

# Cybersecurity Update

Beyond the Headlines: The Everyday Cyber Threats Healthcare Providers Face

**E×PLORE**  
HEALTHCARE SUMMIT

---

---

---

---

---

---

---

**Disclaimer:**  
The information set forth in this presentation is intended as general risk management information. Beazley does not render legal services or advice. It should not be construed or relied upon as legal advice and is not intended as a substitute for consultation with counsel. Although reasonable care has been taken in preparing the information set forth in this presentation, Beazley accepts no responsibility for any errors it may contain or for any losses allegedly attributable to this information.

---

---

---

---

---

---

---

**Today's Topics**

 2024 Year in Review

 Looking Forward

 Threats to Small Practices

 Incident Response & Business Continuity Planning

 When to Notify Insurance

---

---

---

---

---

---

---



---

---

---

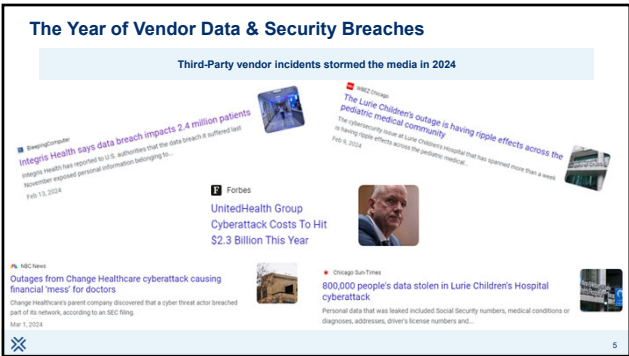
---

---

---

---

---



---

---

---

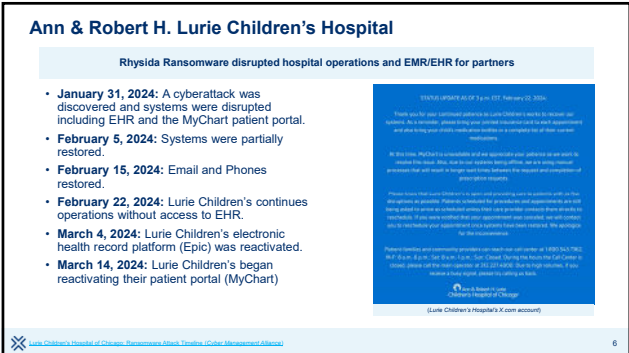
---

---

---

---

---



---

---

---

---

---

---

---

---

### Ann & Robert H. Lurie Children's Hospital

Be prepared to pivot at a moment's notice. Recovery is not a quick flip of a switch.

STATUS UPDATE AS OF 7:45 a.m. CST, March 14, 2024.

Lurie Children's has begun the process of restoring MyChart for patient families. This process will take place over the coming days.

Currently, the MyChart functionality that are coming online to support our patient families include online scheduling, a check-in, provider messaging, and medication refill requests and to the coming days. For more information, please contact your provider. Additionally, some services appointments will also be available via MyChart. Patient Services should refer to their email and/or text message reminders and log into their Lurie Children's MyChart account for information about their upcoming telemedicine appointment.

ALPHV

Ann & Robert H. Lurie Children's Hospital of Chicago

Due to the anticipated high volume of MyChart activity, patient families may experience intermittent service disruptions while using the MyChart web interface. This has not yet occurred during the system restoration. We are actively working to update the information available in MyChart with the information collected during the downtime. We do not have a solution when the system will be complete, and we will provide updates as this process progresses. We thank our patient families for their continued patience.

10/3

Ann & Robert H. Lurie Children's Hospital of Chicago

Can you go 33 days without access to your Electronic Health Records?

