5 STEPS TO PREPARE YOUR CYBERATTACK COMMUNICATIONS AND RESPONSE PLAN
5 Steps to Prepare Your Cyberattack Communications and Response Plan

According to IBM, there were 1.5 million monitored cyberattacks in the U.S. in 2013.\(^1\) Additionally, the Ponemon Institute conducted a study revealing that data breaches cost U.S. organizations, on average, $5.4 million per incident.\(^2\) Despite a company’s best efforts, a security breach can cripple your network, hamper communications and expose sensitive corporate data. In addition to causing this level of frustration, and not to mention serious harm to your company’s reputation, cyberattacks simply impact your ability to conduct business effectively.

If recent, well-publicized security breaches, such as those against Home Depot, eBay, UPS and most notably, Sony Pictures, have taught us anything, it is that the cyberattack protection and preparedness paradigm has shifted. Organizations can no longer rely on security defense measures alone—instead, they need to assume and admit, that a cyberattack is not just a possibility, but a likely event that will impact the organization at some point in the very near future.

So how can organizations prepare for the inevitable? By readying your cyberattack communications and response plan immediately. Having a strategic plan in place for just such an event can be the key to business continuity and crisis resolution.

While no two events are the same, there are 5 key steps that should be followed in order to ensure a quick and successful event resolution for a critical event situation.

**Step 1: Deploy Your Critical Communications System**

**Step 2: Ensure All of Your Employees Are Using the System**

**Step 3: You Have Your System, Now Be Prepared to Use It**

**Step 4: Optimize Your Cyber attack Response and Delivery**

**Step 5: Communicate Externally and Alert Your Customers**

---

Step 1: Deploy Your Critical Communications System

A critical communication system is essential to automating the response, communication and collaboration process for your most essential response team members. As Sony’s CEO Michael Lynton recently detailed, having a critical communications system in place, like in this case, Everbridge, was critical to ensuring effective internal communication in the immediate aftermath of the cyberattack.

According to the Associated Press, at Sony Pictures, “a close-knit senior management team of 10 to 15 people relied initially on word of mouth, an emergency notification system and town hall meetings to disseminate information and calm fears.”

In the case of a cyberattack, you likely will need to leverage your IT operations team. Deploying a system ensures you have the ability to contact relevant or on-call members of your IT team via multiple methods. If contacts don’t respond, the message can be automatically escalated to other resources, optimizing employee productivity during IT incidents. Simply put, if the right people in your organization are notified about an issue, the problem can be identified and resolved quickly and efficiently.

“MAKE SURE YOUR PROVIDER OFFERS...”

- Cloud-Based Service
- Redundant
- Global
- Secure
- 24x7 Support

www.Everbridge.com
Step 2: Ensure All of Your Employees Are Using the System

While a critical communication system will ensure that your IT Operations and response team is ready to act and collaborate immediately, all of your proactive communications will fall on deaf ears if the rest of your staff is not effectively notified of the situation and next steps. As Sony Pictures CEO lamented, one of the issues that the company faced was the scarcity of employees that were actively registered on the system. According to the Associated Press, “While most Sony employees already were on the Everbridge emergency notification system, workers recruited the rest to sign up. If he had to do it again, Lynton said he would have made it mandatory to already be on it.”

To combat this, your organization must make participation mandatory and require all employees to register for the system. Without this, you will be forced to rely on time-intensive and unreliable manual means, such as call trees, to reach all of your employees with the key information that needs to be disseminated in both the immediate aftermath and ongoing wake of a cyberattack. Ensure that your whole team is not only registered, but knows how to receive and consume the information by providing relevant tutorials.

When having employees register, collect quality and relevant data, consider the size and mobility of your organization. If you have employees dispersed on travel or who work remotely, make sure you have location data built into the system to identify where they are. Additionally, don’t rely on one or a few modes of communication. It is important to remember that people answer messages differently depending on a number of facts including time of day, day of the week and location. Encourage employees to provide multiple contact paths such as SMS, work and personal email, cell and many more. By doing this, you can increases the chances a message is received, confirmed and responded to, ultimately leading to a fast event resolution.

Step 3: You Have Your System, Now Be Prepared to Use It

As any effective business continuity professional will tell you, having technology in place is only part of the battle: the solution is ineffective if you do not have the proper plan and process in place to act according. An effective cyberattack response plan enables a company to control an incident, rather than have the incident control it. Faster awareness of the situation, and better collaboration to identify the source and solution, will ultimately lead to faster resolution of incidents.

