ECRI | The Most Trusted Voice in Healthcare

Cybersecurity Threats Disrupting Healthcare Delivery Operations

April 13, 2023

Juuso Leinonen, Principal Project Engineer, ECRI

Learning Objectives:

- Identify why healthcare facilities are being targeted by cybersecurity attacks
- Outline what makes managing cybersecurity risks particularly challenging in a healthcare setting
- Describe why cybersecurity is considered a top health technology hazard
- Identify how a cybersecurity incident can cause significant disruption to patient care operations
- Evaluate areas where implicit bias can influence cybersecurity and patient safety
- Review cybersecurity best practices when using healthcare technologies and review incident response plan essentials to minimize disruption to operations and patient care

©2023 ECRI

ECRI - The Most Trusted Voice in Healthcare

©2023 ECRI

Non-Profit Advancing Effective, Evidence-based Healthcare Globally

Technology Decision Support

- Capital, Supplies & Purchased Services Decision Support
- Healthcare Device Evaluation & Alerts
- Value Analysis Workflow
- Cybersecurity
- Medical Equipment Planning

Patient Safety

- Patient Safety Organization
- Infection Prevention
- Healthcare Risk Assessments & Management
- Safe Medication Practices
- Accident & Forensic Investigation
- Aging Services Care Delivery

Evidence-based Medicine

- Clinical Evidence Assessments
- Evidence-based Practice Center
- Emerging Technologies Profiles & Forecasts
- Genetic Test Assessments
- Horizon Scanning
- ECRI Guidelines Trust™

ECRI's Medical Device Evaluation Program > 50 Years!

Technology Decision Support

Independent Testing & Evaluation Lab

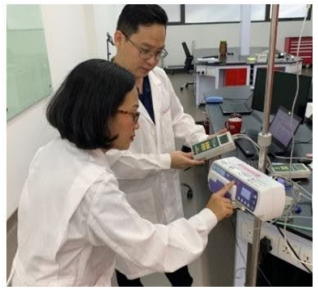
The only independent medical device testing and evaluation lab in North America and Asia Pacific

PROGRAM OBJECTIVES

To improve the **effectiveness, safety, and economy** of health services by:

- Providing independent, objective judgment for selecting, purchasing, managing, and using medical devices, equipment, and systems.
- **Functioning as an information clearinghouse for hazards and deficiencies in medical devices.**
- Encouraging the improvement of medical devices through an informed marketplace.



©2023 ECRI

Top 10 Health Technology Hazards

©2022 ECRI

Top 10 Health Technology Hazards List

- Motivation: Prevent harm by preventing hazards that have the clear potential to:
  - Cause death or serious injury
  - Adversely affect patient care
- Goal:
  - Shine a light on health technology safety issues
    - Persistent hazards / known events (e.g., problem reports)
    - Emerging issues (e.g., identified during testing or investigations)
  - **Awareness → assurance**: Create a tool healthcare professionals can use to:
    - Set patient safety priorities
    - Implement effective changes
- Key features:
  - **Predictive**, not retrospective
  - Step by step recommendations for action