7

---

---

---

---

---

---

---

---

---

---

### Change Healthcare

ALPHV/BlackCat Ransomware disrupted one of the world's largest health payment processing companies

- **February 21, 2024:** Reports from Change Healthcare of a significant network interruption.
- **March 8, 2024:** Restoration of pharmacy services
- **March 15, 2024:** Restoration of electronic payment services
- **March 25, 2024 to April 21, 2024:** Restoration of additional key Change Healthcare products

**The Impact**

**Patients:**

- Inability to Process Claims
- Delayed or Denied Care
- Disruption in Pharmacy Services
- Financial Stress and Unexpected Costs
- Potential Data Privacy Concerns

**Providers:**

- Cash Flow Interruptions
- Furloughed Staff
- A Scramble for Loans

Visit <https://www.changehealthcare.com/newsroom> for more information.

8

---

---

---

---

---

---

---

---

---

---

### Not all large-scale cyber incidents are attacks

9

---

---

---

---

---

---

---

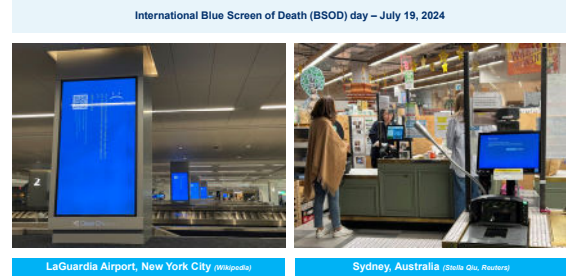
---

---

---

3

CrowdStrike Global IT Outage



[https://en.wikipedia.org/wiki/2024\\_CrowdStrike\\_outage#/media/File:BSOD\\_at\\_LaGuardia](https://en.wikipedia.org/wiki/2024_CrowdStrike_outage#/media/File:BSOD_at_LaGuardia)

10

---

---

---

---

---

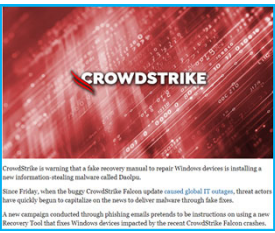
---

---

---

CrowdStrike Global IT Outage

- What Happened?**
- A software update caused millions of Windows users globally to experience the dreaded Blue Screen of Death, leading to system shutdowns, and a "Boot-Loop".
  - This caused widespread disruption affecting travel, shopping, banking, business operations and so much more.
  - Concerningly, the disruption impacted Emergency Services, Hospitals, and critical infrastructure.
  - This was **NOT** an attack. Instead, this was an error attributed for the time being to processes involved in "pushing" updates.
  - Criminals and other threat groups were equally surprised by this outage. However, they jumped on the opportunities opened.



<https://www.crowdstrike.com/newsroom/newsroom-releases/crowdstrike-falcon-update-caused-global-it-outage/>

11

---

---

---

---

---

---

---

---

CrowdStrike Global IT Outage



<https://www.crowdstrike.com/newsroom/newsroom-releases/crowdstrike-falcon-update-caused-global-it-outage/>

12

---

---

---

---

---

---

---

---

### CrowdStrike Global IT Outage

Notable Impacted Health Systems

- Kaiser Permanente
- Providence
- Henry Ford Health
- Nationwide Children's Hospital
- Dana-Farber Cancer Institute
- RWJBarnabas Health
- Emory Healthcare
- Mass General Brigham
- Norton Healthcare
- Penn Medicine
- Seattle Children's Hospital

The Disruption

- Canceled or Delayed Procedures
- Delayed Cases at Ambulatory Surgery Centers
- Delayed Lab and Pharmacy orders
- Implemented Downtime Procedures for Clinics

CrowdStrike outages hit US hospitals, health plans

A closer look at how the CrowdStrike IT outage affected healthcare

13

---

---

---

---

---

---

---

---

### CrowdStrike Global IT Outage

Notable Impacted Health Systems

- Kaiser Permanente
- **Providence**
- Henry Ford Health
- Nationwide Children's Hospital
- Dana-Farber Cancer Institute
- RWJBarnabas Health
- Emory Healthcare
- Mass General Brigham
- Norton Healthcare
- Penn Medicine
- Seattle Children's Hospital

The Impact

- Approximately 15,000 servers
- Approximately 40,000 of 150,000 devices

The Response

- Between July 19<sup>th</sup> and July 24<sup>th</sup> Providence leveraged more than 1,000 team members and volunteers to achieve 90% remediation of impacted systems.

