clearstep

10 Practices for a Resilient Defense Against Cybersecurity Attacks

While cybersecurity within the healthcare industry has always been crucial, the recent Change Healthcare ransomware attacks served as a reminder of the devastating and lasting effects of security breaches.

Impacted organizations have and continue to experience service and financial disruptions, illustrating the profound impact of these attacks on operational stability and patient care.

As a digital health company specializing in AI assistants for self-triage and healthcare navigation, we know that establishing and maintaining the highest data protection standards is not just a priority but a necessity to safeguard data, ensure compliance with regulations, and maintain trust with clients and patients.

In achieving this, it's first crucial to differentiate between various security domains: infrastructure security, organizational security, product security, and internal security procedures. Each plays a distinct yet interconnected role in ensuring comprehensive protection against cyber threats.

Infrastructure Security

Infrastructure security focuses on the physical and virtual components that support an organization's IT environment, including servers, data centers, network systems, and other essential operational elements.

KEY ASPECTS:

- **Physical security:** Ensuring that data centers and server rooms are secure from unauthorized physical access through measures such as surveillance, access controls, and environmental protection.
- **Network security:** Protecting the data as it travels across networks, including firewalls, intrusion detection/prevention systems (IDS/IPS), and secure communication protocols (e.g., VPNs, TLS).
- **Cloud security:** Securing data stored and processed in cloud environments using robust encryption, access controls, and compliance with industry standards. for each hospital/system were counted individually.

EXAMPLE PRACTICES:

- Implementing strict access controls and surveillance for data centers.
- Utilizing robust firewalls and IDS/IPS systems to monitor network traffic.
- Ensuring that cloud service providers comply with security certifications and standards.
- Revoking access for terminated employees.

Organizational Security

Organizational security encompasses the policies, procedures, and practices designed to protect the entire organization from cyber threats. It addresses the human and procedural aspects of security and focuses on employees and management.

KEY ASPECTS:

- **Security policies:** Developing and enforcing comprehensive security policies and procedures that guide the organization's approach to data protection.
- **Training and awareness:** Regularly training employees on security best practices, potential threats, and the importance of following security protocols.
- **Incident response:** Establishing and maintaining a clear incident response plan to quickly address and mitigate the impact of security incidents.

EXAMPLE PRACTICES:

- Regularly updating and communicating security policies to all employees.
- Conducting frequent security training sessions and awareness programs.
- Implementing a robust incident response plan with clearly defined roles and responsibilities.

Product Security

Product security refers to the measures taken to ensure that the software and hardware products developed and provided by the organization are secure from vulnerabilities and threats.

This is especially critical when implementing and maintaining AI-driven technologies, as these systems often handle vast amounts of sensitive data and make autonomous decisions that can impact patient care.

KEY ASPECTS:

- **Secure development lifecycle (SDLC):** Integrating security practices into every development lifecycle phase, from design to deployment.
- **Vulnerability management:** Continuously identifying, assessing, and mitigating vulnerabilities in products.
- **Third-party security:** Ensuring that any third-party components or services used within the products meet the organization's security standards.

EXAMPLE PRACTICES:

- Conducting regular security reviews and testing throughout the development process.
- Implementing a comprehensive vulnerability management program to address identified issues.
- Vetting third-party vendors and services for security compliance and reliability.

Internal Security Procedures

Internal security procedures are the specific processes and protocols followed within the organization to maintain security. These procedures ensure that internal operations and activities adhere to established security standards and practices.

KEY ASPECTS:

- **Access control procedures:** Defining and enforcing who has access to what information and systems and under what circumstances.
- **Data handling procedures:** Establishing clear guidelines for how data is collected, processed, stored, and disposed of.
- **Audit and monitoring:** Regularly auditing internal processes and monitoring systems for compliance with security policies and any signs of security breaches.

EXAMPLE PRACTICES:

- Implementing strict access control mechanisms to ensure only authorized personnel can access sensitive data.
- Establishing procedures for secure data handling, including encryption and secure data disposal.
- Conducting regular audits and continuous monitoring of internal systems and processes to detect and respond to anomalies.

10 Key Cybersecurity Practices

The following cybersecurity practices form the foundation of a resilient defense strategy and are essential for protecting sensitive data and ensuring the stability of healthcare operations.

1 Data encryption

Data encryption protects sensitive information both at rest and in transit. It converts data into a code that can only be deciphered with a key, ensuring that even if data is intercepted, it remains unreadable to unauthorized parties.

BEST PRACTICES:

- **End-to-end encryption:** Implement end-to-end encryption to protect data from the moment it is captured until it reaches its intended recipient.
- **Advanced encryption standards (AES):** Use AES-256 or higher to ensure the highest level of security.
- **Encryption key management:** Employ secure key management practices to prevent unauthorized access to encryption keys.

2 Secure data storage

Properly securing data storage systems is critical to preventing unauthorized access and data breaches.

BEST PRACTICES:

- **Cloud security:** Use reputable cloud service providers that offer robust security measures, including encryption, access controls, and regular security audits.
- **Data segmentation:** Segment data based on sensitivity and apply appropriate security controls to each segment.
- **Redundancy and backups:** Regularly back up data and implement redundancy measures to ensure data integrity and availability in case of an incident.

3 Access Controls

Limiting access to data to only those who need it reduces the risk of unauthorized access and data breaches.

BEST PRACTICES:

- **Role-based access control (RBAC):** Implement RBAC to ensure users have access only to the data and systems necessary for their roles.
- **Multi-factor authentication (MFA):** To add an extra layer of security, require MFA for accessing sensitive systems and data.
- **Regular audits:** Conduct regular audits of access logs to detect and respond to unauthorized access attempts promptly.

4 Routine Security Audits and Vulnerability Assessments

Routine security audits and vulnerability assessments help identify and mitigate potential security weaknesses.

