Executive Incident Response Tabletop Exercise

June 20, 2024

Clearwater | 1ST RESPONDER CYBERSECURITY & DIGITAL FORENSICS | JARRARD A CHARTIS COMPANY

Logistics

- All attendees in “Listen Only Mode”
- Please ask content related questions in Q&A
- Recording, final slides, resources will be shared within 48 hours
- Please take a few minutes to provide feedback via survey prompt at the end of this session

Introductions

Today's Team

Baxter Lee
CFO
Clearwater

Dave Bailey
Moderator
VP Consulting
Clearwater

Ricoh Danielson
Founder &
President
1stResponder

Dan Schlacter
Vice President
Jarrard, Inc.

Angie Santiago
Manager,
Consulting
Clearwater

Agenda

- Introductions
- How did we get here?
- Let’s plan a tabletop exercise
- Example Scenario
- Lessons learned/ End of TTX

You asked:

- How can I make this important to administration?
- What are the advantages of a third-party tabletop/simulation over an internal testing program?
- What tools or resources can help me train my team of incident responders and plan for future tabletop exercises?
- Are there updates on Emergency Planning or Medical Emergency Planning that I would need to update our response?

We have to plan for the worst…

BUSINESS

Change Healthcare cyberattack was due to a lack of multifactor authentication, UnitedHealth CEO says

1 of 5 | Andrew Witty, Chief Executive Officer of UnitedHealth Group, testifies at a Senate Finance Committee hearing examining cyber attacks on healt cyber attack, Wednesday, May 1, 2024, on Capitol Hill in Washington. (AP Photo/Jacquelyn Martin)

Nurses at Ascension hospital in Michigan raise alarms about safety following ransomware attack

Jonathan Greig, The Record. May 29, 2024

'It's putting patients' lives in dange ransomware attack is stressing ho operations

Sean Lyngaas, CNN, May 29, 2024

yahoo!finance | Search for news, symbols or co... | Sign in

CISION

Victoria Eye Center/Victoria Surgery Center/Victoria Vision Center Notice of Data Breach

PR Newswire
Fri, May 17, 2024 • 1 min read

VICTORIA, Texas, May 17, 2024 /PRNewswire/ -- Victoria Eye Center/Victoria Surgery Center/Victoria Vision Center ("VEC") is writing to provide information regarding an event that involves certain information relating to personal health information. On March 21, 2024, VEC became aware that certain computer systems in our environment were inaccessible as a result of malicious file encryption. VEC immediately launched an extensive investigation, aided by third party computer forensic specialists, to determine the nature and scope of the event and worked quickly to secure VEC systems, restore access to the information and investigate what happened and whether this resulted in any unauthorized access to information by any unknown actor. Through VEC's investigation, VEC determined that an unknown actor gained access to a limited number of our systems and

Quote Lookup
U.S. markets closed
Customize Your Dock
MARKETS
US | Europe | Asia | Rates

S&P 500	Dow 30
5,360.79	38,868.04
+13.80 (+0.26%)	+69.05 (+0.18%)
Nasdaq	Russell 2000
17,192.53	2,031.61
+59.40 (+0.35%)	+5.06 (+0.25%)
Crude Oil	Gold
78.23	2,328.00
+2.70 (+3.57%)	+3.00 (+0.13%)

MY PORTFOLIOS
Sign in to access your portfolio
Sign in

Somewhere in the world, people are punching into a job, and their job is to attack us. And so you would imagine they have PI (process improvement) and projects and everything else like we do...

—Augie D'Agostino, CISO, UW Medicine

Public Financial Events Put a Target on Organizations

"The FBI assesses ransomware actors are very likely using significant financial events, such as mergers and acquisitions, to target and leverage victim companies for ransomware infections."

– *FBI Private Industry Notification*
https://www.ic3.gov/Media/News/2021/211101.pdf

"The healthcare industry has become a corporate entity, a corporate structure, and a corporate ecosystem that engages in mergers and acquisitions, and it's in those mergers and acquisitions—in the cracks—where we find some vulnerabilities."