"This is worse than a cyberattack" – Providence CIO, B.J. Moore

14

---

---

---


---

---

---

---

---



Looking Forward

---

---

---


---

---

---

---

---




5

### Notice of Proposed Rulemaking (NPRM)

Published: January 6, 2025  
Comment Period Closed: March 7, 2025  
Comments: 4,745

Will it be shelved?



#### What are the proposed changes/requirements?

- Written documentation of all security rule policies
- Planning for contingencies and responding to security incidents
  - Procedures to restore the loss of Electronic Information Systems (EIS)
  - Written security incident response plans (IRPs)
  - Written procedures for testing and revising IRPs
- Annual Compliance Audits
- Technical Controls
  - Anti-malware protection
  - Disabling network ports
  - Multi-Factor Authentication
  - Vulnerability scanning and penetration testing
  - Network segmentation

<https://www.hhs.gov/privacy-professionals/cybersecurity/notice-2025-01-06/feedback/index.html>

---

---

---

---

---


---

---

---

### Cyber Security Health Check:

- Establish a Security Culture
- Protect Mobile Devices
- Maintain Good Computer Habits
- Use a Firewall
- Install and Maintain Anti-Virus Software
- Plan for the Unexpected
- Control Access to Protected Health Information
- Use Strong Passwords and Change Them Regularly
- Limit Network Access and Control Physical Access

 <https://www.hhs.gov/privacy-professionals/cybersecurity/notice-2025-01-06/feedback/index.html>

---

---

---


---

---

---

---

---



### Threats to Small Practices

---

---

---

---

---

---

---

---

Ransomware:



---

---

---

---

---

---

---

Initial Infection Vector, 2024  
Ransomware-Related



---

---

---

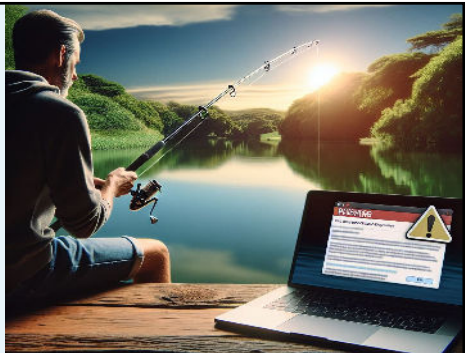
---

---

---

---

Phishing:



---

---

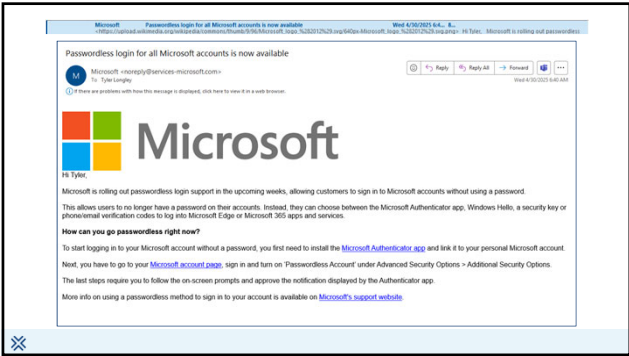
---

---

---

---

---



---

---

---

---

---

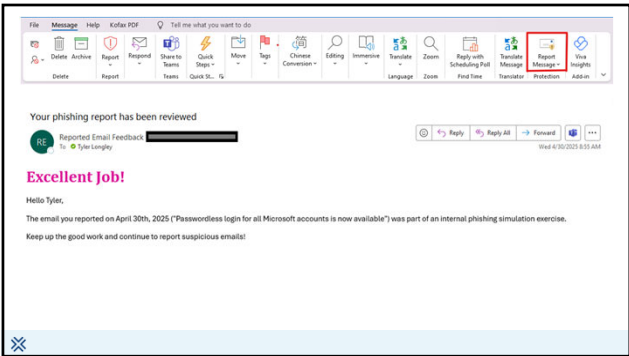
---

---

---

---

---



---

---

---

---

---

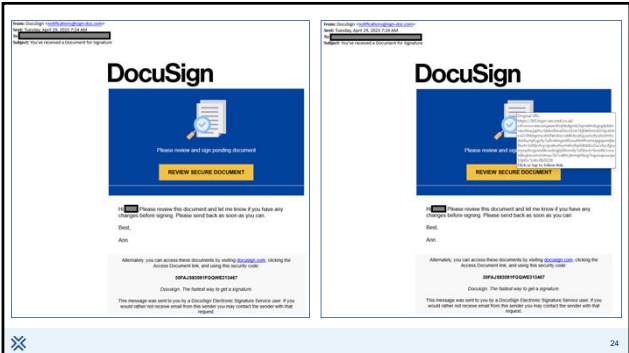
---

---

---

---

---



---

---

---

---

---

---

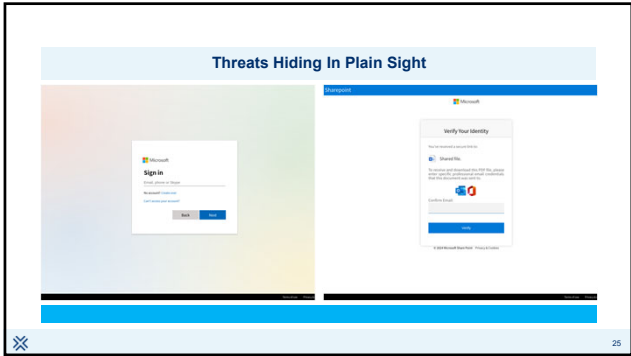
---

---

---

---





---

---

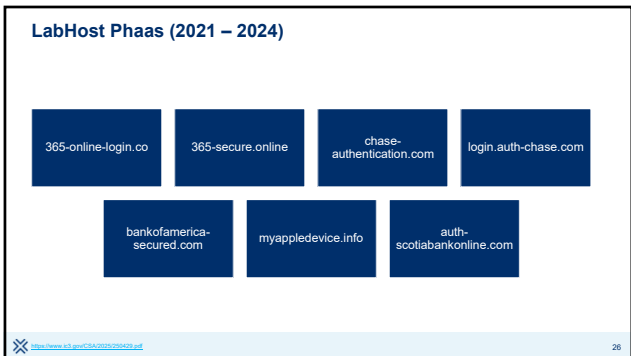
---

---

---

---

---



---

---

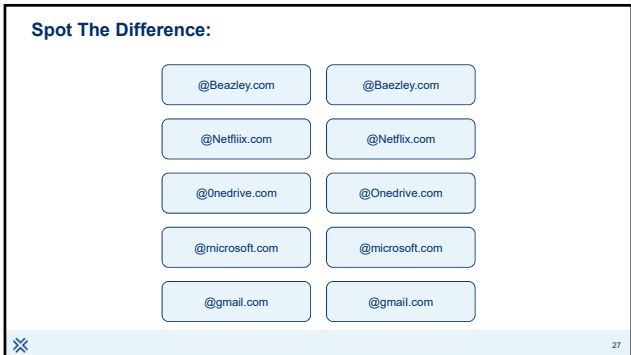
---

---

---

---

---



---

---

---

---

---

---

---

### Phishing of all shapes and sizes:

Urgent or Threatening Language

- 12 Hours to respond
- "Pay Now"
- Threats of registration suspension

Exploitation of Trust

- Purports to be a trusted entity

Creation of a False Sense of Legitimacy

- Convincing but generic website link

12:15

Toll Violation Notice

This is your final notice regarding the unpaid toll balance on your account. You must settle the balance within the next 12 hours to avoid severe penalties.

Unpaid Balance: \$2.57  
Due Date: April 26, 2025

Failure to pay within this time frame will result in the following:

1. Immediate addition of late payment fees to your balance
2. Suspension of your vehicle registration by the Department of Motor Vehicles (DMV)
3. Collection actions, including a negative report to your credit file.

Please make your payment promptly to avoid these severe consequences and protect your driving privileges.

