CYBER STORM

HOW TO PROTECT YOUR BUSINESS FROM A DATA BREACH AND THE RESULTING CYBER STORM OF FINES, LAWSUITS & CUSTOMER LOSS

STEPHEN CRACKNELL

WHY EVERY C-SUITE EXECUTIVE HAS A DUTY TO PREPARE FOR A CYBER-ATTACK

A SPECIAL EXCERPT FROM THE
AMAZON.COM BESTSELLING BOOK

CYBER STORM

CHAPTER 6

WHY EVERY C-SUITE EXECUTIVE HAS A DUTY TO PREPARE FOR A CYBER-ATTACK

BY STEPHEN CRACKNELL
CEO & Owner – USM Technology

Great things are done by a series of small things brought together. ~
Vincent van Gogh

The most dangerous attitude a C-suite executive can have about cybersecurity is thinking a cyber-attack could never happen to their organization, so there's no reason to implement a recovery plan. Some executives say they aren't concerned because their assets are too small to pique a hacker's interest. Tell this to the senior citizens tricked out of a couple hundred bucks after their e-mail accounts are hit.

Others may think that they are safe because they already spend plenty on cybersecurity. Well, leadership at Apple, Chase, and even some branches of the federal government know firsthand that their financial resources do not make them invincible. The truth is that there's no silver-bullet technology to guarantee cybercriminals will not infiltrate a network. If it existed, these behemoths would have been the first in line to purchase it. Instead, they joined the ranks of countless other cybercrime victims spanning the past decade.[1,2,3]

We cannot afford to underestimate the capabilities of today's cybercriminals. Hackers are ruthless, calculated, and organized. They have demonstrated an utter lack of compassion for humanity by stealing from our grandparents, and they have proven high levels of competence by figuring out how to break into the largest, most well-funded organizations on earth.

So, here is the uncomfortable question you must consider. If your organization invests less money and time in cybersecurity than the large entities that have been hacked and are a richer target than the average elder, is there any legitimate reason to believe hackers won't eventually breach your network too and demand a ransom?

WE ARE FIGHTING A WAR

The moniker "cyberwarfare" is no exaggeration, considering war is "a state of competition, conflict or hostility between different people or groups." US-based organizations are the targets of organized cybercrime syndicates that regularly consolidate under hostile nations to steal money from us – so, by definition, this is a war. (lexico.com, 2021)

To emphasize the severity, here are two sobering facts about the cybercrime industry:

- The global cost of cybercrime has climbed from $3 trillion in 2015 to $6 trillion in 2021 and is expected to reach $10.5

[1] Mehrotra, Kartikay (2021, April 21), "Apple Targeted In $50 Million Ransomware Hack Of Supplier Quanta," *Bloomberg*, https://www.bloomberg.com/news/articles/2021-04-21/apple-targeted-in-50-million-ransomware-hack-of-supplier-quanta

[2] Coker, James (2021, August 23), "US State Department Hit By Cyber-Attack," *Infosecurity Magazine*, https://www.infosecurity-magazine.com/news/us-state-department-cyber-attack/

[3] Lakshmanan, Ravie (2021, January 10), "Russian Hacker Gets 12-Years Prison for Massive JP Morgan Chase Hack," *The Hacker News*, https://thehackernews.com/2021/01/russian-hacker-gets-12-years-prison-for.html

trillion by 2025.[4]

- The head of the US National Security Agency stated, "Cybercrime constitutes the greatest transfer of wealth in human history."[5]

The business of cybercrime continues to grow, in part because, although the US federal government knows who many of the key actors are, they are unable to prosecute the most nefarious groups. This is because these criminals are protected by nations that financially benefit from the attacks. Immunity allows attackers to safely develop increasingly sophisticated strategies that lead to escalated levels of damage and more frequent hits. And the greater harm hackers inflict, the higher the ransom they can demand to halt the destruction. As profitability grows, these groups reinvest and the cycle continues, each time more successful than the last.[6]

PREPARE FOR THE WORST

If your organization has repelled a minor cyber-attack in the past, don't be lulled into a false sense of security – surviving a mosquito bite in a land where hungry lions run free does not make you unsusceptible to a big cat attack. Be prepared to respond to the worst-case scenario. It's easier to scale back recovery efforts than amp them up during a crisis.

