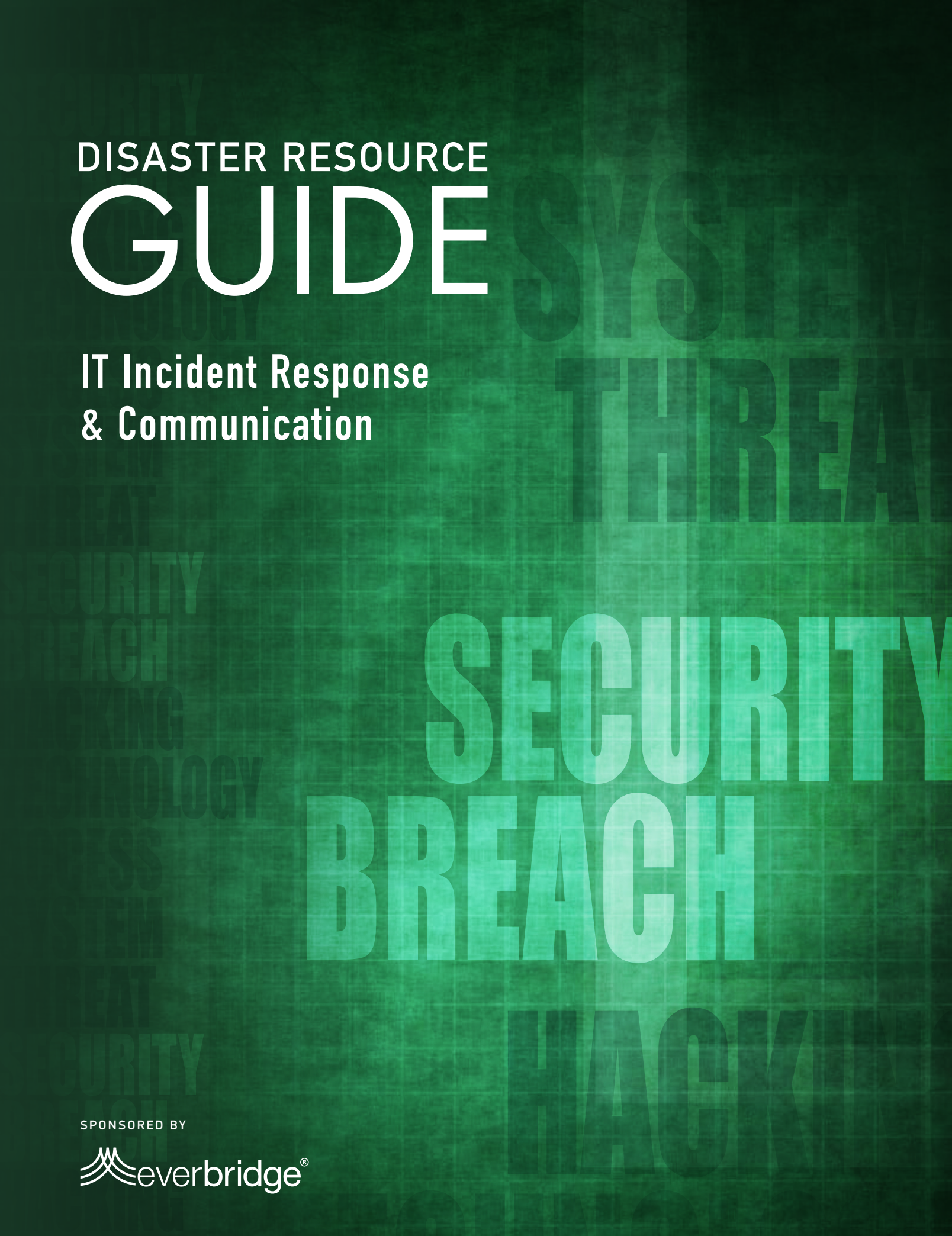
DISASTER RESOURCE GUIDE

IT Incident Response & Communication



SPONSORED BY

everbridge®

DISASTER RESOURCE GUIDE

SPECIAL EDITION

The Disaster Resource GUIDE has been published since 1996 by The Emergency Lifeline Corporation of Santa Ana, CA. Emergency Lifeline was founded in 1985 by Kathy Rainey in response to the devastating Mexico City earthquake, with the mission to help organizations, government agencies and families prepare for earthquakes. The GUIDE is an extension of that mission and provides valuable resources to businesses and other organizations worldwide to help them build resilience.

On the Web Visit the Online GUIDE for more on this subject. **www.disaster-resource.com**
Crisis & Emergency Management • Disaster Recoverey • Business Continuity • Homeland Security

COMMUNICATING DURING IT EVENTS

Information!

It is the lifeblood of most organizations. Without information we cannot connect with colleagues, customers, or the public. We cannot maintain services or produce products. Keeping information both available and secure is absolutely critical in today's 24/7 world.

When any threat to an organization's information occurs, nothing short of an immediate response is appropriate. But with people scattered far and wide, and connected with a multitude of devices, how does an IT group get all hands on deck and return systems to normal?

This special IT Incident Response & Communication edition of the GUIDE has been made possible by our sponsor, Everbridge. Founded after the tragic events of 9/11, Everbridge has developed SaaS-based solutions, which help organizations of all sizes quickly and reliably communicate during any type of emergency or mission critical business events – from man-made or natural disasters to cyberattacks and data breaches. They have partnered with the GUIDE for many years to help organizations worldwide build resilience.

This edition of the GUIDE will help you develop your communications strategy during an IT event, breach or cyberattack. One article offers valuable tips for evaluating different solutions. Another article, by longtime GUIDE author Regina Phelps, will help you develop effective training exercises – something every Business Continuity Professional needs to conduct BEFORE an event. Check out all the articles!

We hope you find this information valuable to your organization! As always, I'd love to hear from you if you have thoughts about this subject, or if you have ideas for a future Special Edition of the Disaster Resource GUIDE.

Kathy Rainey
Publisher
Disaster Resource GUIDE
publisher@disaster-resource.com

One-Stop GUIDE

The comprehensive Disaster Resource GUIDE, published since 1996! Don't miss the upcoming 17th edition, a free resource for businesses and government agencies worldwide.

To subscribe, visit
www.disaster-resource.com/subscribe

Special Editions

Special topic editions of the GUIDE delve deeper into single content categories such as facility issues, IT alerting, satellites, etc.

