Incident Response Table Tops

HIMSS CENTRAL & SOUTHERN OHIO Chapter

Agenda

- Introductions
- SecureState overview
- Need for improved incident response capability
- https://pollev.com/securestate
- Overview of the exercise:
  - Sample incident response table top
- What your team should learn and your board should know

Introductions

- **Anthony Catalano** – Associate Director, Management Consulting
  - Healthcare and Technology Industries Owner
  - 12 Years in Information Technology, 5 in Cyber Security
  - CISSP, PCI QSA, HITRUST CCSFP

- **Ty Smith** – Associate Management Consultant
  - Oversaw multiple Incident Response Tabletops at a Top 5 healthcare system
  - Battalion Staff Officer (S6), Ohio National Guard

CISSP® Certified Information Systems Security Professional

PCI Security Standards Council™ QUALIFIED SECURITY ASSESSOR

HITRUST CSF Certified

HIMSS® CENTRAL & SOUTHERN OHIO Chapter

Established in 2001, SecureState is a management consulting firm specializing in risk management in information security.

HITRUST
Health Information Trust Alliance
NETWORK PRODUCTS GUIDE HOT COMPANIES & TECHNOLOGIES 2013 FINALIST
x2
Inc. 5000
x4
NEO SUCCESS AWARDS
x5
North Coast 99
x5
WEATHERHEAD 100 2014
x6
Info Security Products Guide 2012 GLOBAL EXCELLENCE AWARDS
x1

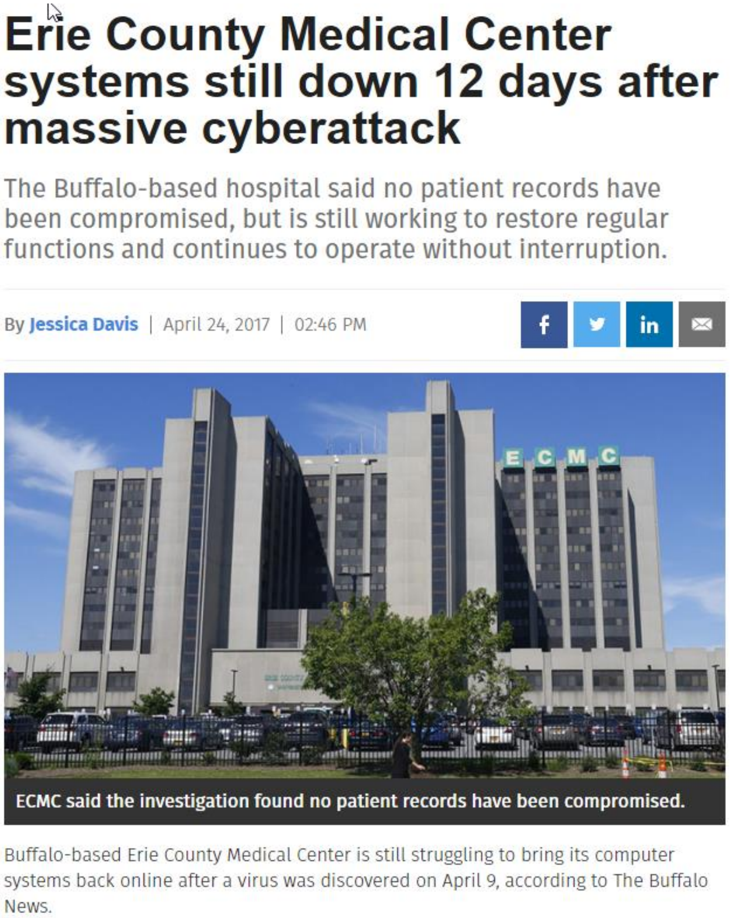
Need for Improved Incident Response Capability

- **Major Cyberattacks On Healthcare Grew 63% In 2016**
  - Some 93 major cyberattacks affected major healthcare organizations this year, up from 57 in 2015
  - Among the largest attacks were those on Banner Health (3.6M records), Newkirk Products (3.4M records), 21st Century Oncology (2.2M records), and Valley Anesthesiology Consultants (0.88M records)
- **Stolen records are sold on the black market from $1.50 to $10 each.**
  - Due to the volume of records available, the price per record has recently dropped ($500-$1000 per record)
  - The falling price for stolen records is pushing scammers to try to monetize their efforts in other ways, like ransomware-based attacks.

Ransomware

“Ransomware is the single biggest threat to healthcare data security according to a recent report. This revealed that around 50 percent of data security incidents from October 2015 to September 2016 stemmed from healthcare ransomware attacks.

The NTT Security 2017 Global Threat Intelligence Report showed that healthcare also contributed to nearly three-quarters of ransomware attacks globally. Healthcare, professional services, government, and retail together accounted for 77 percent of ransomware attacks.”



Erie County Medical Center systems still down 12 days after massive cyberattack

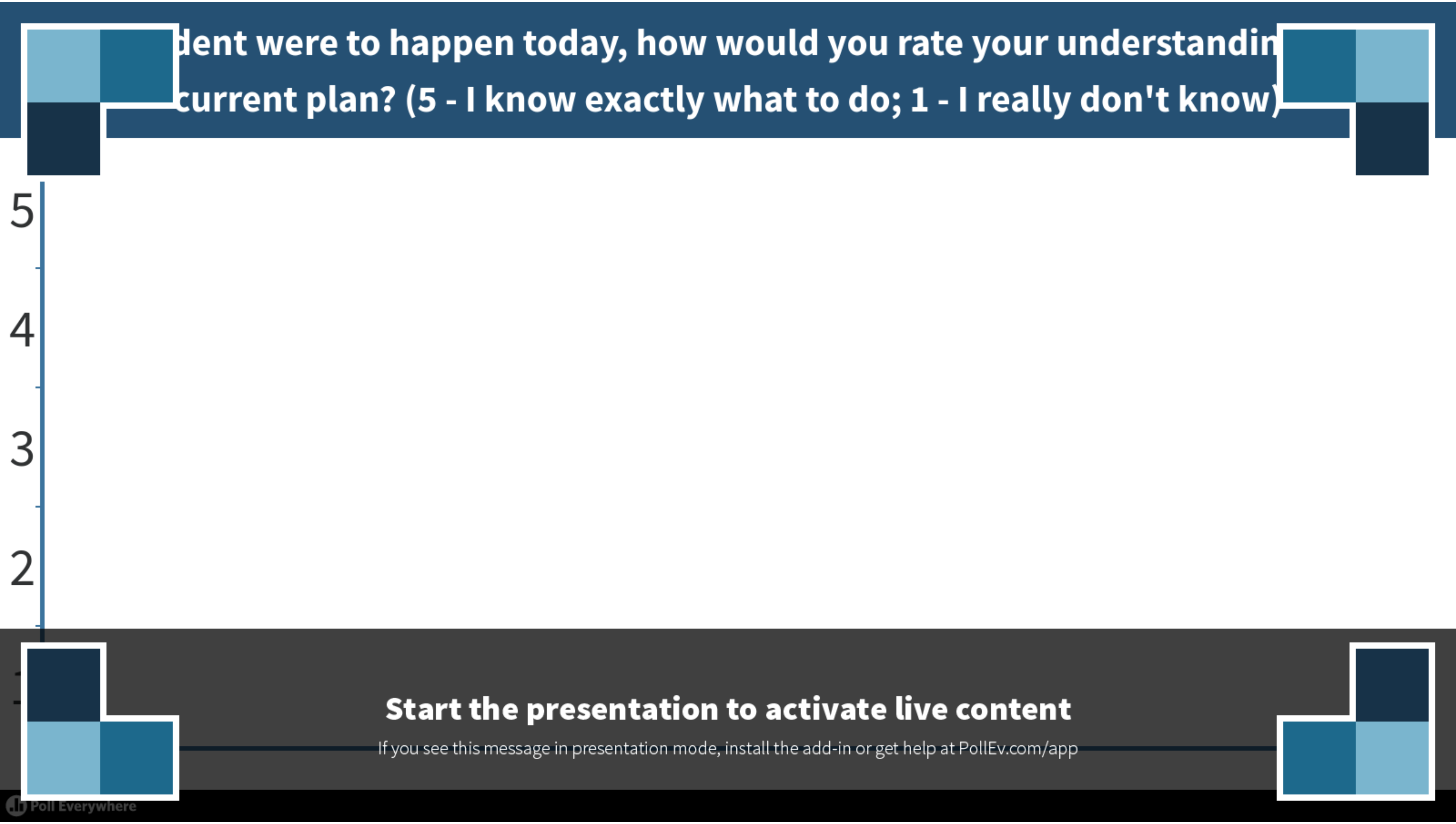
The Buffalo-based hospital said no patient records have been compromised, but is still working to restore regular functions and continues to operate without interruption.