Beware of an extremely harmful and common tactic called the *human-operated ransomware attack*. The actors often start with classic hacking techniques to enter the target network. In teams, they conduct reconnaissance, exfiltrate data, and elevate their

[4] Morgan, Steve (2020, November 13), "Special Report: Cyberwarfare in the C-Suite: Cybercrime to Cost the World $10.5 Trillion Annually by 2025," *Cybercrime Magazine*, https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

[5] Rogin, Josh (2012, July 9), "NSA Chief: Cybercrime Constitutes the 'Greatest Transfer of Wealth in History,'" *FP Insider*, https://foreignpolicy.com/2012/07/09/nsa-chief-cybercrime-constitutes-the-greatest-transfer-of-wealth-in-history

[6] Dixon, William (2019, February 19), "Fighting Cybercrime – What happens to the Law When the Law Cannot be Enforced?" *World Economic Forum*, https://www.weforum.org/agenda/2019/02/fighting-cybercrime-what-happens-to-the-law-when-the-law-cannot-be-enforced/

network privilege and access. This prep work prior to launching the actual attack enables exponentially more damage than with other types of cyber-attacks.

Here’s a walk-through of what could happen to you: Hackers research your organization through publicly available information to learn about your business model, profitability, and pressure points. They find out everything they can about your leaders and their habits. They then enter the network – possibly through targeted phishing. Once inside, they conduct the kind of research that can only take place *within* your network. They attempt to move laterally while escalating their access privileges. They also make a concerted effort to leave themselves multiple “backdoor” entrances to more easily return if the first attack fails. They attempt to exfiltrate sensitive data and house it on their servers for use as future blackmail fodder. Since they are about to have great success converting your organization into a paying client, they can’t wait to return! And that won’t be the last time.

HACKERS ENTER QUIETLY AND LEAVE NO TRACE

How do they get away with this? Sophisticated hackers wait until your organization is most vulnerable – off-hours when leadership is disconnected from technology or a time when your industry is typically preoccupied. They know that an accounting firm is most vulnerable in the middle of tax season, and a retail chain is an easy hit during the Christmas rush. Executives, hackers are watching you. They follow your CEO’s family on social media, so when their spouse posts details of an upcoming overseas vacation, they can plan an attack for these dates.

To kick off the strike, hackers trigger a self-propagating virus to disable recovery tools, destroy backup files and prepare your network for the attack. Then they launch the ransomware, which crawls across the network and encrypts any sensitive data files it can access.

The final step, like Boy Scouts departing a campsite, is to make sure they *leave no trace*. They clean up the crime scene, making a concerted effort to eliminate all recorded evidence of their activity. This process includes deleting log files, which makes your recovery efforts all the more challenging since your forensics team relies on the log files to answer these important questions: Which techniques did the actors use to penetrate the network? When did hackers first infiltrate the network? Which systems and users were compromised? Hackers know that without this information, your recovery effort will be prolonged and likely incomplete, so they will have an easier time re-entering your network.

To ensure you are able to answer those questions, continuously route critical log files to a secure off-site system capable of dynamic analysis. This populates a repository for the forensics team to review in the aftermath of an attack. This system can also alert your technical team when suspicious activity is occurring inside your network, so you'll be better poised to stop an attack from escalating.

UNITED WE PLAN

A house divided against itself cannot stand.
~ Abraham Lincoln

Your best defense is a united front and a well-executed plan. During a major cyber-attack, the entire executive team must operate as a cohesive unit and share one common goal. Leadership's mantra should be "We shall restore our core business processes as quickly as possible."

It is incumbent upon business leaders to work with their IT team to build out a robust incident response plan and to do so immediately. If you do not have one in place, your group will be forced to build it *after* the attack is launched, likely at two in the morning. At this point, staff will be exhausted and likely locked out of the tools they need to document your path to recovery, and meanwhile, the ransom clock continues to tick.

If the executive team participates in the document creation and approval process, then the leaders will have the time and resources needed to set post-attack priorities. These priorities will help to guide the rapid recovery of the organization’s critical business processes during a crisis. The fewer questions and details to sort out during the crisis, the faster your cyber-response team can act and the more likely they will operate as a cohesive unit in the first critical days after a cyber-attack. Moving forward quickly gives your group a better chance of finding an alternative to paying the ransom.

