical locations and the need for improved physical security. SC-7(18) BOUNDARY PROTECTION | FAIL SECURE: This enhancement ensures that SnowBe Online's boundary protection mechanisms fail in a secure state, maintaining protection even during failures. This is critical for maintaining continuous security, especially for their e-commerce operations. SC-7(20) BOUNDARY PROTECTION | DYNAMIC ISOLATION AND SEGREGATION: This enhancement allows SnowBe Online to dynamically isolate or segregate systems as needed, providing flexibility in responding to security incidents or managing access. This is important given their diverse IT infrastructure and multiple locations. SC-7(24) BOUNDARY PROTECTION | PERSONALLY IDENTIFIABLE INFORMATION: This enhancement is crucial for SnowBe Online to protect personally identifiable information (PII) at system boundaries, ensuring compliance with data protection regulations and safeguarding customer data. ."SC-7(28) BOUNDARY PROTECTION | CONNECTIONS TO PUBLIC NETWORKS: This enhancement is important for SnowBe Online to properly manage and secure connections to public networks, which is critical given their e-commerce operations and use of cloud services.

Case study:

"Although, there had been a few attempts that did not cause any harm or alerts to worry anyone."

"The laptops use a VPN to log into the office to access company applications."

"They have multiple storefronts in the U.S. and Europe, which accept checks, cash, or credit cards."

"The need to implement more processes into the access management system since most employees had access to almost all of the data on each server."

"All customer information and purchase history”

"All credit cards are accepted and stored on the company's website database."

"The majority of their sales are processed online through their website, housed on the AWS platform."

"There are twenty desktops and thirty laptops in the main office in Los Angeles."

"The need to lock the servers in a secured area of the office."
"The majority of their sales are processed online through their website, housed on the AWS platform."
"There are six servers (on-premises and AWS) for access management, storage, customer relations management, order management, accounting, and vendor applications."
"All customer information and purchase history are stored on the website indefinitely"

2. **List 5 of the remaining Cryptography and Encryption controls from the list in GROUP item 1, and explain, in 50 words or more, why the group did not select them.**

1. AC-16 SECURITY AND PRIVACY ATTRIBUTES

This control focuses on associating security and privacy attributes with information. While important for data classification and access control, it was not selected by group 5 because SnowBe Online's immediate needs are more focused on basic encryption and key management. Implementing security and privacy attributes requires a mature data governance program, which may be a future consideration for the company as they improve their overall security posture.

2. AC-23 DATA MINING PROTECTION

Data mining protection is designed to prevent unauthorized data mining on organizational systems. This control was also not selected because SnowBe Online's primary concern is protecting customer data and financial transactions, rather than preventing data mining. Their e-commerce platform and customer database may not be at immediate risk of data mining attacks, making other controls more pressing.

3. CP-9 SYSTEM BACKUP

While system backups are crucial for business continuity, this control was not selected as a primary cryptography and encryption control. SnowBe Online most likely already has setup a backup system in place, and the focus of their cryptography efforts is more on protecting live data rather than backup data. However, I believe it should consider encrypting backups in the future.

4. SC-20 SECURE NAME/ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)

This control relates to secure DNS services, which, while important for the network security, it is not a top priority for SnowBe Online's immediate cryptography and encryption needs. Their focus is currently geared more towards protecting customer data and financial transactions rather than securing DNS infrastructure, which may already be managed by their cloud service provider (AWS).

5. SC-37 OUT-OF-BAND CHANNELS

Out-of-band channels for authentication or notification can enhance security but may be seen as an advanced measure that SnowBe Online is not ready to implement yet. The primary focus right now on basic encryption of data at rest and in transit, as well as key management. Implementing out-of-band channels could possibly be considered in future security enhancements.