Cybersecurity in Healthcare

Risk Solutions and Strategies

MedPro Group
a Berkshire Hathaway company

Speaker bio

Richard A. Bryan, MSN, RN, CPHRM, Senior Patient Safety & Risk Consultant, MedPro Group (Richard.Bryan@medpro.com)

Richard has more than 30 years of experience in healthcare, including military, not-for-profit, and teaching facilities as well as the private sector. He has served in progressive leadership roles in nursing management, risk management, and insurance.

Most recently, Richard held an executive leadership role in a healthcare system with 1 hospital and 28 primary care/multi-specialty clinics. During his tenure, his areas of responsibility included risk management, patient safety, insurance, compliance, regulatory readiness, quality, care management, population health and clinical integration, clinical operations of behavioral health and women's and children's services, Epic implementation, and ongoing operations team and information services.

Richard earned a bachelor of science degree in nursing from Union University and a master of science degree in nursing with a major in healthcare systems management from Loyola University New Orleans.

Richard is a member of the American Society for Health Care Risk Management, the Washington Healthcare Risk Management Society, the American College of Healthcare Executives, and the American Organization of Nurse Executives. He is also a certified professional in healthcare risk management.

Designation of continuing education credit

MedPro Group is accredited by the Accreditation Council for Continuing Medical Education (ACCME) to provide continuing medical education for physicians.

MedPro Group designates this enduring activity for a maximum of 1.0 *AMA PRA Category 1 Credits*™. Physicians should claim only the credit commensurate with the extent of their participation in the activity.

MedPro Group
Nationally Approved PACE Program
Provider for FAGD/MAGD credit.
Approval does not imply acceptance by
any regulatory authority or AGD endorsement.
October 1, 2018 to September 30, 2022
Provider ID# 218784

MedPro Group designates this continuing dental education activity as meeting the criteria for up to 1 hour of continuing education credit. Doctors should claim only those hours actually spent in the activity.

Disclosure

MedPro Group receives no commercial support from any ineligible company/ commercial interest.

It is the policy of MedPro Group to require that all parties in a position to influence the content of this activity disclose the existence of any relevant financial relationship with any ineligible company/commercial interest.

When there are relevant financial relationships mitigation steps are taken. Additionally, the individual(s) will be listed by name, along with the name of the commercial interest with which the person has a relationship and the nature of the relationship.

Today's faculty, as well as CE planners, content developers, reviewers, editors, and Patient Safety & Risk Solutions staff at MedPro Group have reported that they have no relevant financial relationships with any commercial interests.

Objectives

At the conclusion of this program, participants should be able to:

- Identify strategies on how to reduce the likelihood of a cyber attack
- Learn how to respond should your practice or facility become a victim of a cyber attack
- Understand basic coverages available should a cyber event or data breach occur

Responding to the threat

What can practices and other healthcare organizations do?

It is not about how much you invest:

It is about the effectiveness of the investment.

What is your current state of readiness?

Only 20% of small practices have internal security officers so they rely on third party health IT firms for security support.

1/3 of physicians are interested in shared security management solutions.

Nearly 1 in 2 physicians wish they could receive security-related hardware or software from other provider groups.

. American Medical Association. (2018). Patient safety: The Importance of cybersecurity in health care. Retrieved from https://www.ama-assn.org/system/files/2018-10/cybersecurity-health-care-infographic.pdf

Practical guidance from the American Medical Association

- Understanding “network security”
- Connected devices = risk
- What it means to be internet connected
- Wi-Fi hotspots are vulnerable
- Use available firewalls
- Wireless access is great when secured
- Safe remote access and use of virtual private networks (VPNs)
- Securing information in modern printers and copiers
- Developing effective back-up and disaster recovery plans

American Medical Association. (2017). Protect your practice and patients from cybersecurity threats. Retrieved from https://www.ama-assn.org/sites/ama-assn.org/files/corp/media-browser/public/government/advocacy/network-security.pdf

Don’t forget one of your greatest vulnerabilities

One of the greatest threats to security are the individual users of your system.