Conversely, if your organization responds to a cyber-attack with internal disputes and focuses on assigning blame, you create a hacker’s dream dynamic. After launching an attack, their primary objective is to divide the people who are responsible for recovery efforts. They want to make your technical executives look foolish and incompetent because when the team loses faith in them, the organization as a whole will become feeble and ineffectual. Cybercriminals have learned that they are typically well-positioned to receive a ransom payment in the near future when a leadership team spends most of its energy fighting against itself.

A SOLID INCIDENT RESPONSE PLAN FOR THE WIN

By failing to prepare, you are preparing to fail.
~ Benjamin Franklin

When disaster strikes your organization, a well-designed incident response plan becomes the difference between surviving an attack and becoming yet another victim. This plan should include a list of team members who will participate in the recovery effort, a workflow of activities, vital network configurations, and contact details for employees and vendors as well as key clients. Everyone should know in advance which tasks they are responsible for completing and have the necessary resources at the ready.

It's critical for your company to have a plan in place to quickly spin up a clean "recovery network" for secure communications. Email and phone systems may be compromised during the attack, making it difficult to coordinate recovery efforts. You may need to wait days or even weeks before these platforms can be fully reestablished on the infected network.

Be prepared for hackers to taunt the leadership team, saying how easy it was to break into your network while providing very clear instructions for how to pay the ransom. They want to convince you that making the payment is the only way to restore your network, and they work to make the ransom transaction effortless. They are getting very, very good at it, by the way. Some cybercriminal syndicates will even offer a "support desk" to set up a cryptocurrency account and expedite payments.[7]

THE FIRST 72 HOURS ARE CRITICAL

Your recovery team's ability to work effectively in the first three days after a ransomware attack is essential to successfully rebuff the cybercriminals. We recommend your goal be to have your core business processes back online within 72 hours of the attack to minimize the loss of income and productivity and to avoid paying the ransom.

Expedience is everything. You won't have time to debate when to call in the insurance company or which cyber-recovery consultants to hire. Your IT team cannot wait for Finance to approve spending requests or for the COO to decide which systems should come back online first.

This time frame is key because hackers often put limits on how long they will wait for payment. They know that as each hour passes, the likelihood that they will get paid drops precipitously.

[7] Crawley, James (2021, July 19), "Anatomy of Ransomware Attack: Chat Support, a Discount and a Surcharge for Bitcoin. *CoinDesk.* https://www.coindesk.com/markets/2021/07/19/anatomy-of-ransomware-attack-chat-support-a-discount-and-a-surcharge-for-bitcoin/

As a result, they often implement fallacious deadlines to add pressure. At the 72-hour mark, they may threaten to double the ransom or, after seven days, refuse to sell you the decryption key.

Don’t give priority to less important issues, such as the hunt for culpability, determining how the hackers infiltrated your network, assessing damage, or responding to inquiries by outside entities. These other efforts can happen alongside recovery efforts but are secondary. Throughout the initial critical days, regularly remind yourself and your team that none of these competing objectives will matter if your organization goes bankrupt as a result of not resuming core business processes in a timely manner.

Recovery from a major attack will take many days or weeks, so everyone must be ready to deal with the inevitable exhaustion. Make sure your response teams work in shifts and that your staff and leadership are given time to recuperate. If you do not plan for this, fatigue will cause focusing difficulties, poor memory, otherwise avoidable mistakes, and irritability.

Also, know that paying the ransom is not a “Get-Out-Of-Jail-Free” card. The hackers may demand more money after you pay the initial amount. They may accept your money but not send you the key or send one that only works to unlock certain files. Once your organization has paid a ransom, chances dramatically increase that the hackers will use one of the back doors they left open to return, re-encrypt your files and start the whole process all over again. Or they may threaten to release sensitive information that they exfiltrated to the media, competitors, or your clients. And there is no avoiding the ugly truth that some of the ransom you paid will fund their next round of attacks.

