



DIGITAL
SECURITY

Cybersecurity Considerations for Clinical Laboratories

David McClintock, MD

Chair, Division of Computational Pathology & AI
Department of Laboratory Medicine and Pathology

Mayo Clinic



Disclosures

In the past 12 months, I have not had any significant financial interest or other relationship with the manufacturers of the products or providers of the services that will be discussed in my presentation.

Any vendors or manufacturers shown are for presentation purposes only and are not an endorsement on my part.

There is no way I can cover everything necessary on this topic in 20 minutes.

'Lives are at stake': hacking of US hospitals highlights deadly risk of ransomware

The number of ransomware attacks on US healthcare organizations increased 94% from 2021 to 2022, according to one report

Cybersecurity is more prominent than ever!



Article from:
<https://www.theguardian.com/technology/2022/jul/14/ransomware-attacks-cybersecurity-targeting-us-hospitals?via=indexdotco>

Article from: <https://www.theguardian.com/technology/2022/jul/14/ransomware-attacks-cybersecurity-targeting-us-hospitals?via=indexdotco>

SECURITY

Parents struggle to get care after cyberattack on Chicago children's hospital

Hospital systems have been affected for more than a week.



Lurie Children's Hospital in Chicago. Alamy file

Feb. 8, 2024, 11:00 AM CST / Updated Feb. 8, 2024, 4:40 PM CST

By Kevin Collier

Chicago's biggest children's hospital, Ann & Robert H. Lurie Children's, has entered its second week of reduced service as it tries to recover from a cyberattack.

Most of the hospital's internet-connected equipment, including phones, email access and electronic health records, have been offline since the start of the incident, the [hospital has said](#), making it significantly more difficult for parents to stay in touch with their doctors. Many appointments and surgeries are still being honored, [the hospital said](#) Monday.

Hackers are even hitting CHILDREN'S HOSPITALS!!

Article from: <https://www.nbcnews.com/tech/security/lurie-childrens-hospital-chicago-cyber-attack-down-help-rcna137446>

Hackers are

“There is a special place in hell for a person who attacks a children’s hospital and disrupts medical care for thousands of innocent children,” said Deborah Land, whose teenage daughter is a patient at the hospital.

SECURITY

Parents struggle to get care after cyberattack on Chicago children’s hospital

Hospital systems have been affected for more than a week.



