PULDY RESILIENCY PARTNERS

Crisis and Incidents

Solving to Normal

puldypartners.com | 877.780.7878

2121 Rosecrans Avenue, Suite 4300, El Segundo, CA 90245

TABLE OF CONTENTS

INTRODUCTION

> ***The Continuous Flow of Information is Inseparable from the Operational Performance of the Firm.***
>
> Donald P. DeMarco,
>
> IBM, Vice President

CRISIS!

By definition, a crisis is a time of intense difficulty, trouble or danger. Yet, one person's crisis is another person's day job. Looking at crisis from a personal point of view, how many times has a home internet service failed only to find the homeowner on the phone with a customer support representative for what seems like hours of frustrating diagnosis? While the homeowner is desperate for a fast resolution to their outage, to the customer service agent, this homeowner is one of hundreds of callers heard from during a single workday. All are anxious to have their service restored.

The image of a bored, overworked, disinterested hourly worker comes to mind. Someone who couldn't care less when your home service is restored.

Yet, when crisis is translated to business, the perspective is as much financial as it is brand reputation. When business is down, the stakes are significant. A business outage translates into thousands, if not millions of dollars lost every day, every hour, every minute, or potentially every second. Loss of revenue, loss of confidence by existing customers, loss of prospective customers, damage to a brand's reputation, litigation, and even government investigations are all potential downstream effects of a crisis.

Yet, a company which successfully and responsibly responds to crisis can transform a crisis into a positive experience. Customers embrace a firm who deals with crises professionally, with speed, with honesty, and with remorse and empathy.

Within the 24/7 world of the business community, hardware fails. Software maintenance is poorly released. Humans make mistakes in applying patches, configuring firewalls, and accidentally pushing buttons while mindlessly responding to an urgent system prompt. On the other end of the spectrum, major design decisions are signed off knowing a single point of failure exists within an infrastructure design that years later might shut down a small company as easily as a multi-billion dollar business.

In short, incidents happen, and it's not a matter of if a crisis between a provider and a customer occurs, but when. And, how a business organizes, plans, and responds to the crisis will become immediately visible at a time of disaster. Being prepared and responding with professionalism plus a focused speed of service endears your customers to your business while strengthening your brand.

Fumbling the ball when a crisis presents itself creates uncertainty, disappointment, brand risk, and potential loss of customers.

This whitepaper presents a blueprint on how your firm should consider not only organizing and responding around an unexpected crisis, but also a series of low-cost, high-value actions which will both separate your firm from your competitors and protect your brand's reputation.

WHAT'S AN INCIDENT?

Incidents happen every day to every company, but in most cases, the incidents are small and hidden. No one from the outside sees the event.

- A worker loses a computer hard drive, and the business keeps running thanks to redundant disk arrays.
- The power goes off in a building, but the firm continues to function thanks to the operation of an uninterruptible power source (UPS) composed of batteries and diesel generators.
- An online order entry system fails, but the redundant backup server kicks in, and orders continue to be accepted with barely anyone outside of operations noticing the failure.

These are examples of *hidden incidents*. Internal, important, yet relatively unnoticeable outside the confines of the local organization charged to resolve the incident, find the root cause and ensure the problem never reoccurs.

The more damaging kind are *visible incidents* that customers can see and feel. These visible incidents could be internally created on a scale impossible to conceal, or worse, triggered from an external source which is significantly more damaging and sometimes impossible to sidestep.

- A single, unprotected telecommunications fiber connection is cut by a firm digging a ditch shuts down a business network.
- During a routine software upgrade, a technician incorrectly executes the upgrade procedure, and the firm is shut down as backup systems are restored.
- An unsuspected link on an email is clicked resulting in the download of malware. Months later, critical files are encrypted and held for ransom.

Visible incidents are a firm's worst nightmare, potentially triggering weeks or even years of damage to the brand and financial loss.

> ***Fumbling the ball when a crisis presents itself creates uncertainty, disappointment, brand risk, and potentially loss of customers***

With today's accelerating electronic news cycle, destructive incidents quickly become front page news. Unfortunately, there's a long list of victims with new tragedies rapidly superseding yesterday's fallen.

