

# Cybersecurity Update

Vendor Interruptions, Best Practices and Preparation




---

---

---

---

---

---

---

---

*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.*

---

---

---

---

---

---

---

---

❖ 2

**Today's Topics**

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

---

---

---

---

---

---

---

---

❖ 3





### Change Healthcare

The screenshot shows a website layout with a grid of service cards on the left and a large solid blue rectangle on the right. The service cards contain text and icons, but the details are difficult to read due to the low resolution. The blue rectangle is a prominent visual element on the right side of the page.

---

---

---

---

---

---

---

---

Not all large-scale cyber incidents are attacks

11

---

---

---

---

---

---

---

---

### CrowdStrike Global IT Outage

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



12

---

---

---

---

---

---

---

---

### 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.



---

---

---

---

---

---

---

---

---

---

### CrowdStrike Global IT Outage



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

---

---

---

---

---

---

---

---

---

---

### 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 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

[Health Care Information Security Alliance: Healthcare Outage Shows How Serious](#)  
[Healthcare Providers Warned to CrowdStrike, says ITWeek.com](#)

16

---

---

---

---

---

---

---

---

---

---

---

---



### Direct v. Indirect Incidents

---

---

---

---

---

---

---

---

---

---

---

---

### Direct v. Indirect Incidents



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

Retrieved from <https://www.shutterstock.com/image-photo/young-woman-physician-consulting>

18

---

---

---

---

---

---

---

---

---

---

---

---



## 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 Information](#)
8. [Use Strong Passwords and Change Them Regularly](#)
9. [Limit Network Access](#)
10. [Control Physical Access](#)

---

---

---

---

---

---

---

---





## Incident Response Planning

An incident response plan should ideally include:

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

---

---

---

---

---

---

---

---



25

## 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.

---

---

---

---

---

---

---

---



26

## 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.safaribooksonline.com/resources/healthcare-cybersecurity-incident-response-plan>

27

### Business Continuity Planning



❖ 28

---

---

---

---

---

---

---

---

### 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?

❖ 29

---

---

---

---

---

---

---

---



### 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!

31

---

---

---

---

---

---

---

---

**beazley**



**Tyler Longley**

Beazley Insurance  
Assistant Claims Manager – BPS Cyber & Technology  
[Tyler.Longley@Beazley.com](mailto:Tyler.Longley@Beazley.com)



---

---

---

---

---

---

---

---