Lurie Children's Hospital in Chicago. Alamy file

Feb. 8, 2024, 11:00 AM CST / Updated Feb. 8, 2024, 4:40 PM CST

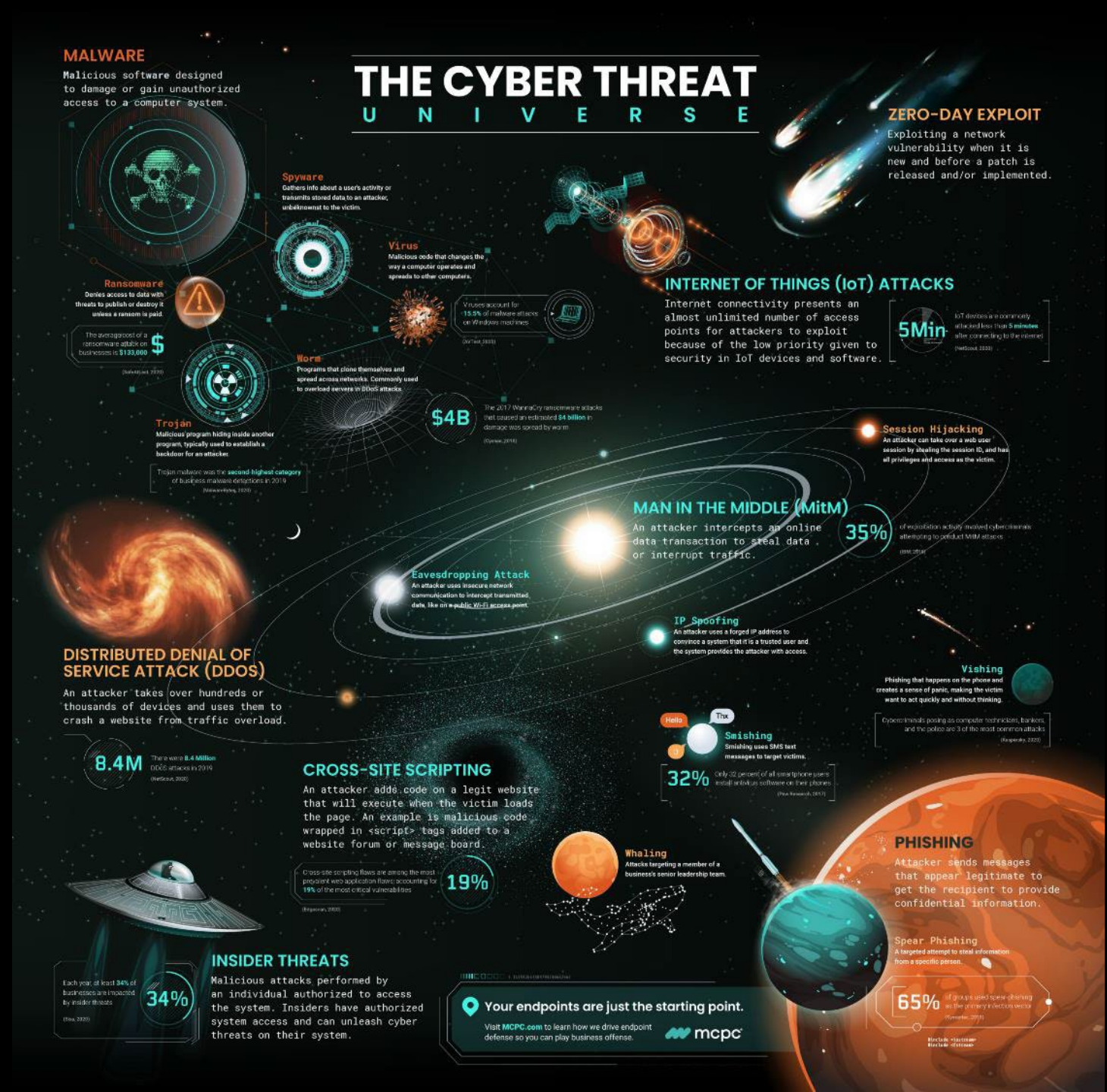
By Kevin Collier

Chicago’s biggest children’s hospital, Ann & Robert H. Lurie Children’s, has entered its second week of reduced service as it tries to recover from a cyberattack.

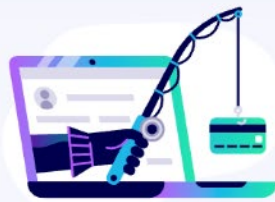
Most of the hospital’s internet-connected equipment, including phones, email access and electronic health records, have been offline since the start of the incident, the [hospital has said](#), making it significantly more difficult for parents to stay in touch with their doctors. Many appointments and surgeries are still being honored, [the hospital said](#) Monday.

Cyberthreats

Infographic from:
<https://www.mcpc.com/insights/infographics/the-cyber-threat-universe/>



Top Ten Cybersecurity Threats in 2024



1 Social Engineering

Any network is hackable if an employee can be duped into sharing access.

2 Third-Party Exposure

Vendors, clients, and app integrations with poor security can provide access to an otherwise well-protected network.



3 Configuration Mistakes

Even the most cutting-edge security software only works if it's installed correctly.

6 Ransomware

Hackers can capture sensitive data or take down networks and demand payment for restored access.



7 Mobile Device Vulnerabilities

Devices that connect to multiple networks are exposed to more potential security threats.



8 Internet of Things

Smart technology users may not realize that any IoT device can be hacked to obtain network access.



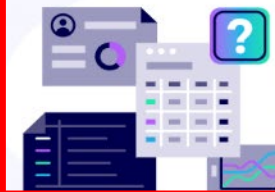
4 Poor Cyber Hygiene

Employee training is essential to ensure those with network access maintain safe cyber practices.



9 Poor Data Management

When massive amounts of unnecessary data are kept, it's easier to lose and expose essential information.



5 Cloud Vulnerabilities

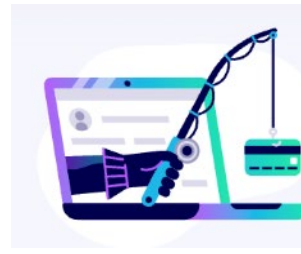
Online data storage and transfer provides increased opportunities for a potential hack.

10 Inadequate Post-Attack Procedures

Security patches must be as strong as the rest of your cybersecurity protections.



Social Engineering



1 Social Engineering


Any network is hackable if an employee can be duped into sharing access.

- Easier to trick a human than exploit a technical vulnerability in a system
 - Preys on human nature and emotional responses
 - ~85% of breaches involve human interaction
 - (2021 Verizon Data Breach Investigations Report)
- Social engineering techniques
 - 75% of data breaches start with an email!
 - Phishing, spear phishing, whaling
 - Vishing, smishing (phone calls, texting)



Spear Phishing

[3] [Liron Email] Greetings ✓

From  mailing2boxio00@gmail.com

☆ Monday

To



From  Liron Pantanowitz, MBBCh <makaksjo80@gmail.com>

☆ Monday

To



Glad to hear from you,

I need you to get an "Steam or Visa" gift card for a friend's daughter who is down with cancer of the Liver, it's her birthday today and I promised to get it for her today, but I can't do this now because all my effort purchasing it online proved abortive and we traveled for a friend's burial who lost his life to Coronavirus (covid19). Wondering if you could get it from any store around you or online? I'll pay back. Kindly let me know if you can handle this.

Await your soonest response.

Kind regards

Liron



Monday



Third Party Exposure

2 Third-Party Exposure

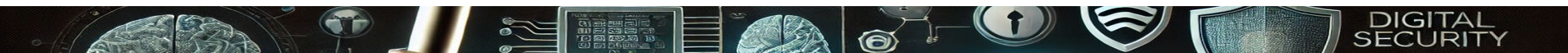
Vendors, clients, and app integrations with poor security can provide access to an otherwise well-protected network.