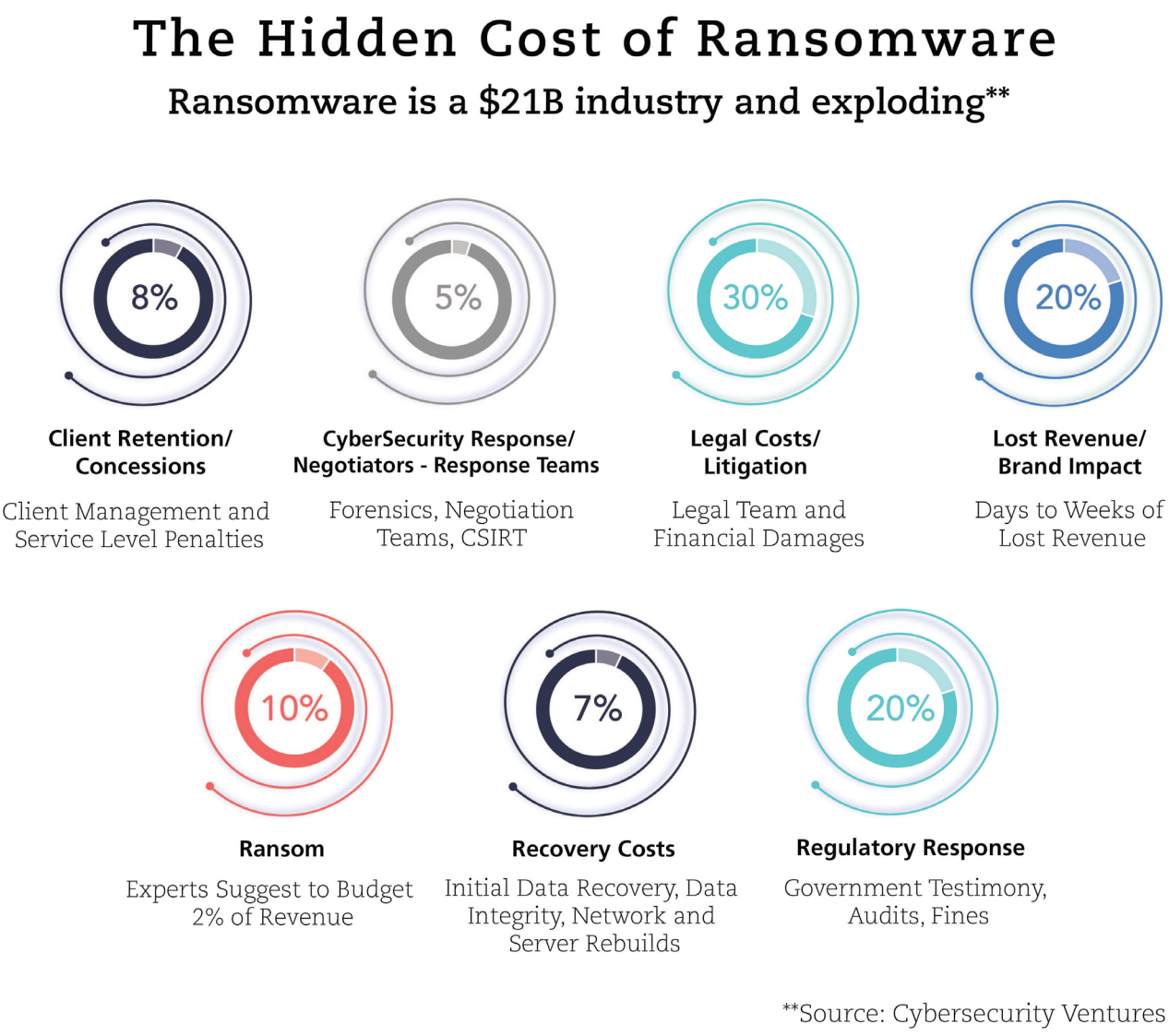
In the early part of 2021, major corporations such as Microsoft, Solar Winds, Colonial Pipeline, Bombardier, Acer, and Sierra Wireless all suffered cyberattacks and were briefly thrust into the limelight long enough until the next company appeared in the news.

