JUSTIN DANIELS AND DAVE OATES

RESPONDING TO A RANSOMWARE ATTACK

A PLAYBOOK

FOR C-LEVEL EXECUTIVES AND DIRECTORS

1ST EDITION

RESPONDING TO A RANSOMWARE ATTACK

FOR C-LEVEL EXECUTIVES AND DIRECTORS

JUSTIN DANIELS AND DAVE OATES

1ST EDITION

“

COMPANIES, NONPROFITS, GOVERNMENT AGENCIES, AND OTHER ENTITIES MUST CONSIDER PREVENTING A RANSOMWARE ATTACK AND HANDLING AN INEVITABLE CYBER INCIDENT.

”

CONTENT

1

WHAT IS RANSOMWARE

CHAPTER ONE

WHAT IS RANSOMWARE

RANSOMWARE CAN NOW SHUT DOWN ANY COMPANY REGARDLESS OF SIZE OR INDUSTRY.

It is Sunday morning, and you are a busy executive. This time is normally reserved for catching up on some rest, but the constant buzz of your phone for the last five minutes makes sound sleep impossible. When you look at your phone, your CTO has written in all caps:

"OUR ENTIRE NETWORK HAS BEEN ENCRYPTED, AND THE HACKER HAS PROVIDED AN EMAIL TO TALK ABOUT HOW WE CAN GET OUR NETWORK BACK."

You begin to feel a knot in your stomach, and your mind begins to race with questions like: Do we have backups? What will our customers say? How long will we be down? Can we recover? After all that you have read in the newspapers, ransomware has become a reality in your business. Now What???

Ransomware is malicious software deployed by bad actors who use it to hold your organization hostage. They do this by encrypting all your data and denying you and your employees the ability to access your business systems. Imagine not being able to fill orders, run payroll, send out invoices, or use your email. Your entire IT department is plunged into chaos at the same time your phone is ringing. The hackers are counting on you caring about your data and business enough to pay a ransom to have your data and systems restored. Now, to sweeten the ransom pot, the hackers have started employing a form of extortion where they threaten to make your stolen data public. How would your customers react to all their data or intellectual property placed on a public website? Who would trust your organization after such a debacle?

DATA AND YOUR INFORMATION TECHNOLOGY INFRASTRUCTURE HAVE BECOME THE MOST IMPORTANT ASSETS IN OUR CONNECTED ECONOMY.

Ransomware can now shut down any company regardless of size or industry. Companies, nonprofits, government agencies, and other entities must consider preventing a ransomware attack and handling an inevitable cyber incident. Data and your information technology infrastructure have become the most important assets in our connected economy. It's as important as any investment into all the other aspects of the organization that delivers its products and services.

Yet far too many companies continue to treat security as an afterthought. How would you feel if your favorite NFL team announced Monday that they would just show up on Super Bowl Sunday and play without any defensive game plan? That would make national news, and everyone would demand that the coach be fired or at least have his head examined! However, when it comes to cyber security incident response, most companies possess no plan and decide to just show up on Sunday and see how it goes. The results are predictably bad.

In today's interconnected economy, organizations, their C-Suite, and essential team members must know how to respond to a ransomware note BEFORE you receive one. Everyone involved needs to understand how to interact with the internal and external response teams. As important, organizations that get hit with a ransomware attack will need to assess how to better prepare for and manage future incidents. These are the major questions we will answer as you turn the pages of this book.

While prevention is always the best medicine, we live in a cybercriminal world today where the likelihood of getting hit with ransomware is just about inevitable.

With that context in mind, let's don our headset and start to prepare your defensive game plan for that Sunday ransomware note.

2

WHO TO PUT ON THE RESPONSE TEAM

CHAPTER TWO

WHO'S ON THE TEAM?

THE TIME TO BUILD YOUR TEAM IS WHEN YOU DON'T HAVE AN ISSUE!