By Jessica Davis | April 24, 2017 | 02:46 PM

ECMC said the investigation found no patient records have been compromised.

Buffalo-based Erie County Medical Center is still struggling to bring its computer systems back online after a virus was discovered on April 9, according to The Buffalo News.

*http://www.healthcareglobal.com/technology/2220/Ransomware-single-biggest-threat-to-healthcare-data-security



dent were to happen today, how would you rate your understandin
current plan? (5 - I know exactly what to do; 1 - I really don't know)

Start the presentation to activate live content

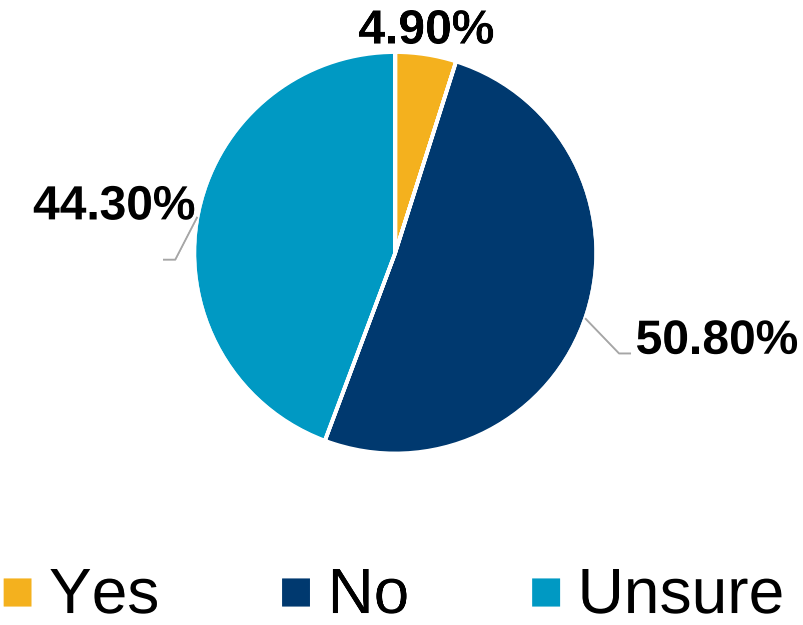
If you see this message in presentation mode, install the add-in or get help at PollEv.com/app

Replace text box with chapter logo

Ransomware

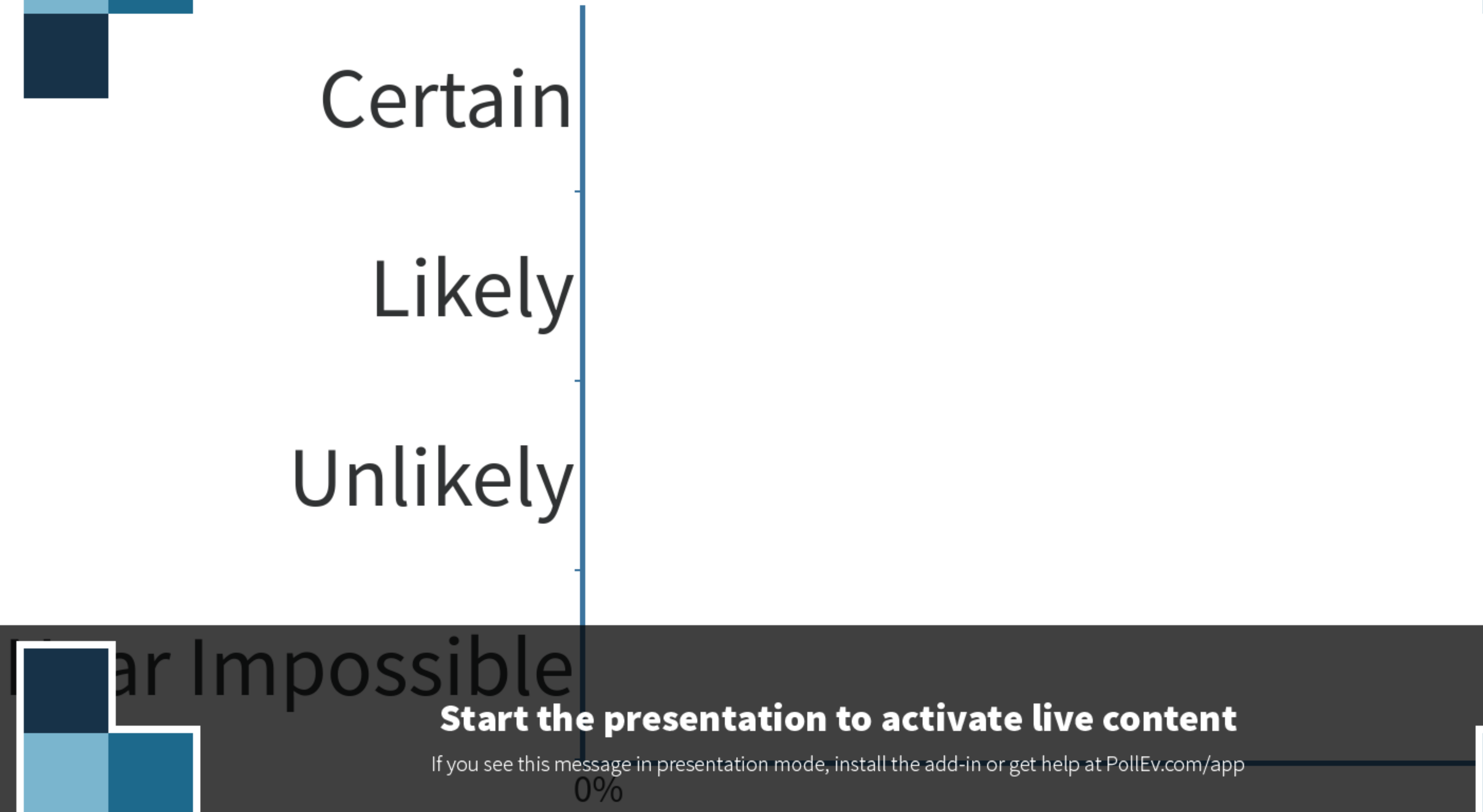
- As many as 75 percent of U.S. hospitals responding to a poll could have been hit with ransomware in the last year, and a chunk of those might not even know it.
  - The average time for detecting a breach is around 200 days

If hackers encrypted your hospital's patient data would you pay the ransom to get it back?