Although they are not the last line of defense, they are the point at which data originate and risk starts.

Top 10 tips for cybersecurity in healthcare

1. Establish a security culture
2. Protect mobile devices
3. Maintain good computer habits
4. Use a firewall
5. Install and maintain anti-virus software
6. Plan for the unexpected
7. Control access to protected health information (PHI)
8. Use strong passwords and change them regularly
9. Limit network access
10. Control physical access

Top 10 tips for cybersecurity in healthcare (continued)

#1
Establish a security culture

- Education and training should occur frequently and remain ongoing.
- Individuals managing or directing others must serve as role models and resist the temptation to create exceptions to policy for themselves or others.
- The organization's core values must include accountability and individual ownership of information security.

#2
Protect mobile devices

- The thing that makes mobile devices so appealing is the very thing that also makes them a potential security threat.
- If mobile devices are deemed essential to practice, effort must be taken to protect the information contained within the device.
- Data should be encrypted and software allowing for the deletion of information in the event of theft or loss should be installed.

Top 10 tips for cybersecurity in healthcare (continued)

#3
Maintain good computer habits

- IT systems, including electronic health records (EHRs), must be maintained and regularly updated.
- Nonessential software should be uninstalled from any computer connected to your system.
- You should be aware of any IT or software vendor that maintains a “back-door” into your system.

#4
Use a firewall

- Any practice that has an EHR and electronic billing systems should have a firewall to protect against outside threats and intrusions.
- Configuring a firewall can be difficult. When in doubt, hire an IT professional.

Top 10 tips for cybersecurity in healthcare (continued)

#5
Install and maintain anti-virus software

- Aside from regular maintenance and updates of applications and operating systems, which often contain bug fixes and security updates, the use of a quality anti-virus software is mandatory.
- Once installed, anti-virus software should be regularly maintained and updated.

#6
Plan for the unexpected

- Cybersecurity efforts should not just be limited to prevention of hacking.
- A primary goal should be the ongoing operation of an organization's systems and protection against loss of the systems and the information they contain.
- System back-up is key.

Top 10 tips for cybersecurity in healthcare (continued)

#7
Control access to protected health information (PHI)

- Access control is not limited to implementation of complex passwords.
- Access to systems containing PHI or protected personal information (PPI) should be limited to only those with a need to know.
- Access should be role based to prevent the potential for inadvertent exposure to information that is not necessary for staff members' job duties.

#8
Use strong passwords and change them regularly

- Passwords are considered the first line of defense in the prevention of unauthorized access to a computer or system.
- Strong passwords make it harder for a hacker to access your systems.
- Requiring scheduled password changes also reduces the risk of automated hacking systems keying in on a password.
- Multifactor identification provides an even greater level of security.
- The emergence of biometric access control is becoming more common.

Top 10 tips for cybersecurity in healthcare (continued)

#9
Limit network access

- If using a wireless network, ensure that it is secure and access password protected.
- Wireless routers should be set up to operate only in an encrypted mode.
- Although often seen as required for patient satisfaction, avoid setting up guest access.
- Prohibit installation of software without prior approval.

#10
Control physical access

- Access to areas containing any device that contains protected health information (PHI) or other business essential software should be controlled.
- Any device that is portable or easily removable should be secured, with policies defining the management of access and removal.

Responding to a cyber attack

How do I know when I have been attacked?