- Partners with privileged access to your systems
- GOAL:
 - Target 3rd party, less-protected systems with access to the hacker's primary target
- For clinical laboratories:
 - Middleware
 - Home grown systems based on open-source software
 - Legacy, must-have applications for your lab



Image: "Digital Illustration of Cyber Attack Targeting Strategy." Created by OpenAI's DALL-E, 04/26/2024.



Poor Cyber Hygiene



"Digital Illustration of Poor Cyber Hygiene in an Office." Created by OpenAI's DALL-E, 04/28/2024

4 Poor Cyber Hygiene

Employee training is essential to ensure those with network access maintain safe cyber practices.



• Cyber hygiene:

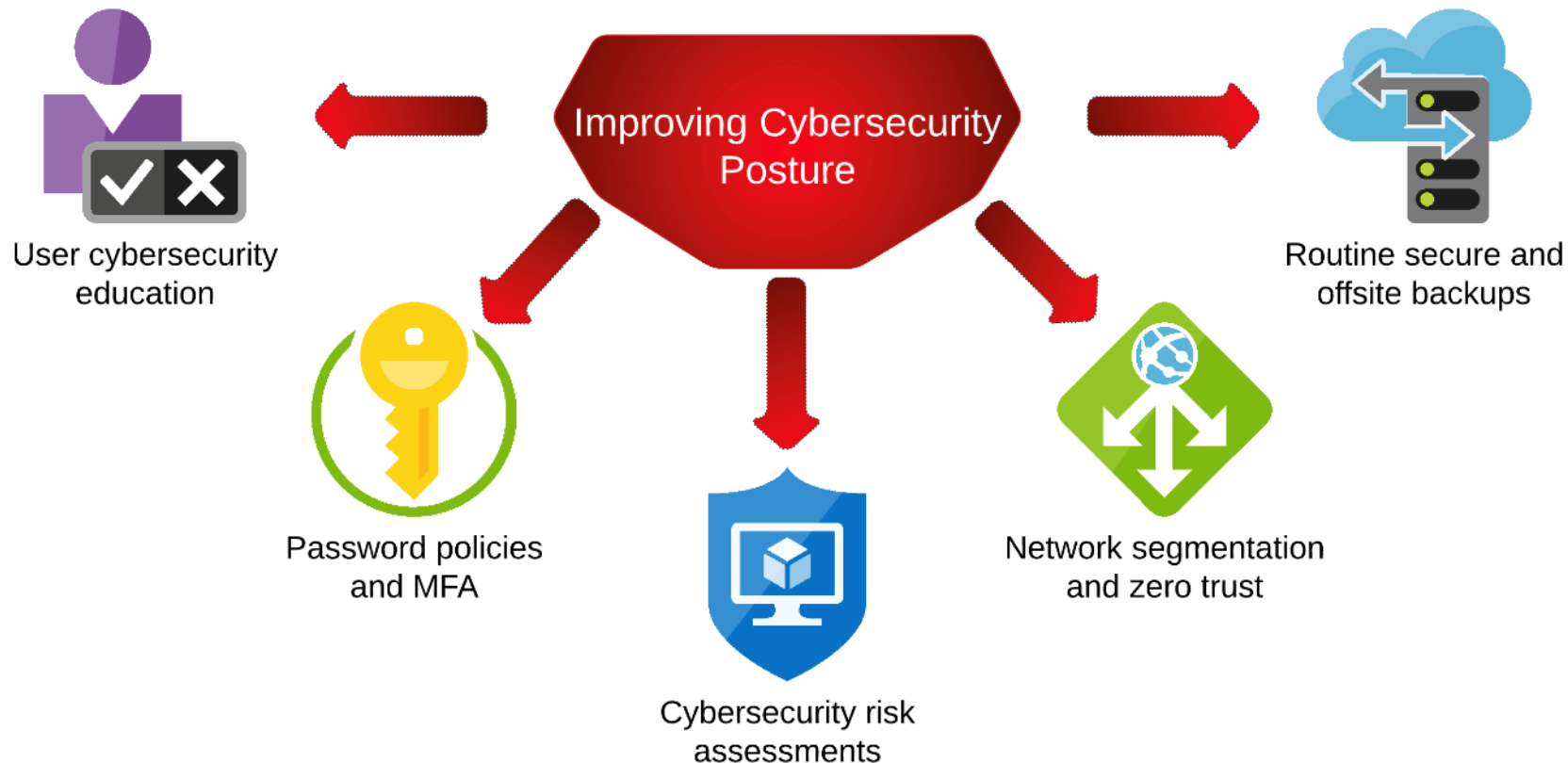
- Practices users take to maintain system health and improve cybersecurity
- Relies on both the institution and its users to work together improve and maintain their overall cybersecurity posture