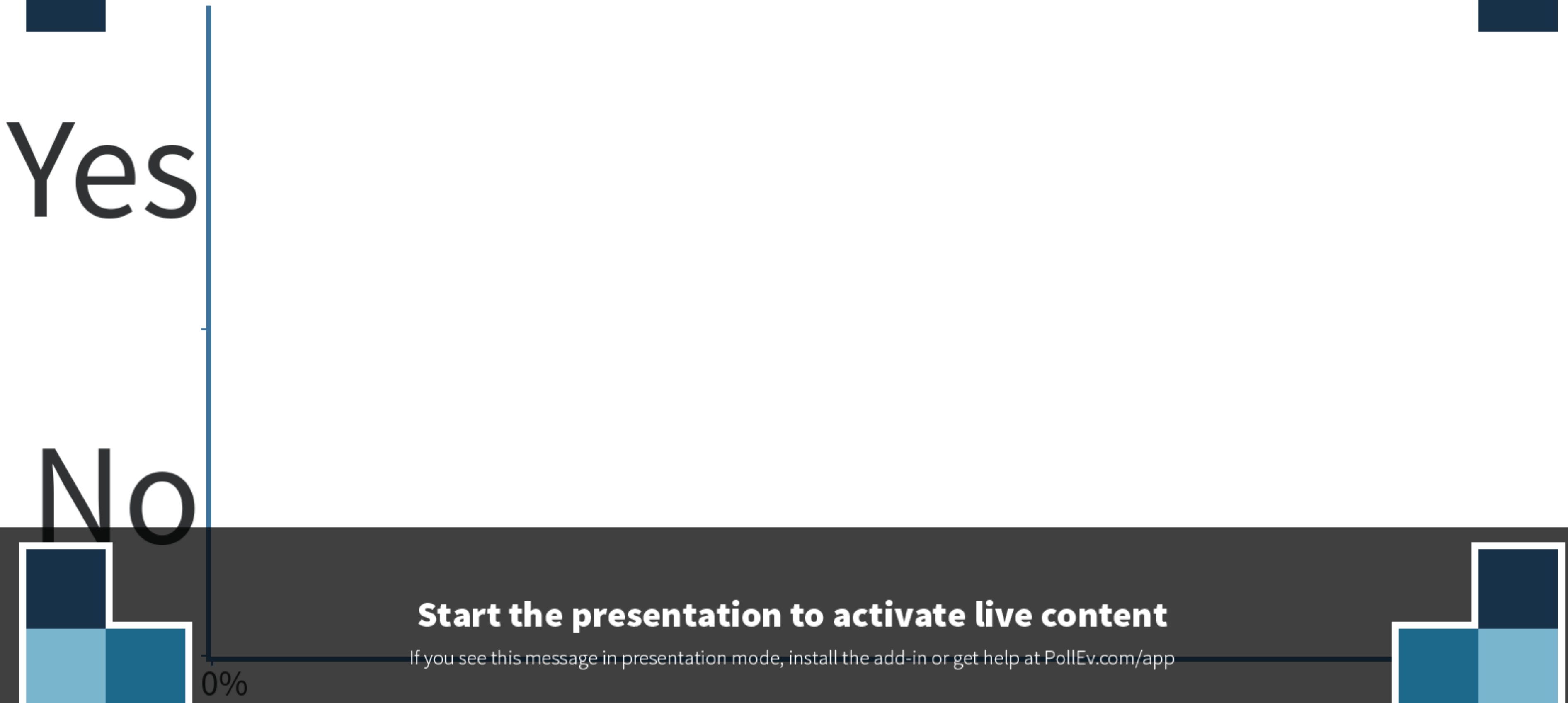


http://www.healthcareitnews.com/news/more-half-hospitals-hit-ransomware-last-12-months

likely do you think a successful ransomware attack is at your locat



lecision were up to you, would you pay a ransom (roughly $20,000) access back to data?



Start the presentation to activate live content

If you see this message in presentation mode, install the add-in or get help at PollEv.com/app

IR Tabletop – What is it and Why

- An IR Tabletop exercise is the process of simulating an event to develop a high-level understanding of current cybersecurity processes, and how information, alerts, and communication traverses the environment.
- This exercise becomes a critical success factor in the development and maintenance of a comprehensive, integrated, and security-focused response plan.

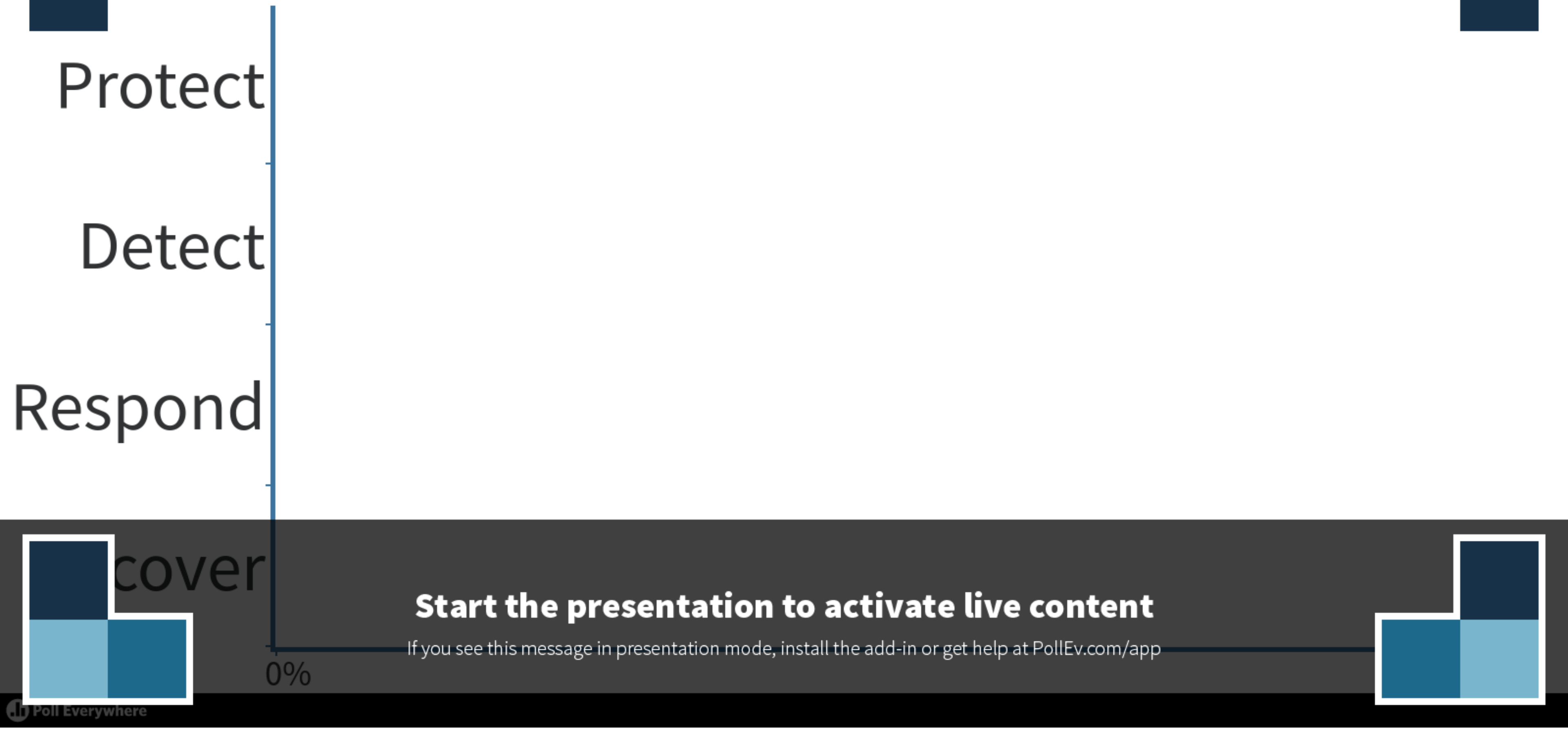
What does an IR Tabletop session look like?

