Cybersecurity Update

Vendor Interruptions, Best Practices and Preparation

EXPLORE
HEALTHCARE SUMMIT

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.

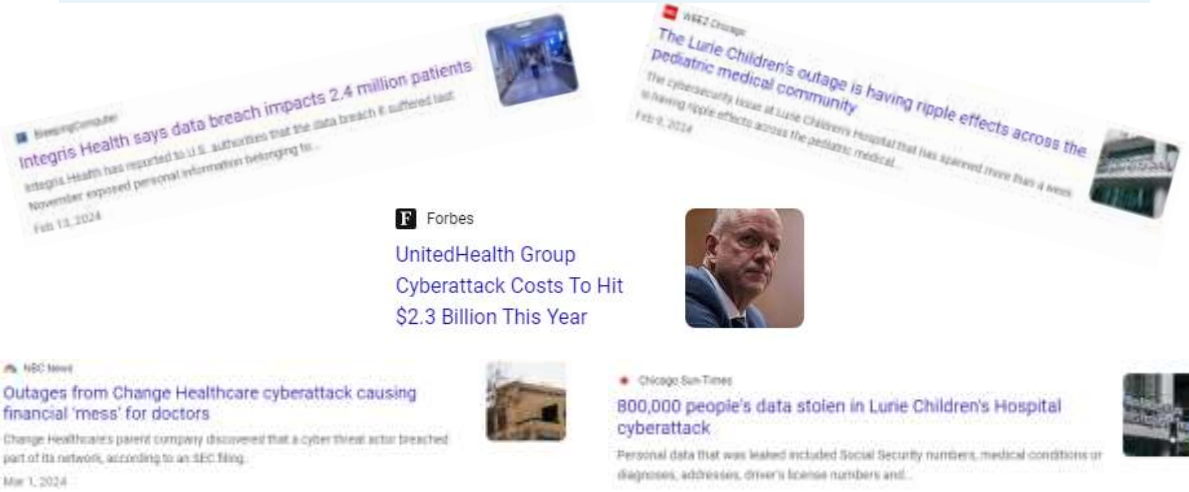
Today's Topics

High-Profile Cyber Incidents	Healthcare Third-Party Vendors
Direct v. Indirect Incidents	
How to Prepare Yourselves	Education & Best Practices Incident Response Planning Business Continuity Planning
When to Notify Insurance	

High-Profile Cyber Incidents

The Year of Vendor Data & Security Breaches

Third-Party vendor incidents stormed the media in 2024



Integris Health

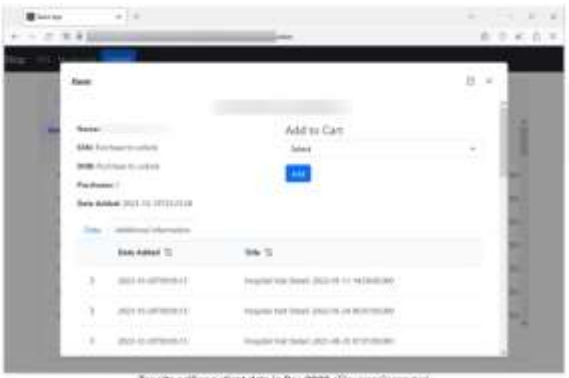
OCR's portal reports 2,385,646 individuals were impacted by the November 2023 Integris Breach

Threat Actor's Offer:

- $50 for "removal" of information
- $3 to view other impacted individual's information

Impacted Information:

- Full Name
- Date of Birth
- Contact Information
- Demographic Information
- Social Security Number (SSN)



Tor site selling patient data in Dec 2023 (BleepingComputer)

Integris Health says data breach impacts 2.4 million patients (BleepingComputer)
Integris Health patients get extortion emails after cyberattack (BleepingComputer)