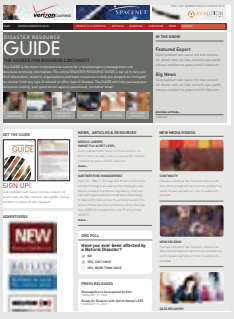
Sign up at
www.disaster-resource.com/subscribe

Continuity eGUIDE

The Continuity eGUIDE is a Wednesday newsletter which provides a concise snapshot of the business continuity and emergency management industry from around the world.

Visit
www.disaster-resource.com/subscribe

Website



The Online GUIDE is the digital platform connecting industry professionals to each other and to valuable educational content, services, news archives, press releases, and hard-to-find products and solutions to help any organization develop resilience.

Visit www.disaster-resource.com

Planning & Management | Human Concerns | Information Availability & Security | Telecom & Satcom | Facility Issues | Crisis Communications & Response

6 KEYS TO DEVELOPING A CYBERATTACK TRAINING EXERCISE

BY REGINA PHELPS

It seems there isn't a day that goes by without another story of a cyberattack or breach. It has almost become a "breach a day"! Not only is there confidential company or customer information exposure to worry about, these events are expensive on many levels: Detection of the problem in the first place, recovery of data, the loss of information, and disruption to the business, among other things. And, of course, this does not take into account the damage to a company's reputation and loss of current and future business. The Ponemon Institute found the average annual cost of responding to cyberattacks was $12.7 million, up 96 percent over the previous five years.[1]

Companies are spending millions of dollars to prevent these attacks from occurring, which is a wise and prudent investment. Few, however, is talking about how to deal with the impact of such a breach. We have surveyed our clients, professional colleagues, and firms and found no one is planning for the impact.

We have done numerous real world cyberattack exercises to train organizations on mitigating the impact of a cyber breach and have found them to be the most effective and rich narratives we have ever used in over thirty years of practice. Do you want to get your executives and incident management team ready for such a cyberattack? Then you need to do a cyberattack training exercise.

What Makes Cyberattack Training Exercises So Different?

One of the things I often hear continuity professionals say is that they "plan for the worse-case scenario." Whenever I hear that come out of someone's mouth, I immediately stop them; this is simply not true. We don't plan for the worse-case scenario, we plan for what we think will happen, what is called a "routine" emergency. What we plan for may be a really bad situation, but there is not enough time, money, or risk appetite to plan for the truly worse-case scenario.

"Routine" Emergency

To be clear, routine emergency[2] does not mean "easy." A routine emergency can still be difficult and challenging. In this context, "routine" refers to the relative predictability of the situation that permits advanced preparation. This risk is in our risk profile and we likely have been able to take advantage of lessons learned from prior experiences. You are likely to have thought about what to plan for and what is needed, and you have probably trained for them and done exercises for them. Our incident management, crisis communications, business continuity, and disaster recovery plans are filled with strategies to manage routine emergencies.

"Crisis" Emergency

A crisis emergency[3] is a much different animal. These types of events are distinguished by significant elements of novelty. This novelty makes the problem much more difficult to diagnosis and then deal with. This type of emergency can have the following characteristics:

- The threats have never been encountered before, therefore there are no plans to manage it.
- It may be a familiar event, however, it is occurring at unprecedented speed and therefore developing an appropriate response is severely challenging.
- There may be a confluence of forces, which, while not new individually, in combination, pose unique challenges to the response.

The novel nature of a crisis emergency becomes a game-changer. Our plans, processes, training, and exercises that may work well in routine emergency situations are frequently grossly inadequate in a crisis emergency, and may even be counterproductive. We realize that we have to start from scratch.

The crisis emergency also requires different capabilities; in other words, the plans and behaviors we use for routine emergencies just won't work. The first thing we must do is to identify the elements of the novelty; we must determine what makes this situation so different from others. In a cyberattack or breach, this novelty can often surprise us. We might begin the process thinking it is one thing, and then over time, we realize it turned out to be something quite different. For example, we may think we are dealing with a routine IT problem or outage, and then over time, we see it is something more significant and sinister.

Senior management needs to understand the value that will come from an exercise and offer complete support.

Once we have identified the real problem and understand that our routine plans won't work, we have to improvise response measures that will be suitable to cope with the unanticipated aspects of the incident. In other words, we are in new territory; this hasn't been done before. Created out of necessity, these responses may be actions quite different than ever done before. Handling a crisis emergency may feel like you're building an airplane while flying it at the same time. It's not pretty, but it may be necessary.

Lastly, in a crisis emergency, we must respond in creative ways and, at the same time, be extremely adaptable as we execute these new and improvised solutions. We have to be on "full alert" at all times, as we don't know how the situation will change, and we must be prepared to shift or dart at a moment's notice. All of this makes people quite

CONTINUED ON PAGE 6

CONTINUED FROM PAGE 5

anxious, and during an exercise, this anxiety often manifests itself in varying degrees of excessively loud voices or hushed voices, frantic activities, and nervous laughter.

There are three styles of exercises that can be used with a cyber narrative: Advanced Tabletop, Functional, or Full Scale.

Six Keys to Developing and Managing a Cyberattack Training Exercise

To manage this very different type of exercise, you need to have six things in place to make it work:

1. MANAGEMENT SUPPORT

Right off the bat, senior management needs to understand that a cyberattack training exercise is likely to produce many learnings and issues that will need to be resolved, and it will present topics that they have never thought about or deeply understood. This could easily make people feel uncomfortable with quite a few unanswered questions at the end of the experience. As you explore the topic, you will also likely need to provide some cover to the IT and Information Security departments so that it doesn't become a blame game or a witch hunt.

2. A WILLING IT DEPARTMENT

IT needs to be an active planner in the exercise. You need several excellent IT staff members who will not be players in the exercise to be part of the design process. You need them to help you determine what the cause will be. When you first begin, this will undoubtedly make them uncomfortable, because in the back of their mind, they are going to be fearful of being blamed. You'll need to reassure them that's not the goal of the exercise.

The first question you need to ask the IT department is, "Could we be hacked?" The answer will inevitably be "yes." The next question is, "How could that happen?" The list is long but could include things such as phishing, watering holes, or infected flash drives. You just need to find a likely means, not a deep exploration of the intrusion. You need the IT team as your ally and you may need to provide them some cover.

