



Cybersecurity at MIT Sloan

Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity (IC)³

Human Risk Management CAMS Roundtable The Culture Club

June 12, 2024



1

Subgroup Kick Off Meeting Agenda



11:00am	Kick Off
5 Min	Introduction
30 Min	Hot Topics Discussion
35 Min	Critical Cyber Comms
5 Min	Wrap Up
12:15pm	Adjourn

2

Chatham House Rule



To encourage interactivity, we will use the Chatham House Rule:

"Under the Chatham House Rule, participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed."

3

Introductions



Please introduce yourself. Tell us your:

Name

Company

Position/Interest in Cybersecurity

(Are you in charge of comms during a cyber crisis for your organization?)

(Yes-No for now, we will get into details later)?

4

Hot Topics Discussion: What's On Your Mind Today?



Audience Participation:
What question would you like to discuss with
this group?

(NOTE: We will table critical communications
questions for now and address them in the
second part of our meeting today)

5

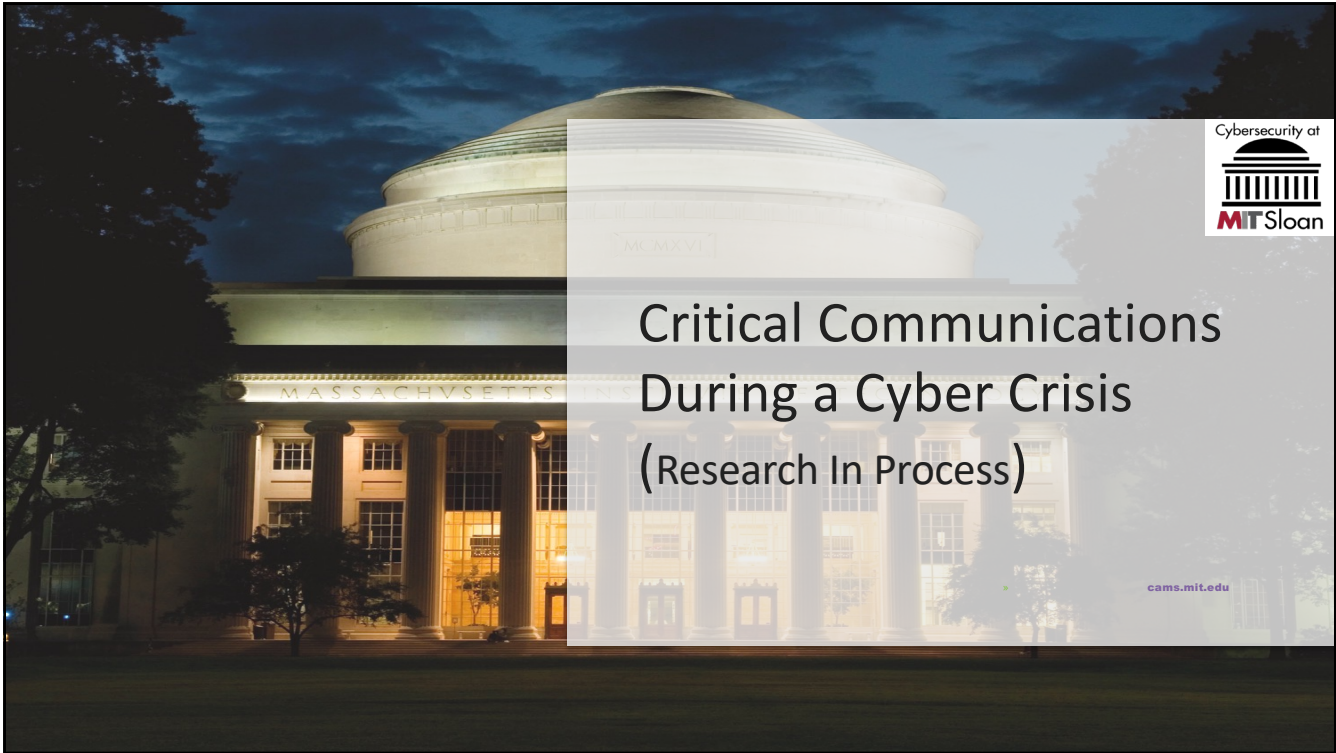
We asked what hot topics we might discuss today. Here's a sample of the responses



1. Threat evaluation. What process do you use to evaluate threats?
(Betsy)
2. Success measures for human risk (Jill)
3. Engaging employees (Heather)

There were also a lot of suggestions about critical communications...
we'll get to that in the next part of today's session.