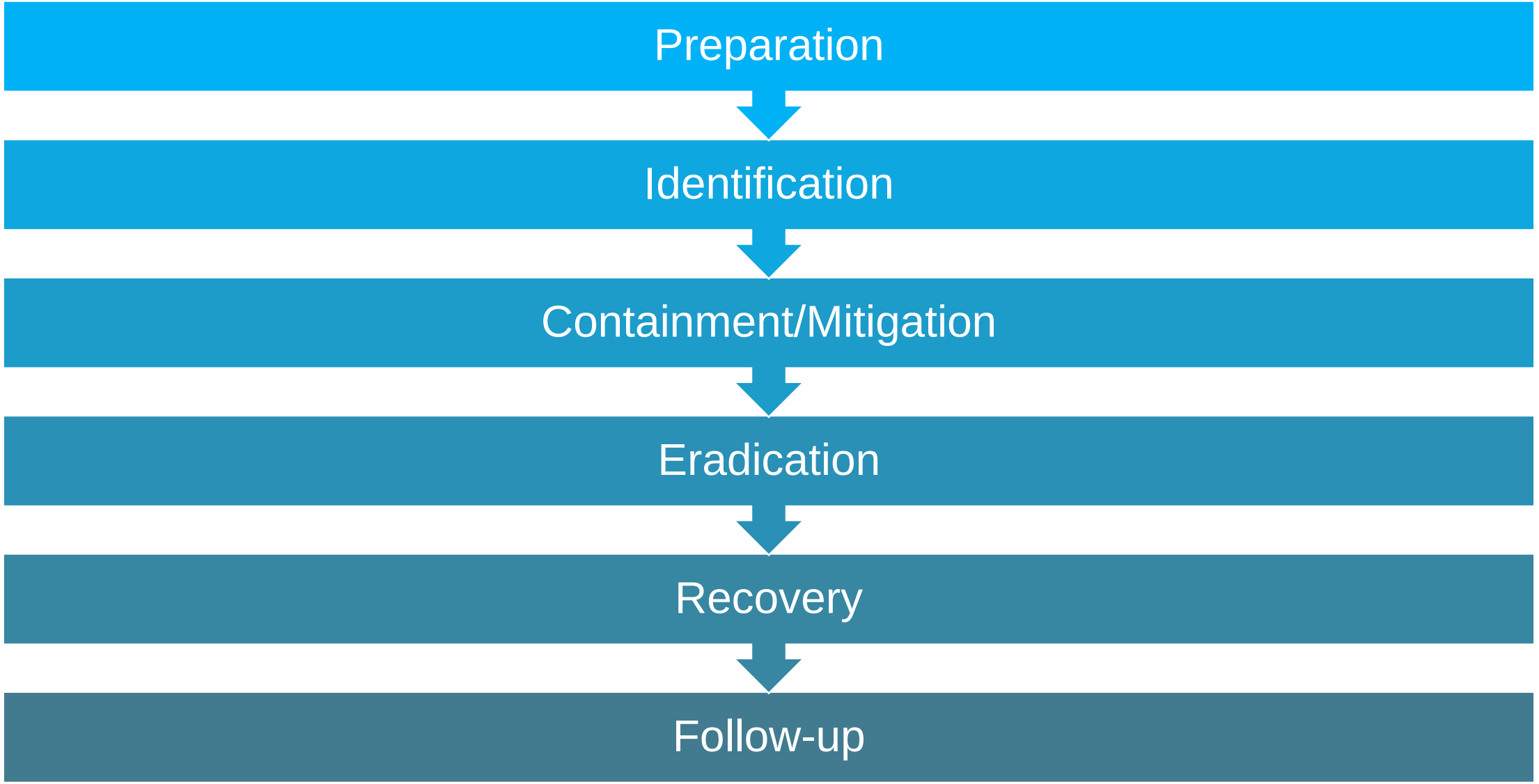
Typical symptoms of a computer virus:

- System will not start normally
- You experience repeated crashes
- Your internet browser is directed to unwanted web pages
- Anti-virus software does not appear to be working
- You start to notice increased spam
- You cannot control the mouse or pointer
- You receive a message announcing that your computer is locked and access to the data is blocked until a ransom is paid

How do I respond to a cyber attack?