Ann & Robert H. Lurie Children's Hospital

Rhysida Ransomware disrupts hospital operations and EMR/EHR for partners

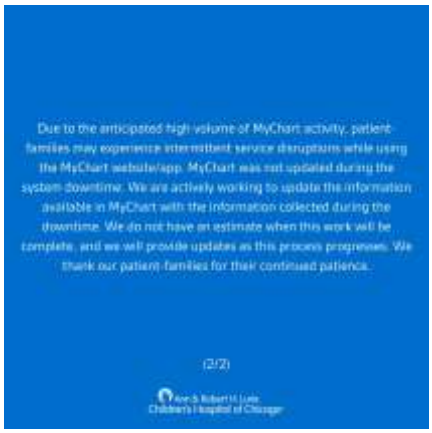
- **January 31, 2024:** A cyberattack was discovered and systems were disrupted including EHR and the MyChart patient portal.
- **February 5, 2024:** Systems were partially restored.
- **February 15, 2024:** Email and Phones restored.
- **February 22, 2024:** Lurie Children's continues operations without access to EHR.
- **March 4, 2024:** Lurie Children's electronic health record platform (Epic) was reactivated.
- **March 14, 2024:** Lurie Children's began reactivating their patient portal (MyChart)

(*Lurie Children's Hospital's X.com account*)

Lurie Children's Hospital of Chicago: Ransomware Attack Timeline (*Cyber Management Alliance*)

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.



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

8

Change Healthcare

ALPHV/BlackCat Ransomware disrupts one of the worlds 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

What We Learned: Change Healthcare Cyber Attack (House Committee on Energy and Commerce); https://solution-status.optum.com/incidents/hqpjz25fn3n7

Change Healthcare

https://www.unitedhealthgroup.com/changehealthcarecyberresponse

Not all large-scale cyber incidents are attacks

CrowdStrike Global IT Outage

International Blue Screen of Death (BSOD) day – July 19, 2024

LaGuardia Airport, New York City ***(Wikipedia)***

Sydney, Australia ***(Stella Qiu, Reuters)***

https://en.wikipedia.org/wiki/2024_CrowdStrike_incident#Healthcare

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.

Fake CrowdStrike repair manual pushes new infostealer malware (Bleeping Computer)

CrowdStrike Global IT Outage

An easy fix in most cases, but a nightmare at scale.

https://beazley.security/alerts-advisories/guidance-support-windows-systems-experiencing-boot-loop-due-to-crowdstrike-update

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 outage hits US hospitals (Healthcare Dive)
4 Things to know About the CrowdStrike IT Outage's Effect on Healthcare (MedCity News)

15

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 19th and July 24th 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

Hospitals Cancel Nonessential Surgeries After Global Technology Outage (New York Times)
Update: Providence response to CrowdStrike outage (Providence)

Direct v. Indirect Incidents

Direct v. Indirect Incidents

Retrieved from https://gastro.org/news/healing-the-healers-understanding-and-addressing-physician-burnout/

What control do you have over the resolution of an incident?

How to Prepare Yourself

Education & Best Practices

You have already taken the first step!

Best Practices

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 Informaiton
8. Use Strong Passwords and Change Them Regularly
9. Limit Network Access
10. Control Physical Access

https://www.healthit.gov/sites/default/files/Top_10_Tips_for_Cybersecurity.pdf

HPH Cybersecurity Performance Goals (CPGs)

HHS partners with CISA to provide support to Healthcare and Public Health (HPH) Critical Infrastructure

Essential Goals

- Mitigate Known Vulnerabilities
- Email Security
- Multifactor Authentication
- Basic Cybersecurity Training
- Strong Encryption
- Basic Incident Planning and Preparedness
- Unique Credentials
- Separate User and Privileged Accounts
- Vendor/Supplier Cybersecurity Requirements

Enhanced Goals

- Asset Inventory
- Third Party Vulnerability Disclosure
- Third Party Incident Reporting
- Cybersecurity Training
- Cybersecurity Mitigation
- Detect and Respond to Relevant Threats and Tactics, Techniques, and Procedures
- Network Segmentation
- Centralized Log Collection
- Centralized Incident Planning and Preparedness
- Configuration Management

