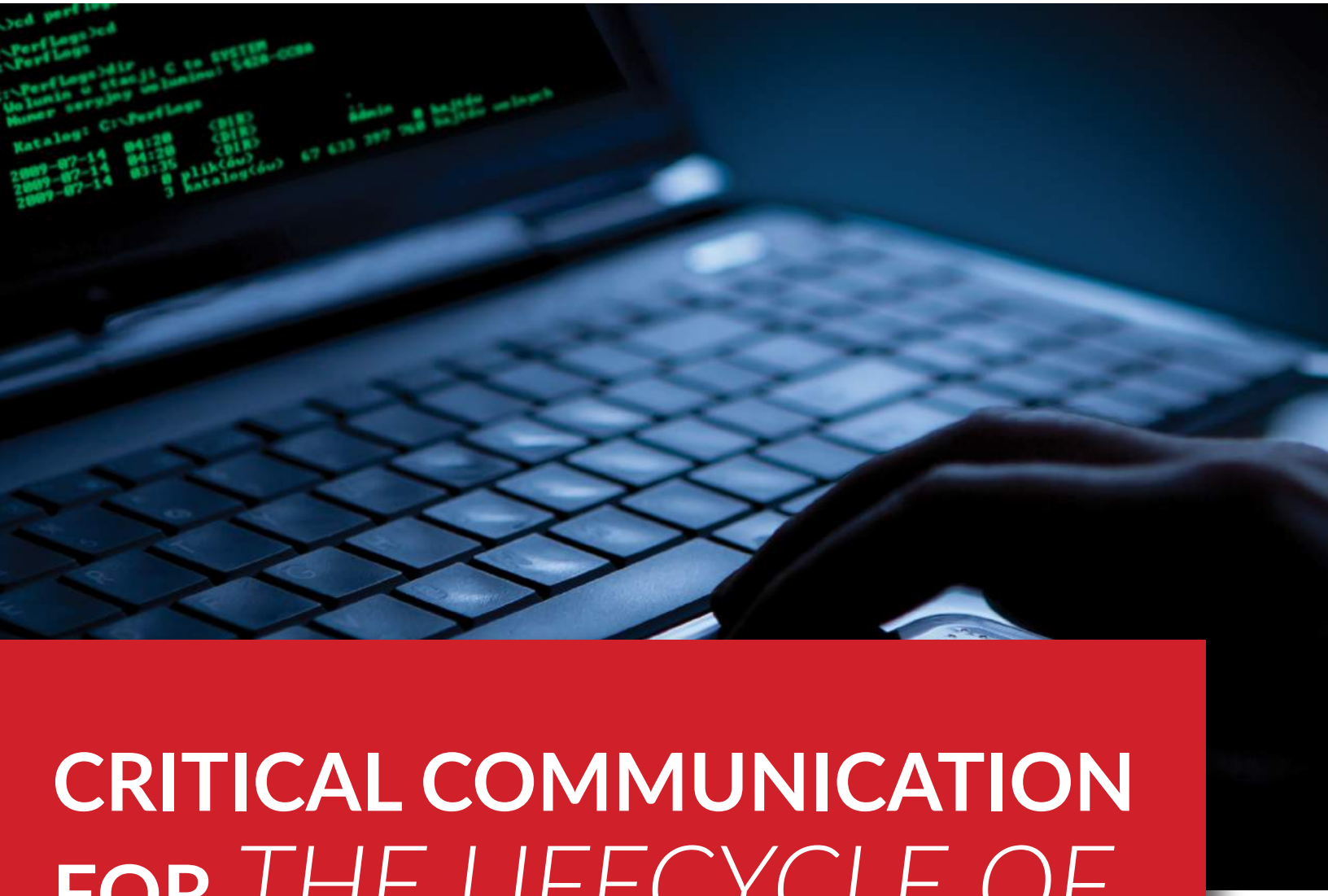
everbridge



CRITICAL COMMUNICATION FOR *THE LIFECYCLE OF A CYBERATTACK*

www.everbridge.com

Communication for the Lifecycle of a Cyberattack

At some point, it is almost inevitable that your company will face a cyberattack. According to IBM, there were 1.5 million monitored cyberattacks in the U.S. alone in 2013. While you may believe that your IT systems are secure, the reality is that systems are used by humans who are vulnerable to phishing and other cyberattack techniques. While your organization should take proper steps to ensure your systems are as secure as possible, you should also assume you are already under attack right now and allocate resources for incident response. Preparing for the worst will ensure you are able to promptly counter the breach, contain damage and communicate effectively with all affected parties.

This white paper outlines actions you can take at various stages of a cyberattack:

- Prior to a cyberattack
- In the immediate aftermath of an cyberattack
- After action communication

Communication During the Lifecycle of a Cyberattack

Preparing for a Cyberattack

To prepare for an eventual attack, the first thing your organization needs to do is analyze all legal obligations. Certifying that your systems are PCI-compliant, for instance, helps to reduce your company's liability in the event of a breach. However, that process is just the start — compliance is ultimately about minimizing liability, rather than securing your system and responding to attacks.