3. TWO DESIGN TEAMS

You need two design teams: An IT/Information Security design team, and a standard Exercise Design team. The IT/Info Sec team needs to do a deep dive on the narrative and develop the timeline of issues that happened before the exercise's scenario date, and then provide a very detailed timeline of what happens during the exercise. Once they have developed the breach timeline, the other design team can begin to develop their injects.

The standard Design Team should include key lines of business, Human Resources, Communications, Facilities, Security, and any other key departments. Those team members should take the IT narrative and timeline, and develop their injects, which will tell the story of the IT problems from their perspective. Remember: In an exercise, if you don't tell the players what's happening, they don't know what's going on and will invent things. The injects are the way we tell them the story.

4. THE RIGHT EXERCISE TYPE

There are three styles of exercises that can be used with a cyber narrative: Advanced Tabletop, Functional, or Full Scale[4]. What they have in common is a Simulation Team. This exercise requires a Simulation Team to make it work. The teams going through the experience need to have someone to speak to as they work through the problems. If you don't have a Simulation Team, you will not be able to work through the issues to a deep-enough level to gain value from the experience.

5. INTERWOVEN NARRATIVE AND INJECTS

The narrative for this exercise will have lots of nooks and crannies. It has a certainly complexity that can't be avoided. The story progresses through the injects, and the injects must "dance" with the IT narrative. The exercise players have to tease the information apart, work with the Simulators to figure out what's going on, and then improvise a plan. When they develop that plan, then the Simulators have to adapt to the new plan and, in some cases, create injects "on the fly" to make it all work.

The narrative and the injects are constantly ebbing and flowing together to tell the entire story.

6. MAKE IT PUBLIC

One of the key aspects of this narrative is the potential damage to the reputation of the company. To damage that reputation, we have to "out" the narrative. We usually do this early on in the exercise by having our "perpetrator" post the story on a social media platform such as Twitter. (NOTE: Of course, we don't put a real post on Twitter. This is all done via "exercise magic.") We often have our AV team produce videos in a similar style as a hacker video, such as those done by Anonymous[5]. In exercises we have done, we play such a video for the participants, and watch as their jaws literally drop.

To make it even more interesting, we then create a second video by one of the local news stations, saying they are sending reporters to the company under siege seeking official comments and interviews with executives. Mission accomplished! Company outed! The players then have to deal with the fallout.

Communication Challenges

On first glance, you may not think this exercise presents unique communication challenges. Think again! There are many actions that are likely to occur in such an exercise that will severely challenge communications. In addition to 'standard' communications issues of putting out press releases and social media posts addressing the issue in general, bigger problems occur if the decision is made to cut the company's internet connection. In even more severe cases, the decision may be made to cut the core network. If connectivity is cut, here are some of the communication challenges you might face:

- If your phone and voice mail system is VOIP-based, you may lose your company phone system, severely hampering communication.
- If your employee hotline runs through your voice system, this could be lost.
- If your company website is hosted in-house, it may go down, meaning your customers, employees the general public, and the media can't find you. (If it's hosted by a third party who hasn't been affected by the breach, you may not have this problem.)
- If company telephone bridges are running through your phone network, they may not be available.
- If you bring down the core network, every computer becomes a standalone machine with no access to your company's records. Your human resource information, employee contact information, vendor lists, or other key phone lists may be inaccessible.

How will you communicate? Once this breach is public and everyone knows, your need to be available, communicating, and visually managing the situation is critical. Our clients with third-party or outsourced emergency notification systems (ENS) were ahead of the game. The big plus for them is being able to use their ENS for the following activities:

- **Employee information:** Pushing information to employees about the company status, and providing talking points and other key pieces of information.
- **Conference bridges:** Using toll-free conference bridges for employee, vendor, senior management, Board of Directors, and other key stakeholder phone calls.
- **Stakeholder groups:** Using pre-defined groups that had been created for all of their key stakeholders to push information via phone, text or email.

If you don't currently use an ENS or IT incident notification system, this may be one of the key learnings in the exercise. If you have an ENS but only use it for a limited set of contacts (i.e., your employees), you will quickly discover that there is a lot more that it can be used for which makes good business sense. Get the most out of your money by using your ENS for as many things as make sense.

Going Forward

For businesses, the risk of experiencing a data breach is higher than ever with almost half of organizations suffering at least one security incident in the last 12 months.[6] The C-suite and Board members can no longer ignore the drastic impact a data breach has on company reputation. Meanwhile, consumers are demanding more communication and remedies from businesses after a data breach occurs.

If the future is anything like the past, cyber incidents in our company's lives are not going away anytime soon. Life will continue to be complicated. Plan your next exercise to be a cyber exercise. Focus it on the impact of a breach and how your company will deal with it. And based on the probability of a cyber event, you had better get going!

ABOUT THE AUTHOR

Regina Phelps, CEM, RN, BSN, MPA is the Principal with EMS Solutions, Inc. She is an internationally recognized expert in the field of emergency management and continuity planning. Since 1982, she has provided consultation and educational speaking services to clients in four continents. She is founder of Emergency Management & Safety Solutions, a consulting company specializing in incident management, exercise design, and continuity and pandemic planning. Clients include many Fortune 500 companies. Ms. Phelps is a frequent top-rated speaker at well-known conferences such as the Disaster Recovery Journal, CP&M, and the World Conference on Disaster Management. She is frequently sought out for her common sense approach and clear, clean delivery of complex topics.

1 Cost of Cyber Attacks Jumps for US Firms: Study, Security Week, October 2014. http://www.securityweek.com/cost

2 Managing Crisis: Responses to Large-Scale Emergencies, Arnold Howitt and Herman Leonard, CQ Press, page 5.

3 Ibid, page 6.

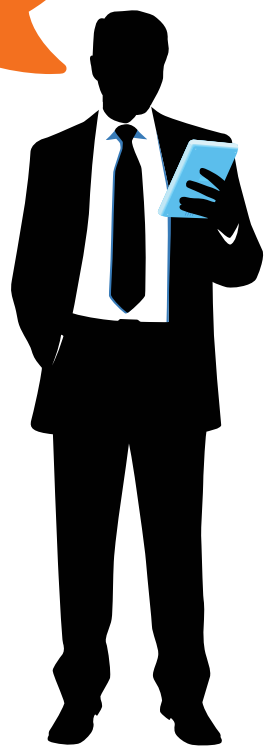
4 Emergency Management Exercises, Regina Phelps, Chandi Media, http://tinyurl.com/pyt9p8x