6



Critical Communications During a Cyber Crisis (Research In Process)

cams.mit.edu

7

Preparing for comms



We asked:

How does your organization prepare for the necessary communications should there be a cyber incident?

Playbooks	Procedures
Regular drills/Crisis exercises	Notification structure
Templates (reviewed regularly)	Threat-specific plans
Escalation teams	Cyber crisis plans
PICERL (Prepare, Identify, Contain, Eradicate, Recover and Lessons Learned) framework	Escalation guide in Incident response plan
Incidence response plan	

8

A reporter shows up...



We asked:

A reporter shows up during an incident asking for the CEO. How does your organization respond?

Refer to comm team/spokesperson/press-relations
Refer to CISO
Follow documented process
Crisis Management Team handles this
Say "No Comment" and refer to PR
Not sure but know there is a plan

9

In the Communications War Room:



We asked:

Who is (or is not) in the communications 'war room' during a cyber incident in your organization?

In the War Room	Not in the War Room
<ul style="list-style-type: none"> • Mgt teams/Top Execs • SMEs • All Key Stakeholders • Depends on level of incident • C-level decisions • Third party • Legal 	<ul style="list-style-type: none"> • We do not have a war room- we have breakouts with comms, legal and incident owners • Depends on level of incident

10

Biggest Comms Concern

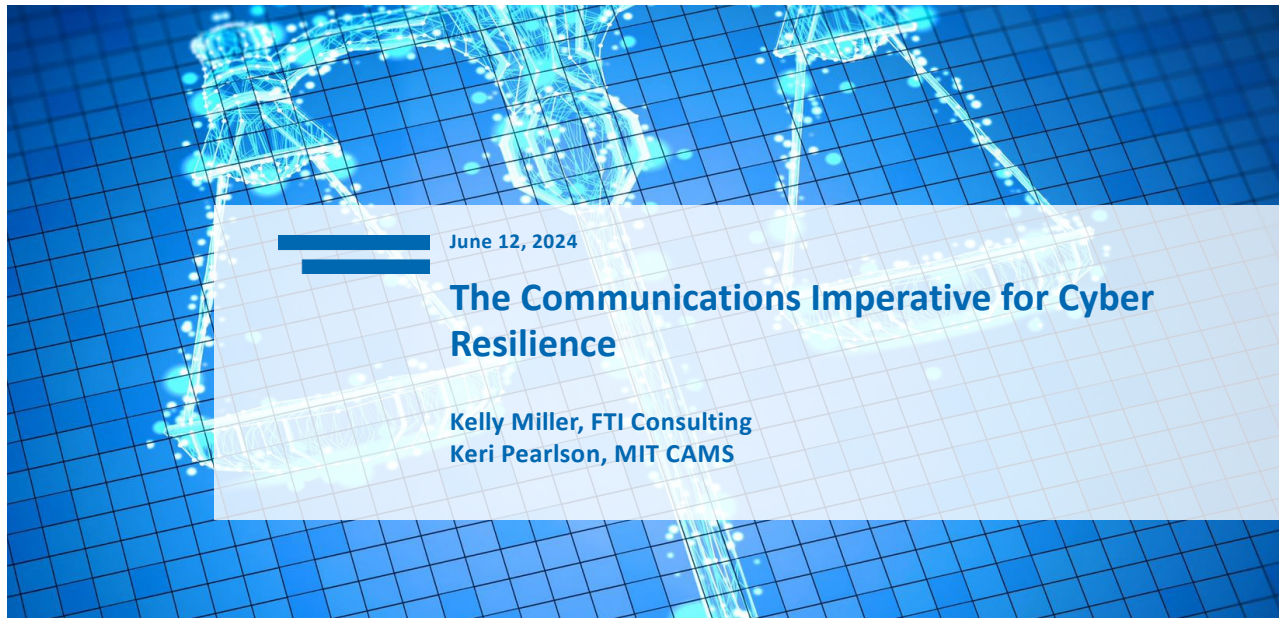


We asked:

What is your biggest concern regarding communicating with stakeholders during a cyber incident?