Colonial Pipeline with over $1 billion in annual revenues, suffered a ransomware attack and initially paid close to $4.4 million in ransom. But the incident will also cost the company countless millions in restoration, legal, and customer management costs. While $4.4 million is a large number, the ransom payment represents a small figure relative to the total cost of a ransomware incident. As represented in **Figure 1**, company costs of an incident accumulates long after the crisis is over.

Another example of a public and broad reaching incident is the JBS ransomware attack. Meat processing company JBS reported they paid $11 million in ransom, but the $11 million cost doesn't include an array of post event costs to JBS plus the broader economic effects on farmers, restaurants, and the general public who all suffered from the JBS incident.[1] As eloquently reported by one analyst, "Even one day of disruption will significantly impact the beef market and wholesale beef prices."[2]

Common estimates place a ransom payment at only 10% of the total cost of a ransomware incident. For example, if a company paid $1 million in ransom, the firm can expect as much as $9 million in additional business costs. And, while cyber insurance will cover some portion of the $10 million hypothetical cost, insurance will not cover the entire business loss.

Figure 1: Exposing the Hidden Costs of a Ransomware Incident.



Also, even though "sexy" ransomware crises are frequently in the news, crises and incidents come in many shapes and sizes.

Power outages, disgruntled employees, natural disasters, hardware and software failures, and supply chain disruptions may not be as exciting as ransomware, but can cause an equal or greater amount of havoc. Checkout the story of the squirrels that took down the NASDAQ not once, but twice.[3]

INCIDENT CLASSIFICATION

While it's important to standardize on incident definitions and responses, most companies will create a definition and response that's unique to their business model and their cost structure. A common style is rating incidents sequentially. For example, a severity 1 incident is the most catastrophic and denotes a complete operational failure requiring "all hands-on deck." At the other end of the spectrum is a severity 4 ranking, an event considered barely noticeable.

Table 1 outlines one way to categorize crises, and equally important, how to respond.

Table 1: Crisis Severity Rankings

Severity	Symptoms	Impact	Customer Response	Example
1	Major impact to a business's ability to deliver products and/or services to customers. Unable to transact normal business.	Inability to transact business. Loss of revenue. Loss of productivity. No immediate workaround.	Regular personal and verbal conversations with customers. Expectation setting on when systems will be available and when root cause analysis will be completed.	Power outage disrupts business's ability to deliver contracted services. Provider, customers and partners experience revenue loss and potentially suffer damage to brand reputation.
2	Significant impact to a business's ability to deliver products and/or services, but there's a functioning workaround.	Short-term disruption to transact business. Customer is operational yet concerned disruption could reappear. Firm has recorded loss of revenue, productivity.	Regular updates to customers and partners on what business is doing to understand the problem, implement short and long-term corrective actions, and present a root cause analysis report disclosing how this problem will never reoccur.	Subsequent severity immediately after a severity 1. Business, customers and partners are once again operating, but the sting of a Severity 1 outage is near and strong. There's an underlying fear the problem could easily reappear.
3	Medium impact to business. Business and customers are able to transact commerce, but major or minor features are not operating correctly.	Minor disruption, no loss of availability but operational functions may not be working.	Weekly, bi-weekly or monthly update on the problem until proper customer expectations can be set (e.g., problem will be resolved in 90 days).	Sporadic operational failure such as an application randomly does not accept data, but easily restarts. The situation can be corrected by the customer. An annoying inconvenience, and relatively small impact to business and to customers.
4	Low to no impact to business operations. Customers have expressed functional or operational concerns. No loss of revenue or productivity. Customer confidence could be improved by correcting problem.	No business disruption but considered a productivity inhibitor.	Acceptance of the request, commitment to review issue and sets expectation the problem will be either solved in the future, or recognized the problem is not financially feasible to resolve in the near term or ever.	Product documentation is incorrect. The application or system is working as designed, but a requested productivity feature is unavailable or is incorrectly documented.