The first step is knowing the key players you need in the incident response context: cyber security/IT management, outside legal counsel, forensic expert, ransomware negotiator, and crisis communications. In addition to having these experts identified before a breach, you need to make sure that your cyber insurance carrier has approved them. Insurance companies have expert panels that work much like your in-network doctor. If the provider is in-network, the insurer will pay for it. Several insurance companies will not cover the fees if the provider is not. Since many breaches happen on the weekend if you do not know if your experts are covered under your insurance, do you wait to confirm which could delay their work or have them start only to be told two days later that the insurance company will not cover their fees? Some insurance companies will allow you to choose your own vendors, provided they agree to it when you bind your insurance. In either case, a failure to plan will cost the most precious resource in incident response -- time!

The first thing to do is get your legal team in place. Many may feel the IT and Information Security Teams should take priority. However, you'll want legal to quarterback your incidence response efforts and be responsible for retaining additional services needed to address a ransomware attack. This step is essential. Suppose you do not hire your experts through outside legal counsel. In that case, you will likely forfeit any right to assert that your communications with your experts are protected by attorney-client privilege.

That is also why the first expert you retain needs to be your legal counsel. Remember, if you hire a forensic vendor first that provides you a report about the breach, hiring legal counsel after the fact will not cloak that prior report or related conversations in privilege. Such documentation and conversations could be devastating to the company in potential litigation. Legal counsel will review all customer communications as you must weigh legal versus business considerations.

THE FIRST STEP IS KNOWING THE KEY PLAYERS YOU NEED.

Certainly, there may be times that you may choose to take legal risks because you decide that the greater risk of losing customers outweighs legal liability protection. Even in those instances, legal counsel can help you weigh these competing interests as you make decisions with incomplete facts and under time pressure.

Seasoned incident response attorneys have pre-negotiated agreements to retain the forensic expert, ransomware negotiator, and crisis communications. If you do not have these agreements pre-negotiated, you could spend several days wrangling over contracts instead of responding to the cyber incident. The result is that once again, you lose the most precious resource, which is how you spend your time responding.

Legal counsel also plays another critical role by acting as your liaison with Federal law enforcement. The Office of Foreign Assets and Control (OFAC, a department within the U.S. Treasury) ensures that U.S. citizens and companies are not dealing with foreign countries, corporations, or people the U.S. government has sanctioned under our foreign policy. In October 2020, OFAC issued a directive stating that anyone who paid a ransom payment to someone on OFAC's sanctioned list could be held liable for aiding and abetting terrorism. The advisory is strict liability. That means if you did it, you are liable even if it comes to light six months later.

OUTLINE YOUR IT AND INFORMATION SECURITY TEAMS AND THEIR ROLES NEXT. IDEALLY, THESE TWO FUNCTIONS ARE SEPARATE DEPARTMENTS.

That means if you did it, you are liable even if it comes to light six months later. However, the ruling went on to say that cooperating with law enforcement would be viewed as a substantial mitigating effect. While that phrase is subject to interpretation, the government does make it clear that you must engage federal law enforcement before paying anything to ransomware attackers. Your legal counsel will act as your bridge to productively doing so. What's more, legal counsel engagement with law enforcement frees your internal team to work on other facets of the incident response.

With the legal team and supporting elements in place, outline your IT and Information Security teams and their roles next. Ideally, these two functions are separate departments. Your InfoSec group should report on potential security issues to senior leadership, while your IT department's role is to support the daily user and business operations. These two missions will sometimes conflict, so it's best to keep these teams separate and resolve any strategic issues at the CIO/Chief Information Security Officer (CISO) level. For smaller organizations with limited staff, consider engaging a third-party security advisor such as a Managed Security Services Provider and/or virtual Chief Information Security Officer (vCISO) to help consult with your in-house IT team and senior leadership on such matters.

Lastly, a proven crisis communications expert is essential to your team. Far too many incident response plans call for the attorneys to take on that role, but that will prove to be detrimental to ensuring the trust and confidence of your employees, customers, partners, and the general public. Your cybersecurity legal team's job is to manage the entire incident response instead of the details of creating and implementing a crisis communications strategy. Having a crisis communications expert on the team offers a different perspective. Be sure to recruit qualified professionals that have a track record of managing corporate communications during ransomware and other cyber incidents.