The full CPGs and a can be found on the CISA.gov/healthcare page

HHS HPH Cybersecurity Performance Goals

22

Incident Response Planning

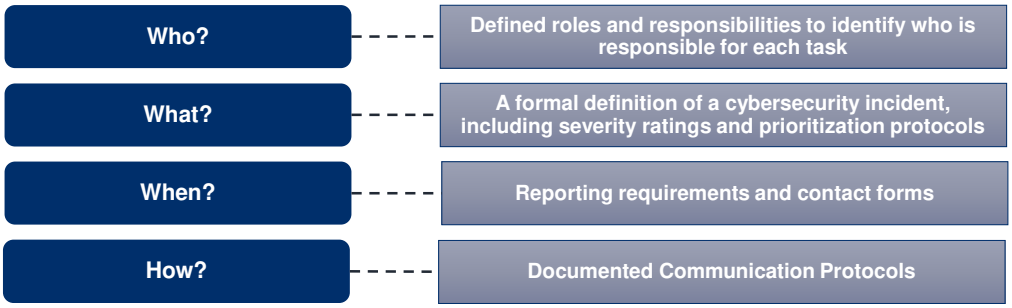
Who are you going to call?

Only 63% of Healthcare organizations have a cybersecurity response plan in place

Software Advice's 2024 Healthcare Data Security Survey

Incident Response Planning

An incident response plan should ideally include:



Incident Response Planning

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

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?

You do not need to reinvent the wheel when creating an IRP. There are many tried and tested IRP templates.

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

Incident Response Planning

Who is on your incident response team?

The Incident Response Team:

May Include the following departments:

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

May only include:

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

Create the team that is right for your organization!

https://www.softwareadvice.com/resources/healthcare-cybersecurity-threat/

Business Continuity Planning

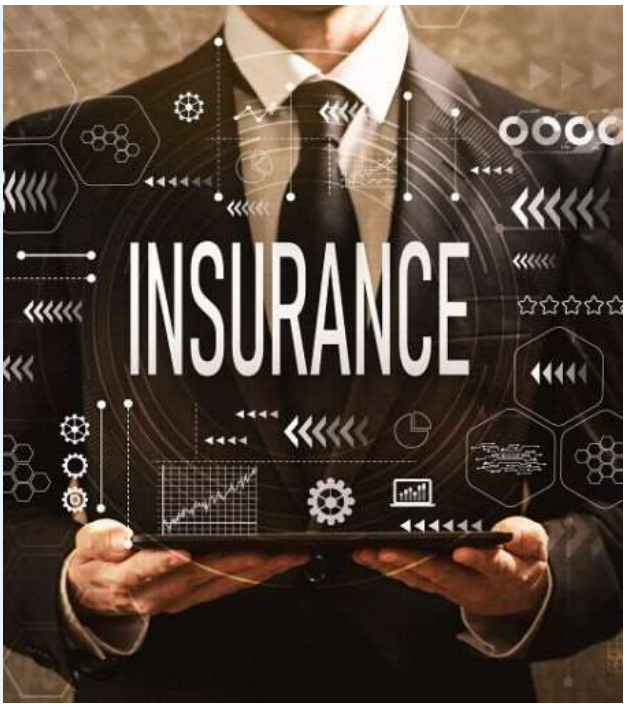
How do you keep moving forward during and after a cyber incident?

Business Continuity Planning

Uninterrupted patient care during and after a cyber incident is crucial

- What is your ability to see patients without an EMR?
- Do you retain paper records or on-prem backups?
- How can you coordinate scheduling?
- What aspects of your practice rely on vendors?
  - Are most systems with one vendor?
- How long can you go without processing claims?
- Do you have easy access to loans or lines of credit?

When To Notify Insurance



When To Notify Insurance

- Use your judgement
- Notifying out of an abundance of caution is always better than holding onto a claim
- Running with Incident Response on your own may have negative implications:
  - Often insureds receive bills and then notify insurance
  - 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!

beazley

Tyler Longley

Beazley Insurance

Assistant Claims Manager – BPS Cyber & Technology

Tyler.Longley@Beazley.com