Miscommunication/accuracy/effectiveness
Speed at which info is uncovered/Time
Right balance between informing and keeping secret
Addressing threat/risk in relatable way to end users
Triggering speculation among clients and employees
Reputation
Info to be shared at different points in time

11



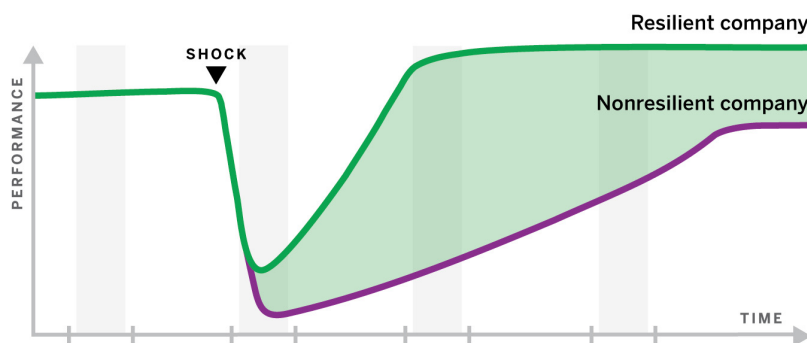
May 2023

12




Cyber Resilience:

Our organizations experience a cyber incident, but recover faster, better, and with less damage (no damage?) to operations, financial positions, reputation, and systems.





The Process of Resilience:





* For more on this model, please see: <https://sloanreview.mit.edu/article/an-action-plan-for-cyber-resilience/>

Communications is an overlooked piece of cyber resilience – and it can be difficult to get right

 TIME CRUNCH	 ABSENCE OF CONCRETE INFORMATION	 INFLUX OF STAKEHOLDER INQUIRIES	 STRESS LEVELS OF ALL INVOLVED
<ul style="list-style-type: none"> Stakeholders will want answers as soon as possible, even when facts aren't fully known. Regulatory reporting guidelines may require you to alert relevant officials in specific timeframe. Concern of incident spreading to other systems requires an immediate response. 	<ul style="list-style-type: none"> Without full certainty, a victim organization may inadvertently share incorrect information. Impossible to quickly determine what data was impacted and to whom it belonged to. Sharing unconfirmed information before investigation is complete could damage key business relationships. 	<ul style="list-style-type: none"> Once stakeholders have been alerted to the situation, their immediate focus will be on if they were affected. Answering complex, technical inquiries will strain existing resources. Stakeholders may not be satisfied until the situation is fully resolved, which could take weeks to months. 	<ul style="list-style-type: none"> Highly technical nature of incidents requires internal IT teams to be fully engaged. Initial incident response phase could take weeks depending on level of impact, raising tensions. Operational impacts to business and/or customers halting business can cause financial concerns.

