Are you ready to rumble?
Wrestling with responding to a data compromise?

Presented by:

Marti Arvin, VP, Compliance Strategy, CynergisTek, Inc.

Stephanie Lucas, Associate, Baker Hostetler, LLP,

John Brown, Chief Information Officer, PAMC LTD

Today’s Agenda

1. What is an Incident?
2. What is an Incident Response Plan?
3. Post Incident Recovery
4. Key Takeaways

Review Objectives, Processes, and Outputs Relating to IR
What is an Incident?

What Could Possibly Go Wrong?

**Incidents come in all sizes!**

- Phishing
- Compromised endpoint device
  - Printer
  - Multi-function device
  - Coffee maker, yes coffee maker!
  - Medical device
What is an Incident?

- Does your organization have a formal definition of an incident?
- Are security and privacy incidents separate?
- Can an incident happen that does not involve PHI?

How does your organization get incident reports?

- Who can report an incident?
- How?
- Has your organization established an incident reporting process?
- Has everyone been trained?
- How do you establish the level of urgency?
What Could Possibly Go Wrong?

**Incidents come in all sizes!**
- Ransomware
- Employee laptop theft
- Credit card payment forms in dumpster
- Missing heart monitor
- Vendor breach
- Compromised user credentials

Do you know the answer?

- In an incident:
  - What are your priorities?
  - Who can make decisions?
  - How fast do you escalate?
  - Do you preserve evidence?
  - For technical incidents, do you have a person with the right technical skills?
Incident Response: What Is An Incident Response Plan (IRP)?

Why Incident Response Matters

**We Are a Target**
Healthcare is a target and attackers are increasingly focusing on healthcare for information and data.

**All Sides**
Attacks are coming at healthcare organizations from all sides and more attackers are jumping on the bandwagon.

**Preparation**
Preparing for breaches, ensuring that the right people know what to do and that everyone is in the know.

**Defense**
Defense alone is a losing battle. We have to be proactive, expect intruders and attacks and be prepared to go on the offense.

**Breaches WILL Happen**
Eventually, every organization will have an incident. Odds are that this will lead to a breach too. Be ready.
The Incident Response Plan

• Like any plan, an incident response plan is an outline of what needs to be done and by whom

• What makes a successful IRP?
  – Is it well thought out?
  – Can be applied to multiple scenarios
  – Goes beyond information technology
  – Has it been tested?
    o In real-life, or an exercise?

If you fail to plan, you are planning to fail!

~ Benjamin Franklin
## When & Who

- An incident response plan will not generally be triggered for a smaller, inconsequential event  
  - Triggered by an incident that has potential to be a significant breach
- The players need to be across multiple business units  
  - There may be core members of the team that will be involved for every incident  
  - There may be ad hoc members depending on the nature of the incident
- There may be players from outside the organization

## Who is Responsible?

- Who are the key stakeholders?
- What are their priorities?
- When are they needed?
- How do you communicate?
- When or if do you engage legal?
Specifically, Who To Involve

• Core team members
  - CIO
    o Multiple specialist across IT and IS
  - Compliance Leadership
    o CCO
    o CPO
    o CISO
  - General Counsel
  - Designated member of the senior leadership team
    o Business Unit Leaders
    o Clinical Leadership

Specifically, Who To Involve

• Key stakeholders representing other functions
  - Media relations
  - Patient relations
  - Procurement
  - Human Resources
  - Impacted business owners
  - Other senior leaders of your organization
    o CEO, CFO, CNO, CMO, & CMIO
    o Senior leaders of a parent organization
Specifically, Who To Involve

- Key outside stakeholders who may need to be involved
  - Cybersecurity insurance company
  - External counsel
  - Key vendors
    - Forensics firms
    - Support for response and recovery
  - Law enforcement
    - Local
    - Federal
  - Impacted business partners such as affiliated healthcare providers