—Kemba Walden, Former Acting National Cyber Director

Source: https://meritalk.com/articles/walden-healthcare-cyber-attacks-beg-congressional-action/

A breach changes the long-term trajectory & value of a business

- Ransomware payment
- Regulatory fines and penalties
- Legal expenses
- Loss of revenue from downtime
- Recovery cost/ increased IT investments
  - Ex: Change Healthcare is rebuilding its systems from the ground up
- Reputational harm
  - The average cost of loss of business from a breach is $1.3M

(Source: IBM Cost of a Breach Report)

A breach or inadequate response to a cyber incident can quickly derail a transaction and negatively impact the value of a healthcare organization.

Incident response planning and testing is one of the top 3 **most effective cost mitigators** in a breach.

Source: 2023 IBM Cost of a Breach Report

Source: Health Leaders Media

Today's Exercise

- This is a **45 minute** exercise: Cyber Extortion and Data Exfiltration.
- The scenario runs in stages as indicated in the table to the right.
- Information provided throughout the scenario is presented through **scenario injections.**
- After some scenarios/injections, you'll be asked a poll question.
- Ask questions! (in the Q&A)
- **There are no wrong answers!**

Tabletop Scenario	Description
Rules of Engagement	Overview of the rules during the exercise
Organizational Intent	What is the organization's intent, and why it is important during an exercise?
Scenario Primer	Background and setup
Injection 1	First element of the scenario
Discussion 1	Discussion of the first element
Injection 2	Second element of the scenario
Discussion 2	Discussion following the second element
Injection 3	"
Discussion 3	"
Recap	Wrap up, and larger scope questions

Objectives

Cyber Crisis Management	Ensuring that the hospital has the approached and allotted ability, process and technology to handle crisis management
BCDR Validation	Validation of BCDR process and plan
Data Exfiltration	Validation of Data exfiltration process and plan
Ransomware readiness	Assessing the hospital's ransomware readiness
Ransomware negotiation readiness	Assessing ransomware negotiations readiness and preparedness

See Appendix A for more detailed information

The Scenario

Injection #1 : CISO SITREP – Cyber Crisis Management

Thursday, 9:45 AM

A threat actor has reached out to the hospital via email and stated that they have the hospital data and will be posting the information on the dark web.

To add to the unsetting news, the threat actor informs them that a ransom note can be found on a critical device. The notification causes chaos, and the situation is immediately escalated to the CISO

The CISO takes immediate action and tasks the information security team to conduct threat hunting to determine if the threat actors' email was legitimate and to locate the ransom note.

Findings:

After a thorough investigation by the CISO and his security team, the ransom note was located, and it is deemed that the threats are authentic.

Time for a Poll

Injection #1 – Discussion Questions

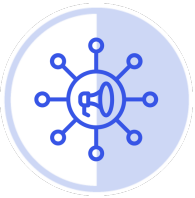
What role does threat hunting play in validating the legitimacy of the threat and identifying potential indicators of compromise?

How do executives interpret the identified IOCs and TTPs presented in the threat actor's communication?

What are the foreseeable implications of the ransomware threat on the hospital's operations, patient care, reputation, and financial stability?

How will the CISO effectively assess the credibility of the threat actor's claims and determine the severity of the situation?

What are the primary and secondary concerns stemming from the threat actor's claims and the potential presence of ransomware within the hospital's network?



Does the threat actor's email and ransom note provide sufficient evidence, Indicators of Compromise (IOCs), Tactics, Techniques, and Procedures (TTPs), and actionable information to warrant any level of alert, event, incident, or compromise classification?

Who needs to be invited to the table to address the ransomware threat and participate in decision-making and response efforts?

Looking ahead, which key stakeholders, both internal and external, need to be promptly notified about the ransomware threat and its potential implications?