First and foremost, when in the planning stages make sure you identify what individuals and groups need to be alerted in the event of a cyberattack. It is equally important to ensure messages are relevant to the recipients. For instance, your IT response team should have a...
unique message compared to your HR or senior leadership teams. For this type of event, your IT response team should be notified and systematically activated to start fixing the issues to minimize any financial impact the outage may have on your business as well as customers’ businesses. Afterwards, key executives and stakeholders need to be alerted to facilitate proactive decision-making.

If your critical communication system has the capabilities, draft an incident template. By doing this you can create the whole notification process, including messages and escalation processes – while having the option to edit on the fly during the incident – for a cyberattack prior to it ever happening. This will allow you to practice the event and become more accustomed to the system without having to deal with the anxiety from a live-event. Being able to run through an event will uncover any deficiencies in your processes, rates of response and confirmation rates – giving you the ability to improve them before facing a real life situation.

**Step 4: Optimize Your Cyberattack Response and Delivery**

During an incident, what contact methods would be used to get messages to stakeholders? Can key contacts be reached quickly? This is where targeting the individual, rather than the device, comes into play. Multimodal messaging is key to critical communication delivery success, as no single delivery path is ever 100 percent reliable. The more communication paths that are available, the more likely key stakeholders will receive important information.

Targeting individuals, and their typical workflows, guarantees the team responsible for fixing the problem can be alerted first. And, of course, keep in mind that this is increasingly a global process – with executives, helpdesk employees and other staffers located around the world. This is just another reason why it is important to ensure that you have the ability to contact these critical members via multiple contact paths and devices—SMS, email, landline, push notification – at a moment’s notice, and with the right information and context.

In addition, an optimized approach to cyberattack communications and response should also involve integrations with tools for situational intelligence. By incorporating social media feeds and other threat alerts, security executives, business continuity professionals, and crisis
management teams can monitor public perceptions and other intelligence in real-time to determine the best approach for response and communication before an event may spiral out of control.

**Step 5: Communicate Externally and Alert Your Customers**

Don’t forget the final important piece of cyberattack response preparedness—external communications. This group involves dealing with the stakeholders who are affected. These may include customers, partners and internal users, where the concern is often financial. It’s crucial to keep these individuals and groups in the loop, because if they’re left in the dark, they can’t effectively cope with the incident. In this final stage, a well-crafted response and message plan communicated to impacted customers and the public provides consistency and transparency, and mitigates fear and anxiety, across all communications channels.

In terms of external communications with external parties, the key is to be transparent, proactive and remain visible during critical events. Misinformation can spread like wildfire on social media and escalate a situation, so maintaining a presence can quell rumors, improve trust and retain customer loyalty. It is also important to provide relevant updates – as an incident progresses, let customers and the public know information as soon as it is relevant and appropriate to share. An added benefit is a reduction in service calls, since customers know the company is addressing the issues.

To conclude, it is critical to reiterate that when an IT incident occurs, internal communication within the IT organization and external communication with your customer community are both important. An automated, template-driven system, guided by a methodical and well-executed critical communication plan, can help you reach the right people at the right time to enable IT to resolve problems faster, while helping internal and external stakeholders make plans and take actions based on accurate, up-to-date information.
About Everbridge

Everbridge provides a unified critical communication suite that helps clients be better prepared, make better decisions, and respond quickly and confidently during disruptive events. When an incident happens, whether it’s a natural disaster or an IT service outage, we automate communications to ensure that the right messages get to the right people at the right time.

Widely recognized by analysts as the market leader, Everbridge solutions are trusted by clients in all major industries and government sectors to connect with over 50 million people around the world.

THE ONLY END-TO-END PLATFORM

• **Planning**: Everbridge is easy to set up, maintain, and organize, meaning that you’re always ready for a quick, coordinated response. Everbridge ensures that the right messages get to the right people - with the most advanced opt-in portal on the market, streamlined integration with internal and external data sources, and simple group and contact management.

• **Assessment**: When trouble strikes, you need rich insight, presented simply - so you can quickly assess potential impact and make an informed decision to avoid loss. Everbridge offers the only solution on the market that meets these demanding requirements, with the most advanced interactive dashboard in the industry.

• **Response**: In critical situations, ease-of-use can mean the difference between an effective response and a mistake that carries serious consequences. Everbridge is engineered to be simple to use under pressure, with a user interface that accelerates time-to-message and reduces the likelihood of errors.

• **Delivery**: Even during large-scale disruptions, Everbridge stays on. The most advanced platform in the industry ensures that you reach your contacts - every time. And with worldwide coverage and capabilities, including globally local calling infrastructure and data storage, we’re ready to support you wherever your people are in the world.

• **Visit** [www.everbridge.com](http://www.everbridge.com) **to learn more.**