With those team members in place, organizations should begin to include other essential stakeholders to ensure proper emphasis on responding to a cyber incident. Most important are the organization's Board of Directors and senior management, who provide the strategic direction of a cybersecurity program. Their collective job is to ensure that the company's risk is being properly addressed and managed.

QUESTIONS TO ASK TEAM MEMBERS

The next step will be to identify each team member's roles and responsibilities. This process includes interacting and developing prevention and incident response plans to counter a ransomware attack. Questions on who will do what and when should be raised to create strategies and processes to mitigate or eliminate threats.

Here are some of the issues that should get asked and by whom:

Legal Department:

- Who will initiate the forensics investigation?
- How will the process unfold and when?
- How will relationships with appropriate law enforcement agencies be established and maintained?
- What is the company's posture on negotiating with the threat actors/ ransomware thieves?
- Who will initiate the negotiations with the threat actor if a decision is made to do so?
- Who will initiate and coordinate the required breach notification to third parties?
- The analysis of relevant breach notification laws may require notifications sent to third parties and attorney generals.

InfoSec/IT/Forensics team:

- How can you identify the origin of the infiltration, or "Patient Zero"?
- How will the forensics investigation be conducted?
- How will backup systems be placed online or the current system decrypted?
- How will the security holes get patched?
- How will you coordinate efforts with legal and the rest of the team?

Crisis PR:

- What's required for customer breach notifications and by whom?
- What audience groups (employees, customers, partners, investors, etc.) take priority in your communications outreach?
- What are the messages you'll convey?
- Under what circumstances will you proactively disseminate information?
- Under what circumstances will you wait to respond to queries before releasing information?
- Who will act as a spokesperson for the organization and to which audiences?
- How will you field inquiries?

3

BEST PRACTICES TO COUNTER A RANSOMWARE ATTACK

CHAPTER THREE

BEST PRACTICES

CHANCES ARE, EVERY ORGANIZATION WILL AT SOME POINT RECEIVE THAT DREADED RANSOMWARE NOTE.

Even the best preventive plans are not foolproof. Cyber threat actors' sophisticated and cunning nature means that a strong possibility exists for any organization of any size to be the victim of such an attack. How, when, and what severity will depend on leadership's importance in preventing and preparing for one.

Should a ransomware event occur, your established team will need to manage forensics, crisis communications, ransom negotiations, and breach notification. Every day during the response brings tough business decisions as you weigh legal and business considerations across these four broad fronts with incomplete facts under time pressure. Let's touch on each of these phases.

First – Isolate

If you or an employee suspects ransomware, you should first isolate the infected machines by removing them from the network, that is, disable any WI-FI connections. If you act quickly, you may help stop the virus from infecting the entire network.

Second - Identify the type of attack and perform a forensic analysis

Next, you will need to identify the type of ransomware that infected your network. There are a variety of strains and remedies. Some websites will help you determine the type of ransomware you've been infected with and, if you're lucky, give you options for removal or disinfection.

Third - Perform required notifications

EVEN THE BEST PREVENTIVE PLANS ARE NOT FOOLPROOF.

The legal breach notification analysis is usually the river Rubicon. A laundry list of potential plaintiffs follows once you notify third parties under state breach notification laws. These range from the state attorney general to a regulator to a class action lawsuit. Breach notification laws typically key off the definition of personal information. They also vary as to whether data was accessed or exfiltrated. In a ransomware event, if all that the threat actor did was encrypt your network to seek payment, they may have never accessed or exfiltrated any data. Thus, while the company might pay the ransom, the firm may not be legally required to notify any third parties. In other situations, where threat actors threaten to dump personal information from the network if the ransom is not paid, that is a very different situation. This analysis can be complicated because a forensic investigation may not conclusively determine that data was accessed or exfiltrated. In such cases, it falls to legal counsel to assess all the facts and make a crucial determination whether the facts warrant notification under relevant state breach notification laws.