What teams need to be stood up or activated to effectively respond to the ransomware incident and support the organization's cybersecurity and BCDR efforts?

How can the hospital ensure the integrity and availability of critical data and systems while responding to the ransomware threat?

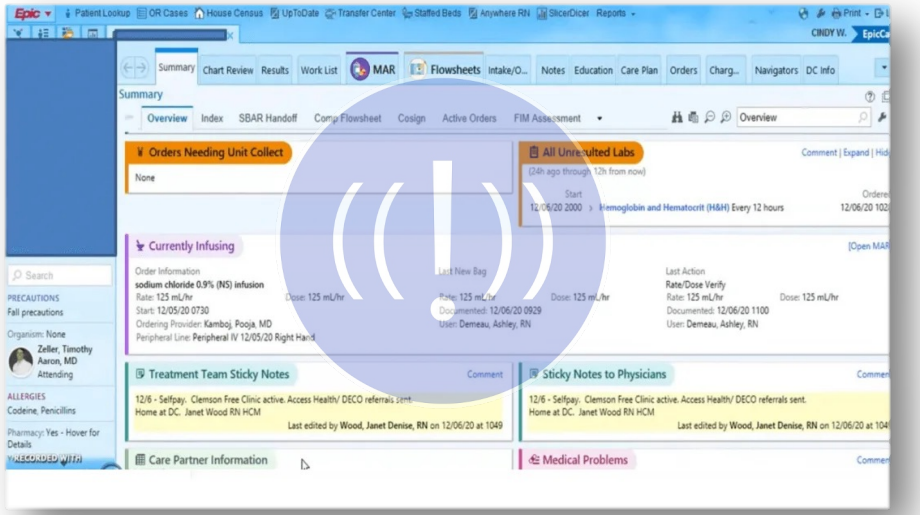
Are there any legal implications or regulatory considerations that the hospital needs to consider when responding to the ransomware threat and communicating with stakeholders?

Time for a Poll

Clearwater | 1STRESPONDER CYBERSECURITY & DIGITAL FORENSICS | JARRARD A CHARTIS COMPANY

Injection #2 – CISO SITREP – BCDR Update

Time for a Poll



Thursday, 10:15 AM Event Escalates

Unfortunately, the threat actor didn't provide all the details to the hospital. Upon review of the ransom note, the CISO and information security team discover that the threat actor has exfiltrated data from the EPIC system along with the database.

During this time, the information security team is informed by the information technology team that they are receiving notifications that the EPIC system and phone lines are not working for departments at the hospital.

It is now confirmed that there is a complete outage in the hospital and the CISO needs to make an executive decision on next steps.

Findings:

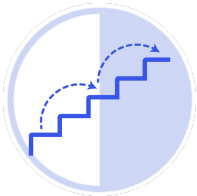
The information security team has begun their investigation to determine if data has been exfiltrated; with systems down, it is likely. This data comprises of Protected Health Information (PHI), such as medical charts and patient records and other Personally Identifiable Information (PII).

Injection #2 – Discussion Questions

Given the information provided by the threat actor, how should command and control decision-making be structured to effectively respond to the situation?

At what stage is the organization in its Incident Response Plan (IRP) and process, and what immediate actions need to be taken to contain the breach, restore system functionality, and mitigate further damage?

Does the hospital have a pre-defined strategy and criteria for evaluating whether to comply with the threat actor's demands, considering the potential consequences and ethical considerations of paying ransom?



As executives, what steps should be taken to validate the credibility and severity of the threat message, considering the potential impact on critical hospital systems and patient data?

What decisions, responsibilities, and processes are in place for promptly notifying and engaging Beazley, the cyber insurance provider, to initiate the claims process and access support services?

Is there a comprehensive plan in place for coordinating communication and negotiations with the threat actor, as well as managing other related activities such as legal, regulatory, and public relations efforts?

Considering the confirmed cyber attack and outage affecting the EPIC system and phone lines, how does this impact the assessment of operational impact and the prioritization of response efforts from an executive level?