5 Anonymous YouTube channel https://www.youtube.com/user/AnonymousWorldvoce

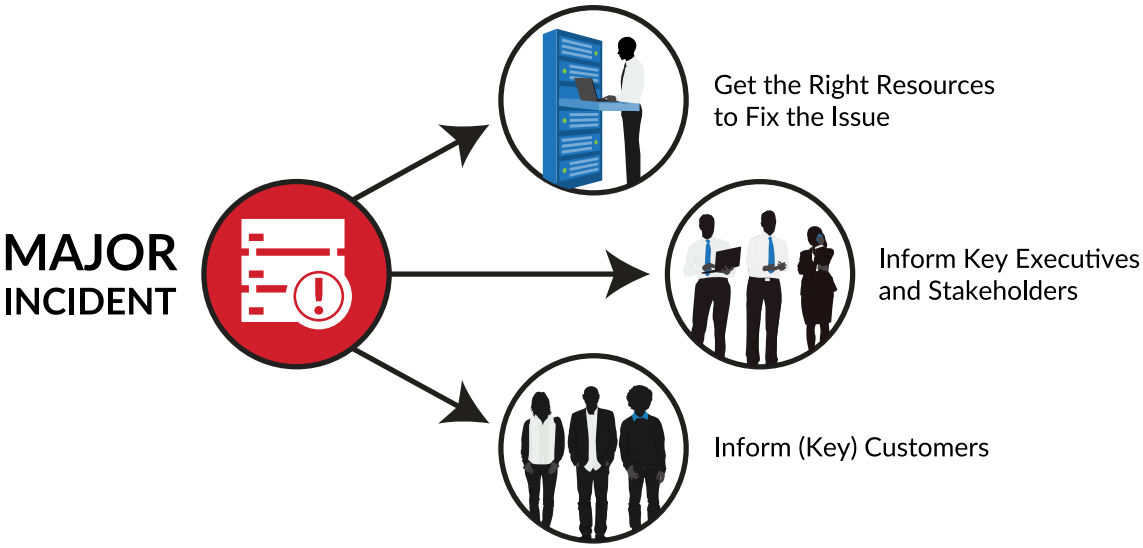
IT ALERTING

REDUCE YOUR MEAN TIME TO REPAIR

WHEN **IT** HITS THE FAN... EVERBRIDGE HAS YOUR BACK!



Everbridge IT Alerting i**ntegrates with your ITSM platform** and uses **automatic escalation** of alerts, **on-call scheduling**, **mobile alerting** and more to **automate manual tasks** and keep your IT operations team collaborative at all times. The solution also ensures your organization can **inform key executives**, **stakeholders** and customers during an IT incident.



OPTIMIZE YOUR IT INCIDENT RESPONSE

+ Integrate with ServiceNow, BMC Remedy and Other ITSM and Monitoring Solutions
+ SMS, Push, Pager, Email and Phone Alerts
+ Global Reach and Team Collaboration
+ "One-Click" Conference Bridging
+ Automated Escalation
+ On-Call Scheduling

everbridge®

REQUEST A DEMO WWW.ITALERTING.COM | +1-818-230-9700

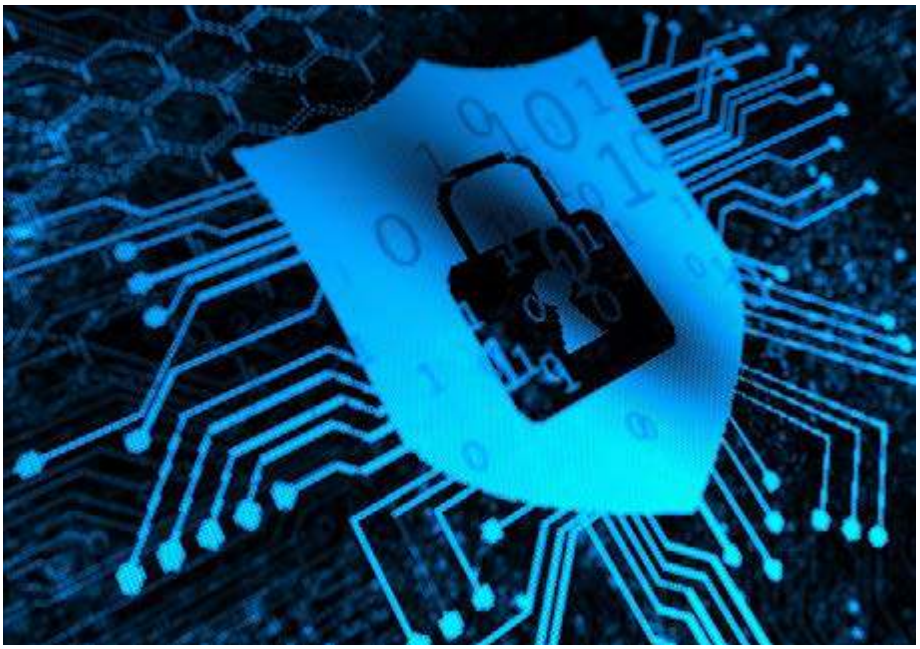
CRITICAL COMMUNICATION
FOR THE LIFECYCLE OF A CYBERATTACK

BY MICHAEL SCOTT

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.

CONTINUED ON PAGE 10

CONTINUED FROM PAGE 9



This article 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 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.

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

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

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.

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 THE AUTHOR

Michael Scott is responsible for managing marketing programs and developing content at Everbridge. He has experience running marketing programs for various industries including financial services, technology, healthcare, state/local government and higher education. At Everbridge, Michael was part of the launch of the new IT Alerting solution, built to ensure organizations can inform key executives, stakeholders and customers during an IT Incident.

CYBER ATTACKS: PREVENTION AND PROACTIVE RESPONSES

An interesting resource on cyber attacks, provided by attorneys at Holland & Knight LLP, examines the issue from the legal and compliance perspective.

The PDF, available at the link below, discusses common cyber attack scenarios and sets out actions that companies can take to prevent or respond to attacks, including developing a cyber attack response plan. It also addresses the chief compliance officer's role in preventing and containing attacks and law enforcement referrals, and civil and criminal actions companies can pursue against attackers. Cyber attacks, including hacking, of business websites and computer systems are increasingly common. These attacks can be extremely damaging to businesses, particularly if security is breached and confidential business and personal data compromised. Cyber attacks and the resulting security breaches are part of a rapidly expanding international cyber threat that costs companies and taxpayers billions of dollars each year in lost information and response costs. Company executives are under increasing pressure to prevent these attacks and must act immediately to contain any damage once an attack occurs.