Companies may also be required to notify their customers under their contracts. That means that companies can no longer overlook the security provisions in their contracts. If you are legally required to inform a customer within 48 hours of a broadly worded security event, you may have to disclose information when you know very little, and it may change quickly. There are other contract clauses from large companies where you must delegate critical decisions to that large customer. Since contracts now have significant security addendums, you need to understand what these clauses really mean in the context of incident response. You know very little in 48 hours after an event happens. Yet, you agreed contractually to notify your customer within 48 hours. Are you prepared for what that might mean to your communications strategy and how that impacts your other key stakeholders? Your contractual obligations could put you in an odd relationship with your customer that does not consider your wider obligations to your other customers.

Fourth - Restoring from backups
If you have your backups on a hard drive, tape, or stored in the cloud, you will have to make several considerations before restoring:

- Is it possible that your backups have also been infected? Hackers can be in your systems for months exfiltrating data and gaining root access so that they can infect your backups. Before restoring, you will need to look at your files to ensure that they haven't been changed.

- Are your applications backed up? Typically, the answer is "No." Without the applications, you will not be able to restore your data and business operations. For example, you can't open your Excel spreadsheet with your sales forecast if you don't have Excel installed on your workstation. Not addressing this is a big miscalculation for small and midsized businesses because they grossly underestimate the time it takes to clean the system, reinstall the applications, and then reinstall the backups. Also, if you have 10 terabytes of data in the cloud, you need to calculate the time to download the data from the cloud. Depending on your bandwidth, it could be days or weeks.

- Do you regularly test and validate your backups to make certain that all the information is there and you can access it when you need it?

- Have you identified what critical systems and needs to be restored first?

- Do you have any idea how long you can be without your data before it's detrimental to the company? This determination is another area that organizations greatly underestimate. Often, we hear business leaders say they can be down a few days. Still, when we help them calculate the total cost of downtime (backorders, employee compensation, third-party penalties, lost customers, etc.), they quickly realize that downtime is a mitigating factor when deciding whether to pay the ransom.

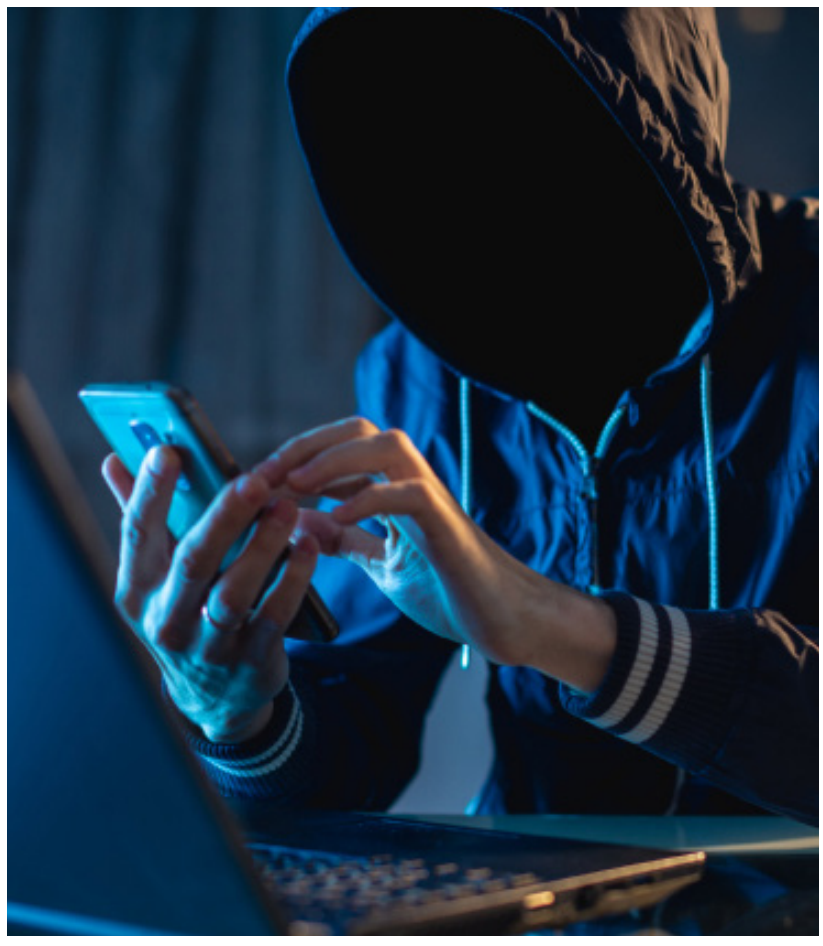
> "EVERY DAY DURING THE RESPONSE BRINGS TOUGH BUSINESS DECISIONS AS YOU WEIGH LEGAL AND BUSINESS CONSIDERATIONS.