Constituent Pieces

A successful incident response plan is only as strong as the sum of its parts

- The parts that typically make up an IR plan:
  - Incident Response Policy/Charter
  - Roles & Responsibilities Definitions
  - IR Program Playbook
  - Incident Response Procedures
  - Incident Response Standards
  - IR Exercise/Test
Preparation is key - knowledge

• Have solid documentation that everyone is trained on to know
  − Who triggers the incident response plan i.e. who declares an incident
  − Who is responsible for what roles in the process
    o Who can make what decisions
      ▪ Can the CISO or CIO decide to cut access to the EHR?
        • Under what circumstances?
    o Who needs to be contacted and when?
      ▪ Immediately
      ▪ Within hours
      ▪ Within 24 hours

Preparation is key - Tools

• To be successful tools must be build before the incident
• Have playbook or run book that identifies all actions and the responsible parties
• Have an inventory of systems
• Have functional back-ups of
  − Data
  − System configurations
• Have a prioritized list of assets
Preparation is key - Tools

• Have a prioritized list for recovery of systems that not only
  – identifies the order of recovery for business continuity but also
  – Any necessary order to assure the recovery is successful.

• Up to date phone tree

• Breach assessment toolkit

• Media relations toolkit identifying the anticipated documents
  for communications
  – Internal controlled and uncontrolled (leaks)
  – Notice to media
    – Notice to key outside parties
Preparation is key - Tools

• Have a prioritized list for recovery of systems that not only
  – identifies the order of recovery for business continuity but also
  – Any necessary order to assure the recovery is successful.
• Up to date phone tree
• Media relations toolkit identifying the anticipated documents
  for communications
  – Internal controlled and uncontrolled (leaks)
  – Notice to media
  – Notice to key outside parties

Preparation is key - Financial

• Pre-contracting with vendors
• Understanding the process for engaging a vendor if you haven’t
  used them before
• Cyberinsurance
  – Do you have any?
  – Do you have enough?
• Where would on the fly funding come from?
What Makes Up a Successful IR Test?

Key Elements of a Successful Incident Response Exercise:

- **Outside Perspective**
  The exercise itself should be planned and executed by an objective 3rd party. Provides added value of external industry perspectives.

- **Buy-In From ALL Levels**
  Everyone, from the CEO to the IT analyst has a crucial role in an orgs incident response. Without buy-in from all levels exercises are significantly less effective.

- **Thoughtful Participation**
  During the actual exercise all participants must take the exercise seriously and partake fully in the events even though they are simulated.

What is Often Missing From IRPs

- Executive Buy-in for planning and execution of IRP
- Council Involvement in Planning and execution of IRP
- Breach notification and compliance
- Thorough communication plans (internal and external)
- Involvement beyond IT and IS departments
- Regular Exercises and updates
- Up-to-date phone trees
Frank Discussions About Reality

Security and privacy incidents WILL happen – the difference is whether the victim was prepared.

- Talk to non-technical roles that have a role in IR, get their support
- With the support of many departments show the executives reality
- We are in a sweet spot right now, breaches are in the news and everyone (technical or not) is worried about them.

Failing to Plan, is Planning to Fail

Needs to be repeatable, regularly reviewed, and flexible enough to deal with any incident...

- “Planning is bringing the future into the present so that you can do something about it now.” — Alan Lakein, author

- “Every minute you spend in planning saves 10 minutes in execution; this gives you a 1,000 percent return on energy!” — Brian Tracy, author and motivational speaker

- “The time to repair the roof is when the sun is shining.” — John F. Kennedy, former U.S. President
### Key takeaways

- Incident response is an ongoing process
- Need to assure
  - the person who can trigger the IRP is identified
  - Understanding of the type of incident that could trigger the IRP
- Identifying the key members of the core IR team to encompass all relevant parties
- Identifying who may need to be - ad hoc members of the IR team and when to add them
- Tools cannot be developed on the fly during an incident

---

### Key takeaways

- Just like you, to stay fit your IRP must be exercised
- Having a broader perspective of the incident by including the right parties in an exercise will help your organization be better prepared and increase buy-in.
- An incident response exercise measures/identifies can help you understand your gaps and better prepare you of the changing threat landscape.
Key takeaways

