New Hanover Regional Medical Center

Leading Our Community to Outstanding Health

Operationalizing the Plan: The Importance of a Communication Strategy

by Rob Bryan, IT Security Analyst

“Stand in the way of threats not patient care.”

Audience: NCHICA

August 2, 2019

Why We're Here

Why We're Here

- ❑ Incidents are more likely than ever before. The ability to not only respond and recover quickly, but also effectively manage the event and its aftermath, is more critical than ever before.
- ❑ Incidents can cause major damage to your brand and undermine patient trust
- ❑ Response and recovery is a team sport and involves virtually every major area of the organization and external partners/vendors
- ❑ During every incident, the response team will be faced with conflicting priorities
- ❑ Many of you here today may be required to facilitate a Crisis Management team to handle a security incident
- ❑ Effective communication is vital
- ❑ In the worst case scenario, there may be lives at risk

Key Challenges

- Leaders and staff are often unprepared to handle communication for security incidents
  - Insufficiency of information and process
  - Lack of focus
  - Believing an incident won't occur
  - Fearing consequences of failing
  - Not prioritizing communications
- Lack of defined security incident crisis communication roles and responsibilities

Objectives

- ❑ Identify practical approaches for improving Incident Response communication
  - ✓ Understand key stakeholders to involve in your communication
  - ✓ Establish severity levels and escalation timing
  - ✓ Develop scripts and downtime messages
  - ✓ Align with existing on-call procedures
- ❑ Increase “communication” confidence

Practical Approaches to Improving I. R. Communication

Some of the basic “do’s”

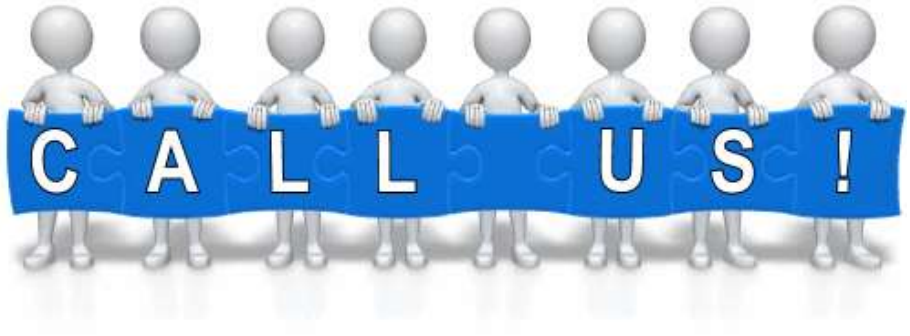
- ✓if it's "bad," say so right away.
- ✓Inform, rather than impress. Use plain language.
- ✓When you don't know something, say so.
- ✓Monitor the internet and social media for damaging information or additional information about the attack.

Practical Approaches to Improving I. R. Communication

1. Add key stakeholders to your address book or contact lists
2. Define severity levels and escalation timing
3. Develop scripts and downtime messages

Identify Key Stakeholders

1. Corporate Compliance
2. Legal Counsel/Corporate Attorney
3. Marketing/Public Relations
4. Risk Management
5. Emergency Management
6. Administrator on-call
7. Human Resources
8. Staff
9. Your boss
10. Local law enforcement (e.g. FBI agent)
11. Trusted partners
    a. Incident Response Retainer
    b. Security Operations Center
    c. Cybersecurity Insurance



Operationalizing the Plan: The Importance of a Communication Strategy

Severity	Impact	Examples
Escalate and Activate NHRMC Command Center		
High	• Required breach notifications are triggered, • Legal and regulatory impact, • Material financial impact, • Outage that impacts >10% of end point devices, • Prolonged critical operations impact that lasts 4 or more hours	**VERY PUBLIC FACING** • Prolonged outage of critical applications or technology infrastructure, • Widespread exfiltration or disclosure of Protected Information, (>500 records) • Allowing unencrypted Protected Information to be accessed without authorization, (>500 records)
Escalate to IS on-call Manager and Activate IS Operations Center		
Medium	• Required breach notifications may be triggered, • Legal and regulatory impact, • Moderate financial impact, • Critical operations impact that lasts less than 4 hours, • Outage that impacts <10% of end point devices, • Possible negative reputational impact • Limited media exposure	**PUBLIC FACING** • Limited exfiltration or disclosure of Protected Information, (<500 records) • Physical breach of data center, • Isolated prolonged outage of critical applications, • Defacement of customer facing websites, • Violations of NHRMC's privacy notices or other public statements, • Failure to respect customers' control or choice over privacy settings,

Some of the basic “do’s”

- ✓ Provide talking points for all workforce members as to how to handle inquiries about the incident. Outside of the crisis communications team, no workforce member should be saying anything. They need to know to whom to refer such inquiries.
- ✓ Ensure your Marketing and Public Relations team are updated and prepared to work with local media on publication
- ✓ Partner with your Compliance and Legal teams for proper notifications to patients and OCR

❑ Develop scripts and downtime messages

Subject Line: Escalated Issue - Ticket # - Short Description

Issue: (Description of the technical issue)

Impact to organization: (What areas were impacted and how did this impact the organization?)

