Can Your Hospital Withstand a Cyberattack?

How to Prevent and Respond to Cybersecurity Incidents
ABSTRACT

The healthcare industry is a top target for cyberattacks in general and ransomware in particular.

According to the IBM Security/Ponemon Institute 2019 Cost of Data Breach Report, the healthcare industry suffered the greatest annual cost of data breaches—$6.45 million compared to the average total cost of $3.92 million across industries.

As the value of protected personal health information increases and new cyberattack mechanisms emerge, cybersecurity has become an important topic for healthcare providers in urban and rural settings.

This white paper discusses ways for community hospitals to protect against ransomware and other cyberattacks and how to respond to a security incident.

INTRODUCTION

Patient data is valuable to steal or ransom. On the dark web, it is generally worth more than credit card numbers. But selling patient data is often not the intent of cybercriminals. Most use ransomware to disrupt operations—and patient care—to coerce healthcare providers to pay a ransom to regain access to their files. Because disruption to patient care can potentially cost lives, the perception is that healthcare providers will be more likely to pay a ransom to recover their files.

Embracing new technologies advances operational efficiencies and patient care, but it also broadens the cybersecurity threat landscape and creates more potential attack vectors and opportunities for human error. Web application attacks are on the rise as more healthcare providers connect medical devices to the internet, open patient portals, deploy telemedicine, and implement remote patient monitoring.

Because cyberattacks are growing threats to large and small healthcare providers, community hospital executives must stop thinking about cybersecurity as an IT issue. Instead, cyberthreats should be regarded as an organizational risk with patient care quality at stake.
Cybersecurity Statistics

82% About 82 percent of hospital IT security leaders reported having a significant security incident in the past 12 months, according to a 2019 survey by Healthcare Information and Management Systems Society.

88% A majority—88 percent—of cybersecurity breaches in the healthcare industry are financially motivated, according to Verizon.

70% In healthcare, ransomware accounts for more than 70 percent of malware infections, Verizon reported.

279 days The IBM/Ponemon study found that it takes an average of 279 days, across all industries, to contain a cyberattack.

Important Terms to Know: Security Incident vs. Breach

Personal information is protected by various industry-specific federal laws and state legislation. With regard to HIPAA, “breach” has a specific meaning and its occurrence triggers certain actions. A “security incident” is a broader term encompassing many types of events. All data breaches are security incidents, but not all security incidents are data breaches.

Security incident: Attempted or successful unauthorized access, use, disclosure, modification or destruction of data, or interference with an information system’s operations.

Security breach (or data breach): A type of security incident resulting in the unauthorized acquisition, access, use or disclosure of protected information such as personally identifiable information (PII) or protected health information (PHI). Breaches require notification of affected parties, regulatory agencies and, under certain circumstances, the media and law enforcement. Consult applicable state and federal data breach notification laws, including the HIPAA Breach Notification Rule, for notification requirements.

Was it an Incident or Breach?

When a security incident occurs and data is compromised, it is necessary to conduct a multifactor risk assessment to determine whether it qualifies as a breach, based on the legal definitions and these four factors:

- The type, identifiability and sensitivity of the information
- Who gained access to the information
- Whether the information was actually accessed or viewed
- The extent to which the risk has been mitigated

Take Action

- Update cybersecurity policies to address remote workers and telehealth activities.
- Stay on top of emerging cybersecurity threats by monitoring vulnerability alert feeds and advisory sites such as the Health Information Sharing and Analysis Center (H-ISAC), the U.S. Computer Emergency Readiness Team (US-CERT), and Infragard.

Security Breach Root Causes

- Malicious or criminal attack: 51%
- Human error: 24%
- System glitch: 25%

Source: 2019 IBM/Ponemon Cost of Data Breach Report
STRENGTHEN CYBERSECURITY IN FOUR STEPS

There is a clear need for healthcare organizations to improve their protection of health information and information systems. Rural hospitals and clinics are particularly vulnerable due to their small staff and limited financial resources.

