When a Breach Occurs, the Whole Hospital Is Our Patient

Health care organizations are under attack. Vicious threats like ransomware can significantly disrupt or even shut down clinical and business operations at a moment's notice. While the implications of cyberattacks are often unknown to health care leaders, clinicians, and staff, they are used to handling critical incidents in patient care. Luckily, the process for handling a cyber incident is nearly the same.

This graphic details how the steps in responding to a clinical crisis mirror one of the most widely used cyber response methods, the SANS Institute's PICERL approach: preparation, identification, containment, eradication, recovery, lessons learned. By relating information security tactics to patient care, everyone can get on the same page and work together.

CLINICAL

CYBERSECURITY

Prepare

- Participate in continuing education and training programs to stay current
- Stay alert to new clinical issues in the community, such as disease outbreaks
- Conduct emergency response drills regularly to ensure adequate preparation for major incidents
- Review clinical policies and procedures often to ensure timeliness and relevancy

- Engage staff in proactive cyber awareness training
- Monitor for threats and provide early alerts to trending cyberattacks
- Conduct simulations and drills; designate Incident Response Team (IRT) members before an attack
- Review and update existing security policies regularly

Triage – Identify

- Intake and triage patient; determine severity of patient condition
- Collect vital signs, symptoms, medical history, recent activities, and other relevant information from patient or family
- React to alerts regarding significant multi-victim local events to ensure clinician readiness

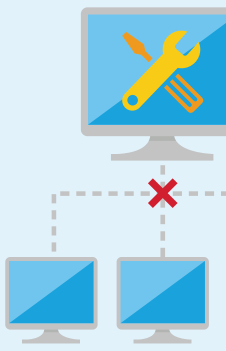
Must manage within minutes to limit damage

- Educate users on immediate steps to take after a cyberattack, such as unplugging from network
- Monitor network through intrusion detection systems, periodic log reviews, and cyber intelligence to spot suspicious activity
- Set up systems to receive notifications from user workstations in the event of a cyberattack
- Assess and determine severity of attack

Stabilize – Contain

- Administer immediate care to prevent shock; ensure heart rate, respiration, and other vital signs are stabilized; control any bleeding; immobilize fractures
- Conduct a thorough review to determine current condition

- Disconnect affected workstation, device, or server from network to prevent the spread and magnitude of damage
- Alert and activate the IRT to manage the incident
- Log details throughout incident for future review



Diagnose – Eradicate

- Run diagnostic tests to better understand patient's condition
- Diagnose patient and determine best course of treatment
- Conduct or administer any necessary procedures, surgery, treatments, and medications to improve the patient's condition

- Run diagnostic tests on affected workstation, device, or server to understand full scope of the problem
- Eliminate the threat with appropriate tools and processes for the issue: run anti-malware software, wipe and restore from backups, etc.

Treat – Recover

- Monitor patient progress to ensure effectiveness of, and adherence to, the treatment plan
- Admit or discharge to home with instructions for after-hospital care
- Document patient case details and decisions made throughout the patient's stay

- Conduct validation tests on the workstation, device, or server to confirm the threat has been eliminated
- Reconnect the workstation, device, or server to the network, monitoring for any renewed suspicious activity
- Document details and decisions made throughout the incident

Review – Learn

- Conduct informal reviews of particularly difficult cases with other physicians who may provide alternative opinions to improve patient care
- Recommend improvements to hospital policy and processes, new resources, and opportunities for clinician/staff education

- Review incident documentation, including attack vector, vulnerability exploited, and observations of malware's activity
- Recommend improvements to cybersecurity preparation efforts, including updates to security policies, technologies, and security awareness training efforts

How IT Staff Support a Healthy Cybersecurity Environment

1 Conduct security awareness training, provide regular updates on the latest phishing techniques, and encourage good cyber hygiene.

2 Ensure basic technical countermeasures are in place to defend against malicious emails and limit access to harmful websites.

3 Maintain and test backups regularly, keeping them disconnected from the network as some ransomware variants target and encrypt or destroy backups.

4 Review and adjust security policies regularly to ensure they address new and emerging threats and account for new technologies and systems within the organization.

Advisory Board | Health Care IT Advisor

Access additional resources on information security in health care
advisory.com/hcita