BEST PRACTICES:

- **Penetration testing:** Conduct regular penetration testing to identify vulnerabilities that attackers could exploit.
- **Continuous monitoring:** Implement continuous monitoring of systems and networks to detect and respond to threats in real-time.
- **Compliance audits:** Regularly audit compliance with relevant regulations and standards, such as HIPAA, GDPR, and HITECH.

5 Employee Training and Awareness

Human error is a significant factor in many cyber incidents, highlighting the need for consistent and thorough employee education.

BEST PRACTICES:

- **Security awareness training:** Provide regular training on cyber security best practices, including phishing detection, password management, and data handling.
- **Phishing simulations:** Conduct regular phishing simulations to test and improve employees' ability to recognize and respond to phishing attempts.
- **Incident response training:** Ensure all employees understand the incident response procedures and their roles in the event of a security incident.

6 Incident Response and Management

A well-defined incident response plan is essential for minimizing the impact of a security breach.

BEST PRACTICES:

- **Incident response plan:** Develop and regularly update an incident response plan that outlines the steps to take in the event of a security breach.
- **Response team:** Establish a dedicated incident response team with clearly defined roles and responsibilities.
- **Post-incident review:** Conduct post-incident reviews to identify lessons learned and improve future response efforts.

7 Compliance with Regulations and Standards

Compliance with industry regulations and standards is not only a legal requirement but also a critical component of a robust cybersecurity strategy.

Regulations such as the Health Insurance Portability and Accountability Act (HIPAA) and the General Data Protection Regulation (GDPR) set stringent requirements for the protection of health data.

BEST PRACTICES:

- **HIPAA compliance:** Ensure that all systems and processes comply with HIPAA requirements, including data encryption, access controls, and regular risk assessments.
- **GDPR compliance:** Organizations operating in or handling data from the European Union must ensure compliance with GDPR requirements, including data protection by design and default, data subject rights, and breach notification.
- **Regular audits:** Conduct regular audits to ensure ongoing compliance with relevant regulations and standards.

8 Leveraging Advanced Technologies for Enhanced Security

AI-driven technologies can also play a role in enhancing cyber security measures.

BEST PRACTICES:

- **AI for threat detection:** Utilize AI and machine learning algorithms to detect and respond to cyber threats in real-time. These technologies can analyze large volumes of data to identify patterns indicative of a security breach.
- **Automated incident response:** Implement automated incident response solutions that can quickly contain and mitigate the impact of a security incident.
- **Behavioral analytics:** Use behavioral analytics to detect unusual user activity that may indicate a compromised account or insider threat.

9 Enhanced Data Protection and Privacy Controls

In addition to the general best practices, implementing specific data protection and privacy controls can further enhance security.

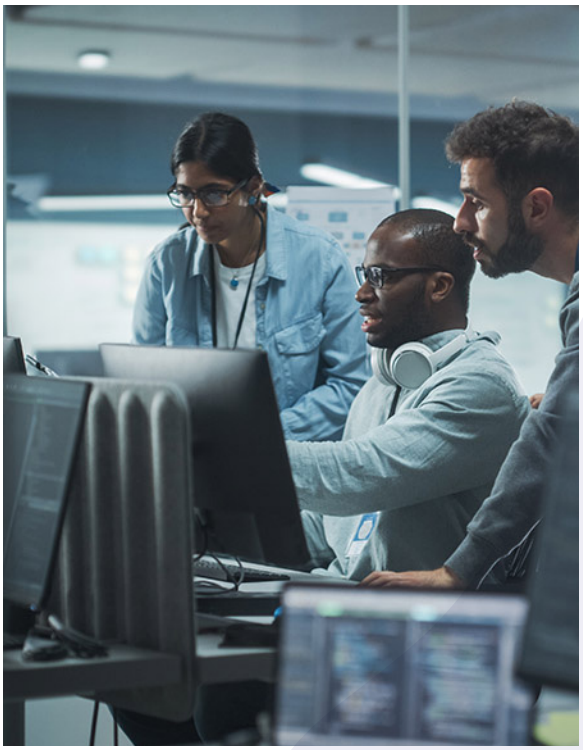
BEST PRACTICES:

- **Data anonymization:** Apply data anonymization techniques to ensure that individuals cannot be identified from stored data, reducing the risk of exposure in case of a breach.
- **Data minimization:** Collect and retain only the minimum necessary data to achieve business objectives, thereby reducing the amount of sensitive information at risk.
- **Data retention policies:** Establish and enforce data retention policies that dictate how long data is stored and when it should be securely deleted.
- **Access transparency:** Implement access transparency tools that allow individuals to see who has accessed their data and for what purpose, enhancing trust and accountability.

10

Transparency and Accountability

Maintaining transparency and accountability in data handling practices is crucial for building and maintaining trust with clients and patients.



BEST PRACTICES:

- **Regular transparency reports:** Publish regular transparency reports that detail data access and usage practices, security incidents, and measures taken to protect data.
- **Third-party audits:** Engage independent third parties to conduct security and privacy audits, which will objectively assess the organization's security posture.
- **Data breach notification:** Implement clear and timely data breach notification procedures to inform affected parties promptly in the event of a breach.

Clearstep prioritizes protecting sensitive data and regulatory compliance within our automated self-triage technology to maintain the trust and safety of our clients and their patients.

Our comprehensive approach ensures reduced risks and enhanced benefits of secure AI-driven technologies so you can focus on delivering outstanding care while ensuring the highest standards of data protection.

For more detailed information on our specific security measures and controls, please visit the Clearstep Health Security and Clearstep Health Trust Center pages.

You can also connect with us at info@clearstep.health or www.clearstep.health for more information.

clearstep

www.clearstep.health