XYX Healthcare

Business Continuity Plan Proposal

for XYZ Healthcare Leadership

Strategic Communication & Information Design
Business Continuity Planning: Translating Risk into Action
Case Study Focus:
Strategic Communication • Information Design • Business Continuity • Stakeholder Communication • Risk Communication
Portfolio Case Study

Overview of Threat

Cyber Security Threats to Healthcare in 2022 …

- Over 600 healthcare data breaches were reported, the 11 largest breaches of 2022 affected more than 21.5 million people
- Average healthcare breach costs more than $10 Million
- About 159 million patients had sensitive information like Social Security numbers or credit card numbers compromised in a hospital data breach in the past 10 years (Witts, 2023)
- The Federal Trade Commission received 27,821 reports of medical identity theft (Andrews, 2023)

What is Medical Identity Theft?

Medical identity theft is when someone steals or uses your personal information (like your name, Social Security number, or Medicare number), to submit fraudulent claims to Medicare and other health insurers without your authorization.

This may disrupt a person's ability to receive medical care, and wastes taxpayer dollars (Frankenfield, 2022).

Overview of Threat

What is XYZ Doing to Prevent this?

- Evaluating all hospital systems for potential threat and building extra protection for our systems and devices
- Creating secure practices and training staff
- Controlling access to private data (DHHS, n.d.)

What is Covered in This Presentation?

- Overview of XYZ's:
  - Risk Assessment
  - Risk Management Process
  - Business Continuity Plan
    - Review of roles and responsibilities of individuals identified in the plan

XYZ's Risk Assessment

XYX Healthcare

Security risk assessment refers to an evaluation of the potential threats to sensitive information and systems including Protected Health Information (PHI).

This includes an evaluation of likely risks and vulnerabilities to the confidentiality, integrity, and availability of sensitive information and systems.

Additionally, this assesses our ability to prevent, detect, and respond to cyberattacks (Attaway, 2021).

Our Risk Assessment Addresses the Following Areas:

1. **Sensitive information discovery**: identifying private patient information and other sensitive information (e.g., PHI, credit card data, intellectual property, financial information)
2. **Threats actors**: identifying potential "bad actors" who may be likely to access or try to steal our data
3. **Threat vectors**: ascertaining likely security threats and pathways for how they could happen
4. **Vulnerabilities**: looking at our systems and those who use them to see how exposed are we and establish what weaknesses or security holes exist in our environment
5. **Impact analysis**: analyzing our systems, and predicting if a breach happened, what would the outcomes be and possible results
6. **Risk determination**: what are the most pressing areas we need to address, and prioritizing the work needed to stay safe
7. **Corrective action planning**: identifying ways to fix issues found and implement safeguards for our systems (Attaway, 2021)

XYZ's Risk Management Process

XYX Healthcare

Risk management is an ongoing process of identifying, analyzing, evaluating, and addressing XYZ's cybersecurity threats – particularly those identified in our risk assessment process.

This practice aims to protect XYX's critical IT assets from cybersecurity threats and malicious acts and establish pathways to keep our patient data safe and maintain our ability to serve our patients and community (Knowles, 2023).

Our Risk Management Addresses the Following Areas:

- Development of strong policies and procedures
- Identification of emergent risks and threats
- Compliance with regulations and standards
- Investigate possible internal weaknesses such as lack of two-factor authentication
- Testing of the overall security in systems
- Delivery of training programs or new policies and internal controls to ensure security
- Documentation of vendor risk management and security for regulatory examinations or to appease prospective customers (Knowles, 2023)

XYZ's Business Continuity Plan

XYX Healthcare

Business Continuity Planning (BCP) adds resiliency to XYZ Healthcare operations by identifying essential functions needed to deliver patient care.

The plan helps us to know how to prepare for continuity of operations in the event of a disaster.

The BCP develops strategies to protect health care information systems, and by identifies other key factors needed to support recovery following an incident (Shulmistra, 2023).