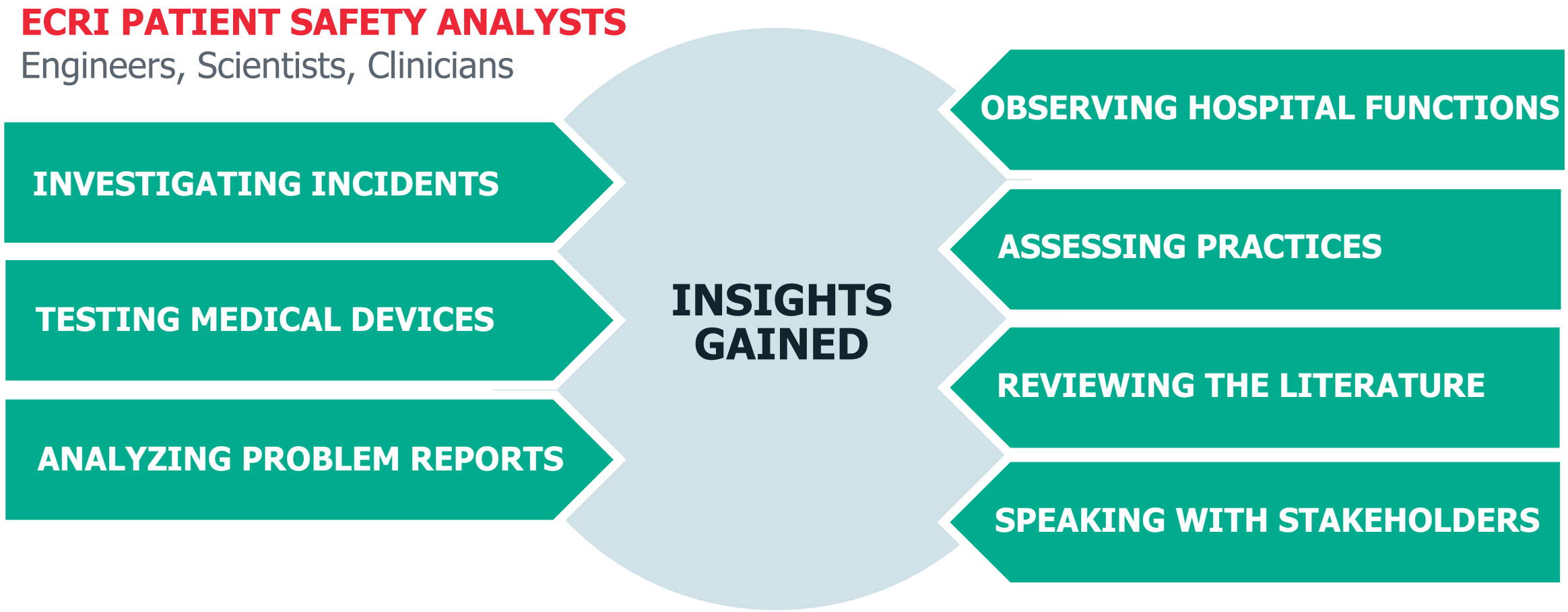
Topic Selection: Scope/Definition

Health technology **hazards**

Device or system faults, design features, or methods of use that might, under certain circumstances, place patients or users at risk.

©2023 ECRI

Topic Selection



©2023 ECRI

Topic Selection: Assessment Criteria

ONE OR MORE APPLY

- SEVERITY
- FREQUENCY
- BREADTH
- INSIDIOUSNESS
- PROFILE

FOR ALL

- ✓ TECHNOLOGY FOCUS
- ✓ GENERIC
- ✓ PREVENTABLE!

Patient harm **can be prevented** if appropriate measures are taken

The 2022 List at a Glance

1. Cybersecurity Attacks Can Disrupt Healthcare Delivery, Impacting Patient Safety
2. Supply Chain Shortfalls Pose Risks to Patient Care
3. Damaged Infusion Pumps Can Cause Medication Errors
4. Inadequate Emergency Stockpiles Could Disrupt Patient Care during a Public Health Emergency
5. Telehealth Workflow and Human Factors Shortcomings Can Cause Poor Outcomes
6. Failure to Adhere to Syringe Pump Best Practices Can Lead to Dangerous Medication Delivery Errors
7. AI-Based Reconstruction Can Distort Images, Threatening Diagnostic Outcomes
8. Poor Duodenoscope Reprocessing Ergonomics and Workflows Put Healthcare Workers and Patients at Risk
9. Disposable Gowns with Insufficient Barrier Protection Put Wearers at Risk
10. Wi-Fi Dropouts and Dead Zones Can Lead to Patient Care Delays, Injuries, and Deaths

©2023 ECRI

What is cybersecurity ?

- Protecting systems, networks, and applications from digital attacks
- A set of practices designed to protect against internal / external threats
- A combination of policies, procedures, technologies, and people

©2023 ECRI | www.ecri.org | 12

Protected Health Information (PHI)

- Health information that can be linked to a person by an identifier as defined by the United States Health Insurance Portability and Accountability Act (HIPAA) privacy rule
- ePHI refers to PHI in electronic form

©2023 ECRI

Mission-Critical Asset

- Failure stops department or organization function / business operations
- **Result:**
  - Loss of revenue
- **Examples:**
  - Point of Sale
  - Scheduling Systems
  - Email

Life-Critical Asset

- Failure that impacts ability to deliver care
- **Result:**
  - Delay to patient care
  - Patient harm
  - Injury / loss of life
- **Examples:**
  - Medical devices and associated systems
    - Infusion Pumps
    - Ventilators
    - Patient Monitors