15

Avoid common pitfalls – impulses are often wrong

Use Terminology Wisely	Avoid Getting Ahead of the Facts	Equip the Front Lines for Success
<p>Ensure the communications strategy is aligned with the legal strategy</p> <p>Remain consistent with respect to the use of terms and phrases that describe the incident</p> <p>Avoid conflating the use of words such as “breach” versus “cyber attack”</p>	<p>Maintain control over the narrative by not getting ahead of the facts</p> <p>Avoid over-promising and/or under-appreciating the severity of the incident by prematurely understating impact</p> <p>Understand that some information will need to be maintained internally</p>	<p>Provide communications guidance and an escalation protocol for employees tasked with managing questions about the incident</p> <p>Continue to keep employees and other stakeholders apprised as a situation evolves and update resources as necessary</p>
Stay Apprised of Media Narrative	Convey Dedication to Cybersecurity	Stay Cautious of Tone
<p>Review media coverage and any public statements made by external parties to identify and correct misinformation as appropriate</p>	<p>Demonstrate a dedication to improving cybersecurity and data privacy practices</p> <p>Share tangible steps the organization has taken to remediate and investigate the incident, including notification to law enforcement, technical security measures, and partnership with external advisors</p>	<p>It can be tempting to lean into the victim mentality... but your customers see themselves as victims too</p> <p>There are many ways to inadvertently cause more panic than necessary</p>

16

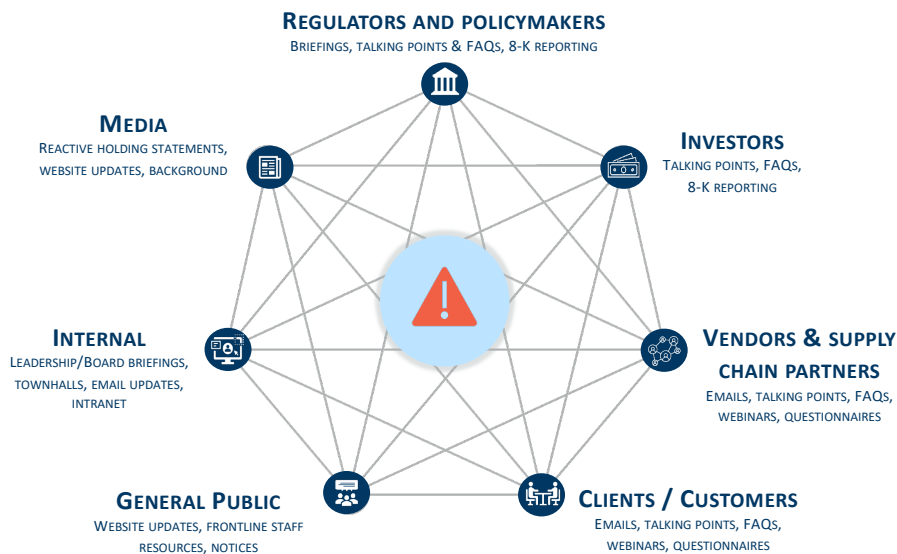
There are three phases of an effective cyber incident communications response



17

17

Communicate with consistency...but tailor to audiences



18

18



Components of a communications playbook

- 1 Instructions for playbook use
- 2 Key messages
- 3 Media strategy and associated statements
- 4 Frequently asked questions
- 5 Stakeholder-specific communications
- 6 Resources, talking points and escalation protocols for front-line staff

19

Questions

Kelly.Miller@FTIConsulting.com
Kerip@mit.edu



20

Discussion



Some of your questions (and ours):

1. Do you address communications the same way for IT and OT cyber crisis?
2. Who should make the final decision regarding how much information to share?
3. When should senior leaders be brought into the fold?
4. What are best practices for cross communicating with different orgs (suppliers? partners? Etc.) during a company-wide incident?

21



22



What's Up Next for our SIG: August CAMS virtual meeting

- **May 15** -CAMS Cybersecurity Innovation Symposium (CIO Symposium May 14)
- **June 12** and **Dec. 5**: Culture Club SIG will meet
- **August 8** (11-12:30 Eastern): CAMS Discuss Research with our Researcher Webinar
- **Oct. 23** (all day) CAMS In Person Workshop

23

CAMS Culture Club/Human Risk Management SIG Archives



Please visit:

<https://cams.mit.edu/cultureclub/>

**To download meeting summaries
from all Culture Club SIG meetings.**

24



THANK YOU!

**We could not do the work we do without our
CAMS members! Thank you for supporting our
work.**

**More info available at: <https://cams.mit.edu> or
contact Debbie or Keri:
defran24@mit.edu, or kerip@mit.edu**

25