THE ROLE OF COMMUNICATION

Beyond the technical work required to navigate a business from disaster to a place of steady state, communications is the most important and overlooked element in resolving a crisis situation. Unfortunately, communicating both internally and externally after an incident is given such a limited focus, and consequently, both anxiety and uncertainty lingers long after the event is over.

Communications can be divided into two categories: **internal communications and external communications.**

Internal communication is critical to reinforce the perception that a proper level of resources are being brought to bear to resolve the situation. In the best world, before crisis, a company has predetermined who is responsible for handling communications inside the company, and what type of information is communicated when and to whom. Moreover, at time of crisis, a communication is developed and transmitted to the employee community at large, and in parallel there is a more detailed, yet concise communications protocol for executives, plus one developed specifically for those who deal directly with customers.

A separate and external customer communique explains the problem so anyone who talks to a customer is figuratively on the same page, knows what to say and how to say it. Equally important, for those who communicate externally, they should be explicitly told what NOT to say.

Even though businesses should be transparent when discussing an incident, during the fog of war, saying the wrong thing will only hurt a business's relationship with their customers. When all the facts have been collected and organized is the time for the heart-to-heart talk on what happened and why.

All too often, a customer may approach different people in the organization only to hear a different story or maybe a different perspective. If everyone knows what to say, how to say it, and what not to say, this goes a long way in eliminating additional chaos for both the customer and the business.

Even though businesses should be transparent when discussing an incident, during the fog of war, saying the wrong thing will only hurt a business's relationship with their customers.

BALANCING COMMUNICATIONS

Communicating with the customer is a balance. Too much data too early leaves a firm exposed to missteps, or transmission of misinformation, and could result in lost customer trust. Too little information too late could have the same negative effect.

Here are some basic recommendations on how to communicate with a customer during a severity 1 crisis.

1. Be empathetic, be remorseful, be personal. Understand your outage is causing this customer a lot of pain. Even though the customer may understand, they will not be happy until life is back to normal and even then only time will heal the wound.

2. Focus the discussion on steps to return the business to a normal status. There will be time to figure out what happened, how it happened and why the problem will never happen again later.

3. Provide regular updates. Updates twice a day, at the beginning and at the end of the workday goes a long way. Also, it's important to give the people working the problem, time to work on the problem. Increased frequency of interruptions only delays resolution. If you have good news, obviously the reporting cycle to the customer can be accelerated.

4. When systems are restored, set a commitment on when the root cause will be reported. Ten to 14 business days is a reasonable outlook.

And then there's communications with the media. Larger companies often have the luxury of having a media communications specialist on staff, while smaller firms should have a communications consultant on retainer. These communications specialists are battle trained professionals who know how to manage the message. And communicating with the media is a huge opportunity to manage and control the message.

Handle the message correctly and the media goes away. Handle the message poorly, and the story stays alive for multiple news cycles. Losing control of the message also exposes a firm to increased scrutiny, needless costs repairing the brand, extensive work repairing customer satisfaction, and increased inspection from regulatory and legal outsiders.

> ***Customers embrace a firm who deals with crises professionally, with speed, with honesty, and with remorse and empathy.***

ACTING AHEAD OF THE SHOCKWAVE

Think of a problem as if you throw a stone into the lake and watch the ripples in the water slowly expand away from where the rock hit the water. When dealing with a crisis, this is exactly what happens. As time grows, more and more people, business processes, and partners are impacted.

At the start of the problem, there's a small group of people who know about the problem and are working hard to fix the problem. In many cases, problems are fixed easily and quickly. These are the best types of problems because there's limited outside inspection and a limited shockwave.

Problems are quickly and easily solved. Unfortunately, as we know, many problems do not end so easily.

In the case of a severity 1 outage, when access to systems are completely lost, not only is it impossible to keep this incident quiet, but with each passing hour, more people – inside and outside an organization – are aware of the problem and for better or worse, become involved.

Consequently, as an incident starts to unfold ask these three basic questions:

1. Will this situation impact a specific customer, multiple customers or every customer?

2. Can the situation be resolved by a small number of organizations (e.g., customer support), or is this going to become an "all hands-on-deck" scenario where "everyone" must or wants to be engaged?

