MIT Sloan Management Review

How to Build a Cyber Crisis Communications Plan

Leaders building cyber resilience often overlook the need develop a crisis communications plan. Here's how to cons and practice a strong response *before* a hack.

Kelly Miller and Keri Pearlson • September 16, 2024 Reading

Carolyn Geason-Beissel/MIT SMR | Getty Images

Business and IT leaders have made large efforts to build

cyber resilience, or the ability to respond to and bounce back after a cyber crisis such as a data breach or operational disruption. But one aspect of cyber resilience deserves more attention from most organizations: the cyber crisis communications plan. The early hours of a cyber crisis are the worst time to realize that your communications plan is incomplete or nonexistent. Circumstances surrounding an incident, during which communication decisions need to be made, are urgent and chaotic. Adrenaline is running high; everyone, from employees to reporters, is demanding answers; and salespeople looking to protect relationships may even be sharing incorrect information. A leader's initial impulses for communication are often wrong and can create additional problems. That's why truly cyber-resilient organizations must have a cyber crisis communications plan in place — and stress-test it regularly.

Communication around a cyber incident is crucial to mitigating reputational harm, regulatory risk, and financial fallout. Delivering the right information at the right time, in the right tone and channel, takes practice.

What's more, your regular business crisis communications plans may not be adequate for a cyber crisis. While the two share many of the same characteristics, unique considerations surround cyber crisis communications planning. Take stakeholder management, for example. If the crisis plan expects emails to be the main mode of communication but systems are locked, the plan is inexecutable. Cellphones, the primary network for most verbal communication, might also be compromised. Even stakeholder information held on the company's computers

might be unavailable if data is encrypted by malicious code. Planning for cyber crisis communications requires attention to the unique aspects of a cyber incident.

The July 2024 CrowdStrike outage serves as a good example of why organizations must anticipate a variety of cyber crisis scenarios and develop effective response strategies, including communications plans. The outage, which was not a cybersecurity breach but a software update issue that disrupted the operations of companies relying on CrowdStrike's cybersecurity services, was fixed relatively quickly on the technical front. However, the communication challenges that stemmed from the outage lingered for weeks, as customers griped about a perceived lack of contrition in the messaging from CrowdStrike leaders that was delivered via social media and mainstream media coverage.

Many people have been quick to criticize CrowdStrike's technical mishap, but it's crucial to recognize that a similar problem could happen at any organization. No organization is immune to cybersecurity breaches: It's not a matter of if you'll get hacked, but when. This humbling reality should compel organizations of all sizes and levels of sophistication to plan for worst-case scenarios. Having an effective cyber crisis communications strategy in place is essential to ensuring that leaders aren't caught off guard and can maintain stakeholder confidence during turbulent times.

To help leaders build effective plans, we conducted research with cybersecurity experts and executives who had weathered a cyber crisis, asking about their greatest

challenges regarding stakeholder communications. The research was done through surveys and interviews with IT, cybersecurity, and business executives who participated in small group discussions about cyber crisis communications during the first six months of 2024. In this article, we explore the factors that make successful communication during a cyber crisis especially difficult. We also outline a three-phase cyber crisis communications process to help leaders take ownership of the situation, engage with stakeholders, and make a commitment to a path forward. Finally, we share four keys to constructing a strong plan for your organization.

Make no mistake: The speed and effectiveness of an organization's response must be finely tuned and precisely executed. Our research, which also involved a review of major ransomware attacks that have occurred in recent years, found that an effective response was not only about actual cyber defenses but also the quality of communication during the crisis. A cyber-resilient organization is one that has prepared for a cyber incident, can recover swiftly with minimal damage, and communicates appropriately as part of the organization's ability to bounce back.