Key points covered include:

- The chief compliance officer's (CCO) key role in preventing and containing cyber attacks.
- Developing a cyber incident response plan to report, investigate and respond to a cyber attack.
- Common cyber attack scenarios.
- Civil and criminal legal claims that may be brought against the perpetrators of cyber attacks.
- Recent case law relevant to some of the key issues discussed in this Note.

The resource is available online; click here.

MEASURING CRITICAL COMMUNICATIONS EFFECTIVENESS: AN ANALYSIS OF PRIVATE SECTOR BROADCAST CONFIRMATION DATA Everbridge Original Research

BY JASON GONZALEZ

Successful crisis management depends on an organization's ability to manage critical communications. This means ensuring fast, efficient delivery of an important message as well as determining if recipients receive and understand its content. Measuring the recipient confirmation rate is an effective way to quantify success of these factors.

An analysis of message confirmation rates from private sector customers (48,162 broadcasts representing 7.1 million messages) revealed the following best practices:

Optimizing for Early Message Delivery is Important

- Using efficient, text-based paths early in the delivery cycle is critical
- On first attempt, text-based paths have a 4X greater confirmation than voice
- In addition, 90% of confirmations occur within the first 3 contact attempts

Using Multiple Communication Paths is Essential

- Using multiple message path types increases the likelihood of confirmation
- Multipath broadcasts have a 79% higher confirmation rate than a single path

Allowing Recipients to Set Preferences Boosts Confirmation

- Broadcasts with contact preferences enabled show higher confirmation
- Confirmation rates are 44% higher than default setting broadcasts

Utilizing Multiple Paths & Contact Preferences is Optimal

- Data shows using more than 3 paths is ideal when both are enabled
- Rates are higher when email, SMS, phone & Mobile Member are used

Measuring Effectiveness

In the critical communications world, analyzing data associated with notifications allows us to measure the overall effectiveness of crisis communications, as well as gauge customer success in using EMNS tools across verticals and industries. Examining this data can reveal fresh insights that can be leveraged to help other customers moving forward. For this reason, an analysis of broadcast confirmation rates was performed using customer data extracted from the Everbridge system. The findings of this analysis are presented in a white paper available online. To download the full White Paper, visit:

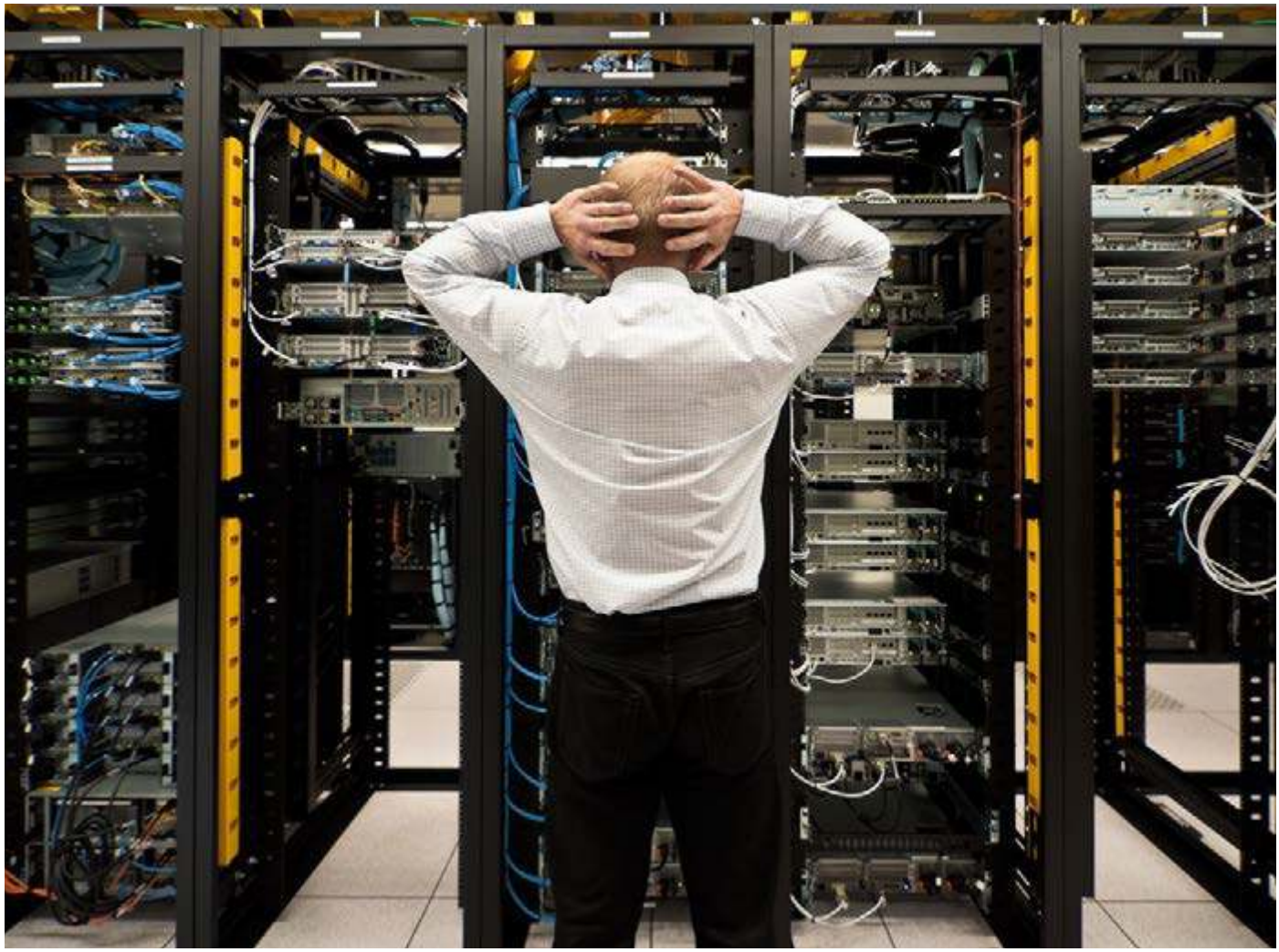
http://go.everbridge.com/communication-effectiveness.html

ABOUT THE AUTHOR:

Jason Gonzalez is responsible for Business Intelligence and Analytics at Everbridge. He has over 15 years of experience in the BI space at both large multinational companies and SMBs. At Everbridge he owns analysis of operational data and generates high-value insights which help customers achieve success on the Everbridge critical communications platform.

