Group Assignment 5.1: Developing a Physical Security Architecture

Jacob Harrison

Joshua A. Wortz

Stephanie Wright

University of San Diego

CSOL-520

Melanie Thomas, M.S.

03/31/2025

Developing a Physical Security Architecture

Builders View:

The physical security architecture for Bene Gesserit Urgent Care (BGUC) is constructed to implement technical solutions with the longevity of business goals in mind. It establishes a pragmatic methodology for the security controls chosen to align with business, operational, and compliance requirements. BGUC needs to reduce costs where feasible by utilizing a cloud infrastructure and central management systems, such as Microsoft Intune, for cost reduction. It reduces hardware costs (Synopetk, 2024) and simplifies administrative logistics due to its integration capability with Microsoft applications, which are widely used in many facilities. Additionally, it supports devices commonly found in clinical environments.

BGUC's framework is constructed with modularity in mind, as it requires components to be independent of each other while remaining compatible. The framework will utilize a combination of encryption, access management, and monitoring tools to facilitate the removal of components that require replacement or separate updates (NIST, 2020). For instance, BGUC can transition from Microsoft Defender to CrowdStrike while continuing to use existing encryption (BitLocker) and identity provider (Azure Active Directory). The flexibility of this system also provides scalability in services.

It provides BGUC with growth opportunities without requiring a complete redesign of the architecture. By integrating standard components such as MFA services and encryption protocols, BGUC's architecture effectively minimizes functional redundancies and enhances operational efficiency within systems. Automated backups, transparent workflows, and centralized log management enhance operability by easing the IT department's workload

(OpenAI, 2024). BGUC's system usability is ensured through intuitive user interfaces and role-based dashboards, which are customized for medical staff, billing departments, and patients. BGUC's **i**nteroperability will be demonstrated by the use of APIs and secure protocols to connect EMR systems with third-party vendors, pharmacies, and insurance providers. The system overview highlights secure access to the supply chain and telemedicine via VPN and privileged access management. Business continuity is ensured by integrating legacy infrastructure with secure communication protocols and middleware, keeping systems functional as technology advances. Overall, BGUC's physical architecture is designed to facilitate service expansion, adopting new innovative technologies, and championing cyber innovation. These solutions enable BGUC to dream big while maintaining an innovative and strategic focus on aligning business objectives.

Enabling Business:

BGUC relies on its planned infrastructure to stay current with the latest cybersecurity measures suitable for today's digital age, as part of its business security strategy. The **internet** enables BGUC to capitalize on business opportunities due to its global reach. Through **global email services**, our architecture supports quick, dependable, and regularly available communication with our patients and business partners in various locations. BGUC streamlines the burden on internal IT responsibilities by ensuring secure access to the supply chain through operational governance that collaborates with the network and system infrastructure (CIS, 2021). The business framework provides remote access capabilities for supply chain vendors, including pharmacies and billing vendors, utilizing VPNs and role-based access controls (U.S. Department of Health and Human Services, 2018). Service growth requires the development of online

business resources, such as patient portals and appointment scheduling, that are secured through encryption and multi-factor authentication (MFA) tools. Patient engagement is facilitated through secure digital document transfer and medical information media platforms, providing both convenience and an engaging experience for patients. Centralized systems ensure consistent user interactions, thereby enhancing customer satisfaction and loyalty. Additionally, they facilitate efficient customer service and improve communication across various departments. This reduces redundancies, such as duplicated data entries and inconsistent information, since all data is logged in a centralized system. Productivity outside the workplace is achievable with secure mobile devices and remote access. BGUC ensures continuous operations and data privacy, maintaining HIPAA compliance through secured mobile access and telework support. Furthermore, software updates and technical support from supply chain vendors are provided remotely via securely managed VPN access and permission-based controls. Implementing time limitations and role restrictions for vendor sessions, along with integrating a BGUC's SIEM for monitoring activities, enhances credibility and auditability. Utilizing tools such as Microsoft Intune and Azure Conditional Access ensures that secure updates are implemented and authorized functions are implemented during contractor sessions (U.S. Department of Health and Human Services, 2018). This perspective reinforces business continuity, improves IT efficiency, and facilitates system authenticity during cloud-based vendor support operations.

Business Data Model

BGUC's business data model is crucial for managing critical operational data while ensuring security and regulatory compliance, particularly in healthcare environments. The model encompasses various data categories, including patient records (comprising medical histories, contact details, and insurance information), employee data (such as job roles and access

permissions), appointment scheduling, billing details, and vendor information (e.g., pharmacies and insurance providers). To secure this sensitive data, encryption technologies such as AES-256 and BitLocker are employed, and digital signatures ensure the authenticity and integrity of medical records and transactions. Audit logs track every access and modification to the data, providing accountability and transparency. Additionally, secure messaging protocols encrypt communications between patients, healthcare providers, and third-party vendors to protect patient confidentiality during data exchanges (Data Guy, 2023).

Security Rules, Practices, and Procedures

BGUC's security framework is designed to maintain system integrity while ensuring compliance with healthcare regulations, such as HIPAA. The rules and practices are focused on access control, encryption, and continuous monitoring. Role-based access control (RBAC) assigns users specific permissions based on their roles, limiting exposure to sensitive data. Multi-factor authentication (MFA) is required for all users to ensure secure system entry. External vendors are granted limited, time-sensitive access via secure VPN connections (Neso Academy, 2021). Data encryption is employed for both data at rest (BitLocker) and in transit (SSL/TLS), securing patient and operational information. Centralized logging, integrated with a Security Information and Event Management (SIEM) system, provides real-time monitoring for detecting potential security threats. Automated alerts notify security personnel of abnormal activities, and incident response procedures are in place to enable rapid action in the event of a breach. Regular audits ensure that BGUC maintains compliance with regulatory requirements while mitigating the risk of unauthorized access or data breaches.