3. Will this situation last for an hour, many hours, or days?

Even though you may not know the answers, trying to develop a perspective or frame of reference will help orient both the approach to solving the crisis and your understanding of who you need to engage and when.

DEVELOP EARLY WARNING SYSTEMS TO PREPARE TEAMS

The connotation of an early warning system has a military feel but, consider creating an early warning system within your organization. One system designed for critical employees who are part of a crisis and incident management team, or perhaps key stakeholders (e.g., development, security, procurement, legal), and a separate system specifically for dealing with customers (e.g., customer help desks, account management, external communications).

Thinking back to the shockwave, as time expands so does the involvement of more and more people and organizations. Sometimes, the problem impact expands too quickly and there's no time to provide a heads up to stakeholders and customers. Nevertheless, as an incident is unfolding, if there's an opportunity to notify teams to be ready to go, this action helps everyone. If you are able to provide advanced notification to your customers that is also a big advantage because your customer can take their own steps in preparing for what might come next.

Looking inside a business, key technical and business leaders must be ready to go at any time. It's much easier to demobilize a pre-assembled team than to cobble a group together on the fly while the building is burning. **Figure 2** provides one example of four groups who must come together to solve complex problems at time of disaster. However, for smaller firms, the crisis team is stitched together with both employees and business partners.

"Twenty-five minutes to shut down the business, and seven months to fix it."

Figure 2: Four Key Organizations Engaged and Interlocked at Time of Crisis

Consider a ransomware scenario.

In most circumstances, a bad threat actor has been in the system for days, weeks or months as they carefully and methodically prepare to encrypt sensitive and important data. When the time comes, a switch is thrown, and in minutes or hours, a firm's entire business comes to a sudden halt. In this situation, the shockwave moves very quickly. The cyber security team may be the front-line team trying to save the day, but the team responsible for data recovery, followed by the crisis communications team will be needed very soon. One global 100 executive made a dramatic, but accurate comment long after a client's ransomware attack: "Twenty-five minutes to shut down the business, and seven months to fix it."

As an incident begins to unfold, ask yourself the three questions outlined on page 9, and based on your best estimate, initiate your early warning system.

The more you and your team can be ahead of the disaster, the better your performance.

THE COMMANDER'S INTENT

Another important military concept considered critical to crisis and incident management is the concept of The Commander's Intent.

Simply put, "the role of [the] Commander's Intent is to empower subordinates and guide their initiative and improvisation as they adapt" to changes in the battlefield or in business.[4]

For example, in a customer help desk environment, how does a customer support representative respond when the entitlement or customer information systems are inoperative? How many times have you heard, "I'm sorry, I would like to help you, but our computers are down." Even though in many situations there may not be another option, at a time of crisis, when backed against the wall, employees become extremely resourceful. Leaning on the Commander's Intent, at a time of crisis, empowers your employees to find resourceful ways to help your customer.

By empowering employees with bold and broad discretion to do the right thing, they will often do just that.

WHERE ARE YOUR DOCUMENTS?

In today's omnipresent world of electronic storage, paper copies have for the most part gone by the wayside and with good reason. Large binders of paper are heavy, expensive to print and maintain, and quite frankly take up a lot of physical space.

Nevertheless, there are many stories where the old ways of paper, pen and typewriter saves the day. Most notably, outages created by ransomware, business email compromise, and long-term loss of computer or network access have built a case that it's still important to keep at least a limited amount of documentation either in hard copy or stored in an easily accessible and "out-of-band" condition.

Run books, business continuity plans, critical employee phone directories, and even call trees are all candidates to be stored in multiple places, and ideally in an accessible, hard copy format. If you lost your mobile phone, how difficult would it be and how long would it take to reassemble your critical phone numbers?

As an experiment, spend 10 minutes and turn off your primary mobile phone and your computer. Next, visualize you have experienced a devastating cyberattack and your computers and mobile phones are unavailable. Who would you call? How would you make the call? What's your plan B? Plan C? Write down your thoughts and mitigation options.