Communications: (How was the downtime communicate to organization and the IS team)

Follow-up: (What additional follow-up was done during the process to remediate)

Root Cause: (What caused the issue?)

Additional work for prevention: (Outline steps to minimize or eliminate the risk of this happening again)

❑ Develop scripts and downtime messages

Immediate notifications for employees and trusted partners:
We can confirm that on [day/date], our network was compromised as a result of a cyberattack known as [name of attack]. We are actively working with our partners to contain the attack.

The safety of our patients, employees, and business operations are paramount. We will continue to provide updates when we have more information to share.

Should you be contacted by any outside channels for information or commentary, please direct those individuals to [name/department/number], who is authorized to speak on behalf of our organization.

Practical Approaches to Improving I. R. Communication

- Utilize your existing on-call procedures
  - Applications staff
  - Infrastructure staff
  - Desktop staff
  - Security team “Ensure you have a “Threat” team member on-call”
  - IS Manager on-call
  - Administrator on-call
- Translate roles and responsibilities
  - Incident Response Coordinator
  - Incident Response Lead
  - Incident Response Investigator

Practical Approaches to Improving I. R. Communication

- **Incident Response (IR) Coordinator:** The IR Coordinator is the owner or custodian of the incident and acts as the primary point-of-contact for incident notification, activation, and remediation activities. This individual documents and maintains records of the incident.

- **Incident Response (IR) Lead**: This individual is responsible for the facilitation, communication, and coordination of NHRMC incidents classified as Medium or high. This person is responsible for activating teams and escalating events classified as High to the Emergency Management team requesting activation of the NHRMC Hospital Incident Command Center.

- **Incident Response (IR) Investigator:** This person will help research an incident in detail. The IR Investigator will ensure evidence and facts relative to the incident are identified and documented.

Practical Approaches to Improving I. R. Communication

- IR Coordinator:
  - ✓ Security team member on-call or technical IS Lead representing Security

  Responsibility: Owner or custodian of the incident and acts as the primary point-of-contact for the incident.

- IR Lead:
  - ✓ IS Manager on-call

  Responsibility: Responsible for facilitation, communication and coordination of escalated incidents.

- IR investigators
  - ✓ IS Team members on-call on any given week

  Responsibility: Staff to help research an incident in detail.

- Summarize/Outline your overall IR Plan for your Incident Response team
  - A formal IR Plan may contain 15 to 30 pages depending on its scope
  - Ensure information is in a format that is easy to consume. For example, use your organization's "standard work" template to align with your IR framework.

Example Step 1 "Detect or Identify"

Step	MAJOR STEPS (WHAT) (WHEN) (High level steps)	KEY POINTS (HOW) (WHO) (Detailed Steps)	REASONS FOR KEY POINTS (WHY)
1	Detect or Identify an incident or issue which is preventing employees and/or Providers from accessing NHRMC systems/applications or an issue which is impacting the performance of applications (e.g. application is running very slow)	1. NHRMC employees are to report all application/system issues, and/or suspicious activity immediately to NHRMC's Help Desk 667-7855. 1. The NOC/Help Desk staff will open a ticket with all relevant information using the IS Page Incident Form template and escalate incidents to the appropriate on-call staff member within 15 minutes for all applications that are impacting patient care and do not have a workaround. The text should contain the incident number. The texting signature line will automatically include the name and phone number of the person sending the text. 1. The on-call representative should respond to the page within ten minutes: • <u>If the on-call representative does not respond within 10 minutes, the Help Desk/NOC personnel will contact the respective on-call using the secondary phone number</u> • If the secondary on-call representative fails to respond within 5 minutes, the on-call manager will be paged for further directions.	Establishes starting point for communication and documentation of the event. Establishes first level of escalation and source for tracking information.

Take Aways

- ✓ Keep it simple!
- ✓ Use plain language when communicating
- ✓ Be honest and straightforward with your team
- ✓ Know your key stakeholders to involve
- ✓ Establish severity levels and escalation timing
- ✓ Develop scripts and downtime messages
- ✓ Align with existing on-call procedures
- ✓ Ensure Marketing and Public Relations are informed and prepared to work with local media
- ✓ Partner with Compliance and Legal for proper notifications to patients and regulatory bodies

NHRMC IS Security

New Hanover Regional Medical Center