Rural and community hospitals can prevent or mitigate the cost of cyberattacks by taking action in four areas:

1. Prepare and Protect

A well-educated workforce is the best cybersecurity protection a community hospital can have. Regular training to help staff, providers, and leadership understand the threats, how to recognize a breach attempt, and the associated risks can make a huge difference.

Take precautions and be prepared for a breach—be it accidental or the work of hackers.

- Encrypt all data in motion—data sent from one individual or device to another.
- Encrypt all data at rest: laptops, desktops, mobile devices, and servers, where possible.
- Educate employees and the board about secure computing and how to avoid being tricked by a hacker and how to report suspicious activity.
- Create an incident response team composed not just of internal IT specialists but also business stakeholders, departmental super users, and external systems/security experts.
- Create a formal (and printed) Incident Response Plan and Communication Plan.
- Ensure you have cloud and offline backups of files, applications, databases, and system and network configurations.
- Keep printed manuals with critical system and network information, including software and application inventories, server names, IP addresses, computer and printer inventories, external connections and vendors, and contact information for the incident response team.
- Patch systems regularly.
- Segment sensitive information, such as patient data, from the broader network to limit malware’s ability to spread.

Take Action

- Conduct phishing simulations and celebrate employees who report the suspicious activity.
- Activate two-factor authentication to ensure the security of online accounts beyond username and password.
- Talk to business associates about their security measures to determine whether their systems could infect your network or impact your ability to care for your patients and develop risk mitigation plans.
2. Detect Breaches Through Vigilance

It can be difficult to tell when a system has been infiltrated, so vigilance is necessary to mount a prompt and effective response.

- Leverage tools like a Security Incident Event Monitoring (SIEM) system to collect real-time data and detect network intrusions from devices across the threat landscape, including:
  - Computing devices
  - Printers
  - Wired and wireless network
  - Servers
  - Cloud infrastructure

- Practice “managed monitoring,” or regularly looking at the tool dashboards and reports. Don’t rely just on automated alerts to signal a problem.
- Conduct vulnerability scans monthly and penetration tests at least biannually.
- Monitor reports from the security team for odd or suspicious activity.
- Configure and test alerting and notification escalation.
- Develop and test a plan for alerting security and IT team members of possible attacks, including escalation plans if alerts are not responded to timely.
  - Third-party assistance for monitoring your SIEM may be a good option for smaller security and/or IT departments.

Take action

- Manage your user permissions in accordance with HIPAA’s Minimum Necessary Requirement, limiting access to protected health information only to those who need it to carry out their job duties.
- Disable user accounts immediately when people leave the organization.
- Note when attack attempts spike, as increased activity may mean hackers have detected a vulnerability and are trying to exploit it.

Signs of a Ransomware Infection

- Files won’t open or error messages say files are corrupted or have the wrong extension.
- Files appear in directories with names like DECRYPT_INSTRUCTIONS.TXT.
- A window has opened to a ransomware program, and it cannot be closed.
- Instructions appear as the computer’s desktop background on how to pay to unlock files.
- A countdown begins to the deadline to pay the ransom before it increases or files are irretrievably lost.
- Servers, desktops, laptops, and mobile devices will not boot or boot to an error screen.
- Portions of critical applications suddenly become inaccessible or return errors.
3. Respond According to Protocol

Responding promptly and effectively to security incidents is critical. Having an incident response plan in place ensures a consistent incident-handling methodology so appropriate actions are taken, damage is minimized, and legal and regulatory issues are addressed.

- Disconnect network and subnet internet circuits.
- Power down servers and any machines suspected of infection.
- Move the organization to disaster or downtime procedures.
- Contact external support teams and ask for assistance.
- Activate the facility’s Incident Response Plan.
  - Evaluate and determine the extent of the infection.
  - Develop a plan to contain the infection.
  - Evaluate backups and recovery options.
  - Evaluate connections to external businesses.
  - Perform a risk analysis to prioritize recovery efforts.
  - Determine if external reporting is required.
- Activate your Communication Plan.
  - Audiences to consider:
    - Executives
    - Board
    - Staff
    - Business Associates
    - Legal Counsel
    - Insurance Carrier
    - Community
    - Media

Take Action

- Test your incident response plan annually by leveraging a desktop simulation of a ransom event.
- Maintain a list of where critical business data is stored beyond just production applications and servers.
- When necessary, maintain a statement and FAQ of the current status of the incident so that communications with the media are consistent and up to date.