Pay Now:

<https://portal.com-eco.hq.gov>

If the link fails, reply with "Y", eat the SMS, and respond to activate the link, or copy and paste it directly into your browser to complete your payment.

This is your last opportunity. Pay now.

---

---

---

---

---

---

---

---

### Payroll Redirect & Fraudulent Instruction Schemes

Update Banking Information

JB Jonny [redacted] <officemalnet0007@gmail.com>

To [redacted]

🔗 We removed extra line breaks from this message.

Hello [redacted]

I will like to reset my direct deposit information before the nextpay is completed.

What is required?

Regards,  
[redacted]

29

---

---

---

---

---

---

---

---

### Spotting the Issues:

John Doe

PAY TO THE ORDER OF

30

---

---

---

---

---

---

---

---



Incident Response & Business Continuity Planning

---

---

---


---

---

---

---

"If you fail to plan, you are planning to fail!"  
— Benjamin Franklin

32

---

---

---

---

---

---

---

Only 63% of Healthcare organizations have a cybersecurity response plan in place  
[Software Advice's 2024 Healthcare Data Security Survey](#)

33

---

---

---

---

---

---

---


### Incident Response Planning

You Do Not Need To Reinvent The Wheel When Creating An Incident Response Plan (IRP)

**Overlooked Questions:**

- Do you have an Incident Response Plan?
  - Where is it?
  - Who is the first person you contact?
  - How do you contact them?
  - What is your involvement in the IRP?
- Do you have Cyber Insurance?
  - Where is your policy?
  - How do you contact your insurer?
  - Do you have a panel requirement?

There Are Many Tried and Tested IRP templates



Incident Response Plan (IRP) Basics (CISA.gov)

34

---

---

---

---

---

---

---

---

### Incident Response Planning

An incident response plan should ideally include:

Who?	Defined roles and responsibilities to identify who is responsible for each task
What?	A formal definition of a cybersecurity incident, including severity ratings and prioritization protocols
When?	Reporting requirements and contact forms
How?	Documented Communication Protocols

35

---

---

---

---

---

---

---

---

### Incident Response Planning

Who is on your incident response team?

**The Incident Response Team May Be:**

- Legal
- Information Security/Information Technology
- Risk Management
- Communications
- Human Resources
- Privacy Office
- Physical Security
- Business Continuity

**Or It Could Be:**

- Practice Owner
- Practice Manager
- Internal/External IT Manager

Create the team that is right for your organization!

https://www.offensiveonline.com/resources/healthcare-cybersecurity-team/

36

---

---

---

---


---

---

---

---

Business Continuity Planning



just keep  
SWIMMING

How do you keep moving forward during and after a cyber incident?

37

---

---

---

---

---

---

---

---

Business Continuity Planning

Uninterrupted patient care during and after a cyber incident is crucial

Operational Continuity

- What is your ability to see patients without an EMR?
- Do you retain paper records or on-prem backups?
- How can you coordinate scheduling?

Third-Party Dependency

- What aspects of your practice rely on vendors?
- Are most systems with one vendor?

Financial Continuity

- How long can you go without processing claims?
- Do you have easy access to loans or lines of credit?

38

---

---

---

---


---

---

---

---

When To Notify Insurance



---

---

---

---

---

---

---

---

### When To Notify Insurance

**Use your judgement:**

- Does the situation have the potential to result in an insurance claim


**Notify out of an abundance of caution:**

- Untimely reporting may lead to coverage issues
- Notifying out of an abundance of caution is often better than holding onto a claim

**Avoid negative implications of responding on your own:**

- Does your policy have a consent requirement?
- Does your policy have a panel requirement?
- Did you wipe systems and jeopardize a forensic investigation?
- Did you over notify?
- Did you exceed your notification window?

**If you see something, say something!**

40

---

---

---


---

---


---


---

---



**Tyler Longley**  
Assistant Claims Manager  
BPS Cyber & Technology | Claims  
West Hartford, CT  
tyler@brazley.com





---

---

---

---

---

---

---

---