1 2022 Top 10 Health Technology Hazards

Cybersecurity Attacks Can Disrupt Healthcare Delivery, Impacting Patient Safety

Cybersecurity Attacks Can Disrupt Healthcare Delivery, Impacting Patient Safety

THE ISSUE

- Network-connected medical devices and data systems are integral to how patients are diagnosed, treated, and kept safe within healthcare environments.
- A cybersecurity incident, or even the process required to remediate or respond to a security vulnerability, could render these systems unavailable.
- Managing cybersecurity risks in a healthcare environment, is uniquely challenging:
  - Requires an understanding of the clinical implications of the protective measures being considered
  - Actions that might be commonplace in other IT environments could themselves cause problems if their potential impact on patient care is not assessed

©2023 ECRI

Cybersecurity incidents don’t just interfere with business operations—they can disrupt patient care, posing a real threat of physical harm.

©2023 ECRI | www.ecri.org | 17

- **2023** - #5. Failure to Manage Cybersecurity Risks Associated with Cloud-Based Clinical Systems Can Result in Care Disruptions
- **2022** - #1. Cybersecurity Attacks Can Disrupt Healthcare Delivery, Impacting Patient Safety
- **2021** - #7. Vulnerabilities in third-party software components present cybersecurity challenges
- **2020** - #7. Cybersecurity Risks in the Connected Home Healthcare Environment
- **2019** - #1. Hackers Can Exploit Remote Access to Systems, Disrupting Healthcare delivery
- **2018** - #1. Ransomware and Other Cybersecurity Threats
- **2017** - #6. Software Management Gaps Put Patients, and Patient Data, at Risk
- **2016** - #10. Misuse of USB Ports Can Cause Medical Devices to Malfunction
- **2015** - #9. Cybersecurity: Insufficient Protections for Medical Devices and Systems

Cybersecurity Incidents Are Impacting Healthcare Globally

Ransomware Attacks on U.S. Hospitals Have Doubled Since 2016

By HealthDay | Jan. 4, 2023, at 8:35 a.m.

Ransomware attack delays patient care at hospitals across the U.S.

CHI Memorial Hospital in Tennessee, some St. Luke's hospitals in Texas and Virginia Mason Franciscan Health in Seattle all have announced they were affected.

Scripps enters fourth week of ransomware attack

Medical implants vulnerable to cyber attacks, experts warn

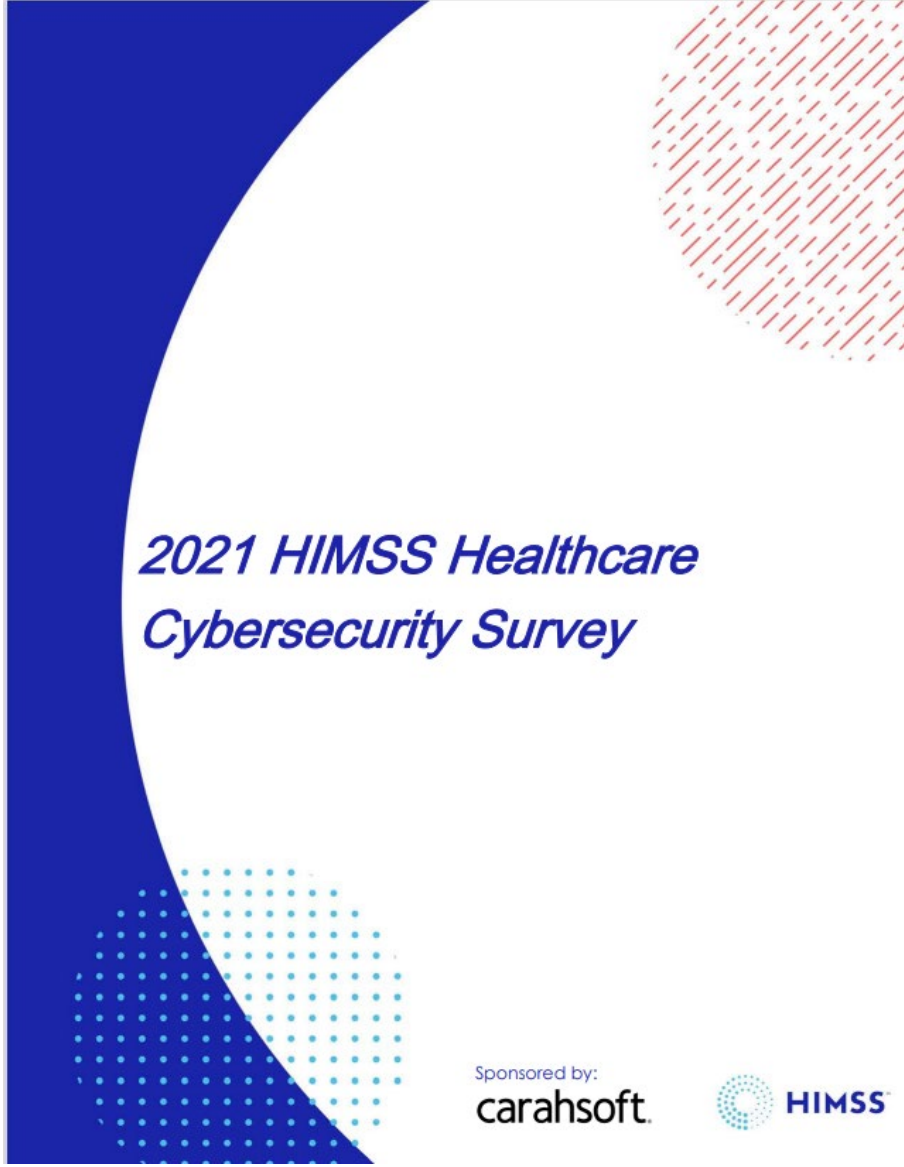
Universal Health Services Ransomware Attack Cost $67 Million in 2020