THREE ESSENTIAL RESOURCES NEEDED TO RECOVER A NETWORK

Whether working with an external IT firm or your internal department, after a cyber-attack you'll need to give the technical professionals access to these vital tools in order to recover your network:

1) *Off-site Data Recovery Solution:* A ransomware-resilient off-network data recovery solution will allow critical servers and their data to be quickly brought back online after an attack.
2) *On-site Log Repository:* A comprehensive off-site Security Incident and Event Management (SIEM) solution that gathers, analyzes, and stores key log files will allow a forensics team to determine how and when the hacker first entered a network.
3) *Incident Response Plan:* Key details about critical business processes, network configurations, and a plan for the initial response, along with contact information for key vendors, clients, and staff, poises you for a successful recovery.

CYBERCRIME IS A SERIOUS MATTER

Globally, malicious cybercrime continues to escalate in severity and frequency. As a business leader, you have a duty to ensure your organization is prepared for battle. You need to have a robust incident response plan in place so, in the event of a cyber-attack, you and the other C-suite executives are in a position to model efficacy, inspire unity, and quickly recover those core business systems.

ARE YOU READY TO TAKE ACTION?

During a serious cyber-attack, your incident response plan becomes your company's most valuable asset. To help your C-suite executives start this critical recovery planning process, we have developed a resource that outlines the core components. (https://guide.usmtechnology.com)

CYBER STORM

FEATURING

STEPHEN CRACKNELL

Stephen Cracknell is the CEO and owner of USM Technology. He founded Dallas and Houston based USM Technology in 2010 to provide IT solutions and cybersecurity services to mid-market organizations across the US. Along with his wife, Stephen also owns US Medical IT, a managed services provider (MSP) that caters to the health care industry.

USM Technology assists businesses with IT projects, cloud computing environments, servers, networking, and help desks. Their highest priority, though, is to help business leaders repel cyberattacks.

He has witnessed the destructive power of ransomware firsthand too many times. In one case, cybercriminals dismantled a healthy business – a small medical clinic – in a matter of minutes. After the attack, the physician-owner reached out for help. It turned out that ransomware had encrypted the medical records server as well as the backup drives that were connected to the network. Unfortunately, the doctor didn't know he needed to maintain an offline copy of the backup files. If he had received the right training and preparation, the clinic would still be operating today.

On the flip side, the team at USM is energized when helping IT leaders implement technology such as custom automation, digital forms, workflows, and business intelligence to evolve their business and enable staff to reach their potential.

Stephen knows about the creative use of ones and zeroes himself. During his 12-year career at Microsoft, he worked on many projects involving security, databases, and network architecture. Then, after Hurricane Katrina hit the Gulf Coast, he was asked to assemble a team to design a digital registration system for American Red Cross disaster shelters. Stephen's team formulated a ruggedized, battery-powered solution that allowed volunteers to digitally collect and relay demographic and medical details of displaced persons – even when the disaster area lacked power and Internet. Bill Gates was so impressed that he presented Stephen and his team with Microsoft's Innovation Award. Stephen built on these experiences when he launched USM Technology. The company has been a Microsoft Gold Competency Partner for over a decade and was twice named Microsoft's South Central US Partner of the Year.

Stephen holds a bachelor's degree in economics and finance from the University of Guelph in Ontario, Canada. He currently serves in a leadership role with the Health Industry Council Foundation of North Texas and is a member of Voices for Innovation, an advocacy group that works to build laws that support privacy, security, and STEM education. He also volunteers with the Geneva-based CyberPeace Institute as a Master CyberPeace Builder, providing free cybersecurity services to nongovernmental organizations (NGOs) that protect vulnerable communities around the world. Stephen can also be found volunteering with his son's Boy Scout troop, as well as camping and hiking with his wife and two children.

To contact USM Technology:

- Email: stephen.cracknell@usmtechnology.com
- Web: USMTechnology.com
- Phone: Dallas/Fort Worth: 214-390-9252; Greater Houston: 832-975-0035

The authors of this book have donated all royalties to St. Jude Children's Hospital.

For more information please visit **www.stjude.org**

DESIGNED AND PRODUCED BY TECHNOLOGYPRESS™
Printed in the USA

$19.95
ISBN 978-1-7369881-5-2
51995>
9 781736 988152