Fifth - Engage (or not) the threat actor

WHETHER OR NOT YOU ENGAGE WITH THE THREAT ACTOR IS A BUSINESS DECISION. IT WILL DEPEND ON WHETHER THE THREAT ACTOR HAS ALREADY TAKEN COMPANY DATA AND THREATENED TO RELEASE IT.

Whether or not you engage with the threat actor is a business decision. It will depend on whether the threat actor has already taken company data and threatened to release it. It may also depend on whether your company has backups that the attack did not compromise. You will also consider whether it is faster to restore from backup than paying the threat actor's decrypt key. As we discussed earlier, the U.S. Department of Treasury's Office of Foreign Assets Control (OFAC) issued an advisory that will fine organizations that make ransomware payments to criminal organizations on their Specially Designated Nationals. According to the OFAC, "Facilitating a ransomware payment that is demanded as a result of malicious cyber activities may enable criminals and adversaries with a sanctions nexus to profit and advance their illicit aims. Ransomware payments may also embolden cyber actors to engage in future attacks. In addition, paying a ransom to cyber actors does not guarantee that the victim will regain access to its stolen data."

Even if you ultimately decide to pay, you may wish to delay the payment as you assess whether your backups work or how real the threat of releasing company data is. If you need to make the payment quickly, a ransomware negotiator is key in helping to facilitate the payment. We do not recommend that you buy and hold cryptocurrency yourself. The reason for this is that containing cryptocurrency is not your core business, and its value may widely fluctuate. It is better to have a resource who can procure it for you quickly should you decide to make the payment.



Sixth - Execute your crisis communications plan

From a communications standpoint, timing becomes critical at the onset of a ransomware attack. Not rapidly communicating to audiences will allow others to set the narrative. Employees, customers, business partners, investors, and the general public want to hear from you. If they do not, they'll soon question whether you have control of the situation or, worse yet, don't care.

As self-evident as it seems, most organizations neglect to engage ALL audiences. I grant you that most crisis communications strategies pay significant attention to news organizations but forget other vital groups. A good plan prioritizes audiences like this:

- Employees
- Customers
- Business partners
- Agency officials/government entities
- Investors (or donors if a nonprofit)
- Press/general public

Staff must always – ALWAYS – get informed about an adverse news event before any other audience. It doesn't matter what type of crisis. Employees serve as the most effective and valuable marketing assets. They operate as your director of first and last impression. Provide staff with the information on the crisis matter and empower them to convey your message clearly and effectively.

There's one crucial point to note here. You'll want your crisis communications team to determine if you should operate in an **"Active"** or **"Passive"** mode. Active covers situations where an organization announces an issue that, if not a crisis already, will soon evolve into one. Tactics include sending out a press release, posting a notice on social media, distributing an email blast, making phone calls, and other activities without prompting. The intent is to tell specific audiences proactively about an adverse event or issue. This mode usually occurs due to one of three factors:

- State and Federal regulations regarding cyber security attacks require you to notify one or more audiences proactively.
- One or more audiences know of the issue and will imminently inquire if they have not done so already.
- The issue will generate significant backlash for the organization if audiences find out you didn't disclose the news before.