• Cybersecurity posture

- Security status of an organization's networks, information, and systems

Improving Cybersecurity Posture

- Cybersecurity posture is based on:
 - Information security resources (e.g., people, hardware, software, policies)
 - Capabilities in place to manage the enterprise's defense and to react as the situation changes



Cybersecurity Controls

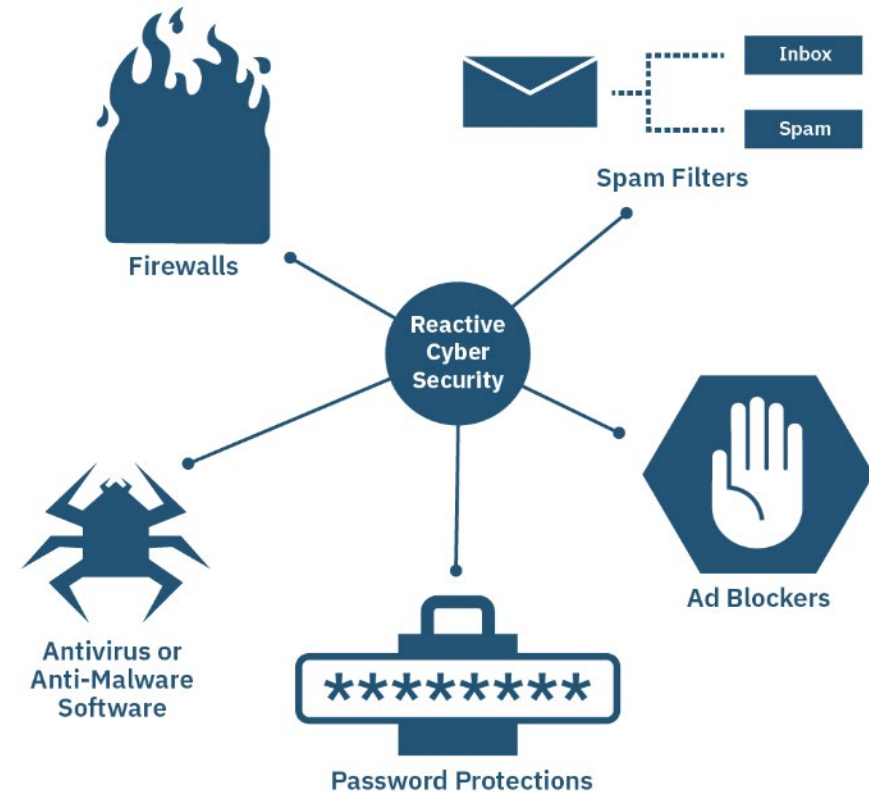
Proactive cybersecurity controls

A proactive approach to cyber security locates and corrects your system's potential vulnerabilities before they can be exploited by criminals.



Reactive cybersecurity controls

A reactive approach to cyber security bulks up your defenses against common attacks and tracks down hackers inside your network.



User Cyber Hygiene Practices



- **PC/device practices:**
 - Core image machines / corporate standard builds
 - Limited privileges, approved applications/functions only, controlled use
 - Antivirus software, regular OS/software updates
 - Password change requirements, 2-factor authentication (2FA/MFA) use
 - Remote monitoring of PC use, network connections
 - Restrictions on who can use VPN and on which devices
- **Mobile device management (MDM):**
 - Laptops, tablets, phones, and other supported mobile devices
 - Examples: Microsoft InTune, VMWare Workspace One (Intelligent Hub)



Organizational Cyber Hygiene Practices



Network access

- NAC – network access control
- Network Segmentation
 - Clinical vs research vs guest networks
- Network traffic monitoring and control

Devices & storage

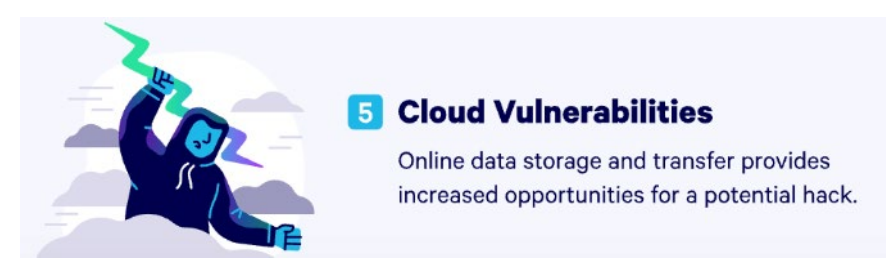
- Inventory / track all networked devices and storage media
- Require encryption and password protection
- Permission based access
- Establish retention policies, acceptable content policies

Applications

- Require SSO (single sign on) / Active Directory integration
- Disable local accounts whenever possible
- Perform regular risk assessments
- Integrate security reviews as part of every supply chain / procurement processes



Cloud Vulnerabilities



- Cloud vulnerabilities have reportedly increased 150% over the past five years
- More and more lab systems (digital pathology and AI systems especially) are using cloud-based systems
- Mitigation includes:
 - Moving to a zero-trust cybersecurity strategy
 - Becoming certified by HITRUST and other cybersecurity certifications
 - Certifiable framework providing global organizations a comprehensive, flexible, and efficient approach to regulatory/standards compliance and risk management; serves to demonstrate HIPAA Compliance