- Typically, each step of the tabletop process is aligned with the **NIST Cyber Security Framework (CSF)** for Incident Response.
  - They differ from IR tests, which focus on observing personnel during a live incident, such as a penetration test.
- **INJECTS** are specially crafted variables that affect the scenario by changing or evolving it entirely, or causing the exercise to spawn in different directions.
- The tabletop will test the organization's ability to classify incidents based on severity and impact, notify the appropriate individuals, collect artifacts, escalate the event when necessary, and respond from both a technical and organizational perspective.

IR Tabletop - Goals

- Tabletop exercises are an effective method for testing incident response (IR) plans and processes via simulated real-world events and facilitated discussions. The tabletop session should cover:
  - Understand the role of Security and their interaction with other parts of the organization
  - Understand the importance of emergency response procedures from all groups within an organization (IT, Legal, HR, Marketing)
  - Provide insight into response capabilities to a Ransomware or other “real world” situation
  - Discuss overall effectiveness of internal/external communications

at do you think is the most important phase in the incident respor methodology?



Start the presentation to activate live content

If you see this message in presentation mode, install the add-in or get help at PollEv.com/app

Foundation Methodology

- **Pre-Assessment Phase:**

  Identification Phase: Assess the organizational understanding of how to manage cybersecurity risk to systems, assets, data and capabilities. Examples within this phase include the assessment of security and response plans.

  - Asset Management; Business Environment; Governance; Risk Assessment; and Risk Management Strategy.

  Protection Phase: Assess the development and implementation of appropriate controls to ensure deliver of response services.

  - Access Control; Awareness and Training; Data Security; Information Protection Processes and Procedures; Maintenance; and Protective Technology

- **Fieldwork Phase:**

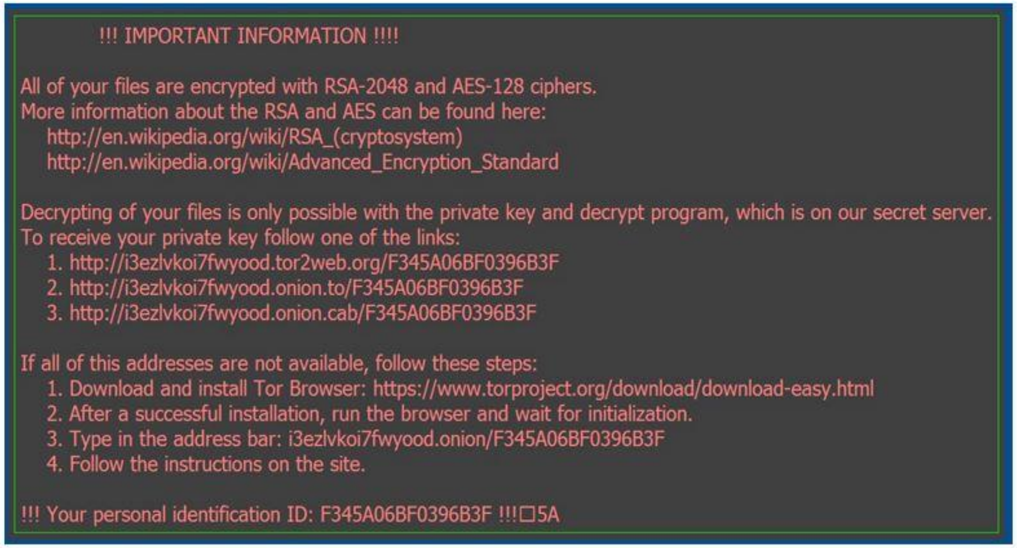
  Detection Phase: Assess how the organization implements the appropriate actions to identify the occurrence of a cybersecurity event.
  Respond Phase: Assess how the organization takes action once an incident is validated.
  Recover Phase: Assess how the organization maintains plans for resiliency and to restore business operations affected by cybersecurity incidents.

Table Top Exercise

Scenario Information

Detect

- **Time:** 10:07am
- **Event:** Help desk ransomware call
- **Description:** At 10:07am John Doe calls the help desk stating that there is a ransomware note on his screen. He was recently browsing a popular social networking site just prior to receiving the notice. At first he thought it was an advertisement, but now he cannot get it to close.



```
          !!! IMPORTANT INFORMATION !!!!

All of your files are encrypted with RSA-2048 and AES-128 ciphers.
More information about the RSA and AES can be found here:
   http://en.wikipedia.org/wiki/RSA_(cryptosystem)
   http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

Decrypting of your files is only possible with the private key and decrypt program, which is on our secret server.
To receive your private key follow one of the links:
   1. http://i3ezlvkoi7fwyood.tor2web.org/F345A06BF0396B3F
   2. http://i3ezlvkoi7fwyood.onion.to/F345A06BF0396B3F
   3. http://i3ezlvkoi7fwyood.onion.cab/F345A06BF0396B3F

If all of this addresses are not available, follow these steps:
   1. Download and install Tor Browser: https://www.torproject.org/download/download-easy.html
   2. After a successful installation, run the browser and wait for initialization.
   3. Type in the address bar: i3ezlvkoi7fwyood.onion/F345A06BF0396B3F
   4. Follow the instructions on the site.

!!! Your personal identification ID: F345A06BF0396B3F !!!□5A
```

Detection

- How would this alert be detected and reported in your organization?
  - Are we confident in our alerting, logging, and reporting structure?

Impact

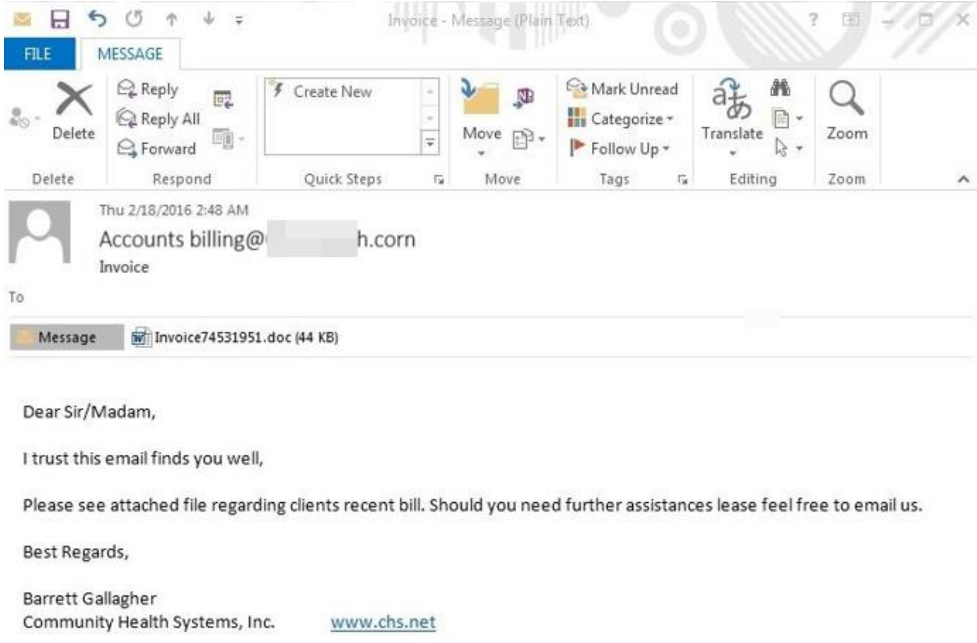
- What type of data does this employee have access to?
- What is the employee’s organizational role?
- Is there a risk of spreading or pivoting throughout the environment?
- Are any files accessible?