Four Factors Affecting Cyber Crisis Communications

When we spoke with business and technical cyber leaders, almost all of them said that miscommunication, accuracy, and the effectiveness of communication were their biggest communication concerns during the cyber crisis. Unlike, say, a software programming error or a consumer packaged

goods incident where the facts are quickly ascertained, the facts in a cyber incident typically unfold slowly. What looks like a breach of critical data may or may not be as extensive as initially feared, and the specific information extracted may or may not be as valuable as initially thought. Ransom demands may or may not be met. Sharing the wrong information can only damage recovery because leaders will then need to explain both why the wrong information was shared and what the right information actually is. This can also diminish confidence in future communications.

Communicating too much too soon can also be damaging, our data suggests. Finding the right balance between what to share and what not to is a key concern for leaders. And while transparency is highly valued, there are often details that shouldn't be shared right away, or maybe ever. A leader's impulses on what to share are often wrong: Our data found that leaders often inadvertently trigger speculation, creating an additional hurdle to overcome. Knowing what to share and when emerges from a thoroughly tested plan.

The first step to planning for effective communication during a cyber incident is recognizing the factors that make success so tricky.

1. Time is of the essence.

From the moment a cyber incident is discovered, the clock is ticking. Whether the trigger is a consumer-facing website crashing or a corporate rumor swirling on the dark web, stakeholders will demand immediate answers.

The urgency is often driven by the organization's customers

and connected partners, who have their own compliance needs and incident protocols. Organizations that share data or connectivity feel pressure to respond to their partners' deadlines and priorities, both to meet regulatory reporting requirements and to prevent further damage from the spread of malware.

2. There is little concrete evidence.

Without full certainty of the facts, a victimized organization risks sharing incorrect information that can lead to decreased credibility. In our research, we found numerous examples where leaders insisted on Day 1 that no data had been compromised only to find out later that it actually had. Cybersecurity forensic investigations take time, sometimes months, and the early days of an incident are crucial for building trust. Even if there's no concrete evidence that sensitive data has been accessed, it's important not to prematurely declare that data wasn't touched.

Cybersecurity forensic investigations take time, sometimes months, and the early days of an incident are crucial for building trust.

Leaders must resist the urge to address short-term concerns with statements that could have long-term repercussions. While it might be uncomfortable to lack concrete answers initially, a leader's restraint is an investment in trust-building. By waiting to communicate with confidence and clarity, organizations can ensure that stakeholders will believe future

statements. In the realm of cybersecurity, measured and accurate communication is key to maintaining credibility.

3. A diverse array of stakeholders wants answers.

Shareholders, board members, employees, past employees, customers, partners, and regulators all have unique concerns and require tailored information during a cyber crisis. For example, while investors may be concerned with materiality, employees are more concerned with how to do their work if networks are down.

Producing tailored answers can be resource intensive, and resource allocation during a cyber crisis is already challenging. Priority customers may require white-glove attention and regular updates via lengthy phone calls with top executives. In addition to planning what to say and to whom, cyber-resilient organizations also decide who is the right person to communicate with each type of stakeholder.

Without a system to intake and triage all of the questions, along with a strategy to delegate resources, an organization can quickly become overwhelmed. Each stakeholder requires a different set of channels for proper communication. Here are the main communication types to prepare for, broken down by stakeholder group:

- **Regulators and policy makers:** Briefings, talking points and FAQs, and 8-K reporting.
- **Investors:** Talking points and FAQs, and 8-K reporting.
- **Media:** Statements, website updates, and background interviews.

- **Internal staff:** Leadership/board briefings, town hall meetings, emails, and intranet updates.
- **Vendors and supply chain partners:** Emails, talking points and FAQs, webinars, and questionnaires.
- **General public:** Website updates, materials to be shared via front-line resources such as help desk staff, and formal notices.
- **Customers/clients:** Emails, talking points and FAQs, webinars, and questionnaires.

4. Individual stress levels are high.

Amid the technical chaos of communicating during a cyber crisis, the human challenges often get overlooked. All of the organization's decision makers, who are often stressed and sleep-deprived, are grappling with the potential for saying something that might have career or reputational consequences, or even result in corporate lawsuits. Executives must navigate multiple types of liability risks while guiding recovery efforts. Often, the technical experts are too busy working to fix the breach to accurately share progress with the communications team, adding another stressor to the mix.