Sources: 1) 2021 IBM Security X-Force Cloud Threat Landscape Report, available at <https://www.ibm.com/downloads/cas/WMDZOWK6>; 2) Verizon 2021 Data Breach Investigations Report, available at <https://www.verizon.com/business/resources/reports/2021/2021-data-breach-investigations-report.pdf>; 3) <https://www.techment.com/top-5-cloud-vulnerabilities-to-consider-in-2022/>



Cybersecurity Strategy: Castle and Moat

- Legacy strategy still used by some
- Focus on **strong network security perimeter** → **MOAT**
- Keep out malicious agents from **inner networks, systems, & data** → **CASTLE**
- ***Once inside the castle, you have the keys to the kingdom!***
 - Great for internal users (easy access)
 - Bad for malicious agents (easy access!)
 - Cybercriminals
 - Internal bad actors/insider threats

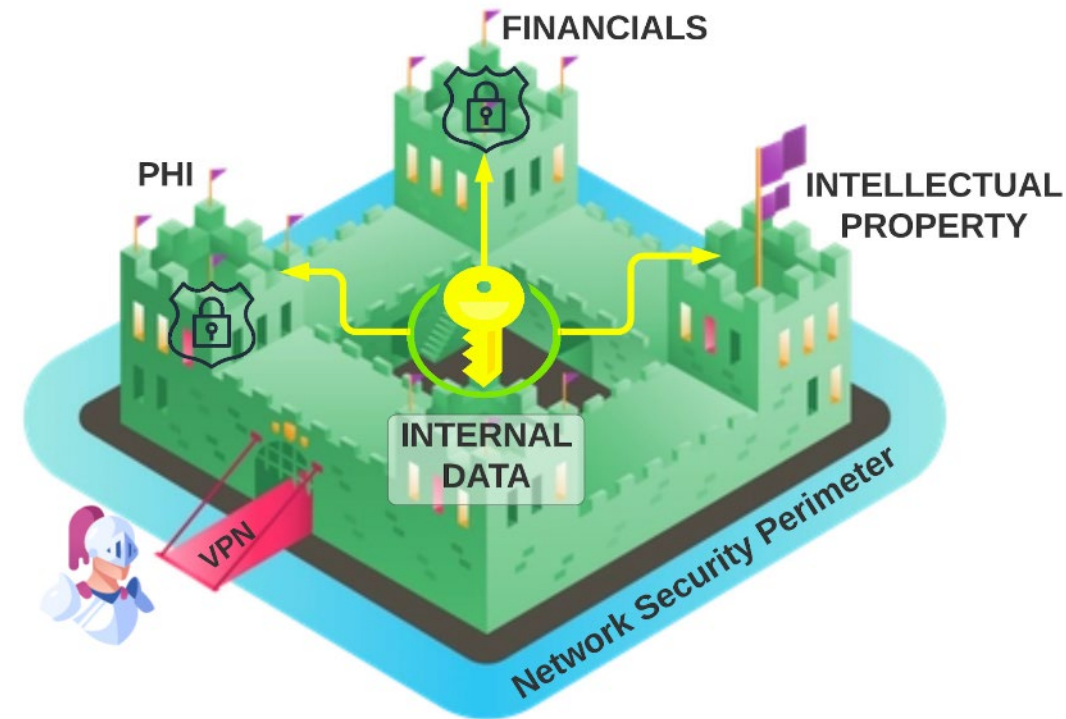


Figure from: Patel AU, Williams CL, Hart SN, Garcia CA, Durant TJS, Cornish TC, McClintock DS. Cybersecurity and Information Assurance for the Clinical Laboratory. J Appl Lab Med. 2023 Jan 4;8(1):145-161. doi: 10.1093/jalm/jfac119. PMID: 36610432.



Cybersecurity Strategy: Zero Trust

- Modern information security strategy
- **NO ONE CAN BE TRUSTED**
 - No central/single security perimeter/ moat, no keys to the kingdom
- ***Presumes risks are present both inside and outside the organization***
 - **ALL** incoming connections and source controls are verified throughout **ALL** layers of a network
 - Users/devices have to authenticate themselves when accessing practically every application within the organization



Figure from: Patel AU, Williams CL, Hart SN, Garcia CA, Durant TJS, Cornish TC, McClintock DS. Cybersecurity and Information Assurance for the Clinical Laboratory. J Appl Lab Med. 2023 Jan 4;8(1):145-161. doi: 10.1093/jalm/jfac119. PMID: 36610432.



Poor Data Management



- Data management today is more than just keeping your data organized
- What is the "right" data to keep?
 - For some, all data is saved...but without organization and curation, think hoarders...
- Who has access to your data?
 - Who SHOULD be using your data and in what format?
 - Is your data easily accessible in a usable way?
- What changes in your pathology assets and data occur as more labs go digital
 - Think AP digitizing, less paper in lab medicine
- **With great data comes great responsibility**



Image: My parents' old garage...did my dad really need to keep everything??? Was it all important?



