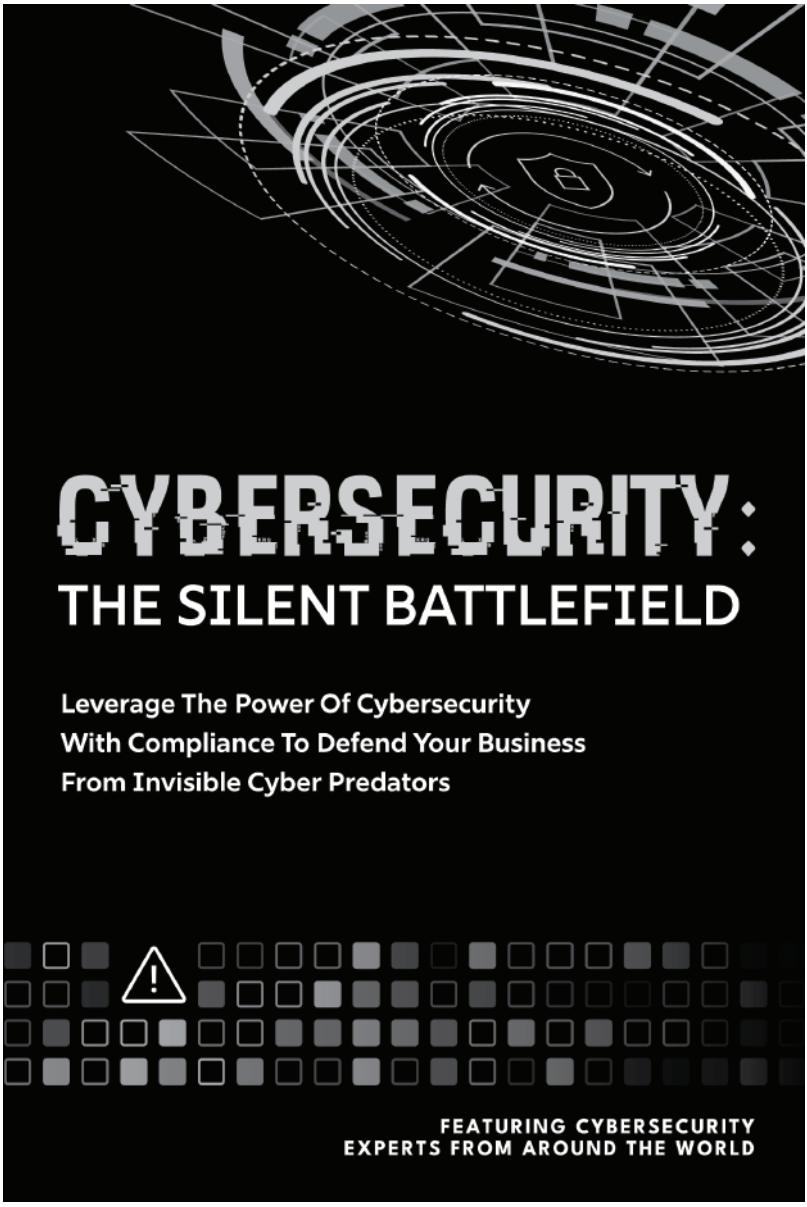
CYBERSECURITY:
THE SILENT BATTLEFIELD

Leverage The Power Of Cybersecurity
With Compliance To Defend Your Business
From Invisible Cyber Predators

TODD HOLLOWAY

FEATURING CYBERSECURITY
EXPERTS FROM AROUND THE WORLD



BigRedMedia
a TMT company

Nashville, Tennessee

Chapter 9:
What To Do When Hacked: A Business Survival Guide

Todd Holloway
CEO, Custom Technologies, Inc.

It happened two months after I'd been turned down on my cybersecurity and MSP services proposal for the third year in a row. The prospective client was a local chiropractor with approximately 20 employees, including four or five chiropractors. We presented them with a proposal every year, but each time, we always got the same answer: "It's too much money." But this year, after rejecting our proposal again, they got hit with a ransomware attack.

Cybercriminals locked down their entire network. The chiropractor called me up and wanted us to come in and "fix everything." The hackers were asking for $400,000. The chiropractor told me he'd write me a check for $100,000 immediately if I could restore everything to how it had been. I asked him if he'd implemented any of the steps we discussed in our last meeting. When he replied, "No," I had the unfortunate task of delivering the bad news to him. We couldn't do anything for him. After talking with me, he reached out to his antivirus software company. They explained to him that they handle viruses and that ransomware is a whole different level of problem. He then sent his hard drives to a data recovery company, but they couldn't help him

either. He ended up going out of business. Twenty people lost their jobs, and he lost everything he had worked so hard to build.