- It is important that in the event of a suspected cyber attack, you also think data breach
- Immediately execute your response plan
- Report the crime to law enforcement
- Contact your insurance broker (agent) and respective insurance carriers
- Report any breach to the Department of Health and Human Services, Office for Civil Rights in accordance with HIPAA requirements

Best practices for a successful incident response plan



Sher-Jan, M. (2012, October 2). 7 best practices for a successful incident response plan. *Healthcare IT News*. Retrieved from https://www.healthcareitnews.com/news/7-best-practices-successful-incident-response-plan

Incident response plan – preparation phase

Preparation

Identification

Containment/Mitigation

Eradication

Recovery

Follow-up

- Get buy-in at the top levels of the organization.
- Define the membership of the incident response team ahead of time.
- Define the scope of the incident response team.
- Document the incident response plan (IRP).

Incident response plan – identification phase

Preparation

Identification

Containment/Mitigation

Eradication

Recovery

Follow-up

- The organization identifies the scope and severity of the incident, including source if possible.
- Using the framework of your pre-established plan, determine your response to initiate actions to implement it.

Incident response plan – containment/mitigation phase

Preparation

Identification

Containment/Mitigation

Eradication

Recovery

Follow-up

- Once the incident is identified, the organization transitions to the containment phase, taking steps to prevent further spread or damage introduced by the attacker.

Incident response plan – eradication phase

Preparation

Identification

Containment/Mitigation

Eradication

Recovery

Follow-up

- Upon containment of the incident, take steps to remove any traces of the attack from any systems that were targeted.

Incident response plan – recovery phase

Preparation

Identification

Containment/Mitigation

Eradication

Recovery

Follow-up

- Affected systems and data are verified and returned to regular service.

Incident response plan – follow-up (lessons learned) phase

Preparation

Identification

Containment/Mitigation

Eradication

Recovery

Follow-up

- Review the incident and response in its entirety to gain insight and identify opportunities for improvement. Use this information to refine the preparation phase in anticipation of future events.

Cyber and privacy coverage

What is cyber and privacy coverage?

- Cyber and privacy coverage should include third party liability coverage, first party coverage, and supplementary benefits.
- Network security/data privacy coverages are designed to provide pre- and post-breach support services as well as legal defense and indemnity, and to pay certain expenses necessary to respond to a data security breach.

Health IT Security. (2019, February 5). What is cyber insurance for healthcare organizations? Xtelligent Healthcare Media. Retrieved from https://healthitsecurity.com/features/what-is-cyber-insurance-for-healthcare-organizations

Cyber and privacy coverage examples

First party liability coverage

Offers coverage for business owners in the event that a data breach compromises sensitive customer or employee information. It applies to the direct costs for responding to a privacy breach or security failure. Any company that stores customer/patient data (in the form of records, email lists, credit card records, or other files) could be victimized by a data breach and benefit from first party cyber coverage.

- Crisis management expense: Notifying and answering questions from affected persons whose protected personal information (PPI)/protected health information (PHI) may have been lost, accessed, or stolen.
- Fraud response expense: Credit and identity monitoring services or identity theft insurance to affected qualified person(s) resulting from an unauthorized disclosure of protected information.
- Public relations expense: Hiring a public relations firm, law firm, or crisis management firm for communication services. This includes the costs of advertisements, web content, and other communications recommended by the firm.
- Forensic and legal expense: System investigation to determine the cause of an enterprise security event and identify those persons whose PPI/PHI may have been improperly accessed, lost, or stolen.

HealthIT Security. (2019, February 5). What is cyber insurance for healthcare organizations? Xtelligent Healthcare Media. Retrieved from https://healthitsecurity.com/features/what-is-cyber-insurance-for-healthcare-organizations

Cyber and privacy coverage examples (continued)

Third party liability coverage

Provides protection to insureds (even if they used a service contractor) who were responsible for the safe storage of data (e.g., those who manage a network that was breached or attacked by a phishing or pharming incident).