Event Notification

- Is the business owner/manager notified?
- Who else is initially notified of the event?
- How are notifications communicated?

Inject

- A second user at 10:32AM has reported similar issues with a ransomware note which prevents them from using the computer. The same message is displayed indicating files are now encrypted, and how to proceed with retrieving the decryption key. The user stated the system showed infection shortly after opening up an invoice attachment.



Thu 2/18/2016 2:48 AM

Accounts billing@[redacted]h.corn

Invoice

Invoice74531951.doc (44 KB)

Dear Sir/Madam,

I trust this email finds you well,

Please see attached file regarding clients recent bill. Should you need further assistances lease feel free to email us.

Best Regards,

Barrett Gallagher
Community Health Systems, Inc. www.chs.net

Event Correlation

- Were the affected users performing same activities?
- What things do these users have in common?
- Are there shared local admin passwords?
- Any unusual traffic or other indicators?
- What was the user doing?

Respond Phase: Incident Prioritization and Mobilization

Incident Declaration and Prioritization

- *Incident Declaration*
  - How was it determined that there was an incident?
  - *How did the organization invoke the IRP?*
  - Was it possible to correlate other information?
  - What immediate actions will prevent the spread of ransomware?
- *Prioritization*
  - How is priority determined?
  - Is it based on CIA?

Respond Phase

Declaration – Prioritization – Notification/Escalation – Analysis - Containment

Notification/Escalation and Analysis

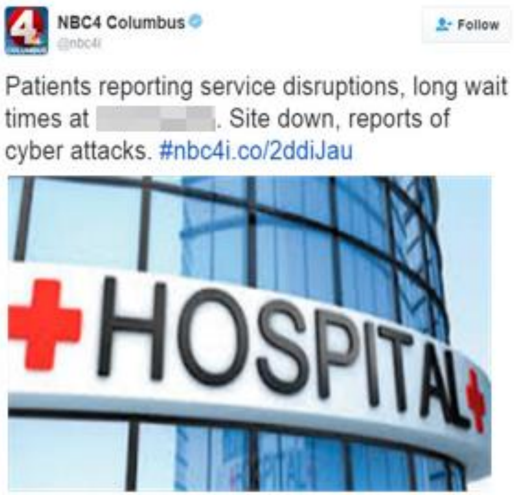
- ***Notification/Escalation***
  - Who gets notified of the incident
  - How are the notifications communicated?

- ***Analysis***
  - Who performs the analysis?
  - What permissions are granted to users (r vs rw)?
  - Is the local admin account shared between workstations and/or servers?
  - How does analysis lead to indicators of compromise

Respond

Inject!

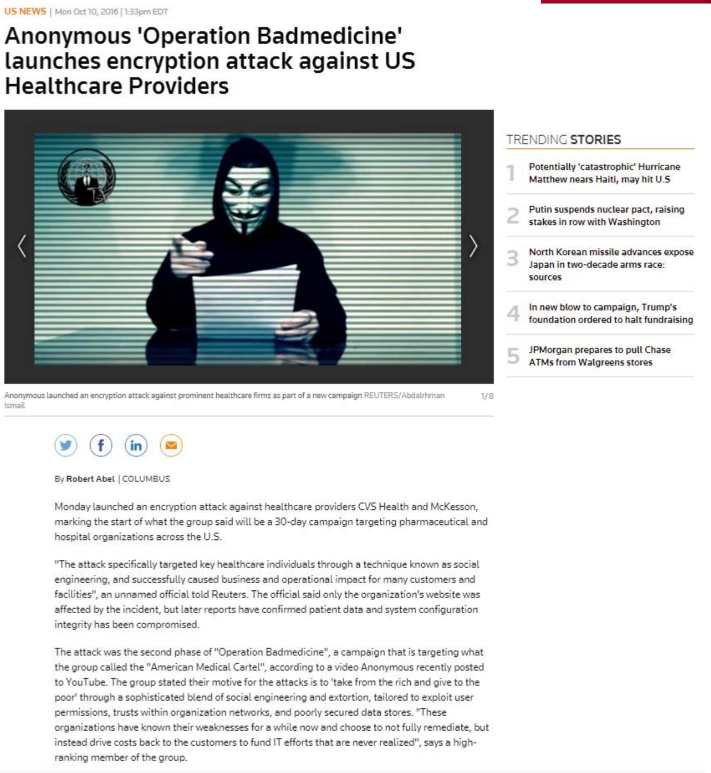
A local media outlet picks up the story from social media, contacts someone inside the hospital that confirms systems are down (unknown who confirmed this). Person assigned to assist marketing needed for 2 hours in order to respond to inquiries and assist with PR needs. Note that Hospital INC is not the only hospital affected. Marketing was able to correlate media reports with a recent attacker campaign called “Bad Medicine” as a likely cause.



NBC4 Columbus
@nbc4i

Follow

Patients reporting service disruptions, long wait times at [redacted]. Site down, reports of cyber attacks. #nbc4i.co/2ddiJau



US NEWS | Mon Oct 10, 2016 | 1:33pm EDT

Anonymous 'Operation Badmedicine' launches encryption attack against US Healthcare Providers

Anonymous launched an encryption attack against prominent healthcare firms as part of a new campaign REUTERS/Abdalrhman Ismail

1/8

TRENDING STORIES

1 Potentially 'catastrophic' Hurricane Matthew nears Haiti, may hit U.S

2 Putin suspends nuclear pact, raising stakes in row with Washington

3 North Korean missile advances expose Japan in two-decade arms race: sources

4 In new blow to campaign, Trump's foundation ordered to halt fundraising

5 JPMorgan prepares to pull Chase ATMs from Walgreens stores

By Robert Abel | COLUMBUS

Monday launched an encryption attack against healthcare providers CVS Health and McKesson, marking the start of what the group said will be a 30-day campaign targeting pharmaceutical and hospital organizations across the U.S.

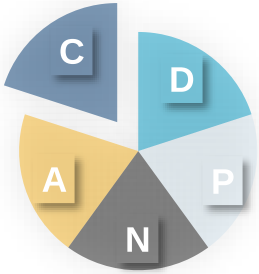
"The attack specifically targeted key healthcare individuals through a technique known as social engineering, and successfully caused business and operational impact for many customers and facilities", an unnamed official told Reuters. The official said only the organization's website was affected by the incident, but later reports have confirmed patient data and system configuration integrity has been compromised.