That chiropractor made several mistakes; if he had corrected them, it would have helped him avoid his unfortunate demise:

- He thought his business was too small to be hacked, so he implemented no cybersecurity measures except antivirus protection. Hackers do not discriminate based on the size of a business. Your information is valuable to a hacker because it is valuable to you. Small to medium-sized companies are considered easier targets than larger ones because they generally have weaker cybersecurity defenses. In addition to installing ransomware on your systems, hackers want your passwords, bank details, and client information to sell on the dark web (or wherever). Keep in mind that hacking is a legitimate business model in some countries. Hackers come into the office Monday through Friday and work from 8 a.m. to 5 p.m. Their goal is to crack as many networks as possible. They are just waiting for someone in your organization to make a mistake. If one of your employees clicks on the wrong link, it can tell the cybercriminal everything about your network they want to know, including all your passwords, in about 15 minutes.
- He had no cybersecurity insurance. Only 17% of small businesses have cybersecurity insurance (with 48% of them purchasing insurance after they experience an attack). Another survey found that 55% of all organizations in the United States claim to have some form of cyber insurance. Still, only 19% of organizations have insurance for events beyond $600,000. Although $600,000 is a lot of money, it's not enough to cover the cost of most cyberattacks, as expenses increase quickly. There are recovery, forensic, legal, and public relations costs, as well as the costs related to lost business.

- He did not have a business survival guide to follow if his business was hacked. He had no idea what to do or who to call. In addition to preventing chaos, a business survival guide can limit the extent of damage to systems and your data while also reducing your downtime. A well-prepared response plan also helps ensure compliance with legal regulations to avoid penalties. Plus, it can help you maintain employee morale and customer loyalty and preserve your business's reputation.

As you read this chapter, you will discover the components of a successful business survival guide you can implement if your business is hacked. To make sure your business survival guide is as successful as possible, you must do the following ASAP:

- **Meet with your cyber insurance provider** – Before any hack occurs, it's essential to have a meeting with your insurance provider. Find out exactly what they want you to do in the event of a breach. Talk to them about what legal and regulatory obligations you must fulfill should you have a data breach. Ask for their advice on communicating the incident to employees, customers, stakeholders, the public, and law enforcement.
- **Assign roles and responsibilities** – All the key players involved in the response team must know what's expected of them. Designate someone in upper management to oversee and coordinate the overall response. Assign individuals to various roles, such as internal communication with employees and external communication to stakeholders, clients, and the media; overseeing reporting to the relevant authorities and regulatory bodies; maintaining business operations during the breach; and so on.

- **Test your backups regularly** – Many hackers now delete or change your backup routine, so you think you're backing up everything, but you're only backing up a few files. Your morning report says that everything has been successfully backed up. When you restore it, you discover that you only backed up one or two files. Always back up your data in multiple places (locally and in the cloud). Test your backups once a month at a minimum.

The following steps might vary depending on what your insurance company wants you to do, but they must be included in your plan. When you get hacked, the first things you do are:

- **Call your cyber insurance provider** – After giving them your policy number, you'll need to report an overview of what happened, when you first noticed the breach, the extent of the hack, and the type of attack (ransomware, phishing, malware, etc.), if known. You'll need to talk about the potential consequences of the hack, such as data loss, business interruption, or client data exposure. At this point, they will most likely put you in communication with their incident response team or forensic investigator. It's critical that you follow their instructions exactly. If you don't, they could deny you coverage.
- **Contact the appropriate government authorities** – In the United States, the primary contact for reporting cybercrimes is the FBI. The number to call is 1-800-CALLFBI (1-800-225-5324). You should also file a complaint with the Internet Crime Complaint Center (ic3.gov). The IC3's Recovery Asset Team works as a liaison between law enforcement and financial institutions to help recover stolen funds. The Cybersecurity and Infrastructure Security Agency should also be notified. Their number is

1-844-Say-CISA. You should also inform local law enforcement and the office of your state's attorney general. Further, industry-specific regulators should be notified. For example, healthcare companies must contact the Department of Health and Human Services. In addition, many states have established their own cybersecurity agencies or divisions within their public safety or homeland security departments. For instance, California has the California Cybersecurity Integration Center, while Texas is served by the Texas Department of Information Resources. If your data breach involves personal information, it might need to be reported to the Federal Trade Commission. In Canada, a data breach must be reported to the Office of the Privacy Commissioner of Canada and industry-specific authorities (e.g., a healthcare business should notify the provincial healthcare regulator).