- Digital security event: Unauthorized access to your computer system that results in damage or alteration of data, transmitting harmful software code or denial of access.
- Privacy injury: Privacy breaches involving loss, accidental disclosure, or theft of protected information, common law invasions of privacy, and violation of privacy regulations with respect to the use or control of protected personal information (PPI) or protected health information (PHI).
- Privacy regulation liability: Violations of HIPAA or other similar state, federal, and foreign identity theft and privacy protection statutes, rules, and regulations.
- Payment card industry data security standard (PCI-DSS) claim: A written demand for monetary or nonmonetary relief brought by a credit/debit card company or credit/debit card processor seeking PCI-DSS assessments.

HealthIT Security. (2019, February 5). What is cyber insurance for healthcare organizations? Xtelligent Healthcare Media. Retrieved from https://healthitsecurity.com/features/what-is-cyber-insurance-for-healthcare-organizations

Cyber and privacy coverage examples (continued)

Supplementary benefit

- Data recovery expense: Recover and/or replace compromised, damaged, lost, altered, or corrupted data due to a third party's unwanted malicious, reckless, intentional, or negligent act.
- Computer system extortion: To commit an attack against computer hardware, software, and all components to disseminate protected data for the purpose of extorting funds.
- Breach preparedness information services: Carrier identifies pre-approved vendors to provide breach-related services to insureds, subject to the terms and conditions of the specific policy.

Summary

- Cyber events represent a frequent, serious, and costly risk in healthcare practices, facilities, and organizations.
- Identifying and better understanding the practices and vulnerabilities that contribute to cyber events and the associated operational disruption offers healthcare organizations and providers the ability to adopt the processes and practices necessary to improve cybersecurity and reduce potential exposure.
- Through gaining an understanding of the risks, providers and organizations can develop strategies and plans on what, when, and how best to respond in the event an attack occurs.

MedPro Group resources

- 10 Ways to Establish a Security Culture at Your Healthcare Organization
https://www.medpro.com/security-culture

- Cybersecurity Risk Resources List
https://www.medpro.com/documents/10502/2824311/Risk+Resources_Cybersecurity.pdf

- The Frontline: Cybersecurity Training for Healthcare Workers
https://www.medpro.com/cybersecurity-training-for-healthcare-workers

- Using Physical Safeguards to Prevent Security Breaches
https://www.medpro.com/documents/10502/3667697/Using+Physical+Safeguards+to+Prevent+Security+Breaches.pdf

- Using Technology-Based Safeguards to Prevent Security Breaches
https://www.medpro.com/documents/10502/3667697/Using+Technology-Based+Safeguards+to+Prevent+Security+Breaches.pdf

More resources are available at www.medpro.com/dynamic-risk-tools

Other valuable resources

- Department of Health & Human Services: Top 10 Tips for Cybersecurity in Health Care https://www.healthit.gov/sites/default/files/Top_10_Tips_for_Cybersecurity.pdf

- Healthcare Industry Cybersecurity Practices: Managing Threats and Protecting Patients https://www.phe.gov/Preparedness/planning/405d/Pages/hic-practices.aspx This link will take you to a web page that lists several great resources. Physician practices should click on this link Technical Volume 1: Cybersecurity Practices for Small Health Care Organizations

- American Medical Association https://www.ama-assn.org/topics/cybersecurity

- American Dental Association: It appears that ADA's cybersecurity resources are contained within the members only section. You can access the ADA, type cybersecurity in the search engine, and it will take you to publically available information or click this link https://www.ada.org/en/search-results#q=cybersecurity&t=all&sort=relevancy

Disclaimer

The information contained herein and presented by the speaker is based on sources believed to be accurate at the time they were referenced. The speaker has made a reasonable effort to ensure the accuracy of the information presented; however, no warranty or representation is made as to such accuracy. The speaker is not engaged in rendering legal or other professional services. The information contained herein does not constitute legal or medical advice and should not be construed as rules or establishing a standard of care. Because the facts applicable to your situation may vary, or the laws applicable in your jurisdiction may differ, if legal advice or other expert legal assistance is required, the services of an attorney or other competent legal professional should be sought.