Congratulations, you've just created an elementary business continuity plan.

ELECTRONIC MESSAGING SYSTEMS

A quick way to communicate is through electronic message systems. While email qualifies as an electronic messaging system, many people aren't always looking at email. In fact, some people only look at emails a few times a day so email can never be considered an urgent form of communication.

At times of crisis, a hyper-accelerated form of communication is a must. Speed is life. Have a system that's fast!

Standardize on a Short Message Service (SMS) texting platform or identify one or more group messaging tools that can rapidly improve response and facilitate command and control of any situation.

While voice and video conferencing systems are the best way to tactically attack a crisis, SMS and group messaging will save the day.

As outlined in **Table 2,** different tools offer unique solutions at various price points.

SMS texting tools such as **WhatsApp** allow for easy text style messaging services to an individual or small groups, while more robust systems including **Starfish Constellation,** Slack, Everbridge and Whispir allow broader and more content rich solutions all with various features, security and price points. The point is a crisis management system should engage multiple forms of communication systems to accommodate a business's style of communication, unique security and operation requirements, and varying tolerance for spend.

In addition, these Software-as-a-Service (SaaS) systems provide an active communication system when traditional environments are shut down due to ransomware, business email compromise, and even the larger extreme, a regional telecommunications outage.

Remember, especially in a ransomware or business email compromise situation, your regular email may be monitored so find an option outside your business network.

Table 2: Sample Communication Tools

	Direct SMS	Texting App	Small Group Systems	Mass Notification
Content Rich	Limited	Limited	Medium	Extensive
Workflow	No	No	No	Product Dependent
Security	Depends	Yes	Yes	Yes
Sender/ Receiver	1:1	1:1 or 1:Many	1:1 to 1:Many or All	Variable
Cost	Free	Free	$	Free to $$$$
Examples	*iMessage*	*WhatsApp*	*Starfish Constellation*	*Whispir, Everbridge*

TELEPHONE

Having a working telephone at a time of crisis is a no brainer. Prior to the year 2010, everyone had a landline and many people also carried mobile phones. Today, land-based telephone lines are declining as more and more companies have moved to either voice-over-IP phones or a complete reliance on mobile phone systems. In addition, many employees have jettisoned their home phone altogether and rely on a single mobile carrier.

For critical employees, and senior executives, consider the option of a second mobile phone from an alternate carrier from your primary phone. Even though carrying two mobile phones sounds extreme, the two-phone concept creates significant benefits such as reducing the reliability on a single phone network and having a backup plan in case the primary phone is unavailable due to theft, power outage, or damage.

When the inner circle is immediately required, costs are rarely a point of discussion.

BUY A SAT PHONE

The first satellite phone for the consumer was introduced by Iridium in 1998, and since then the satellite market has come a long way. Today, there are many brands and plans available for consumers and commercial businesses. While many businesses still balk at purchasing a satellite phone, for companies with multiple locations, and especially those with international locations, at a time of crisis, there's no substitute for talking to a live person on the ground.

Even though email and text messaging traditionally carry the day, having the option to speak to a live person when normal internet and telecommunications systems are down is priceless. Consider satellite phones as another key tool in the critical toolkit when systems are truly in their worst conditions. Think about what options were available to businesses in Nashville on December 25, 2020, when a bomb explosion shutdown mobile and land communications across the southeast.

> ***On December 25, 2020, when a bomb explosion in downtown Nashville shut down mobile and land communications across the southeast, think about what communication options were available to businesses? How could they have transacted business?***

Satellite phones should be tested monthly, or at least quarterly, to ensure they are both working and people know how to send and receive calls. It's equally important to remember that a satellite phone needs a clear view of the sky. Calls from a conference room deep inside the building will fail.

A new Globalstar GSP Satellite phone can be purchased for as little as $500, and the number of phone plans based on minutes per month or megabytes transmitted vary as much as traditional wireless phones. There are also options to purchase pre-paid phone cards or go for an annual or monthly contract for as little as $35 a month for basic service.