Are there any additional third-party cybersecurity firms or legal advisors that should be called in to provide specialized expertise and assistance in responding to the cyber attack and managing potential legal and regulatory implications?

Injection #3 – CISO SITREP - Data Exfiltration

Time for a Poll!

Thursday, 4:10 PM Escalation

The CISO and his security team has confirmed that network traffic packet sizes align with the threat actor's claim of data exfiltration.

With the systems being down and services being disrupted, the local news outlets are now seeking comments from the hospital regarding the ongoing incident.

To add to the criticality of the situation, federal agencies have reached out via email to discuss the threat actor's Indicators of Compromise (IOCs) and Tactics, Techniques, and Procedures (TTPs), indicating a heightened level of concern and interest in the incident.

Findings:

Data exfiltration of PHI, and PII has officially been confirmed. Executives must determine the best steps to take as local news outlets and federal agencies are involved.

Injection #3 – Discussion Questions

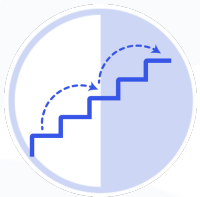
Given the severity of the incident and the potential data exfiltration, how does this impact the decision-making process regarding whether to comply with the threat actor's demands for ransom payment?

Considering the sensitivity of the situation, what key messages need to be conveyed to external parties, and how should they be communicated to maintain transparency and manage expectations?

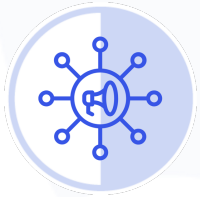
Are downtime procedures and contingency plans in place for all departments and business functions to mitigate the impact of system outages and disruptions?

With the EPIC system and phone lines down and services disrupted, how is the hospital ensuring continuity of care and providing essential services to patients?

How is the hospital gathering and maintaining situational awareness regarding the status of critical systems, infrastructure, and business functions affected by the incident?



Given the severity and criticality of the incident, should any specific response plans or protocols be activated at this time, and what are the key considerations for implementing them effectively?



What communication strategies and channels are being utilized to effectively communicate with partners, third-party vendors, and stakeholders regarding the incident?

Injection #4 – Ransomware Readiness

Friday 10:30 to 11:30 AM

As a precautionary measure, third-party partners have terminated their connections following repeated connection failures and rumors circulating about a potential cyber attack.

With local news gathering, a reporter from KATV ABC 7 News states they received a tip regarding a cyberattack on the hospital and seek confirmation.

Additionally, a local FBI field agent arrives onsite at the hospital due to the IOCs and TTPs provided. The FBI field agent stated that they have been monitoring this threat group's activities. The FBI offers their assistance to help the hospital handle the incident.

Furthermore, the FBI is initiating their own investigation into the attack and has requested cooperation from the hospital. This includes providing a designated work area, access to physical space, information systems, infrastructure, etc.

Findings:

Data exfiltration of PHI, and PII has officially been confirmed. Executives must determine the best steps to take as local news outlets and federal agencies are involved. the hospital is informed by the FBI that the threat actor group is called the Daixin Team aka Holiday Spider.

Injection #4 - Discussion Questions

How does the termination of third-party connections impact the hospital's ability to respond effectively to the potential cyber attack, and what measures should be taken to mitigate the disruption caused by this precautionary measure?

In light of the FBI's involvement and offer of assistance, what steps should the hospital take to coordinate with law enforcement agencies and leverage their support in handling the incident, particularly in terms of threat intelligence sharing and collaboration on the investigation?

Considering the request for cooperation from the FBI, what logistical and operational challenges may arise in providing access to physical space, information systems, and infrastructure, and how can the hospital effectively address these challenges while maintaining security and confidentiality?

How should the hospital effectively communicate with the local news outlet and respond to inquiries from the reporter regarding the rumored cyber attack, while ensuring transparency and maintaining control over the dissemination of information?