- **Contact your MSP and your attorney** – Your MSP has the tools and expertise to contain the breach and get you up and running ASAP. Your attorney will help ensure you comply with all legal requirements and provide guidance on data protection laws. Due to attorney-client privilege, you may want to run everything through your attorney first and let them act as your spokesperson throughout the entire process. It would be best to have your attorney present during any interactions with law enforcement.
- **Isolate the infected devices** – Isolating an infected device ASAP is critical because it minimizes damage and prevents the spread of malware. A good MSP can detect any nefarious traffic on your network and immediately isolate the device or devices from your network so they can no longer send or receive traffic. However, this is an area where you must be sure what your insurance company wants you to do – one insurance company might want you to

isolate the infected device(s). In contrast, another might want you to leave everything as is for forensic reasons.

- **Change passwords** – It's crucial to change your passwords ASAP. If your business uses password-manager software, changing your passwords will be significantly easier. Changing passwords can prevent cybercriminals from continuing to exploit compromised accounts, which is especially important if the breach involves credential theft.
- **Turn on two-factor authentication** – Turn on 2FA for all software and log-in accounts on your local devices and in the cloud. If possible, use a 2FA provider like Duo Security that gives you better control over the logins and detailed visibility into each session.
- **Document everything** – All your systems have logs associated with them. Keep a minimum of a year's worth of logs. Take screenshots of all relevant data. We even take pictures of the server closet so we know which color wires are plugged into which portal.
- **Get your business up and running again** – The ideal situation is to get your business back up and running within four to six hours. This generally involves uploading clean backups to the cloud so employees can access applications and data.
- **Inform the appropriate parties** – Your public relations strategy should focus on transparency, empathy, and clear communication to maintain trust with the public. The immediate response should include acknowledging the breach, expressing concern for those affected, and outlining the steps being taken to contain the incident. Providing clear information about what happened, the type of data compromised, and the potential impact is crucial. Additionally, offering support such as credit-monitoring services and a dedicated helpline can help affected individuals protect their

information. Ongoing communication is essential to keep the public informed about the investigation and remediation efforts. Regular updates demonstrate transparency and commitment to resolving the issue. It's also vital to communicate existing measures and the measures the company will implement to prevent future breaches, such as enhancing security protocols and conducting employee training. By following these steps, you can rebuild trust and mitigate reputational damage.

- **Do a root cause analysis** – An RCA is a systematic process for identifying the cause of a data breach. There are three types of root causes: 1) *Physical* – A physical security breach is less common than other root causes, but protecting your business from them is still extremely important. This involves either an intruder or a disgruntled employee or contractor entering your building and accessing your computer systems and network. Mistakes in security settings can also create vulnerabilities that hackers can exploit. 2) *Human Error* – 95% of cyberattacks are caused by human error: an employee clicks on a malicious link, confidential information is accidentally emailed to a cybercriminal, easy-to-guess passwords are used, security updates aren't installed, and so on. 3) *Organizational* – A company lacks comprehensive (or has outdated) security policies, opening gaps that can be exploited. Some employees might have excessive access privileges that increase the cyber-threat risk. A successful RCA can prevent similar future attacks and help your business implement better security measures and policies.

To build confidence in your ability to respond effectively to cyberattacks, minimize damage, and ensure a swift recovery, conduct a test run of your business survival guide at least once a year. This process

involves several key steps: defining objectives, selecting a realistic scenario, assembling the incident response team, and developing a detailed script with specific events and triggers. During the exercise, team members role-play their responsibilities, simulate communications, and practice containment, investigation, and recovery actions. The goal is to identify strengths and weaknesses in the response plan, improve team coordination, and ensure compliance with regulatory requirements. After the exercise, a thorough evaluation and debriefing are conducted to review performance and update the plan accordingly.

While a cyberattack can devastate the finances and reputation of any business, the good news is that if your business survives, your company will be stronger. A cyberattack exposes security vulnerabilities, which, when addressed, will lead to more robust cybersecurity measures and better employee training. A well-managed response can enhance a business's reputation for transparency and responsibility, which can build trust with your employees, clients, stakeholders, and the public. Plus, an attack will refine your business survival guide, making your company better prepared in the event of a future attack.