The attack was the second phase of "Operation Badmedicine", a campaign that is targeting what the group called the "American Medical Cartel", according to a video Anonymous recently posted to YouTube. The group stated their motive for the attacks is to 'take from the rich and give to the poor' through a sophisticated blend of social engineering and extortion, tailored to exploit user permissions, trusts within organization networks, and poorly secured data stores. "These organizations have known their weaknesses for a while now and choose to not fully remediate, but instead drive costs back to the customers to fund IT efforts that are never realized", says a high-ranking member of the group.

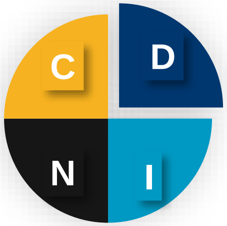
2nd Detect Phase

- Expect notification to arrive through multiple channels (e.g. safety huddle, help desk tickets, hospital paging system).
- Any playbooks associated with this activity?
- Discussion around how to begin managing communications
- Respond to requests, open ticket and identify nature of the issue.

Ransomware Event



New Event:
Outages Reported



Detect Phase

Detection – Impact – Notification - Correlation

2nd Respond Phase

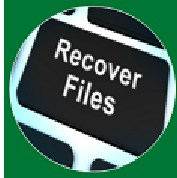
- Who owns this incident? What type of incident are you going to declare?
- How is this prioritized?
- Do any additional resources or stakeholders need to be notified?
- Who performs the analysis?
- What are options to deal with outage?

Respond Phase	Declaration – Prioritization – Notification/Escalation – Analysis - Containment

Recover

Recovery Phase

Incident Eradication



Recover

- How can the ransomware be prevented from spreading to additional systems?

- What is the process for connecting a previously compromised system to the network again?

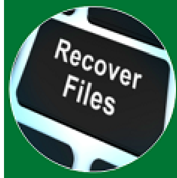
Recovery Phase

Eradication - Recovery – Communication

Incident Recovery

Recover

- On or offsite backups?
- How often are backups taken
- How long to restore from backup?
- Who is responsible?
- How often is the restore process exercised?
- How long to wait before removing defenses?

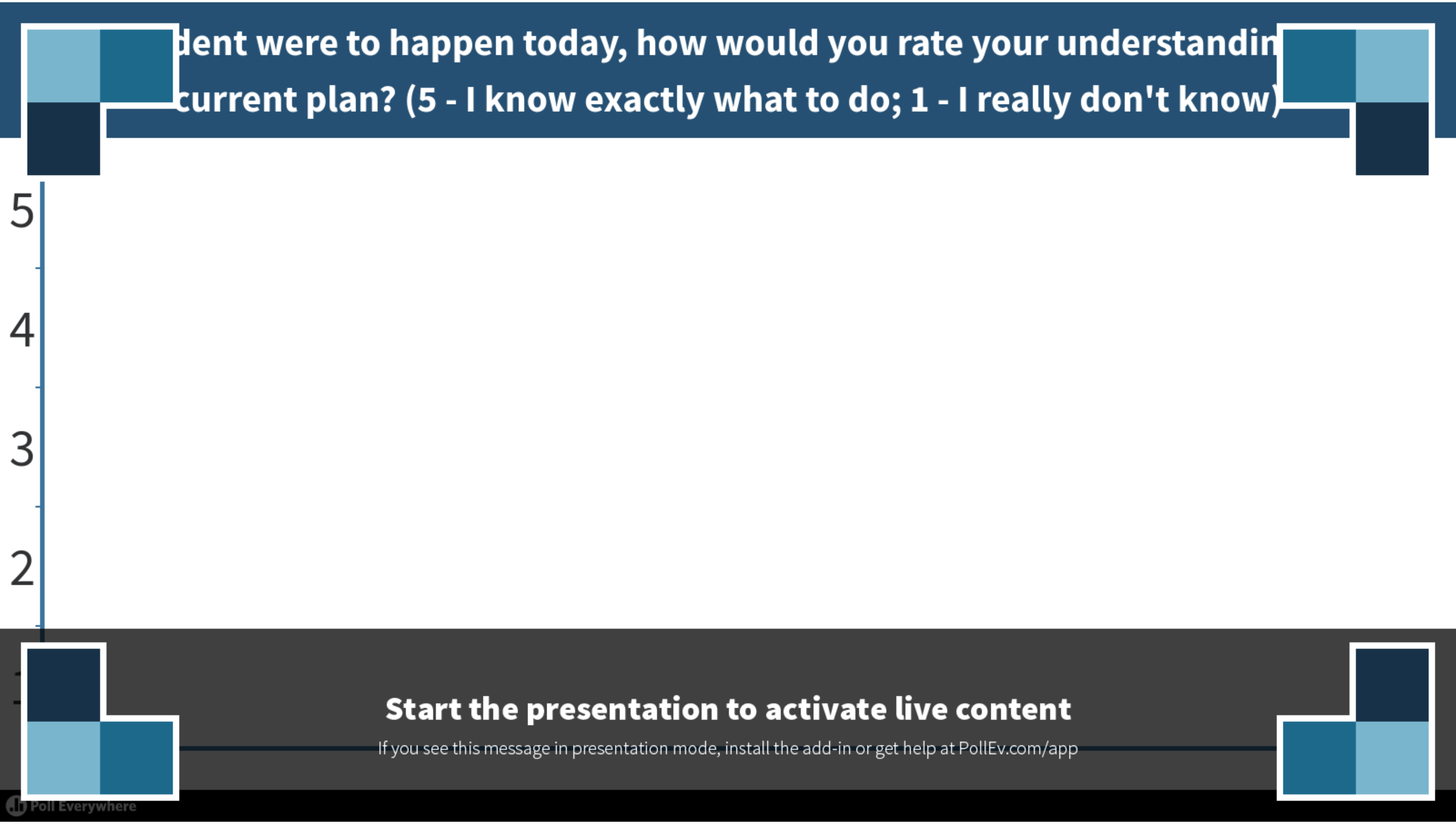


Incident Communication

- Is the rest of the organization notified of the incident?
- Is there any external communication?
- Who is responsible for notifications?
- Is an after action review performed?
- Is the IRP updated with information obtained from this incident?

Board Level Discussion points

- **When was the last time we practiced our cyber incident response capability?**
  - What is my role in a particular incident?
- **If an incident happened right now could we continue operations?**
  - Payment vs Recovery
- **What is OUR determined difference between a short term incident and a long term incident – as defined by the business**
  - Corporate environment vs subsidiaries
- **Do we have retainers in place for Legal, PR, and Cyber Security**
- **Do we have cyber insurance to cover this?**