What are the potential implications of the FBI's investigation on the hospital's incident response efforts, and how should the organization adapt its BCDR and IR plans to accommodate the involvement of law enforcement and ensure compliance with any legal or regulatory requirements?

Given the disruption caused by the cyber attack, including the downtime of the EPIC EHR system and phone lines, how can the hospital effectively leverage cross-functional collaboration between IT, clinical staff, executive leadership, and external partners such as the FBI and third-party IR firm to ensure continuity of patient care, communication, and incident response efforts while mitigating the impact of the attack?

Injection #5 – Ransom Negotiation

Sunday 11:30 AM

Amidst the chaos caused by the Daixin Team, the executive team at the hospital realizes the urgent need to bolster their ransomware readiness and BCDR capabilities. With the EPIC system and phone lines still down, the hospital's ability to provide critical patient care and communication remains severely impacted.

In response to the escalating crisis, the executive team decides to enlist the expertise of an Incident Response (IR) firm, Kroll, to assist in handling the threat actor and mitigating the damage caused by the ransomware attack.

Additionally, the FBI's involvement in the investigation provides valuable support, enhancing the hospital's incident response capabilities and facilitating collaboration between law enforcement and the hospital.

Findings:

The decision to engage an external IR firm, demonstrates the need for specialized expertise and resources to effectively respond to the cyber attack.
The involvement of the FBI in the investigation showcases the importance of collaboration between law enforcement agencies and healthcare organizations in combatting cyber threats.

Injection #5 – Discussion Questions

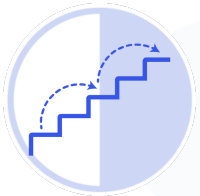
Time for a Poll!

What specific roles and responsibilities should be assigned to internal teams, external partners such as Kroll, and law enforcement agencies like the FBI to ensure a coordinated and effective response to the cyber incident while minimizing further disruption to hospital operations?

What communication strategies and protocols should be implemented to keep stakeholders informed and engaged throughout the incident response process, particularly given the ongoing challenges with the EPIC system and phone lines?

How does the collaboration between the hospital, Kroll, and the FBI exemplify the importance of leveraging external expertise and resources in responding to cyber incidents, and what strategies can the hospital employ to strengthen partnerships with external stakeholders for enhanced incident response capabilities in the future?

How can the hospital leverage the expertise of Kroll and the investigative resources of the FBI to identify and mitigate the damage caused by the ransomware attack, including containment of the threat, restoration of systems, and preservation of evidence for forensic analysis?



How can the executive team at the hospital effectively prioritize and allocate resources to bolster their ransomware readiness and BCDR capabilities in response to the cyber attack, considering the ongoing impact on critical patient care and communication channels?

Injection #6 – Payment Decision

Based on the results of the poll the decision to pay the threat actor is ….

Data Published	Booby Traps	Unavailable Services	Recovery and Restoration	Third-Parties
the hospital data was published to KATV News and to the dark web.	Booby traps went off when the timer expired.	Telephone system, internet services, and access to data center are still unavailable.	Partial restore of communication and network infrastructure could take 2 to 3 weeks	They will not re-establish their connections until the hospital can formally demonstrate the environment is free and clear of any threats.
Patient complaints are being received.	Some did nothing. Others shut down other parts of the network.		System rebuild requires at least 4 weeks.	
	Control tools remain within the the hospital environment.		It will take at least 3 weeks to identify what backup files to restore from and verify data is clean.	
	There may be other hidden, dormant booby traps.		There is not enough the hospital staff to do all this.	
	Until these are addressed, recovery activities will be hampered.			

Summary & Hotwash

Technical Exercise: Hotwash/After Action Review

- Consider the following questions about your team's response:
  - **Incident Response Plan (IRP):** Was the Incident Response Plan invoked during the exercise? When was it last updated, and was it effectively followed during the tabletop exercise?
  - **Playbooks and Processes:** What playbooks, processes, and methods were utilized by your team in response to the simulated event? How effective were these resources in guiding your response actions?
  - **Collaboration with Agencies:** What level of collaboration was exchanged with external agencies, such as CISA, FBI, and other relevant entities, during the tabletop exercise? How well did this collaboration facilitate information sharing and coordinated response efforts?