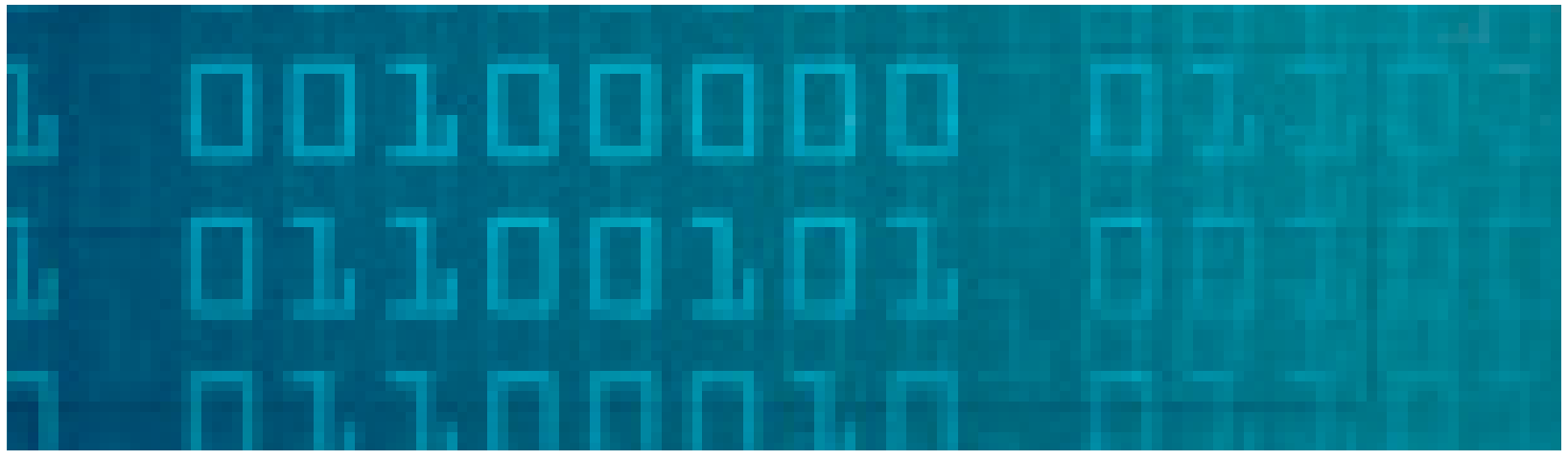
Otherwise, consider operating in a Passive mode by preparing to respond but only to inbound inquiries. You don't need to sound alarms if it's not warranted. Of course, developments can change quickly, so get ready to shift to Active mode at a moment's notice.

Keep this in mind. You can operate in different modes under the same Crisis PR plan for different audiences. It's not an "all or nothing" scenario.

If you've determined that you must operate in "Active" mode, get out and in front of it as soon as you can. Craft the initial message, however brief. Stick to the facts and don't over speculate. Send these same updates to your teammates before you blast everyone else. You can use email, your intranet page, workplace messaging app, or other vehicles.

From there, post information on a separate section of your website to direct outside parties to get the latest. Post links to the information on your website via social media and distribute the press release simultaneously. Update as often as needed, sometimes hourly if necessary.

> "STAFF MUST ALWAYS – ALWAYS – GET INFORMED ABOUT AN ADVERSE NEWS EVENT BEFORE ANY OTHER AUDIENCE.



As you do, state as much as you can without disrupting any of the negotiations underway with the threat actor or disrupting the efforts to restore systems. That said, it's best to convey what's going on in as specific terms as possible. Doing so will undoubtedly cause friction with lawyers, executives, and consultants. There will always be careful consideration of what to say internally and externally when facts change rapidly. While you do not want to convey information that will hamper negotiations with the threat actor or create unnecessary liability risk, there are countless examples where being too ambiguous only causes more angst and anxiety with audiences. They'll see the organization as inauthentic and willfully misleading. Work in advance with the legal team and other entities to assess how specific your communication can be balancing business and legal considerations.

RARELY WILL YOU COMMUNICATE YOUR WAY THROUGH RANSOMWARE ATTACKS WITH A "ONE-AND-DONE" APPROACH.

The organization cannot assume it can speak once and diffuse the tension for good. Rarely will you communicate your way through ransomware attacks with a "one-and-done" approach. Audiences need to hear from you not just early but often. You have the opportunity – and responsibility – to be present in whatever in-person or virtual form that requires. Look at how you need to reprioritize the existing communications channels during workplace disruption.

