HIROC

Planning for Cyber Security Incidents

A Crisis Communications Guide

Crisis Communications Planning

A crisis communications plan is a vital part of emergency preparedness and response. An organization's success in managing a crisis event is dependent, in part, upon its ability to communicate. Such communication plays a fundamental role in maintaining the trust of internal and external stakeholders. Plans should be well-tested, understood, and practiced by both leadership and staff. Having a solid crisis communications plan will not only save an organization's reputation, but may also save lives.

A crisis communications plan is part of, but not a substitute for a disaster recovery plan. It is not intended to provide guidance regarding the actual resolution of a situation. This plan should work in tandem with an organization's Incident Management System (IMS) or crisis response plans, as well as business continuity plans.

Elements of a Cyber Crisis Communications Plan

It is important to have a specific plan for crisis communication during a cyber event as there are a few elements that differentiate a cyberattack from another type of crisis (e.g., compliance and reporting requirements, disrupted communication channels).

While the length and depth of a communications plan will vary across organizations, below are some of the main elements to consider when creating a cyber crisis communications plan.

- List of potential cyber events, detailing potential impact to critical systems, operations and patient care (e.g., Ransomware – outage of internal and external network connection)
- List of **Crisis Management Team** and/or **Crisis Communications Team**, with contact information
- Central point of contact for employees to report a suspected or known incident (e.g., 24/7 crisis hotline)
- Outline of an organization's process in the event of a cyber security emergency.

Nine steps to consider:

1. Understand the crisis
2. Activate the Crisis Communications Team
3. Assess the situation
4. Develop the response(s)
5. Communicate with audiences
6. Monitor feedback, evaluate conditions
7. Document the crisis
8. End of crisis, debrief, evaluate response(s), gather observations, make changes
9. Decompress, take steps to reduce the stress and to support staff

- List of internal (staff, clients/patients, board of directors) and external stakeholders and partners (e.g., ministry of health, integrated health partners, community, vendors, third-party service providers, insurer)
- Emergency communication channels to reach employees, patients and clients (e.g., hotline and fanout); include a notification protocol for frontline staff both on site and off duty, senior leaders, board members, patients/family members and the community
- Draft templates approved by leadership (e.g., media releases, internal briefing notes, patient notification, Information and Privacy Commissioner notification)
- List of approved notification channels, by type and severity of breach (e.g., letter, email, verbal, website)
- List of approved and trained media spokespeople within the organization
- Media contact list, law enforcement and cyber-specific contacts
- Social media monitoring process and responsibilities – during and after the event

Creating Alignment Across the Organization

Consulting Communications Colleagues

Depending on the size of the organization, your communications team may already have plans in place and valuable templates to get through a crisis.

Always reach out to those in the organization who manage communications before embarking on a communications plan.

In a crisis situation, the role of the communicator is to help the incident response come together. They maintain focus on all stakeholders (internal and external), to drive when and how the crisis team communicates and responds to each stakeholder. These individuals have a good lens on what is happening across the organization at any given time, so they are well positioned to act as conveners before, during and after a crisis.

Educating

A crisis communications plan exists to facilitate timely, appropriate and effective communications in emergencies. **It should be prepared in advance of a crisis.**

Before you begin planning an organization's communications response to a cyber event, it is important to understand the language of cybersecurity and the potential impact at your specific organization. Leadership, HR, communications teams, and other critical staff members must understand the language around cyber emergencies (ex. the difference between a "breach" and "brute force attack", or the difference between "malware" and "ransomware").

Media training is also important for leadership and key spokespeople. Consider working with a respected media training organization to ensure spokespeople are well prepared.

Engaging Critical Departments

Working with IT departments and privacy officers is essential when it comes to engaging staff and educating around cyber risks.

Refer to ★ *HIROC's Cyber Risk Management Guide* for more information on building resilience through cyber security and training.

Success Factors

Like most things, practice makes perfect. Creating a thorough communications plan is only half the battle. Just as you train staff on emergency procedures, conducting regular drills and putting your communications plan and the response team to work is key. This is how organizations iterate and improve.