10 QUESTIONS TO ASK
WHEN CHOOSING AN IT ALERTING VENDOR

BY TOMMY RAINEY



Which IT alerting solution is right for you?

When dealing with critical IT outages time is of the essence and rapid communication plays a major role in minimizing the impact of outages, such as loss of revenue and damaged reputation of your service. Having the right IT alerting solution in place can dramatically help organizations address critical IT outages.

If you're in the market for a critical IT communications solution, there are a number of questions you should consider for an informed buying decision. To determine which questions are most relevant, first you need to think about how your organization will use the solution and understand which features drive the ROI requirements of the solution.

Most organizations want to be able to communicate with the right technical teams to get IT outages solved as quickly as possible. But do you need to reach key executives and perhaps even customers? Do you have a need for global communication? Does critical IT communications play an isolated role in the organization or should it tie into the organization's broader critical communications platform? If you have a communications platform under contract at your company, is expanding that solution to include critical IT alerting a logical choice?

CONTINUED ON PAGE 14

CONTINUED FROM PAGE 13

Understanding the right questions you should ask when considering a vendor can help uncover which one is the right fit for your organization now and in the future.

1 Am I overbuying?

Every organization deals with IT outages. But when looking at the Return on Investment (ROI) of a solution, it is important to note that critical IT incidents are the most costly to the company's reputation and bottom line. Hence, the key value of an IT alerting solution lies in its ability to address Priority 1 (P1) and Severity 1 (Sev1) incidents for the right price. When purchasing a solution for critical IT communications, you should search for one that helps you reduce Mean Time To Repair for the critical outages.

Has an independent, third-party organization measured and reported on the system's reliability?

In addition to being able to address P1/Sev1 incidents, it may be possible to address lower priority (P2-P5) incidents. However, it is critical to recognize the diminishing value of lower priority incidents and therefore the possibility that additional features to address those incidents might be overpriced or unnecessary. While it might seem attractive to have bells and whistles which would allow you to address a low priority issue such as one of the office printers being down, it is important to not overvalue those features and complexities. This situation can lead to overbuying whereby the largest part of the cost of the solution lies in functionality that is not critical in terms of ROI. The functionality that allows you to reduce MTTR during P1/Sev1 incidents is what saves you money, but paying for the functionality and complexities to handle the much smaller incidents can cancel out those savings and delay time to value because it takes time and effort to implement the processes for addressing P2-P5 incidents. For this reason, you'll want to be sure that you're only paying for functionality that you actually use and that saves your company money.

2 Am I paying too much?

With any type of purchase, price is generally an important deciding factor. If you're being charged too much for a product, typically you won't make the purchase. When it comes to a critical IT communications solution, find yourself a vendor that meets the key criteria for an IT alerting solution and does so at a competitive price. One metric to consider is the cost per user per month. Prices for IT alerting solutions can range from $10 to $70, per month, per user. If you are considering a solution on the higher end of this scale, is the additional cost worth those additional features? Your best case scenario is finding a vendor that allows you to address the most important critical IT incidents – P1 and Sev1 – at a price that won't eliminate any savings you expect to realize from being able to address these incidents much quicker. If the cost outweighs the savings realized by implementing IT alerting, it doesn't make much sense to purchase the solution.

Regarding price, it could be valuable to consider the constituents in a major IT outage, and assess the types and the value of communications with each constituent. Personnel involved in the delivery of critical IT resources would be primary, followed by those using the applications, and then 'customers' of the system, both internal to the company and external users. Each level of stakeholders requires different types of communication and the pricing should not be based on the highest (most expensive) level.

Finally, are there real-world and quantifiable examples from the vendor's customer base where the system has reduced the time required, for example, to get key team members into a conference call?

3 Is the solution reliable?

If a vendor you're considering has an IT alerting product that is supported on premise, you should eliminate them from your list of options. On-premise solutions are no longer acceptable, as an incident such as a power outage could disrupt or shut off your service. If you're unable to use the IT alerting solution you purchased to help save your company money, it could actually end up costing you, not only on the financial side but also in reputation. For this reason, it is important to find a solution that is supported in the cloud, because what good is a critical IT communications solution if it doesn't work during crunch time when you need to send out messages about a critical outage? To ensure uptime, your system has to guarantee a few things. First, the provider needs to have multiple data centers in case one should fail. Second, they need to have data centers that are geo-dispersed. This helps ensure that you're able to send communications even if a localized event happens that brings down one data center.

When asking a provider if the system they provide is reliable, it is also important to understand how that connects with scalability. Numerous factors can affect performance and a system's overall resiliency – including scalability. If a system is pushed to its limits because of extremely high usage and then fails, it is not resilient. A vendor has to be able to harness the cloud for additional data centers – located in different areas, unaffected by an event – for additional capacity and as a failover if one or all of the providers' systems should be down.

Another question you should ask of a vendor is their basis for claims of reliability. Has an independent, third-party organization measured and reported on the system's reliability, or are the claims of reliability solely based on internal records or hearsay?

4 Was the vendor's solution designed from the ground up as a SaaS product?

If choosing a SaaS-based IT alerting solution, has the vendor always offered the SaaS solution, or is the SaaS solution a relatively recent offering to complement or migrate from an on-premise solution? As many vendors follow the industry and begin to migrate their hosted solutions to SaaS, it is important to take into account the potential downfalls that come with learning the ins-and-outs of offering a SaaS-based solution. The IT marketplace has many examples of companies who have attempted to play catch-up by migrating an offering from a hosted solution to a SaaS platform. One example of this is Siebel Systems, which after years of selling a successful hosted solution, began to migrate their CRM solution to the cloud. Salesforce.com, on the other hand, was created from the beginning as a SaaS offering and based on that strength, far surpassed Siebel in the CRM marketplace. Be sure you recognize the importance and value of a notification solution that was designed from the ground up as a SaaS offering.

5 Is the solution easy to use?

A critical IT communications solution must be easy to use. But ease of use is difficult to fully quantify because "easy" is often a personal opinion based on an individuals' capacity to assimilate technology. Every vendor will claim its system is the easiest to use, which can add confusion to your buying decision.