Also, be mindful of your tone and body language as you convey information. Offer a sense of assurance and commitment to your teammates. That doesn't mean you must "sugar coat" the issues or present a false, unbelievable "remain calm; all is well" persona — quite the opposite. Present the problems in absolute terms, but then provide solutions and participate in them. Give them a sense of control, and you'll generate an energy level that can overcome practically anything. I've seen this in many workplace environments, from military settings to investment management firms. Your body language and tone supersede the spoken word.

In doing so, you will reinforce the key messages you implemented to respond to the ransomware attack. You can also celebrate those that adjusted to care for customers and other stakeholders. It will generate a feeling of empowerment by staff and hope for your customers, investors, and partners when they feel a bit helpless.

With your messaging in place, ensure you've got an internal process where those who receive them, such as a receptionist, website administrator, HR, or marketing person, know which appropriate spokesperson they should forward the request right away. Delaying an answer while figuring that out or allowing the first available person to respond, such as the underutilized VP of the breakroom foosball table, are never good options.

You should also prepare for the "Gotcha" questions that seemingly come from nowhere. They often carry an inherent bias, insinuating that the organization and its leaders did something wrong, either maliciously or through negligence. Many times saying "No Comment" or letting the accusation go unchecked cedes the narrative to others.

As the crisis evolves, your messaging and tactics will most certainly change. A crisis communication situation, most certainly one applying to a ransomware attack, is never a "set it and forget it" event. Activities will continue to evolve and require regular messaging, tactics, and coordination updates. You'll need to keep revising the plan, likely several times, throughout the ordeal.

To do this, get your Crisis Communications Team – along with senior leaders – to huddle daily about what has changed and what new developments need to get conveyed to specific audiences. Then figure out whether you need to adjust your tactics accordingly. Schedule the get-together for as long as the crisis remains active. You can always dial it back when things stabilize.

The effectiveness of your specific spokesperson's becomes essential during a ransomware crisis. Like most initiatives, the CEO may drive the general direction and message. Still, others like your Chief Revenue Officer, VP of Customer Service, VP of Channel/Distribution, and HR Director will help deliver the news, sometimes more effectively than your top executive. You can spot the good spokespeople during a crisis and those who need more training.

> "MANY TIMES SAYING "NO COMMENT" OR LETTING THE ACCUSATION GO UNCHECKED CEDES THE NARRATIVE TO OTHERS.

Another key element to establish trust in your communications during a ransomware attack is how well you respond to inquiries. It's hard to stay on topic when you're getting barraged with leading and accusatory questions. Developing "muscle memory" through regular practice will allow you to address audiences quickly and in an empathetic and action-oriented manner. If you don't practice it, particularly on the gotcha questions, you'll wind up defaulting into a "fight" or "flight" mode when a Crisis Communication event occurs.

The fight mode happens when you instinctively argue against everything said online or in the press in sharp and, sometimes, angry tones. Some organizations go a step further by discrediting the person making the accusation. All that gets accomplished by taking this route is to elevate the anxiety and anger your audience feels about you and hamper your ability to return to normal operations.

On the other hand, other companies go into flight mode during a crisis communications situation by saying very little or nothing. Such silence can give an even stronger voice to the other side. The better you are at getting your message out in a thoughtful, well-understood manner can determine whether you're able to connect with your audiences and secure their support.

4

WHAT TO DO AFTER THE CRISIS IS OVER

CHAPTER FOUR

EVALUATE AND TRAIN

IMPROVING YOUR READINESS FOR ANOTHER CRISIS, BE IT RANSOMWARE OR AN ENTIRELY DIFFERENT MANNER, IS CRITICAL.

The military has an after-action report to assess what went well, what did not, and opportunities for improvement. In the context of breach response, we are talking about resiliency.

You need to view cybersecurity as a strategic business enterprise risk from a legal perspective. It should be at the forefront of your risk management plan for the network. This step consists of two buckets: incident response and proactive services.

From an IT and tech standpoint, conduct a root cause analysis and create follow-up objectives. Questions to ask yourself and the executive team are:

- How did the virus get into the system?
- How well did we execute our incident response plan? Does it need to be updated?
- What other lessons have we learned?
- How can we best evolve our security strategy to mitigate future attacks?

On the crisis communications front, you want to start asking hard and reasonable questions about what went well and what didn't. Canvass your team and your target audiences to get feedback on the following.