These crises don't just create a few hours or days of stress; cyber incidents can drag on for weeks or months. This type of long-term stress leads to poor decision-making and personal burnout. Our research suggests that leaders must approach the life cycle of a cyber incident as a marathon, not a sprint, and communicate often with their teams to reinforce the critical value they're providing during the

response.

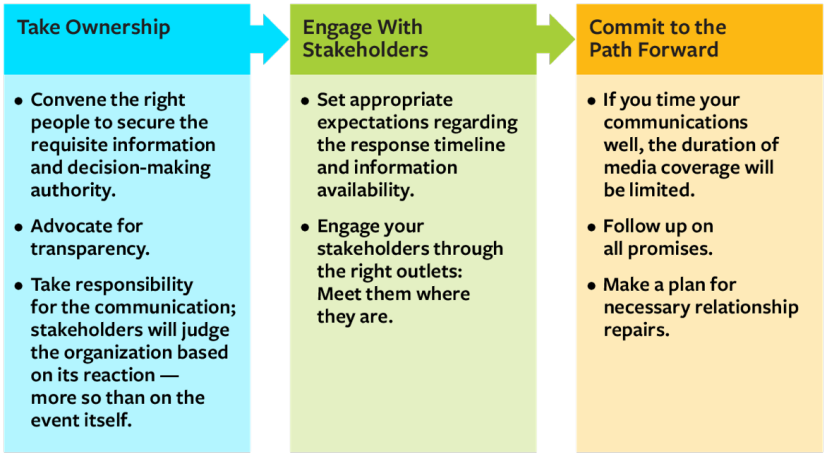
Effective cyber crisis communication from leaders includes acknowledging the human toll of a cyber crisis on themselves, their teams, and their ecosystem of stakeholders and ensuring that people feel valued and supported throughout the ordeal. The resilience of an organization depends not only on its technical defenses but also on the well-being of the people behind those defenses.

Three Main Phases for Effective Cyber Crisis Communications

While every cyber incident has its own twists and turns, our research suggests that there are three main phases for effective cyber crisis communications, as shown in the figure below. For leaders, this process requires a blend of crisis management skills and communication savviness.

Cyber Crisis Communications: Three Phases

During a cyber crisis, the communications work for leaders can be broken out into three key phases. In the first stage, taking ownership, leaders need to build goodwill and set the stage for continued communication. During the second phase — an especially uncomfortable one — leaders must engage with stakeholders before they have complete information. Finally, in the third phase, leaders should follow up on all promises made during the incident and tend to relationships.



Source: FTI Consulting and the Cybersecurity at MIT Sloan research consortium

Phase 1: Take Ownership

Effective cyber-communications responses strike a balance between managing risk and maintaining transparency. Communicators focused on long-term reputational impact are the best advocates for transparent communication.

For example, consider an initial statement from an organization victimized by a ransomware attack. Systems are encrypted and inoperable, and employees have seen a ransom note. An experienced cyber crisis communicator knows how to proceed. Legal and risk-averse voices might be inclined to downplay the incident as an “IT issue” or, worse, to say nothing. But this is the moment where C-suite leaders must claim ownership, acknowledging the situation and sharing appropriate information. Taking ownership builds goodwill with stakeholders and establishes a foundation for effective communication throughout the incident.

Phase 2: Engage With Stakeholders

The second phase of an effective communications response

is perhaps the most uncomfortable: engaging with stakeholders when there is incomplete information. After the first intense days of a cyber incident — once outages have been managed, external advisers are in place, and initial reports have circulated — organizations often face slow-moving restoration efforts. The forensic investigation to determine what happened and what data was impacted, which is crucial for legal notifications and other reasons, typically takes months.

For leaders, discipline and adaptability are crucial during this phase. A regular cadence of communication is often more important than the content of the communications. During these long stretches with little to no new information, stakeholder questions will persist, and frustration can grow due to a lack of updates. A consistent, measured strategy for communicating with stakeholders sets appropriate expectations about the timelines and nature of forthcoming information.