So, if all the systems are easy to use, should "ease of use" even be a primary factor in the final purchasing decision? Yes – given the critical nature of a notification system, ease of use is important. In fact, high levels of stress can reduce a person's cognitive capabilities during a critical incidents; a system that was easy to use yesterday may prove to be overly complex when it's really needed.

You should use a set of standard criteria to measure ease of use to help strip away some of the subjectivity. During critical IT incidents, you need simple, intuitive interfaces. When considering any critical IT communications solution, determine whether the average person will be able to use the system with little to no training, or if the system will require some type of specialist. Many of the systems on the market today are flashy, but are also primarily focused towards a highly technical user. While this type of system can be very impressive during a vendor-led product demonstration, the user can quickly get lost within the menus when an actual critical IT incident occurs.

Below are a few questions you should ask each vendor:

- How many clicks does it take to send a message?
- How many pages must be visited to send a message?
- How many clicks does it take to launch a pre-existing message?
- How much training is required to get users up and running?

Your IT alerting solution should also easily integrate with other processes to simply how you send out notifications. For example, you may want a vendor that offers APIs that allow for email broadcast initiation, and synchronization with HR systems to keep an automatically updated contact list.

6 Does the solution have global reach?

If your organization uses or relies on technical support teams in international locations or has internal and external stakeholders outside of the US, it is important that your critical IT communications solution has global reach. Today, international voice calling is very simple and inexpensive. This simplicity might cause you to mistakenly believe critical communications are similarly easy to accomplish. However, there are many international communications challenges resulting from infrastructure differences, the need for local call routing, carrier acquisitions and mergers, different regulations in Europe, content filters used to protect cultural practices in China, limits on delivery volumes to comply with SPAM initiatives in the US, India and Australia, and other carrier connectivity issues all over the globe. For example, Caller ID and SMS functionality is almost taken for granted within the US. However, implementing Caller ID and SMS internationally involves different standards across multiple countries and telcos. Does a vendor

CONTINUED ON PAGE 16

CONTINUED FROM PAGE 15

have the necessary arrangements to facilitate global inbound calling, and if so, from what countries? To meet all of these challenges, when evaluating a vendor, you'll want to be sure that they have processes in place to help you increase the success of international notifications and comply with local contact data protection regulations. If a vendor doesn't have this functionality, you may struggle to send global notifications about critical IT incidents to customers, executives or any other stakeholders who need to be informed.

7 Does the IT alerting product offer multi-modal communication?

Multi-modal messaging – SMS, cellphone, email, landline, push notification, etc. – is key to delivery success, as no single delivery path is ever 100 percent reliable worldwide. The more communication paths that are available, the more likely your customers and stakeholders will receive important information and updates. Targeting individuals guarantees the team responsible for fixing the problem can be alerted first, key stakeholders are not caught by surprise and customers are informed.

A significant benefit of a robust notification solution is the possibility of eliminating (and saving the cost of) existing 'point' solutions, such as pagers. The cost of pagers could be $20/month per pager, and many hospitals or IT departments could have hundreds of pagers in use at great expense. If your notification solution is multi-modal and can communicate across various platforms, there could be significant savings in your organization by eliminating 'point' solutions entirely.

Will you realize cost savings by eliminating expensive "point" solutions such as pagers, which could cost $20 per month per user?

8 Does the IT alerting product allow for customer outreach?

Scalability is important for any solution. Not only should your vendor allow you to communicate internally, it should also offer the ability to communicate with customers. During IT incidents, you need to be able to keep customers in the loop. If your critical IT communications solution doesn't have the capability for customer outreach, your organization's reputation and bottom line could take a major hit.

The best way to manage customer complaints is to be proactive and remain visible during critical incidents. Misinformation can spread like wild fire on social media and escalate a situation, so maintaining a presence by communicating with customers can quell rumors, improve trust and retain customer loyalty. An added benefit is a reduction is service calls, since customers already know the company is addressing the issues. In order to keep your customers happy and protect your organization's reputation and bottom line, it is crucial that your vendor allows for customer outreach. Even though this may not be an immediate need, the capability to scale up to customer outreach without having to use a different solution is not to be overlooked. This type of scalability – and beyond – should be a requirement of any vendor you choose for critical IT communications.

Simply being able to communicate with customers is great, but you also want the capability to send notifications about information people care about. This means you should find a vendor that allows you to set up subscription-based customer notifications, which allows customers to be alerted about issues that actually impact them as opposed to every, single issue. For example, a personal banking customer may care about data breaches but not an issue with the commercial online banking portal.

9 Does the vendor offer personal 24x7x365 support, and free best practices and other training?

Calling a customer support line and getting and automated response can be frustrating. For this reason, you'll want to find a vendor who can offer you 24x7x365 personal phone support. Whenever you call in with an issue, you should get an actual human answering

the phone who can solve your problem – not a robot.

After your vendor sells you a solution, they shouldn't disappear. In order to be as successful as possible with your system, you need to buy from a vendor that offers excellent training programs so you can successfully deploy and use your solution. It is important that you find a vendor who offers free online training programs that are always available, as well as additional customized on-site training if necessary.

Whether you need assistance implementing your system, want to learn best practices or simply need help logging into the system, your vendor should be ready and willing to help.

10 Does the vendor solve more than one business problem?

Most organizations have more than one need for a critical communication system. Those that use critical communications for IT outages typically also need critical communications for needs around business continuity, life-safety, emergency preparedness or some other use case. The issue with some vendors is that they aren't able to handle the different communication needs each organization requires. One vendor may offer critical IT communications, and not offer BC/DR communications or vice versa. For this reason, it is of great benefit to you to find a vendor that offer solutions for all of your communication needs, which means you'll only need one contact database, as opposed to multiple if you use different systems for each use case.

When searching for a critical IT communications vendor, move away from point solutions and find someone who is able to offer enterprise critical communications. Find a solution that allows you to communicate with technical teams to fix IT issues as well as one that offers the functionality to reach employees if there is severe weather that could endanger them on the way to work. And consider the increasing regulatory compliance issues such as HIPPA regulations and other privacy regulations; can your vendor meet those requirements with their existing solution?

Choose the Right Solution for Your Organization

Selecting a solution for critical IT communications is a major decision that will impact your organization for years to come. It is important that you understand the key questions to consider when evaluating vendors to make sure you choose a system that meets all of your communication needs. By completing this process, you should be able to find a vendor that allows you to respond to critical IT outages in a variety of ways to reduce MTTK and thereby MTTR, which, in turn, can help deliver a significant and quantifiable return on investment.