• Assess your environment
• Develop a comprehensive IRP that is repeatable, efficient and effective
• Assure your IRP does not have missing pieces
Assessing for Breach Notification

- Understanding what HIPAA Requires
  - The clock starts when the event is discovered
  - Notification must occur without undue delay
    - The maximum for undue delay is 60-day
- If you are a business associate you must notify the covered entity of a breach without undue delay but not more than 60 days from discovery
  - Your BAA agreement may have a shorter timeframe

Assessing for Breach Notification

- Understand what state law requires
  - Your state law may differ in:
    - Criteria regarding data involved
    - Process for determining if notification is req.
    - Timelines from federal law
  - You may have obligations in other states
    - Because you are multi-state entity
    - Because you have data of residents from other states
Breaches WILL Happen

An impermissible use or disclosure of unsecured protected health information

1. Presumed to be reportable
2. Safe harbor for encrypted PHI
3. Exceptions for certain inadvertent and incidental used & disclosures
4. The entity must perform assessment for probability of compromise of protected health information

Breach: Assessing Probability of Compromise

Assessment to determine probability of compromise

1. The nature and extent of PHI involved
2. The unauthorized person who used the PHI or to whom the disclosure was made
3. Whether the PHI was actually acquired or viewed
4. The extent of mitigation present

Additional factors to be considered in ransomware incidents:
- Whether there is high risk of unavailability of PHI?
- Whether there is high risk to the integrity of PHI?
Notification of others

• In addition to regulatory obligations to notify there may also be other obligations
  – Contractual obligations
    o Are you a BA to another covered entity?
    o Does the organization have contracts that require notification regarding a data incident or breach

Key Takeaways
Key takeaways

• You must be prepared to quickly
  – Triage the incident
  – Determine what needs to be handled first
  – If stopping the propagation if possible and if so how
  – Kept the right parties informed at the right times

• Assessing whether a breach has occurred and who needs notification involves understand your
  – regulatory obligations and
  – Contractual obligations

Key takeaways

• Talk to senior leadership in business not technical terms.
• Provide statistics that demonstrate the cost of an event.
• Discuss how preparation can reduce the cost of the incident.
• Be honest, IR will not prevent an incident.
Ransomware Lessons Learned

• Analysis of three incidents over the past 24 months
  – All are publically known
• Organizational names have been removed
  – Hospital
  – Hospital network
  – Business associate/Cloud hosting provider
• Level of preparedness varied widely
Ransomware: Acute Facilities - Infection

- The use of SIEM and anti-virus systems did not specifically ID the ransomware due to the zero-day nature of the attack
- From the moment of infection, to the spread to nearly all vulnerable devices was under 1 hour
- Recovery took weeks, as each device had to be ‘touched’
- Infection was not limited to IT systems
  - Laboratory system had to be replaced – long lead time

Ransomware: Acute Facilities – Operational Impact

- All systems were off-line, including EHR, timekeeping, HR, payroll, supply chain management
- Prior BCM/DR efforts focused primarily on clinical systems, but without supporting infrastructure, operations were significantly impacted
- Intensive staffing impact to just ‘deliver the mail’
- Without ability to process claims, cash flow became an immediate problem (> $60M)
  - Months after the attack, cash deficit still > $30M
Ransomware: Business Associate

• Large ambulatory network infected with ransomware
  - Ransomware attempted to encrypt shared drives hosted on EHR hosting provider’s servers - but quick detection allowed the link to be severed.
  - Virtual server was rebuilt and back online in approximately an hour.
  - The ambulatory network remained offline for over a week while the on-site networks and systems were rebuilt.

Summary

• The level of preparedness did not slow the speed of the attack
  - All attacks used zero-day vulnerabilities
  - All vulnerable devices compromised in 14 to 60 minutes
  - Attacks work faster than humans – “man in middle” won’t work
• Operational impacts were not previously anticipated
• The recovery time, operational impact, and cost were mitigated by well-prepared organizations