Sharing Information with Outside Parties

Security breaches trigger notification requirements or courtesies. Depending on the type and severity of the incident, outside communications may include:

- Seeking external expertise
- Advising regulatory agencies
- Contacting law enforcement
- Informing the media and fielding media inquiries
- Discussing incidents with other involved parties, such as internet service providers or the vendor of vulnerable software
- Sharing relevant incident indicator information with peers to improve detection and analysis of incidents

The incident response team should have a formal Communication Plan in place with input from the public affairs office, the legal department and management. The team should document all contacts and communications with outside parties for liability and evidentiary purposes.

Source: “Computer Security Incident Handling Guide” by the National Institute of Standards and Technology
4. Learn from the Event
The U.S. Department of Commerce’s National Institute of Standards and Technology recommends that organizations hold a “lessons learned” meeting after handling a major security incident.
  • After a security incident, conduct a root cause analysis.
  • Review the effectiveness of the incident response plan, and evaluate what worked and what needs to be corrected, improved or updated.
    – Assess your people, processes, and technology
  • Be transparent with the internal team, and discuss findings with the board.
  • Update documentation, processes, technology, and employee education based on what you learn.

To Pay or Not to Pay
The FBI does not advocate paying a ransom; but in 2019 the agency softened its stance, acknowledging in a public service announcement that “when businesses are faced with an inability to function, executives will evaluate all options.”

In absence of a complete and accurate data backup, healthcare leaders sometimes feel that paying the ransom is their only recourse. In some cases, the cost of recovery and downtime exceed the ransom, so hospitals pay up. The hackers will provide payment instructions and, typically, a countdown timer.

Usually, hackers demand some form of cryptocurrency, such as Bitcoin, in exchange for decryption software or decryption keys. The FBI warns that in some cases victims who paid a ransom were never provided with decryption keys. In addition, due to flaws in the encryption algorithms of certain malware variants, victims may not be able to recover some or all of their data even with a valid decryption key.

Take Action

- Consider the benefits of cyber liability insurance.
- Talk to the board about defining cybersecurity as an organizational risk, not an “IT issue,” and encouraging a shared responsibility for security.
CONCLUSION

The expanding cybersecurity threat landscape puts rural and community healthcare organizations at greater risk of cyberattacks or security incidents that originate internally (usually inadvertently, through poor cyber hygiene). Organizations must vigilantly monitor their information system and be ready to respond to security incidents and data breaches. Developing cybersecurity policies and procedures, as well as a formal Incident Response Plan, helps these healthcare organizations identify these incidents and minimize the damage, as well as prevent incidents in the first place.

Cybersecurity Services

CHC Consulting specializes in providing comprehensive IT services for community and rural hospitals. Our expertise includes network security management and evaluation. CHC also conducts external security audits and risk assessments, provides monitoring services, helps providers mend any security gaps, and strengthens overall preparedness and response readiness.

Take the Next Step

Learn more about CHC Information Technology Services at: https://communityhospitalcorp.com/services/operational-improvement/information-technology/

www.communityhospitalcorp.com
7800 N. Dallas Parkway, Suite 200
Plano, TX 75024
Phone: 972.943.6400
Fax: 972.943.6401

Community Hospital Corporation owns, manages and consults with hospitals through CHC Hospitals, CHC Consulting and CHC ContinueCARE, with the common purpose to guide, support and enhance the mission of community hospitals and healthcare providers. Based in Plano, Texas, CHC provides the resources and experience community hospitals need to improve quality outcomes, patient satisfaction and financial performance. For more information about CHC, please visit www.communityhospitalcorp.com.