ABOUT THE AUTHOR

Tommy Rainey is Executive Publisher of the Disaster Resource GUIDE. For over twenty years he has worked with organizations worldwide to promote business continuity and resilience. He can be reached at tommyr@disaster-resource.com.

NUGGETS

ISO 22301 – THE INTERNATIONAL STANDARD FOR BUSINESS CONTINUITY

The International Organization for Standardization published ISO 22301:2012 to help companies address risk and business continuity. The abstract about this standard states:

"ISO 22301:2012 specifies requirements to plan, establish, implement, operate, monitor, review, maintain and continually improve a documented management system to protect against, reduce the likelihood of occurrence, prepare for, respond to, and recover from disruptive incidents when they arise.

"The requirements specified in ISO 22301:2012 are generic and intended to be applicable to all organizations, or parts thereof, regardless of type, size and nature of the organization. The extent of application of these requirements depends on the organization's operating environment and complexity."

ISO 22301 is available at the following link: http://www.iso.org/iso/catalogue_detail?csnumber=50038

HELPFUL CRISIS COMMUNICATIONS PLAN TEMPLATE FOR ASSOCIATIONS

A crisis communications plan template to help associations prepare has been made available at the IASE website link below. According to the Indiana Society of Association Executives,

"In today's fast-paced, technology-driven world, news travels faster than many of us can comprehend. The effects of this technologically based form of new media include:

- Word of Mouth – This now not only includes traditional word of mouth communication, but also email and blogs that can be created and reported internationally in just seconds.
- Internet – Anyone, including visitors or media, can use the Internet to receive news alerts or to search for topics. This means that news can be revisited for years and "bad press" can be particularly detrimental.
- News Wire – The Associated Press, Copley News Service, etc. all share stories. If a story is picked up by one service, it can spread within minutes to all major outlets in every country.

The plan, in a Word document format, is available by clicking here.

FORMER FBI AGENT MARY GALLIGAN ON PREPARING FOR A CYBER ATTACK

Another interesting perspective on the issue of cyber security is provided in a Wall Street Journal article by Mary Galligan, a former FBI agent.

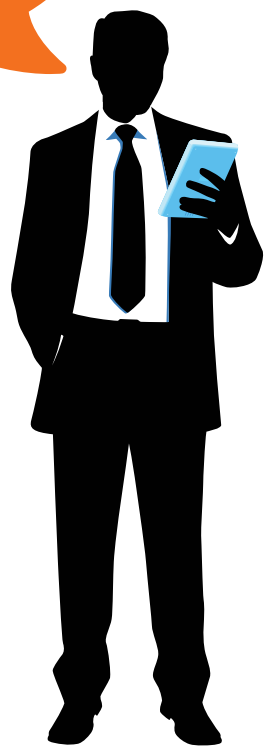
According to an introduction to her comments, "Mary Galligan, a director with the Cyber Risk Services practice of Deloitte & Touche LLP, advises companies to prepare for the likelihood of an attack by implementing risk-based security measures and an incident response plan that details the steps and communication protocols required for reacting to and recovering from an attack. In this Q&A, Galligan, a retired FBI agent who was in charge of cyber and special operations for the New York office, discusses a wide range of topics, including questions corporate boards should ask about cyber security, the effectiveness of cyber wargaming activities, and misconceptions about cyber security.

You can access the full article by clicking here.

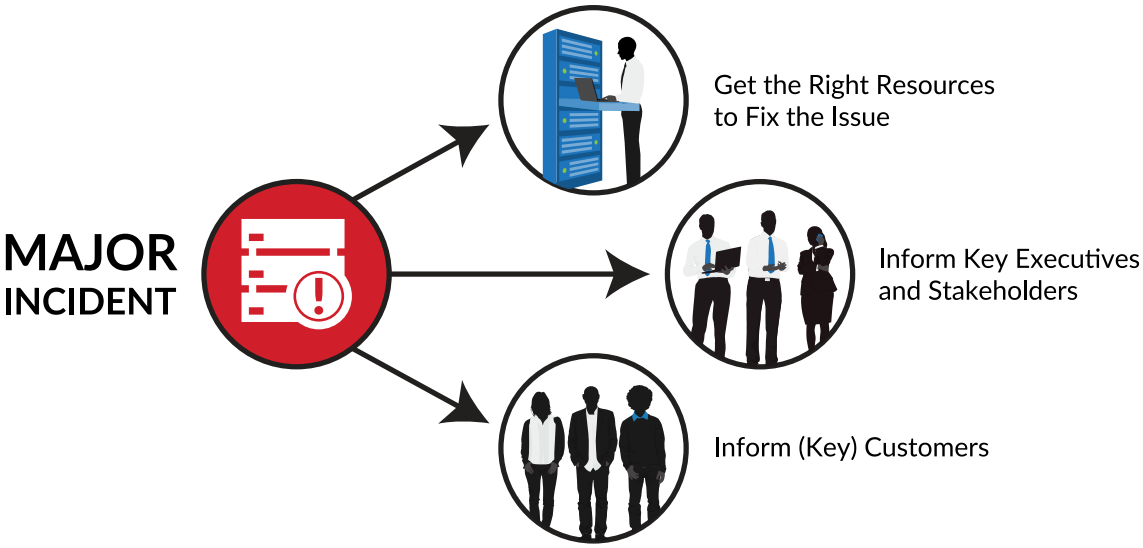
IT ALERTING

REDUCE YOUR MEAN TIME TO REPAIR

WHEN **IT** HITS THE FAN... EVERBRIDGE HAS YOUR BACK!



Everbridge IT Alerting i**ntegrates with your ITSM platform** and uses **automatic escalation** of alerts, **on-call scheduling**, **mobile alerting** and more to **automate manual tasks** and keep your IT operations team collaborative at all times. The solution also ensures your organization can **inform key executives**, **stakeholders** and customers during an IT incident.



OPTIMIZE YOUR IT INCIDENT RESPONSE

+ Integrate with ServiceNow, BMC Remedy and Other ITSM and Monitoring Solutions
+ SMS, Push, Pager, Email and Phone Alerts
+ Global Reach and Team Collaboration
+ "One-Click" Conference Bridging
+ Automated Escalation
+ On-Call Scheduling

everbridge®

REQUEST A DEMO WWW.ITALERTING.COM | +1-818-230-9700