Security Mechanisms

To protect BGUC's infrastructure and ensure the privacy of sensitive data, a comprehensive set of security mechanisms will be implemented. These include encryption techniques like BitLocker for device protection and AES-256 for securing data, both at rest and in transit. Secure communication is ensured through SSL/TLS protocols, safeguarding interactions between internal and external systems. User identities are managed through Azure Active Directory (AAD), which supports Single Sign-On (SSO) and Role-Based Access Control (RBAC) to enforce secure authentication (Neso Academy, 2021). Additionally, digital signatures verify the authenticity of critical data, such as medical records or prescriptions, and prevent tampering with them. Endpoint protection tools, such as CrowdStrike, safeguard against malware, viruses, and unauthorized access to systems and data. Secure remote access is provided via VPNs, and Privileged Access Management (PAM) governs users with elevated permissions to reduce the risk of misuse. These mechanisms work together to maintain a secure, seamless, and compliant infrastructure for BGUC.

Users, Applications, and User Interface

BGUC's system is designed with multiple user types in mind, including healthcare staff (doctors, nurses, administrative personnel), billing departments, vendors, and patients. Each user group has tailored access to specific data and functions based on their role, ensuring secure interactions and minimal risk of data exposure. Applications such as Electronic Medical Records (EMR/EHR), appointment scheduling tools, and Microsoft 365 will be used across the organization. The user interface is optimized for usability, featuring intuitive, role-based dashboards that display only the relevant information to each user. For example, medical staff will access patient health records and appointments, while billing staff will interact with payment

and insurance data. Multi-factor authentication (MFA) and role-based access control (RBAC) ensure that only authorized individuals can access sensitive data, minimizing the risk of unauthorized access (Codecademy, 2022). These security measures, combined with user-friendly interfaces, enhance system usability, reduce the burden on users, and ensure strong data protection.

Platform and Network Infrastructure

BGUC's platform and network infrastructure will rely on a hybrid cloud model using Microsoft Azure for scalable storage and computing resources. This approach enables BGUC to leverage the flexibility and cost efficiency of cloud services while integrating with legacy on-premises systems for critical functions. The infrastructure includes secure Local Area Networks (LANs) and Wide Area Networks (WANs), protected by firewalls, Intrusion Detection Systems (IDSs), and Intrusion Prevention Systems (IPSs) (Messer, 2015). Network segmentation ensures that sensitive data, such as patient records, is isolated from less critical systems, reducing the risk of widespread damage in the event of a breach. Communications with external partners, such as pharmacies or insurance providers, will be secured using SSL/TLS encryption to maintain confidentiality. Secure API communication will enable BGUC to seamlessly exchange data with third-party vendors while maintaining strict security controls. Real-time monitoring through a SIEM system tracks all network and system activities, ensuring that potential security incidents are detected and addressed promptly. This platform is designed to be both secure and scalable, supporting BGUC's growing needs.

Control Structure Execution

BGUC's control structure ensures that operations run smoothly and securely by implementing transparent time management processes and sequences. To prevent unauthorized access, sessions will automatically expire after a period of inactivity. Vendor access will be tightly controlled, with time-limited sessions to restrict their access to BGUC systems. Scheduled backups of critical systems and data will occur regularly to ensure that information is protected and can be quickly restored in the event of data loss or system failure. BGUC will also implement automated updates using Microsoft Intune, ensuring that all software patches and security updates are applied promptly without disrupting ongoing operations. Security events will be monitored in real-time, and automated alerts will notify security personnel of suspicious activity, enabling them to respond quickly to threats (Kalodikis, 2022). All user and vendor activities will be logged for audit purposes, supporting BGUC's compliance requirements and ensuring transparency in system access. This structure allows BGUC to maintain operational continuity while ensuring robust data protection and swift incident response.

References:

Center for Internet Security (CIS). (2021). CIS Controls v8. https://www.cisecurity.org/controls/cis-controls-list

Christopher Kalodikis. 2022. Control Structures: Sequence, Selection, and Iteration Explained. https://www.youtube.com/watch?v=Yw2Rxa6gfVg

Codecademy (2022). What Is User Interface (UI)? What is User Interf https://www.youtube.com/watch?v=Z-BO6IYTgJgace (UI)?

National Institute of Standards and Technology (NIST). (2018). Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1) https://www.nist.gov/cyberframework

National Institute of Standards and Technology (NIST). 2020. Security and Privacy Controls for Information Systems and Organizations (SP 800-53 Rev. 5) https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5-draft.pdf

Neso Academy (2021). Security Mechanisms. https://www.youtube.com/watch?v=H5ifNVeDXkg

OpenAI. (2024). *ChatGPT (Mar 14 version)* [Large language model]. https://chat.openai.com/

Professor Messer. (2015). Network Infrastructures - CompTIA Network+ N10-006 - 1.7. https://www.youtube.com/watch?v=rM0jJm0pEDc

Sherwood, C., & Lynas (2005). *Enterprise Security Architecture: A Business-Driven Approach* (1st edition). CRC Press.

Synopetk. (2024). *How can Microsoft Intune help in staying HIPAA compliant?* https://www.synopetk.com/insights/its-blogs/it-outsourcing/how-can-microsoft-intune-help-in-staying-hipaa-compliant/

The Data Guy. 2023. What is Data Modelling? Beginner's Guide to Data Models and Data Modelling. https://www.youtube.com/watch?v=CUR6rKrIEGc&t=533s

U.S Department of Health and Human Services. (2018). Health industry cybersecurity practices: Managing threats and protecting patients (HICP) Technical Volume 1. https://405d.hhs.gov/Documents/tech-vol1-508.pdf