Q&A

We are here to help.

Moving healthcare organizations to a more secure, compliant, and resilient state so they can achieve their mission.

Clearwater

Healthcare – Secure, Compliant, Resilient

www.ClearwaterSecurity.com

800.704.3394

LinkedIn | linkedin.com/company/clearwater-security-llc/

Legal Disclaimer

Although the information provided by Clearwater Security & Compliance LLC may be helpful in informing customers and others who have an interest in data privacy and security issues, it does not constitute legal advice. This information may be based in part on current federal law and is subject to change based on changes in federal law or subsequent interpretative guidance. Where this information is based on federal law, it must be modified to reflect state law where that state law is more stringent than the federal law or other state law exceptions apply. This information is intended to be a general information resource and should not be relied upon as a substitute for competent legal advice specific to your circumstances. YOU SHOULD EVALUATE ALL INFORMATION, OPINIONS AND RECOMMENDATIONS PROVIDED BY CLEARWATER IN CONSULTATION WITH YOUR LEGAL OR OTHER ADVISOR, AS APPROPRIATE.

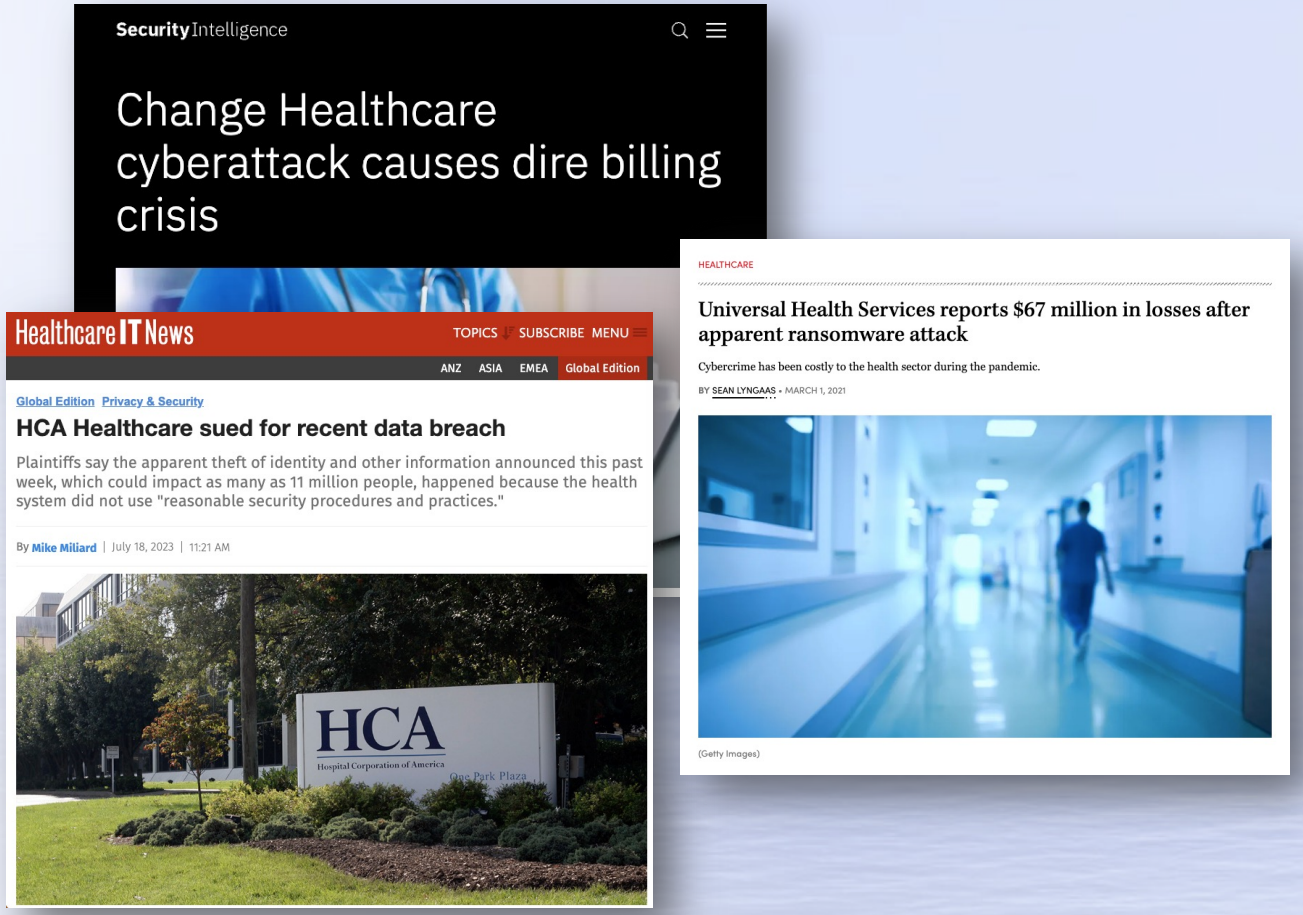
Copyright Notice

*The existence of a link or organizational reference in any of the following materials should not be assumed as an endorsement by Clearwater Security & Compliance LLC.

Appendix A

Cyber Crisis Management

- Cyber Crisis Management is on the rise due to several factors:
  - Increasing Cyber Threats (e.g., ransomware, supply chain)
  - Value of Data
  - Expanding Attack Surface (e.g., third-party connections, cloud environments)
  - Remote Work/Hybrid Environments
  - Regulatory/Compliance Requirements

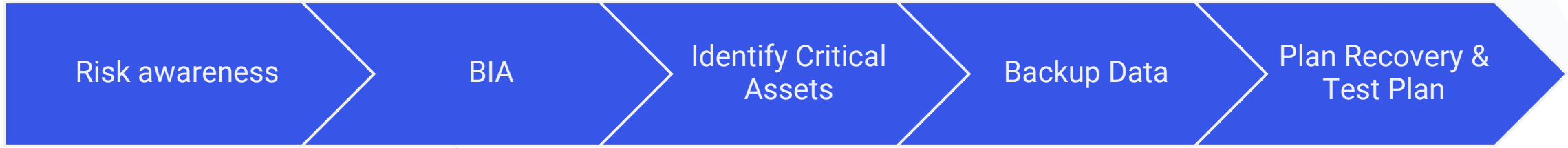


Preparedness → Detect → Analyze and Contain → Eradicate and Recover → Lessons Learned

Ransomware BCDR Validation

- Backup and Disaster Recovery (BCDR) validation is critical, particularly in ransomware incidents.
- Threat actors often target backups as a primary objective during cyberattacks.
- Compromised backups significantly hinder recovery efforts and exacerbate the impact of cyber incidents.
- The integrity and accessibility of backup data directly influence the speed and success of recovery.
- Validating and fortifying the BCDR strategy is essential to ensure timely recovery and mitigate the consequences of ransomware attacks.

Ransomware attacks can lead to an enterprise-wide system outage with the inability for a healthcare firm to recover. Thus, a BCDR plan is critical.



Data Exfiltration

Social Engineering & Phishing Attacks

Outbound Emails

Downloads to insecure devices

Uploads to External Devices

Human Error and Non-Secured Behaviour in the Cloud

Means of Exfiltration	Tool Circumvention	Network
• Leverage privileged accounts. • Un-noticed/unapproved applications.	• DLP tools frequently fail to detect exfiltration.	• Often, firms lack the proper rules, alerting, or logging mechanisms to detect network exfiltration traffic.

Ransomware Negotiation