Data Management Changes for Digital Pathology

- Glass slides vs digital slides:
 - Glass slides
 - Limited distribution, only 1-2 patient identifiers if lost, person viewing slide has to know histopathology to learn more about the patient
 - Digital slides
 - Easily distributable, have metadata wrappers, contain varying degrees of patient identifiers and protected health information
 - Digital slides with annotations – same as digital slides, but with potentially much more actionable PHI
- Improper data management for DP can include:
 - Allowing improper access/use of clinical WSIs
 - Inadequate deidentification processes for WSIs
 - Slide labels embedded in the original WSIs for education/research

18 HIPAA Identifiers

Below we've listed the 18 types of information that qualify as PHI according to guidance from the Department of Health and Human Services (HHS) Office of Civil Rights (OCR). HIPAA protected health information examples include:



Inadequate Post-Attack Procedures

10 Inadequate Post-Attack Procedures

Security patches must be as strong as the rest of your cybersecurity protections.



- What happens in the event of a cyberattack? How does this differ from current lab downtimes?
 - Lab medicine and pathology practices require network connectivity now for almost everything!
 - When you have a ransomware attack, one of the first post-attack responses is to...**SHUT DOWN THE NETWORK!**
- For pathology → when going digital, you need ways to fall back to paper and glass!
 - Don't throw out your microscope quite yet!



Strengthening Lab Preparations

- Cyberattacks can debilitate hospitals & labs for days to weeks
 - Labs need specific post-attack procedures that address how you react without any network connectivity
- Business continuity plans should include which lab systems are required when to help with bringing systems back online
- Third-party risk management reviews **(TPRM) ARE A MUST!**
 - Both internally developed and externally purchased solutions
 - ALL software applications, platforms, systems, and even laboratory hardware (equipment/devices), should be reviewed on a regular basis



Cyberattacks are real! And can decimate your lab...



Article from: <https://www.captodayonline.com/weeks-of-lab-turmoil-follow-cyberattack/>

CAP TODAY

PATHOLOGY ♦ LABORATORY MEDICINE ♦ LABORATORY MANAGEMENT

APRIL 2021

Weeks of lab turmoil follow cyberattack

Anne Paxton

After he finished interviewing for a fellowship one morning last October at the University of Vermont Medical Center, pathology resident William O. Humphrey, MD, checked in to attend grand rounds virtually. Then the cyberattack struck.

First of two parts

Next month: cybersecurity

It began mysteriously, with people dropping one by one off the Zoom screen and emails arriving only intermittently. Internet service grew patchy and a hospital staffer unmuted and canceled grand rounds, saying, "We aren't really sure what's going on."

From there, a cascade of failures indicated serious trouble. "All of a sudden we're realizing we can't sign into our EMR. We can't get into our email either. My phone isn't working on the Wi-Fi. Something is wrong," recalls Dr. Humphrey, a member of the CAP Informatics Committee. That was the prelude to a siege in which fax ma-

chines and penmanship were unre-tired from obsolescence, paperlessness became a relic of the past, and words like "runners" and "bouncers" entered routine laboratory vocabulary.

External agents had maliciously

invaded and at least partially disabled the system. "It was certainly something abrupt. And our impression was that it may have been related to email phishing," Dr. Humphrey says, though no official word to hospital

staff has clarified how it occurred and who engineered it and why.

Such attacks have become a serious risk for any enterprise reliant on IT, which in this decade is nearly all enterprises. But cyber- —continued on 12

David Sawyer



Dr. Andrew Goodwin (from left), Dr. Christina Wojewoda, and Dr. William Humphrey at the University of Vermont Medical Center, where a cyberattack last fall sent the lab into prolonged downtime and chaos. "A cyberattack shuts down much more than you anticipated," Dr. Goodwin says.

'Know your panel': Blood culture ID cautions

Amy Carpenter Aquino

The interpretive challenges of blood culture identification panels were the focus of an AMP2020 virtual presentation on false-positives and false-negatives and their sources and solutions.

The spotlight was on *Proteus*, but "it's not the sole organism we have to worry about," said Susan Butler-Wu, PhD, D(ABMM), SM(ASCP), director of the clinical microbiology laboratory, LAC+USC Medical Center, Los Angeles, and associate professor of clinical pathology, Keck School of Medicine of USC.

Her co-presenter, speaking on antimicrobial resistance targets, was Richard Davis, PhD, D(ABMM), MLS(ASCP)^{CM}, of Providence Healthcare. (See CAP TODAY, May 2021, for coverage.) Dr. Davis and Dr. Butler-

Cyberattacks have real consequences – would your lab survive without the internet?