- How well did we prepare for this event?
- What tactics met or exceeded expectations?
- How should we include additional tactics in future incidents like this one?
- Who were the best spokespeople, and who needed improvement?
- Who else should we put on the Crisis Communications team?
- How well was our messaging received?
- How quickly were inquiries routed, and how fast did we respond?

It is essential to evaluate performance when it is fresh in your mind. When the crisis ebbs, catch your breath, get a good night's sleep, and then begin the evaluation. Your fresh memory will help capture all the nuances of the activities and strategies that the team undertook. This process helps make your plan much better and based on the most up-to-date threats to the organization.

The candid feedback from your counterparts in IT, HR, legal, customer service, and other departments is also vital. They will provide invaluable insight into where the messaging and tactics helped and when they fell short. Many of these groups also dealt directly with confused (if not angry) customers and other audiences. Getting their help to improve your readiness for another crisis, be it ransomware or an entirely different manner, is critical.

Conveying messages with the proper approach takes practice. Moreover, your practice drills should happen without warning. Create situations where management walks in during the day, gathers the team around, and throws a scenario at them to tackle with no preparation time. That's what will happen in real life.

5

CONCLUSION

CHAPTER FIVE

CONCLUSION

RANSOMWARE IS AN INEVITABLE CONSEQUENCE OF OUR RELIANCE ON TECHNOLOGY. YOU NEED TO PREPARE FOR IT MUCH LIKE YOU BUY INSURANCE.

Every business is a data business in our knowledge economy, and data is its most important resource. Companies spend millions of dollars building trust so customers will buy their products and services. Consider gaining customer trust by respecting their data by demonstrating that data security is essential. A vital piece of this respect is preparing for responding to a data breach. You can also expect other businesses to not do business with you if you cannot substantiate your data protection practices and have an incident response plan.

You must identify your breach team and ensure your insurance provider approves them. Your legal response needs to be flexible and acknowledge that sometimes business considerations drive legal decisions. Suppose you protect yourself from liability and lose significant customers that is not a good result. Making sound business decisions under time pressure with incomplete information is the art of incident response. At any time, customers, the threat actor, or breach notification may drive the prioritizing of issues you face at any given moment. At the same time, are you considering best practices to protect your organization from these attacks better? Do you require that everyone in your organization use multi-factor authentication? If not, why not? At the same time, are you requiring your vendors to use multi-factor authentication? It is by far the most cost-effective tool against ransomware that you can implement at a reasonable cost.

Ransomware is an inevitable consequence of our reliance on technology. You need to prepare for it much like you buy insurance. You hope not to have to use it, but you have it when necessary. Those who fail to plan have already planned to fail.

ABOUT THE AUTHORS

JUSTIN DANIELS

Justin is a Shareholder at Baker Donelson and provides his corporate clients a pragmatic approach to addressing cybersecurity as a business enterprise risk at every stage in the business lifecycle. He specifically advises the c-suite and boards on identifying and managing cybersecurity risk with respect to mergers and acquisitions, investment capital transactions, lending, vendor and customer contracts, and cyber insurance. He leads breach incident response teams on ransomware and wire fraud cases in industries ranging from medical IT, health care SaaS and logistics to manufacturing. Companies regularly seek Justin's advice on preparing to handle breach response and proactively managing cybersecurity risk. He received his J.D. and MBA from Duquesne University in 1998 and is bachelor's degree, cum laude, from Virginia Tech University in 1993.

DAVE OATES

Dave is the Founder of PR Security Service and possesses more than 25 years of strategic public relations experience dealing with a wide array of adverse public events. Starting as a U.S. Navy Public Affairs Officer and later as a Corporate Chief Marketing Officer and Non-Profit President, he excels in expertly addressing a myriad of crises spans non-profit, military, government, corporate, education, charity, and start-up environments. His Crisis Communications experiences, including handling employee and executive misconduct, cybersecurity attacks, product recalls, mass layoffs, large-scale accidents, criminal investigations, and civil litigation matters. Dave received his MBA from San Diego State University in 2004 and his bachelor's degree from the University of Maryland in 1991.