About Todd Holloway

Todd Holloway, CEO of Custom Technologies, Inc., provides services in Metro Atlanta and North Georgia, with a client base extending beyond Philadelphia. Custom Technologies, with a 34-year track record, is one of the most established IT companies in the Atlanta region. Today, they are a managed services provider focusing on security. Powered by ongoing education and support, Custom Technologies provides its clients with a robust security infrastructure, enabling them to effectively protect their assets and operations.

Todd started his career as a firefighter in Atlanta in 1990. Given the low pay for firefighters at the time, he needed additional income, so he partnered with a friend to build computers on his days off. After five years, he bought his partner out. Although Todd initially planned to finish law school and become an attorney, his passion for firefighting and the financial success of his computer-building business led him to continue his firefighting career. Finding immense satisfaction in turning adverse, life-changing events into manageable situations, he cherished the challenge of running into burning buildings and helping people. Todd witnessed firsthand the devastating consequences business owners face when unprepared for natural disasters. He saw similar devastation in businesses unprepared for cyberattacks. As the leader of Custom Technologies, he gets deep satisfaction in helping companies turn negatives into positives and avoid cybersecurity-related disasters.

Over the years, his IT business evolved from building computers to offering managed services and cybersecurity solutions. Todd became involved with Microsoft, serving on their advisory council for small business servers and contributing to the development, delivery, and release of Microsoft products. When he retired from the fire department at the beginning of the COVID-19 pandemic, Todd returned to Harvard to study cybersecurity management and incident response. Today, Todd is entirely focused on running his IT business day-to-day, leveraging his extensive experience and education to provide top-notch services to his clients.

Todd and his team believe in "underpromising" and "overdelivering." They always prioritize doing the right thing for their clients over maximizing profits. They avoid providing inferior products and services to cut costs, ensuring their clients always receive the highest quality of service and protection available in today's marketplace. At least once a quarter, they meet with clients to discuss their plans and goals and help with IT budgeting. They encourage their clients to share information about other technology-related contracts, including printer and copier agreements, Internet service provider contracts, and Voice over Internet Protocol (VoIP) agreements, to ensure they receive the best value and service for their needs. Clients appreciate this proactive approach, which helps them manage their technology investments more effectively and efficiently.

Another unique aspect of their customer engagement involves sending out king cakes for Mardi Gras instead of traditional holiday cards. This idea originated when Todd visited New Orleans in 2009. He now orders king cakes fresh from New Orleans and delivers them to clients, who look forward to this yearly tradition.

For more information, contact Todd Holloway at
Custom Technologies:
Phone: 770-792-6700
LinkedIn: linkedin.com/in/todd-holloway-494117a/
Email: todd@custech.net
Web: custech.net

CYBERSECURITY:
THE SILENT BATTLEFIELD

ABOUT TODD HOLLOWAY

Todd Holloway is the CEO of Custom Technologies, Inc., a leading managed IT and cybersecurity provider serving Metro Atlanta, North Georgia, and beyond. With 34 years in business, Custom Technologies helps companies protect their operations with cutting-edge security solutions and proactive IT management.

Todd's career began in 1990 as a firefighter in Atlanta. To supplement his income, he built computers on his days off, eventually turning his side business into a full-time IT company. While firefighting, he saw firsthand how unprepared businesses were for disasters—both physical and digital—fueling his passion for cybersecurity.

Over the years, Custom Technologies evolved from hardware sales to managed IT services and security. Todd worked with Microsoft as an advisor for small business servers and later studied cybersecurity management at Harvard. Today, he and his team focus on delivering enterprise-level security and IT solutions to small and midsize businesses.

Todd believes in "underpromising and overdelivering," prioritizing long-term client relationships over profits. His team meets quarterly with clients to review IT strategy, budgeting, and vendor contracts—helping businesses maximize their technology investments. Custom Technologies ensures clients receive top-tier security without cutting corners.

Adding a personal touch, Todd started a unique tradition: sending king cakes for Mardi Gras instead of holiday cards. Inspired by a trip to New Orleans in 2009, he now delivers fresh king cakes annually, a tradition his clients look forward to every year.

With a commitment to security, integrity, and client success, Todd continues to lead Custom Technologies as a trusted IT partner in an ever-evolving digital landscape.

Designed and Produced by Big Red Media
Printed in the USA

BigRedMedia
a TMT company