One common mistake is the instinct to overstructure communication processes at the onset of an incident, committing to daily updates when the situation is most intense. During the subsequent drought of information, these daily updates with no new facts can frustrate stakeholders and erode trust.

A regular cadence of communication is often more important than the content of the communications.

Each communication is an opportunity for leaders to build trust by providing new, relevant, and actionable information to different groups of stakeholders. Adjusting communications strategies as trends within stakeholder inquiries become apparent also sends a strong message. For example, if multiple customers are asking the same question, an FAQ section on an easily accessible incident-specific landing page may reduce future customer communications needs.

The appropriate medium for different communications is also assessed during this phase of the process. For example, when customer lists reside on servers that have been encrypted or disabled by the cyber incident, accessing this information for group emails is impossible, and an alternative medium is needed. Some companies turn to social media in a situation like this. If critical operational information is getting buried in search engine results, a paid ad campaign might be a better means of reaching customers who need updates. For example, in one case we studied, hospital leaders didn't want patients showing up for appointments because systems were down, but getting this information out was difficult, given the compromised environment. These leaders chose to reach out using paid advertisements — so when customers looked up the hospital using a search engine, they received updates on the operational issue and instructions about rescheduling their appointments.

Phase 3: Commit to a Path Forward

If an organization executes phases 1 and 2 effectively — by timing responses appropriately, and rigorously responding to

relevant stakeholders — excessive news cycles and public scrutiny can be reduced. However, the incident itself can still erode trust with key stakeholders. Communications are only as effective as the actions behind them. For example, if an organization's cyber defenses were inadequate, no amount of messaging will strengthen its actual defense, and the communications plans should reflect this reality.

When moving out of the crisis, leaders must prioritize following up on all promises made during the incident. The worst misstep an organization can make is to set expectations and then fail to meet them. Stakeholders will remember the failure to fulfill promises more than the incident itself. If the organization committed to investing in strengthened defenses in its messaging, follow-up communications must confirm that it happened.

Not all relationships are equal, and some may be more strained than others during a crisis, requiring tailored communications about promises. Leaders must take stock of different stakeholder groups and individuals, just as they did during the incident, to develop and execute appropriate relationship repair campaigns. By addressing these concerns and following through on commitments, organizations can begin to rebuild trust and demonstrate their resolve to improve security and data privacy.

How to Construct a Strong Cyber Crisis Communications Plan: Four Keys

Great communication decisions aren't made in the heat of the moment. They're the result of careful planning by leaders who have weighed the many conflicting priorities and voices demanding attention.

We spoke with cybersecurity experts and crisis communicators across various industries to identify common pitfalls and pain points in planning and to learn what holds organizations back from true readiness. Our research revealed four key actionable insights to help leaders clear the hurdles as they prepare a cyber crisis communications plan.

1. Expect to modify your plan — then practice.

As we've established, the chaotic beginning of a cyber crisis is not the time to build your communications plan. By preparing ahead of time, the organization can establish an order of attack with details that can be modified as necessary to accommodate the actual situation. The plan should include high-level tactics around whom to contact with what information, and when. Stakeholders include everyone with an interest in the business: C-level execs, the board of directors, general employees, customers, supply chain participants, and possibly the press, regulators, law enforcement, a government cyber emergency response team, cyber consultants, and others whose help will be needed.

Once you have a plan, practice it regularly with tabletop exercises or fire drills at all levels, simulating a cyber situation rather than a general emergency situation. Practicing the plan and its various scenarios is perhaps more important

than the actual plan so that your team is prepared to adapt during a real cyber emergency.

Building the muscle memory necessary to respond quickly makes it possible for the organization to pivot during the crisis.