Articles from:

1. <https://www.burlingtonfreepress.com/story/news/local/vermont/2021/07/27/uvmmc-vermont-health-network-hospital-2020-cyberattack-cause-malware-phishing-vermont-hospital/5388399001/>
2. <https://www.usnews.com/news/best-states/vermont/articles/2020-12-09/recovery-cost-of-vermont-hospital-cyberattack-could-be-63m>
3. <https://www.nytimes.com/2020/11/26/us/hospital-cyber-attack.html>

Patients of a Vermont Hospital Are Left 'in Dark' After a Cyberattack

A wave of damaging attacks on hospitals upended the lives of patients with cancer and other ailments. "I have no idea what to do," one said.

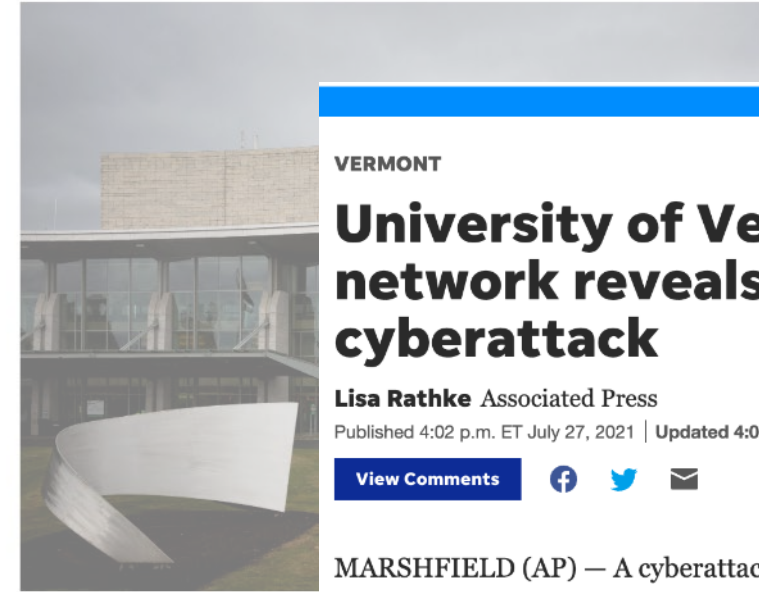


Home / News / Best States / Vermont News

Vermont Hospital Cyberattack Cost Estimated at \$1.5M a Day

University of Vermont Medical Center officials say a late October cyberattack is costing the hospital about \$1.5 million a day.

By Associated Press | Dec. 9, 2020



VERMONT

University of Vermont hospital network reveals cause of 2020 cyberattack

Lisa Rathke Associated Press

Published 4:02 p.m. ET July 27, 2021 | Updated 4:04 p.m. ET July 27, 2021

View Comments



The University of Vermont Medical Center in late October. Elizabeth Frantz for The New York Times



By Ellen Barry and Nicole Perloff

Published Nov. 26, 2020 Updated

At lunchtime on Oct. 28, 2020, the University of Vermont Medical Center was closed for chemotherapy infusions. Patients were frightened, but the nurses provided a warm blanket, a seat w

MARSHFIELD (AP) — A cyberattack that crippled the computer systems of a hospital network affecting six hospitals in Vermont and New York last fall happened after an employee opened a personal email on a company laptop while on vacation, a University of Vermont Health Network official said Tuesday.

The email was from legitimate local business that had been hacked, Doug Gentile, network chief medical information officer told The Associated Press. The email contained an attachment that had the malware. When the employee returned from vacation and logged onto the UVM network through a virtual private network, the attackers were ready and launched the attack, he said.

"We have no evidence at all that UVM was specifically targeted. We just got caught up in a broad phishing attack," Gentile said Tuesday.

tack on the computer systems costing the hospital about \$1.5 million a day, its CEO said.

ns of the hospital system that [The New York Times](#) reported.

Are You Prepared?

Laboratory Ransom

Toby C. Corn

From the ¹Department of Pathology, University of

At 11:30 AM on October 1, 2017, our laboratory information system was suddenly and without warning down. Just after the Epic EHR network was down, our network was down for hours or less. While our procedures were not affected, initially, the interface was immediately unresponsive, no interface

Anatomy of a Cyberattack

Part 1: Management of a Laboratory Cyberattack

Anne M. Stowman,
Timothy St. John,
Valerie Cortright,
Scott R. Anderson

From the ¹Department of Pathology, University of Vermont, USA; and ²University of Vermont

ABSTRACT

Objectives: Our institution was the victim of a cyberattack that led to a complete shutdown of our laboratory information systems. The attack affected our department-specific systems, including our electronic scheduling, billing and coding systems. Our EHR lasted 25 days, with significant disruptions to patient care and transition to networked systems. This article focuses on the transition of our laboratory to continue operations during the downtime.

Anatomy of a Cyberattack

Part 2: Management of a Laboratory Cyberattack

Andrew Goodwin,
Jessica Mesec,
Lori S. Cacciatore,
and Anne M. Stowman

From the ¹Department of Pathology, University of Vermont, USA; and ²University of Vermont

ABSTRACT

Objectives: Our institution was the victim of a cyberattack that led to a complete shutdown of our laboratory information systems, including our electronic scheduling, billing and coding systems, and digital systems affecting our clinical operations.