Our BCP Addresses the Following Areas:

- Checklists that includes supplies and equipment, data backups and backup site locations
- Identification of plan administrators and contact information for emergency responders, key personnel and backup site providers at XYZ
- Detailed procedures establishing how business operations will be maintained for both short-term and long-term outages of system which support patient care and hospital activity
- Pathways to reestablish productivity and regain ability to use systems to support patient care in the event of an emergency (Shulmistra, 2023)

BCP Roles and Responsibilities

XYX Healthcare

Role	Responsibility
Executive Sponsor	Facilitates risk assessment to support program development and decides levels of mitigation or acceptance of risks associated with BCP.
Risk Committee	Oversees development and monitors implantation of BCP and associated policies and procedures required under BCP – ensures execution of BCP.
Program Manager	Develops, coordinates, and implements the enterprise-wide business continuity plan; prepares associated long-range plans, defines objectives, and prepares a forecast of financial needs and related budget; assists with regular updates of business impact analyses, risk assessments, and recovery point and recovery time.
Crisis Management Team	Ensures BCP is in sync with emerging and relevant external trends or threats to XYZ's systems; prepares XYZ to continue in the event of a crisis.
IT and Infrastructure Recovery Teams	Planning, implementing, maintaining, and auditing/testing of systems against the BCP and XYZ policies/procedures
HR & Communication Teams	Ensuring communication of plans and maintaining clear channels of communication for staff, patients, and community in the event of a disaster situation

(Strawser, 2021)

Conclusion

XYZs Ability to Fight Against Medical Identity Theft

XYX Healthcare

XYZ is ready to treat our patients, bring them back to health, regardless of the situation or potential crisis.

We have established measures and pathways to keep our hospital running, even in times of emergency or cyber threat.

We have considered all threats against our hospital, the systems we use, and are doing our best to keep your information private and confidential.

We Pledge Our Best to Ensure Our Patients:

- Medical Care is Available, Regardless of Normal Times or Crisis Situations
- Limited Exposure of Records and Keeping Them Away from Criminals
- Protection from Fraud and Cyber Threat (Insurance, Medical, Credit)
- Communication to keep hospital staff, patients, and community advised of threats and XYZ actions and safety plans
  - In the event of a breach, plans to stop the event, limit affects of breach, and remediate problems will be communicated

Resources

Andrews, M. (2023, July 26). Someone could steal your medical records and Bill You for their care. NPR. https://www.npr.org/sections/health-shots/2023/07/26/1189831369/medical-identity-fraud-protect-yourself#:~:text=Compared%20with%20other%20types%20of,accounts%20totaled%20more%20than%20400%2C000.

Attaway, S. (2021, November 16). Healthcare Security Risk Assessment & HIPAA Security Risk Analysis Faqs. Meditology Services. https://www.meditologyservices.com/healthcare-security-risk-assessment-hipaa-security-risk-analysis-faqs/

Department of Health and Human Services. (n.d.). *Top 10 tips for Cybersecurity in health care - onc*. healthit.gov. https://www.healthit.gov/sites/default/files/Top_10_Tips_for_Cybersecurity.pdf

Frankenfield, J. (2022, July 8). *Medical Identity Theft*. Investopedia. https://www.investopedia.com/terms/m/medical-identity-theft.asp

Knowles, M. (2023, March 1). Cybersecurity Risk Management: Frameworks, plans, & best practices. Hyperproof. https://hyperproof.io/resource/cybersecurity-risk-management-process/#:~:text=What%20is%20Cybersecurity%20Risk%20Management,has%20a%20role%20to%20play.

Shulmistra, D. (2023, June 16). The urgent need for business continuity planning in healthcare. Invenio IT. https://invenioit.com/continuity/healthcare-business-continuity-planning/

Strawser, B. (2022, August 11). Business continuity program roles & responsibilities. Bryghtpath. https://bryghtpath.com/business-continuity-program-roles-responsibilities/

Witts, J. (2023, March 28). Healthcare Cyber Attack Statistics 2022: 25 alarming data breaches you should know. Expert Insights. https://expertinsights.com/insights/healthcare-cyber-attack-statistics/