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

*







The Year of Vendor Data & Security Breaches



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)



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)

-

| | 991 /r | | | |
|--|--------|--|--|--|
| | | | | |
| | | | | |

Ann & Robert H. Lurie Children's Hospital



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
- March 15, 2024: Restoration of electronic
- March 15, 2024: Restoration of electropayment services
 March 25, 2024 to April 21, 2024: Restoration of additional key Change Healthcare products

Delayed or Denied Care Disruption in Pharmacy Services Financial Stress and Unexpected Costs Potential Data Privacy Concerns

Patients: • Inability to Process Claims

The Impact

Providers: Cash Flow Interruptions
 Furloughed Staff
 A Scramble for Loans

-

Change Healthcare

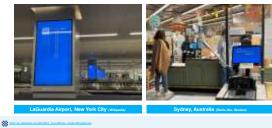
| Table of the local division of the local div | - | and the second second | Conception of the | and the second second | |
|--|--|---|------------------------------|--|--|
| and a second sec | | | an salati san Sruhagai | and the second s | |
| - | Territoria | Company Sector | | | |
| - | Institute to state and state | Lossowick London | | Annual Statement | |
| Address of the other | coloring protocophings | State of Manual Street | manual . | manar . | |
| - | animation of the local division of the local | instante i sense instante i s | Trat, America | a provent of the second s | |
| | | | - | | |
| inter the state | International Avenue of the | Carlo di Scotto | Conception of the local data | Conception of the local division of the loca | |
| | - | | | terroritet t | |
| | | 102210.000.0 | | | |
| | | | | | |

Not all large-scale cyber incidents are attacks

CrowdStrike Global IT Outage

*

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



11

CrowdStrike Global IT Outage

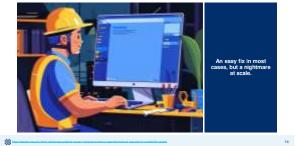
What Happened?

*



13

CrowdStrike Global IT Outage



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
 Perm 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 Global IT Outage

| Kaiser Permanente | Approximately 15,000 servers |
|---|--|
| Providence Henry Ford Health Nationwide Children's Hospital | Approximately 40,000 of 150,000 devices |
| Dana-Farber Cancer Institute RWJBarnabas Health | The Response |
| Emory Healthcare Mass General Brigham Norton Healthcare Penn Medicine Seattle Children's Hospital | 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 cyb | erattack" – Providence CIO, B.J. Moore |



Direct v. Indirect Incidents



18



Education & Best Practices



Best Practices

- 1. Establish a Security Culture

- Establish a Security Culture
 Protect Mobile Devices
 Maintain Good Computer Habits
 Use a Frewall
 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
 Control Physical Access

*

20

HPH Cybersecurity Performance Goals (CPGs)

| Essential Goals | Enhanced 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 | Asset Inventory Third Party Winkerability Disclosure Third Party Unicedent Reporting Opbersecurity Training Opbersecurity Training Detect and Respond to Relevant Threats and Tacitics, Techniques, and Procedures Network Segmentation Centralized Log Collection Centralized Incident Planning and Preparednes Configuration Management |
| The full CPGs and a can be | e found on the CISA.gov/healthcare page |

22

Incident Response Planning



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

ᆋ

Incident Response Planning



Incident Response Planning

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

WHERE IS THE INCIDENT RESPONSE PLAND

ON THE SERVER

26

Overlooked Questions:

*

- Do you have an Incident Response Plan?
- Do you have an Incident Response F 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 re

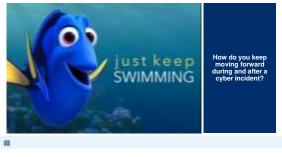
-

Incident Response Planning

| 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 i | s right for your organization! |

ᆋ

Business Continuity Planning



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?
 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

- · Use your judgement
- Notifying out of an abundance of caution is always better than holding onto a claim

If you see something, say something!

- Nothlying out of an abundance of caution is always better than holding onto a cir Running with Incident Response on your own may have negative implications: Often insureds receive bills and then notity 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?

*

beazley **Tyler Longley** Beazley Insurance Assistant Claims Manager – BPS Cyber & Technology Tyler.Lonaley@Beazley.com