Consider these success factors:

- Ensure communications plans are practiced as part of testing or drills done on cyber incident response plans or cyber tabletop exercises.
- Conduct regular testing of emergency communication channels.
- Undertake environmental scans to identify opportunities to improve communications planning. Reach out to organizations that have gone through a cyber breach to learn from their experience (what worked and what did not).

- Be aware that during a crisis, information may need to be managed both internally as well as publicly – two audiences that often require a different level or complexity of information.
- Have draft or sample messaging for internal and external stakeholders ready to revise and update as needed for the specific crisis.
- Use plain language in all communications planning, training, and while a crisis is taking place. The safety of your staff and the community depends on clear and easy-to-understand messaging.
- Always undertake post-incident reviews to see if the communications plan aided in managing the crisis and to understand what tactics and tools worked well for future use.

Resources

For more information on mitigating cyber security risks, consult the following resources:

- ★ *Key Measures for Preventing and Mitigating Cyber Attacks and Ransomware* (HIROC)
- ★ *Cyber Risk Management Guide* (HIROC)

Sample Messaging Templates

In the event of a cyber incident or related outage, your communications systems may be offline or not functioning as normal. Please ensure your organization has contingency methods in place, such as an emergency broadcast system, to maintain an open communication channel with staff.

The following templates are sample messages your organization can use to communicate with staff, as well as patients, clients, and community members, in the event of a cyber incident or related outage. We encourage you to customize these messages depending on the requirements of your organization.

Sample Crisis Messages

SHORT-FORM Messages

For Emergency Broadcast Systems, Intranet Bulletins, Social Media, etc.

OPTION 1

We are currently investigating a systems outage and apologize for the inconvenience.

Any further updates will be communicated on this channel.

The safety of our patients, clients, staff, and community is paramount. Rest assured, care will not be compromised during the outage.

OPTION 2

We are currently investigating a systems outage affecting:

- Website
- Patient portal
- _____

Any further updates will be communicated on this channel.

The safety of our patients, clients, staff, and community is paramount. Rest assured, care will not be compromised during the outage.

OPTION 3

We are currently investigating a systems outage and have called a CODE GREY.

Here's what's affected:

- Website
- Patient portal
- _____

Any further updates will be communicated on this channel.

The safety of our patients, clients, staff, and community is paramount. Rest assured, care will not be compromised during the outage.

Sample Crisis Messages

LONG-FORM Messages

For Internal Emails, External Emails, Holding Statements, etc.

We are currently investigating a systems outage that happened at approximately [insert time] at [insert location].

At this time, we have confirmed that [insert confirmed general information, i.e., staff and patient safety status, systems affected and still operational, etc. – REMOVE SECTION IF NO CONFIRMED INFO AVAILABLE].

As we continue to monitor the situation, and more information becomes available, we will be providing regular updates through this channel.

[This sentence is for INTERNAL use only] In the meantime, please refer to your employee handbook for emergency procedure guidelines and connect with your team lead or manager should you have any questions or possess pertinent information about the outage.

The safety of our patients, clients, staff, and community is paramount. Rest assured, care will not be compromised during the outage.

Subscriber Case Study

At HIROC, knowledge sharing between Subscribers and partners is one of our main priorities. To avoid reinventing the wheel, consult like-minded organizations that may have experienced a cyber emergency. Talk about your plans and see how you can work together to create and share resources.

We hope the following Subscriber case study will help your organization in communications planning around potential cyber events.

This resource is evergreen. If your organization would like to share its experience with HIROC's Subscribers as part of this guide, please reach out to us at *communications@hiroc.com*.

Case Study: *Michael Garron Hospital, 2019 Code Grey*

What Happened at a Glance

- On September 25, 2019 at approximately 2 a.m., Michael Garron Hospital (MGH), Toronto East Health Network went into a Code Grey. A malware (a strain of Ryuk virus), had entered their servers and was affecting several major computer systems.
- On October 4, after restoring service to key clinical applications and major administrative systems, MGH introduced "Code Grey Recovery" to help teams shift from emergency operations to a transition phase as teams continued to make progress on repairing and rebuilding systems.
- On October 29, after several weeks of restoring and repairing more than 70 clinical and administrative applications, MGH transitioned back to regular hospital operations.