Methods: During the downtime, we implemented multiple communication systems, including a dedicated response, employing interdisciplinary engagement.

Anatomy of a Cyberattack

Part 3: Communication, Development, and Education

Anne M. Stowman,
Valerie Cortright,
Clayton Wilburn,
Alexandra N. Kalof

From the ¹Department of Pathology, University of Vermont Medical Center Information Technology, USA; and ²University of Vermont

ABSTRACT

Objectives: Our institution was the victim of a cyberattack that led to a complete shutdown of our laboratory information systems for more than 25 days. These manual processes had to be taken offline, as well as the laboratory information

Anatomy of a Cyberattack

Part 4: Quality Assurance and Error Reduction, Billing and Compliance, Transition to Uptime

Nora K. Frisch, MD,¹ Pamela C. Gibson, MD,¹ Anne M. Stowman, MD,¹ Andrew Goodwin, MD,¹ Michelle Schwartz, PA(ASCP),¹ Valerie Cortright, HTL, QIHC,¹ Tania Hong,² and Alexandra Kalof, MD¹

From the ¹Department of Pathology and Laboratory Medicine, University of Vermont Medical Center, Burlington, VT, USA; and ²University of Vermont Health Network, Burlington, VT, USA.

ABSTRACT

Objectives: Our institution was the victim of a cyberattack that necessitated use of manual laboratory systems for more than 25 days. These manual processes had to be created not only to enable us to process our case volume without bottlenecks but also to maintain patient safety and allow for billing.

Methods: Our laboratory needed to create a safe reporting process to ensure ongoing patient safety and error reduction during the downtime. Additionally, we needed to ensure the ability to bill for performed tests in some areas of the lab and maintain compliance with

KEY POINTS

- Patient safety and error reduction are essential, especially during an extended downtime. Despite inefficiencies, identifying sources of error and correcting mistakes are best done in real time.
- Gathering the appropriate information for billing and compliance requirements is important when creating workflows and templates for reporting during a downtime.
- Plan for the transition to uptime, including communications with providers, information technology, faculty, and billing/compliance, when faced with prolonged downtime.

KEY WORDS

Informatics; Management/administration; Quality

Series of five publications, reviews how to better prepare for a cyberattack – THIS IS ESSENTIAL READING!

INSIDE THE LAB



PODCAST EPISODE

S2Ep17: Anatomy of a Cyberattack

Inside the Lab

Cybersecurity and Information Assurance for the Clinical Laboratory

Ankush U. Patel,^{a,†} Christopher L. Williams,^{b,†} Steven N. Hart ^a, Christopher A. Garcia,^a Thomas J.S. Durant,^c Toby C. Cornish ^d, and David S. McClintock ^{a,*}

Background: Network-connected medical devices have rapidly proliferated in the wake of recent global catalysts, leaving clinical laboratories and healthcare organizations vulnerable to malicious actors seeking to ransom sensitive healthcare information. As organizations become increasingly dependent on integrated systems and data-driven patient care operations, a sudden cyberattack and the associated downtime can have a devastating impact on patient care and the institution as a whole. Cybersecurity, information security, and information assurance principles are, therefore, vital for clinical laboratories to fully prepare for what has now become inevitable, future cyberattacks.

Content: This review aims to provide a basic understanding of cybersecurity, information security, and information assurance principles as they relate to healthcare and the clinical laboratories. Common cybersecurity risks and threats are defined in addition to current proactive and reactive cybersecurity controls. Information assurance strategies are reviewed, including traditional castle-and-moat and zero-trust security models. Finally, ways in which clinical laboratories can prepare for an eventual cyberattack with extended downtime are discussed.

Summary: The future of healthcare is intimately tied to technology, interoperability, and data to deliver the highest quality of patient care. Understanding cybersecurity and information assurance is just the first preparative step for clinical laboratories as they ensure the protection of patient data and the continuity of their operations.

Review to help drive home concepts

Patel AU, Williams CL, Hart SN, Garcia CA, Durant TJS, Cornish TC, McClintock DS. Cybersecurity and Information Assurance for the Clinical Laboratory. J Appl Lab Med. 2023 Jan 4;8(1):145-161. doi: 10.1093/jalm/jfac119. PMID: 36610432.

Available at:
<https://academic.oup.com/jalm/article/8/1/145/6965173?login=false>

Final Thoughts

- Many cybersecurity risks exist today!
- There is no 100% secure, or zero risk system
 - Cybersecurity should be equated to continuous QA/QM in the labs
- **RECOMMENDATION: Become part of the process**
 - Actively seek out your information security team(s)
 - Be a part of the information security process
- At some point, you will likely be part of a cyberattack and it will suck



The image is a vibrant collage of scientific and technological symbols. At the top, there's a brain with a rainbow gradient, a microscope, and several test tubes with colored liquids. To the right, there's a flask with blue liquid and a grid-like icon. The background is filled with various icons like a padlock, a biohazard symbol, a circuit board, and a globe. The overall theme is the intersection of biology, chemistry, and technology.

QUESTIONS?