There are many plans that align with both budget and with where in the world you require service.

GOVERNMENT EMERGENCY TELECOMMUNICATIONS SERVICE (GETS)

During the events of 9/11, even though network failure was partially related to infrastructure disruption at ground zero, the sheer call volume of family and friends calling into and out of area code 212 quickly ground network traffic to a halt. The volume of phone calls to New York City easily overloaded the capacity of a telephone network already in distress. Most people who called area code 212, or tried to call out of New York City, were met with a recorded message, "All circuits are busy, please try later" or no signal at all. And even though wireless and land-based phone capacity is constantly being improved, it's economically unaffordable to build a network to support 350 million simultaneous phone calls.

Responding to this crisis after the fact, the United States Department of Homeland Security's Cybersecurity and Infrastructure Security division implemented the Government Emergency Telecommunications Service or GETS designed for those businesses and governments, who have a stake in protecting the infrastructure of the United States, with working telephony at a time of disaster.

To net it out, GETS provides card holders with a special priority access when making a phone call. In addition, GETS card holders are also permitted to add mobile phones through the Wireless Priority Services option.

Not everyone is eligible for GETS service, and a business must apply and preferably have a sponsor within the city, state or the federal government. Nevertheless, if your business and key members of your organization require priority telephone services at a time of a local or regional crisis, apply for your GETS card today. Remember, these systems must be set up in advance, and the process could take roughly 30 days to 45 days.

Only through testing can an organization truly understand how they will perform at a time of disaster.

TESTING THE PROGRAM

The success of any crisis and incident management program will depend upon the extensiveness of program testing. Are your processes well documented? Are essential employees considered identified and available? Can you recover your data backups? Are the relevant organizations engaged at a time of disaster and before the growing shockwave visibly impacts their business?

Only through testing can an organization truly understand how they will perform at a time of disaster, and more importantly, what corrective actions can be taken to both evolve the crisis program and improve responsiveness so there's confidence when the moment of truth arrives.

Both the firm's board of directors and the executive leadership team must be knowledgeable on where your model is strong and where there are soft spots that need improvement. At a minimum, incident management testing should be performed annually, and the results need to be documented and communicated so there's no surprises when something doesn't work when the real crisis strikes.

THE RELEVANCE OF BLACK SWANS

No discussion on crisis would be complete without reviewing the topic of black swans.

In the wild, actually seeing a black swan is rare. In business, a black swan event is that rare form of disruption that just can't ever happen. The event by definition is rare and often too far-fetched.

- A dirty bomb explodes in Chicago or Atlanta
- Solar flares disrupt all mobile and satellite communications for five days
- A cyberattack disrupts power grids in western Europe and across the US Eastern Seaboard

Alice Hill, senior fellow for climate change policy at the Council on Foreign Relations, and author of the book, Building a Resilient Tomorrow, discusses the concepts of "past extremes" and "future extremes." To paraphrase, future extremes are rare situations that may never happen. The examples listed above are future extremes.

A power outage across the State of Texas was once considered a future extreme. However, reviewing recent history, a power outage has shut down the State of Texas three times since 1989 (full state outages have occurred in 1989, 2011, and again in 2021). This State of Texas power outage scenario used to be considered a black swan, but really should be considered a "past extreme."

Based on the recurring past, it's more plausible than ever that Texas can expect another massive, all-encompassing power outage. Unless the Electric Reliability Council of Texas (ERCOT) takes action to mitigate issues now encountered three times since 1989, the vulnerabilities in the state's energy system will not change and another collapse is imminent.

At the macro level, the State of Texas power loss demonstrates what was once thought to be impossible has now occurred three times in the last two decades. Even though the probability of the problem reoccurring is low, the probability is no longer low enough to call this situation a black swan.

SUMMARY

Having an active and regularly tested crisis program is a game changer when a real crisis hits your business. But it truly only functions when part of the bigger picture.

Technically, an active cyber security program and regularly monitored data backups, combined with a tested recovery process are key technical elements and are the front line to any technology-related disaster. And, from a business perspective, documented, well maintained, and tested business continuity plans comprise another key cornerstone, and will ultimately save the day long after the security and information technology teams return to their laptops.