One note: These communications plans should not exist in a vacuum. Instead, leaders should seek to integrate them with existing plans, such as a cyber security incident response plan and a comprehensive crisis plan for the organization. This ensures that the organization is ready to move beyond theoretical documents and fictional press releases because governance and processes are aligned to preserve stakeholder relationships during a real incident.

Building the best responses and muscle memory necessary to respond quickly makes it possible for the organization to pivot during the crisis. As former U.S. President Dwight D. Eisenhower once said, “Plans are worthless, but planning is everything.”

2. Choose the right decision makers to convene in a crisis.

When a cyber crisis strikes, it’s imperative to gather the right people with the necessary information and decision-making authority. But often, a leader’s initial impulses are to bring only a small core of people together to oversee recovery and minimize leaks. These impulses are usually counterproductive. Legal, cybersecurity, data privacy,

investigative, communications, and operational teams (or consultants) need to be part of the discussions from the beginning. Planning on when and how to assemble the mix of point people ahead of time will ease some of the stress later.

Assigning and adhering to clear lanes of responsibility for communicating different aspects of the cyber crisis also ensures that everyone knows their role. This lets team members focus on their specific tasks with minimum redundancies or bureaucratic delays. This clarity not only makes everyone feel essential to the process but also streamlines the communications effort and emphasizes its integral role in the response strategy. During the crisis, communications experts need to be ready to share strong messaging and strategy with internal and external stakeholders, even when faced with competing priorities.

3. Avoid analysis paralysis.

Planning cyber crisis communications can sometimes become more complex than necessary. Initially, leaders may want to consider every reasonable option for communicating what is happening. However, few people across the organization will have concrete answers to stakeholder questions. Testing a well-thought-out cyber communications plan can help the team avoid the paralysis that comes from having too many choices for each step of recovery communications.

Meet your organization where it is today, and apply principles of change management. Communicators and leaders who aim to kick-start cyber crisis communications planning must understand their organization's capacity to

absorb and execute change. If significant pushback from colleagues is expected, leaders should consider starting with incremental, and perhaps smaller, initiatives. Demonstrating value through early wins and building trust with internal stakeholders can pave the way for a more robust program.

4. Prioritize building communications structure versus press releases.

Having the right communications structure and processes in place is far more critical than having draft press releases ready. This is another place where first impulses are often counterproductive. When an organization faces a particular crisis, finding the right prewritten drafts or templates can become overwhelming. Instead, having the right decision makers identified and empowered ahead of time will prove to be more valuable.

Before drafting messages, ensure that you have essential process elements in place: Do you have a way to reach clients if corporate email is down? Have you established relationships with regulators to ensure that there are open lines of communication for reporting requirements? Who has the closest relationship with local or trade industry reporters? Do you have a checklist of stakeholders who need to be informed during an incident? Can you quickly pause marketing campaigns?

Building these mechanisms to address key issues and avoiding missteps are more important than crafting the perfect words. Holes in a communications plan can become major disruptors to effective recovery. Circling back to the CrowdStrike crisis, we see an example of this: The technical

issue was solved relatively quickly, but the crisis lingered because of a complex communications challenge.

The beginning of a cyber crisis can be one of the worst days of an executive's career. In the hours following a hack, communication is one of the most critical challenges amid the many issues leaders must address quickly. Yet it's often one of the last challenges to be considered in cyber resilience planning.

However, with proper planning and rigorous pressure testing, teams can build the capability and, ultimately, the confidence to navigate the actual twists and turns they will face during a cyber crisis. In an era when cyberthreats are an ever-present reality, investing in robust communications strategies is not just advisable — it's essential for cyber resilience.

Topics

Leadership | Managing Technology | Crisis Management | IT Governance & Leadership | Security & Privacy

ABOUT THE AUTHORS

Kelly Miller is a managing director in the Cybersecurity & Data Privacy Communications group at FTI Consulting. Keri Pearlson, DBA, is the

executive director of the CAMS (Cybersecurity at MIT Sloan) research consortium.

TAGS:

Communication | Corporate Reputation | Cybersecurity | Scenario Planning | Trust

REPRINT #: 66201