Communications Must-Haves

In addition to traditional communications tools, such as crisis plans, media releases, social media, and interviews with spokespeople, here are a few of the other tools and templates that MGH valued:

- **Emergency channels to communicate out** to employees (e.g., huddle boards, rounding, fan-out phone calls), physicians (e.g., secure text), clients (e.g., call centre, website), and external partners. Assume you will not have access to email or documents saved on your organization's network. Establishing redundant communication channels is important.
- **A command meeting template** the team can follow to ensure meetings flow, all critical areas are discussed, and everyone knows what is expected of them.
- **A quick situation assessment template** for what happened, when, why, what is impacted, who needs to know, and who is the most appropriate spokesperson. This can be integrated with an organization's list of potential audiences and communication channels.

★ *See Sample Communications Checklist.*

- **A pre-developed list of IT systems** to enable timely communication to staff and physicians regarding which systems are impacted. For each system, include the name and function (what it does in plain language). Leave space for whether the system has been affected, and what the downtime processes are during the cyber incident.
- **Colour coded daily briefing notes** for internal use, for physically posting on huddle boards and in break areas.

- **Designated helpdesk call centre** that staff and physicians can use to get information and ask questions.
- **Key messages for sharing with the community, public, patients, and families** at existing public access points (such as hospital locating department, booking team, information desk, patient relations office). See ★ *Sample Message to the Public.*
- **A script** for staff to discuss the situation with patients and families at the bedside.

Other Considerations

- **Share Gratitude:** Don't forget to pause, take pictures and share gratitude for your staff throughout the crisis.
- **Plan time and energy for the recovery phase:** During this phase there is a significant effort on the part of communications and leadership. Staff and the community need to feel secure and know that operations have resumed.

Thank you to Shelley Darling, Director Corporate Communications, and Laurie Bourne, Director, Quality, Operational Excellence and Innovation at MGH for sharing your organization's story.

Sample Crisis Communications Checklist

Source: Michael Garron Hospital

Sample Crisis Communications Checklist

Situation Assessment	
Date	
What happened?	
When did it happen?	
Who does it affect/impact? (Are patient services disrupted cancelled?)	
Who needs to know?	
Who is the most appropriate spokesperson(s)?	

Potential Audiences to Consider			
	Patients and families, visitors		Public Health
	Residents/public		Partners
	Management (executive team, directors, managers, supervisors)		Elected officials — councilors, MPs, MPPs, Office of the Premier, Minister of Health
	Employees		EMS
	Physicians and residents		Police services
	Volunteers		Other local hospitals
	Board of Directors		Universities and education partners
	Community neighbours (businesses, homeowners)		Regional health network
	Offsite locations		Transportation providers
	Vendors and food retailers		Family physicians
	Ministry of Health		Contractors
	Local Community & Social Service Providers		HIROC, legal
	Media		Donors
	Other		Other

Source: Michael Garron Hospital

Sample Crisis Communications Checklist (cont.)

Communication Channels for Consideration	
Internal	**External**
• Overhead annoucements • Broadcast emails • iCare • Print communications/memos • Meetings with management (managers, supervisors for fanout to staff) • Rounding with key messages • Physician text messaging tool • Open forums – in person or video • Fanout lists • Vocera broadcasts	*Patients and families in the hospital:* • Alert volunteers at info desk of any changes • Signange (entrances) • Memos to patients on meal trays • Key messages to frontline staff about situation to communicate to patients • Memos in waiting room or admitting • Family Information Centre/Patient Experience • Translations (as required) *Patients, families and the public outside the hospital:* • Change central voice message • Public command centre/hotline • Phone calls to patients if appointments are cancelled • Website, social media, traditional media • Foundation newsletter and website
Include communications channels for regional health networks as applicable (bulletins, newsletters, social media, meetings, websites, etc.)	

Source: Michael Garron Hospital

Sample Crisis Communications Checklist (cont.)

Communications Plan				
Audience	**Message**	**Person Reponsible for Communicating**	**Channel/Tactic**	**Notes**
Patients & families				
Staff & physicians				
Community residents				
Management				
Employees				
Physicians & residents				
Volunteers				
Board of Directors				
Vendors & food retailers				
Ministry of Health				
Elected officials				
EMS				
Police services				
Local hospitals				
Educational institutions				
Regional Health Network				
Transportation				

Source: Michael Garron Hospital