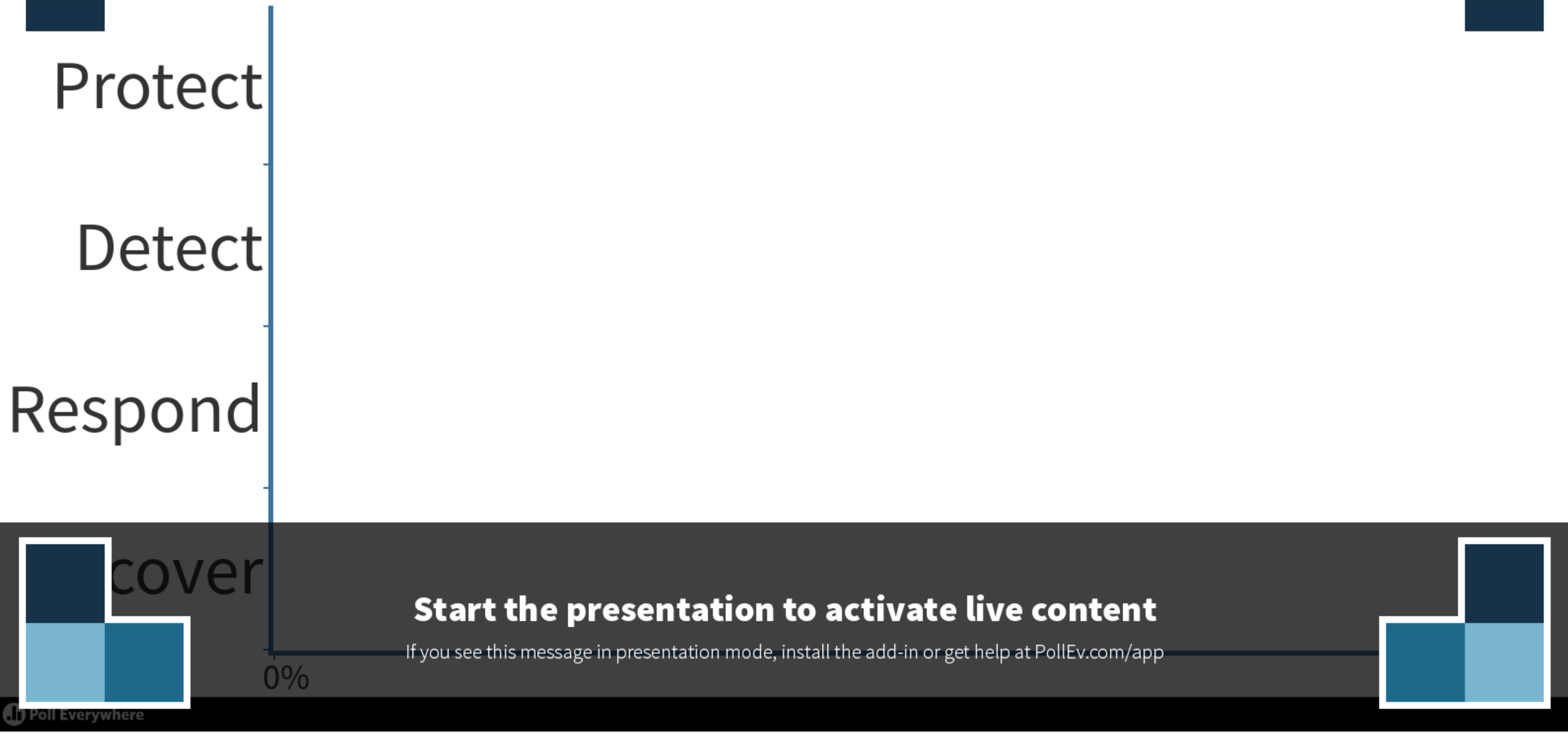


dent were to happen today, how would you rate your understandin
current plan? (5 - I know exactly what to do; 1 - I really don't know)

Start the presentation to activate live content

If you see this message in presentation mode, install the add-in or get help at PollEv.com/app

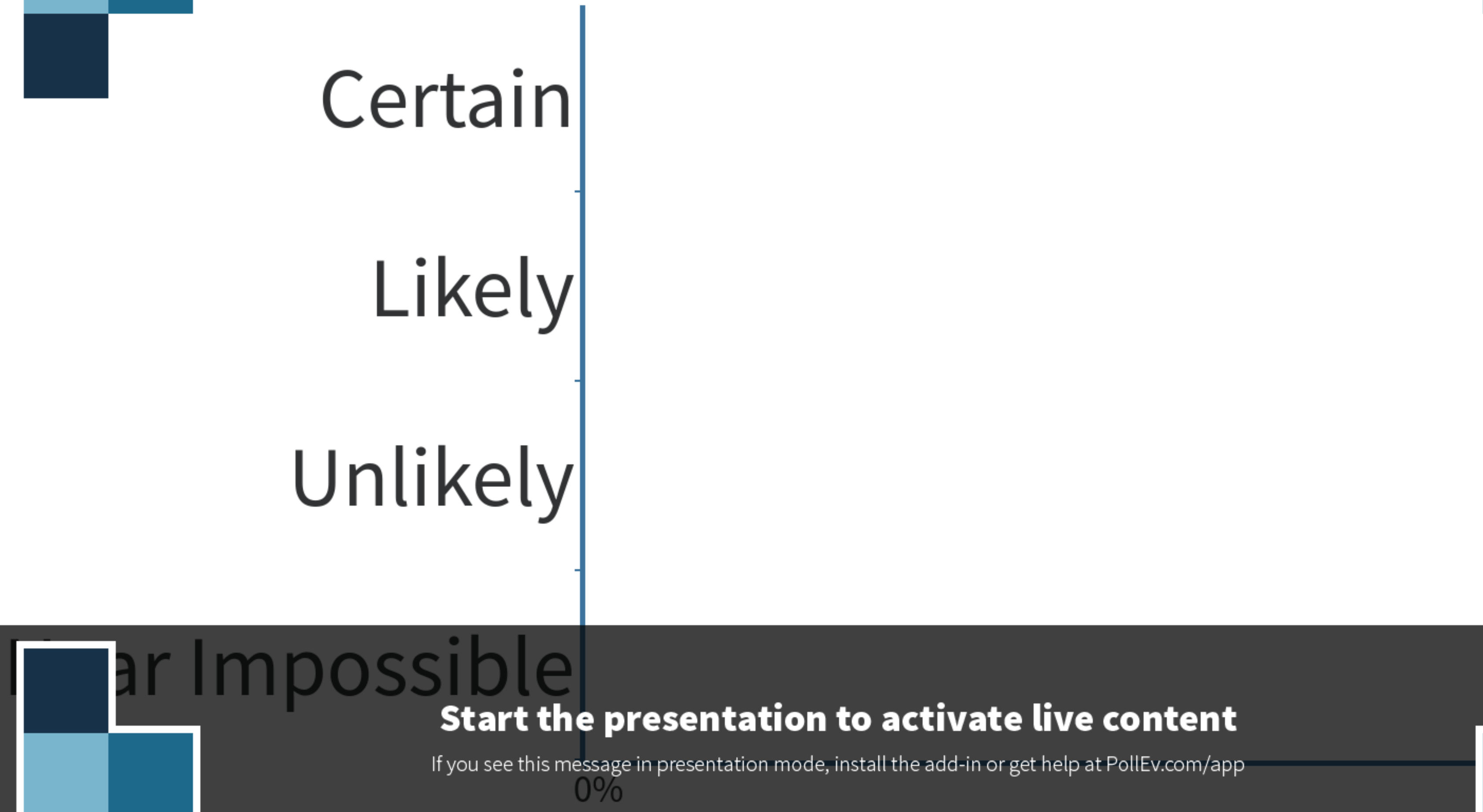
hat do you think is the most important phase in the incident respo methodology?