Global Edition Privacy & Security

Half of ransomware attacks have disrupted healthcare delivery, JAMA report finds

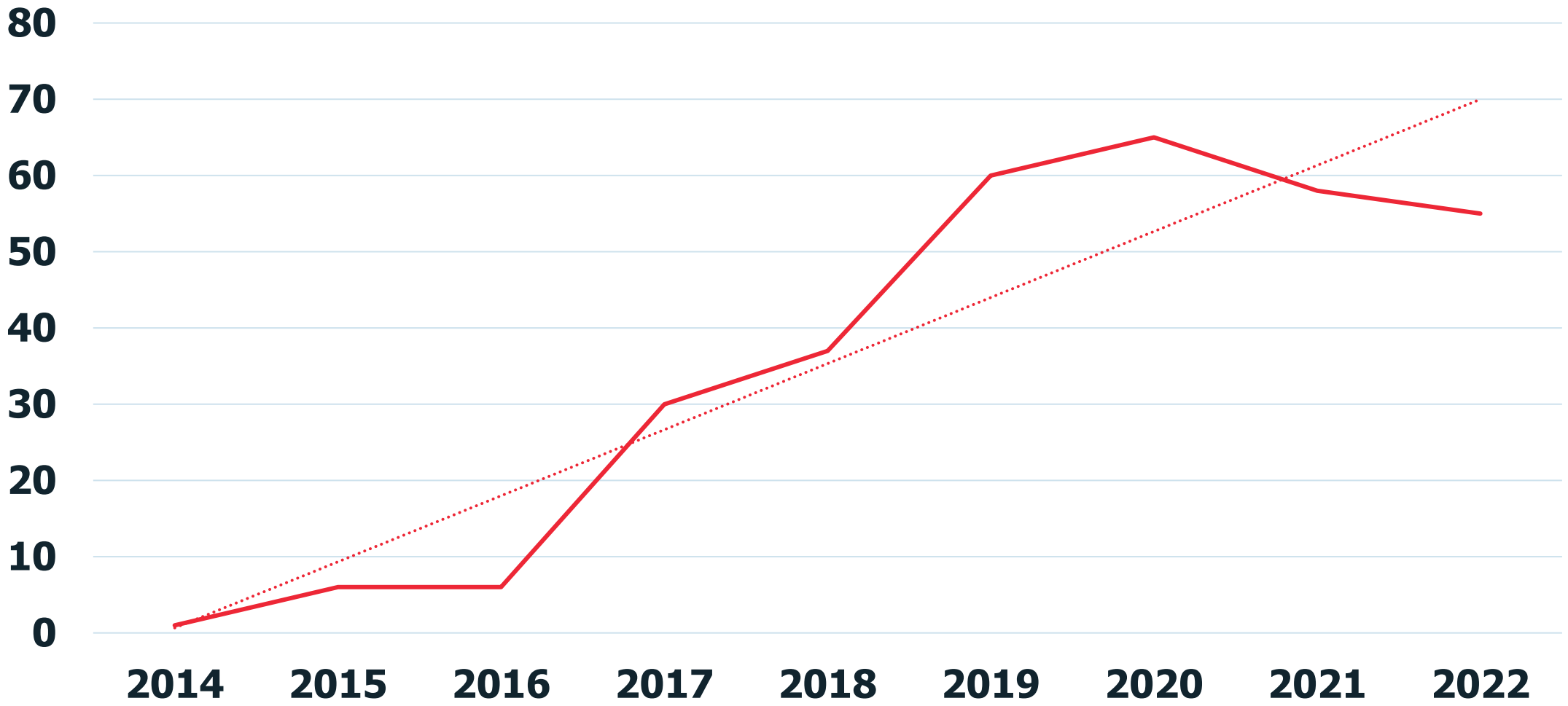
HIMSS 2021 Cybersecurity Survey

- "The most significant security incident was typically either a **phishing attack (45%) or ransomware attack (17%)**"
- Impacts:
  - **Disruption of systems/devices impacting business operations (32%)**
  - **Data breach or data leakage (22%)**
  - **Disruption of systems/devices impacting clinical care (21%)**



[2021 HIMSS Healthcare Cybersecurity Survey Report | HIMSS]

Medical Device Cybersecurity Alerts



Source ECRI Alerts Database

©2023 ECRI

Cybersecurity Incident Will Occur!

©2023 ECRI | www.ecri.org | 22

How Could a Cybersecurity Incident Impact a Healthcare Organization?

©2022 ECRI | www.ecri.org | 23

How Could a Cybersecurity Incident Impact a Healthcare Organization?

SCHEDULING SYSTEM

EHR / PATIENT RECORDS

IMAGING SYSTEMS

MEDICATION SAFETY TECHNOLOGIES

LAB RESULTS

INTERNAL PHONE SYSTEMS

©2023 ECRI | www.ecri.org |

Unauthorized Disclosure of PHI

- High value data
  - e.g., social security number, address, prescriptions, diagnosis, billing information
  - Information that cannot be altered
- Multiple malicious uses
- Can result in HIPAA Violations
- High recovery costs for the organization

©2023 ECRI

“$408 per lost or stolen record”

The average total cost for healthcare (data breach) increased from $7.13 million in 2020 to $9.23 million in 2021, a 29.5% increase.

Cost of a Data Breach Report 2021 (ibm.com)

How Could a Cybersecurity Incident Impact a Healthcare Organization?

- **Patient harm**
  - Worst case scenario!
- **Disruption to operations and clinical workflows:**