In addition to ensuring compliance, you will need to invest in the resources necessary to protect your system, as well as create a useful incident response plan – including use of s a critical communication system. As part of this preparation you will also need to

brainstorm different scenarios you could face and create incident templates for specific case studies. Conduct training drills to walk through the each incident, as this will allow you and your team to see what worked, what didn't work, how long it took to respond, the event duration and more. As the saying goes "practice makes perfect", and the more frequently you can practice for different situations, the better equipped your team will be to respond quickly to an attack.

Immediate Responses to a Cyberattack

By establishing a plan for dealing with cyberattacks in advance, you can avoid making decisions in the moment — decisions that probably won't match a comprehensive, well thought-out cyberattack response and communication plan. If you aren't careful, what you do during a crisis can create more damage than the crisis itself.

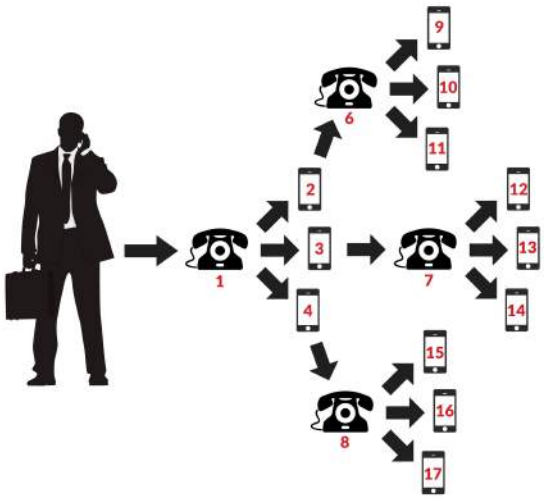
The first step should be to proactively set up an incident management team and instill them with the authority to make decisions and act on them, rather than forcing them to scramble for the "okay" in the midst of a crisis. Your incident management team should also include someone from your legal team, if only to ensure that you're checking the appropriate boxes to minimize liability as you're responding to an attack.

> Sony's CEO Michael Lynton recently detailed how they used Everbridge's critical communications platform to deal with a recent cyberattack. The lesson: set up all of your employees on the communication system *before* an incident.

One of the more difficult decisions to make as part of your incident response plan is to decide when your organization should engage law enforcement. Unfortunately, this is a decision that can't really be made until you see the extent of a real cyberattack. In general, bringing in the FBI, or any other relevant law enforcement, helps show customers that you're taking the appropriate steps to respond to an attack, but the need to protect your brand should be balanced against concerns such as making public information available that will be relevant to a lawsuit.

Effective Communication after a Cyberattack

Setting your communications plan up requires consideration of all the stakeholders: you need to control the flow of information as much as possible. Depending on the severity of an attack, you may need alternate methods of communication. In addition, your organization may not be able to immediately guarantee that a hacker doesn't have access to your environment — that he or she *can't* monitor or control your email and other communication tools. You can get around these concerns by planning ahead and establishing the redundant tools that your team will use in the event of a breach.



One of the most important tools that you can deploy following a breach is a critical communication system that will automate the response, communication and collaboration process for your most essential response team members. In addition to notifying all relevant employees, deploying a system ensures you have the ability to contact relevant or on-call members of your IT team via multiple contact paths. If contacts don't respond, the message can be automatically escalated to other resources, optimizing employee productivity during IT incidents. It is important, however, to have a system that does not rey on your organization's infrastructure, as this can be susceptible following a hack. A hosted, or SaaS solution, is ideal since it resides outside your organization's network.

Alerting and updating staff and stakeholders isn't enough during a crisis.You're also going to need to notify your customers after a cyberattack. It's crucial to keep these individuals and groups updated, because if they're left in the dark, they can't effectively cope with the incident. **The key is to be transparent, proactive and remain visible during these 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.

Keep in mind that customer communications can be tricky, depending on your industry. HIPAA, PCI, PII and SOX all add their own layers to the external communication process. Having an IT communications plan that includes solutions for secure messaging and data encryption will ensure that you won't be trying to figure out these details in the midst of cleaning up from a cyberattack.

In the wake of a cyberattack, several groups may need to be contacted, and each may need a specific communication strategy:

- Frontline IT staff
- Internal staff
- C-level executives
- Partners
- Affected customers
- Non-affected customers
- Press
- Law enforcement
- Legal counsel

By having a good plan in place, your marketing team can be allotted ample time to put together an effective strategy to deal with public fallout because of a cyberattack.

What’s Next? How Proactive Planning Empowers Your Cyberattack Response

A well-designed IT incident response plan will help your organization establish standard response processes and communication protocols, making it easier to respond to cyber threats quickly, and in an organized manner. Otherwise, in addition to inflicting major financial losses, lack of timely responses can damage the reputation of your company and cost you customers. Fortunately, an automated critical communication system, guided by a methodical and well-executed IT response plan, can help you reach the right people at the right time to keep internal and external stakeholders informed, while enabling IT to resolve problems faster and more successfully. Additionally, tools with the right functionality, such as reporting capabilities can help your team verify continuous improvement. With these reports you can analyze how your team performed, who responded, how fast responses were delivered, and even see how long it took from the first notification broadcast to the last event resolution broadcast. Pairing good preparedness planning with a system can be the ultimate cyberattack defense strategy.

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.s

Visit www.everbridge.com to learn more.