Start the presentation to activate live content

If you see this message in presentation mode, install the add-in or get help at PollEv.com/app

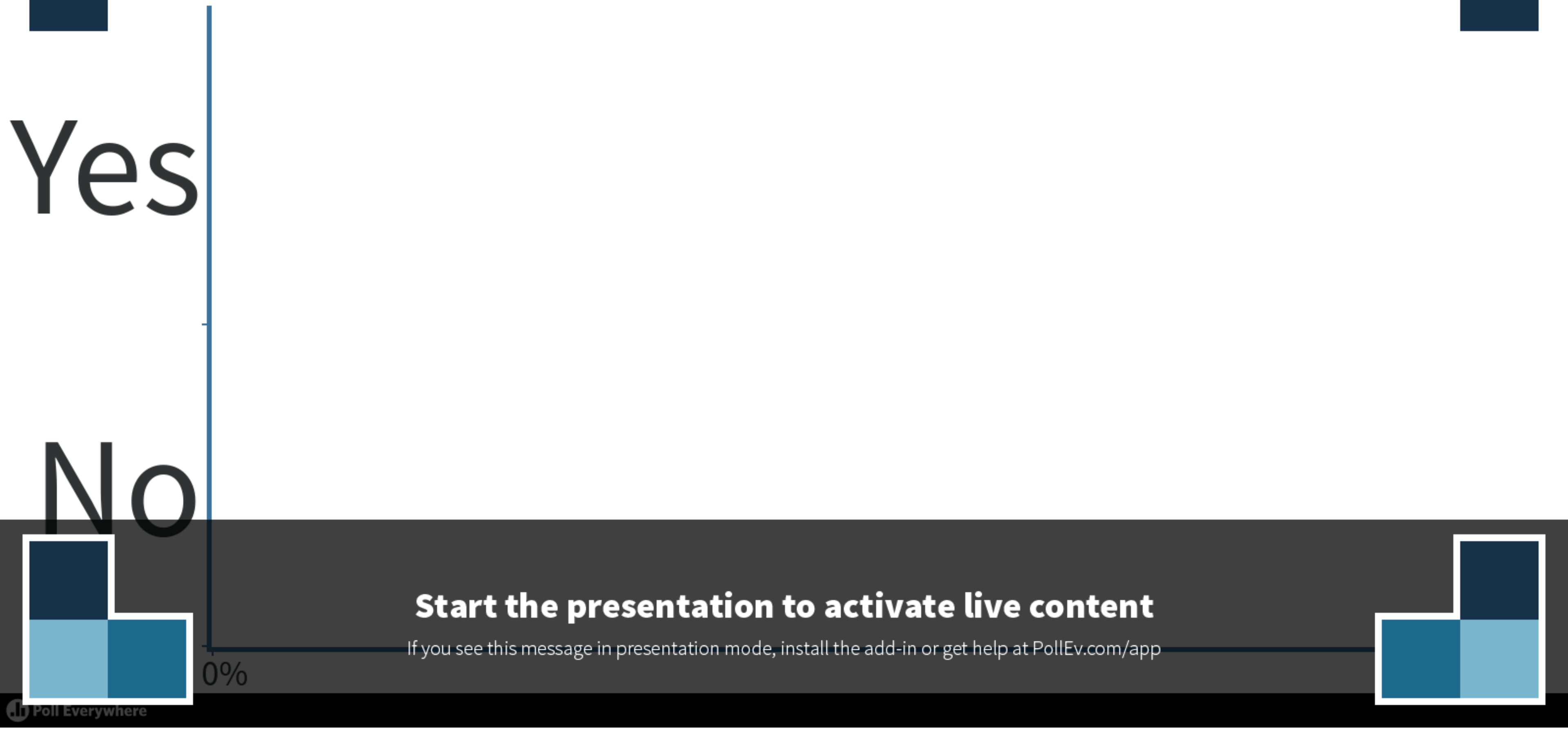
likely do you think a successful ransomware attack is at your locat



Start the presentation to activate live content

If you see this message in presentation mode, install the add-in or get help at PollEv.com/app

lecision were up to you, would you pay a ransom (roughly $20,000) access back to data?

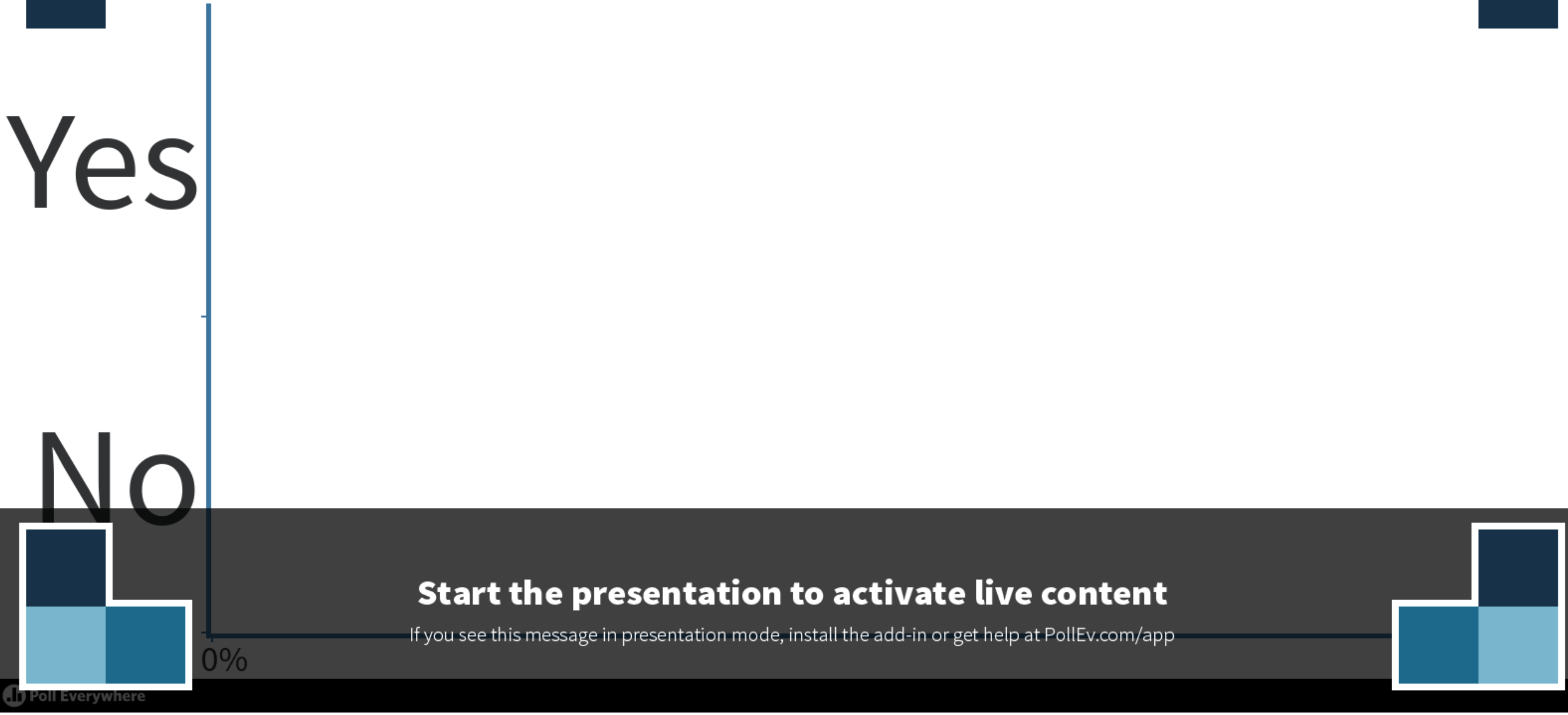


Start the presentation to activate live content

If you see this message in presentation mode, install the add-in or get help at PollEv.com/app

Replace text box with chapter logo

you confident you and your team fully understand the roles neede successfully navigate a major incident



Start the presentation to activate live content

If you see this message in presentation mode, install the add-in or get help at PollEv.com/app

Questions?