  - Altered clinical and administrative workflows
  - Rescheduling of appointments and surgeries
  - Diversion of emergency vehicles
  - Closure of care units or entire organizations

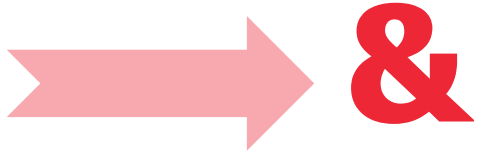
- **Loss of revenue**
- **Loss of data, destruction of systems**
- **Penalties and fines**
- **Impact to reputation**
- **Recovery costs**
- **Ripple effect on other area providers**

What can organizations do to help prevent cybersecurity incidents?

KEY RECOMMENDATIONS

Implement a security program

- Select & implement a standard framework
- Estimate the resources needed
- Assess the organization's current state
- Prioritize areas that require improvement
- Establish goal timelines
- Periodically assess and improve the program
- Document the process



Develop an incident response plan

- Identify mission-critical processes and systems
- Develop strategies for continuing operations if:
  - A medical device or system becomes unavailable
  - You lose access to support systems (e.g., PACS, EHR) or infrastructure (network)
- Educate staff about response strategies
- Practice the plan – tabletop exercises
- Periodically review & update the plan

©2023 ECRI

What can you do to help prevent cybersecurity incidents?

1. **Be mindful of suspicious emails!**
2. **Exercise caution before clicking links or opening attachments**
3. **Keep your devices updated!**
4. **Participate in tabletop exercises**
5. **Use strong passwords and multi-factor authentication where possible**
6. **Report any suspected or confirmed security incidents**

©2023 ECRI

Cybersecurity is a Patient Safety Issue

©2023 ECRI

Questions

©2023 ECRI

Thank You

©2022 ECRI