External threats such as cyberattacks require a unique form of diligence against what feels like an unlimited number of known and unknown forms of impact. Yet, there are also internal threats through self-inflicted wounds created by human error, or software changes improperly executed. Here's where a disciplined change management, problem management and quality program, creates value by reducing outage time or business missteps easily visible to customers and partners.

The sad reality is it's only a matter of time before a problem finds a way to your business's doorstep or returns for another round of mayhem.

A company who implements and nourishes an incident and crisis management system will immediately see benefits at time of disaster. More importantly, when discussed with customers this type of differentiation will lend value to both your business proposition and the value customers will see in doing business with you.

Everyone suffers problems at some point in their business. Being able to respond professionally and calmly will always reduce the outage time, protect the reputation of the brand, and pay huge business dividends in the form of revenue growth, improved profitability, and happy customers.

REFERENCES

"The Internet Under Crisis Conditions: Learning from September 11," **The National Academies Press**, 2003.

The Government Emergency Telecommunications Service (GETS), www.dhs.gov/gets

Hill, Alice. **Building a Resilient Tomorrow.** Oxford University Press, November, 2019.

Kaspersky, Eugene. "The Hidden Costs of Ransomware Attacks," **The Banker,** April 1, 2021.

REPORTS AND INSIGHT

"The Global Risks Report 2021," World Economic Forum, January 2021.

Storlie, Chad. "Manage Uncertainty with Commander's Intent," Harvard Business Review, November, 2010,

BLOGS

Cyberint Research. "Colonial Pipeline Incident," May 13, 2021.

Liebermann, Erez and Andrew Pak. "Three Lessons from the Colonial Pipeline Breach," May 8, 2021.

Puldy, Michael. "NASA's Asteroid Destroys New York City, the Return of the Black Swan and Other Thoughts on a Normal Work Day," May 13, 2019.

Puldy, Michael. "Leveraging the Texas Power Outage to Add Business Value," February 26, 2021.

Rene, Dan. "Crisis Lessons from This Morning's Broken Internet," June 8, 2021.

PODCASTS

The Crisis Ahead Podcast, "Why, When and Hot to Test Crisis in Management Plans," November 9, 2020.

Deep Background with Noah Feldman, "Bigger Than Texas," March 10, 2021.

Risk Stories! "Crisis Management: Bad News Doesn't Get Better with Age," March 30, 2021

Risk Stories! "When Data Stops Flowing, So Does the Revenue," December 15, 2020

SmallBizCast with Joel Volk, "Avoiding Disaster!" June 8, 2021.

FOR MORE INFORMATION

Puldy Resiliency Partners is ready to develop and grow your business resiliency program. Creating business resiliency is what we do all day, every day.

For businesses looking for a cloud-based solution to access critical documents and processes, plus exercise a unique messaging system to report incidents or act at time of crisis, check out the Starfish Business Platform. A limited-feature, small business owner version is now available on the Apple app store or contact us for a demonstration.

To learn more about business resiliency programs, testing services and related IT risk management advisory and training, please email contact@puldypartners.com or visit us at puldypartners.com.

Contact The Author

Michael L. Puldy
CEO, Puldy Resiliency Partners, LLC
michael@puldypartners.com

Special thanks to Michael Georgen (consultant, m.georgian.il@gmail.com) for his counsel, advice and edits during the creation of this document.

Published in the United States of America June 2021

[1]Bunge, Jacob and Jesse Newman. "Ransomware Attack Roiled Meat Giant JBS, Then Spilled Over to Farmers and Restaurants," **The Wall Street Journal**, June 11, 2021.

[2]Bunge, Jacob. "Meat Buyers Scramble After Cyberattack Hobbles JBS," **The Wall Street Journa**l, June 2, 2021.

[3]The impact of squirrels on the power grid is so disruptive, the American Public Power Association has developed a "squirrel index" to track the phenomenon.

[4]Storlie, Chad. "Manage Uncertainty with Commander's Intent," **Harvard Business Review**, November 3, 2010.