THE ROAD TO CYBERSTRENGTH

Your Cyber Risks
10 Things You Can Do About Them

THE LANDSCAPE

You don’t know it, but you’re in a race against time.

Malicious hackers could be residing in your network right now, gathering information on your business processes, waiting for the perfect time to strike. Or they could be stealing your valuable customer data and intellectual property. Only 47% of small-to-medium-businesses (SMBs) find breaches within days of occurring.

In 2021, food companies, utilities, supply chains and software providers all fell to hackers. Business email compromise proved it could still exploit human error. Ransomware took down corporations, vital infrastructure and government offices.

But small-to-medium-sized businesses were not exempt. In fact, 60% of hacked SMBs declared bankruptcy within 6 months. Was it error or complacency on the part of business owners?

You may not want to address cybersecurity—but it’s addressing you. You think you won’t be hacked, that it can't happen to you. But it can happen to you.

What you will do to prepare?

CONTENTS

04 A Note From The Editor

05 SMBs at Risk: It's not you—yet.

06 SMBs: The Fallen

07 Hackers: Their Methods

09 Hackers: The Stats

10 Is Your Internet Down?

12 Know Your Cyber Security Insurance

14 Responding to Risk

17 10 Things You Can Do To Respond

18 What Is Your Cybersecurity Posture Now?

20 Buyer's Guide

21 Why You Should Work With Tech Kahunas

Authors

Peter Bondyark is owner and founder of Tech Kahunas, a managed security service provider in San Diego. He is a Microsoft Certified Systems Engineer and holds a bachelors of applied science in technology management from St. Petersburg College. He lives in San Diego with his wife and two children.

J.C. Berry (Cross) is a cybersecurity analyst (CySA+), web developer and freelance writer. He holds a BA in English from Point Loma Nazarene Univeristy and an MA in journalism from Regent University. He lives in San Diego with his Boston Terrier Jax.

1

SMBs at Risk: It's Not You - Yet

Hackers do not discriminate when it comes to the size of your business. They use giant email lists which they purchase from the "dark web"--the shady, un-indexed, but massive side of the internet. Using these lists, they send out phishing emails, that in turn expose targets to business email compromise, ransomware, or other malware and cyber attacks.

Phishing emails are mass mailed to unsuspecting receivers and look like legitimate emails from a merchant, a bank, a credit card company, law enforcement, the IRS or other government offices. Clicking on links or opening the attachments in these emails initiates a download of malware, compromises the receiver's computer or exposes his data. While in the past these emails could be spotted because of unprofessional-looking design or imperfect English, today they are almost indistinguishable from true official or merchant emails. Your users can be the weak link that clicks or opens a devastating attack.

Thousands of attacks are happening right now and **for 60% of small-to-medium businesses (SMBs), lead to bankruptcy within six months** (Cybercrime Magazine).

Take ransomware, one of the fastest growing threats (105% increase in attacks from 2020 to 2021, for a total of 623.3 million reports in 2021) (TechTarget). Ransomware involves hackers gaining access to a network, encrypting the organization's files and systems, and then demanding a ransom payment to decrypt the files. The company sometimes gets only a small percentage of their data back; other times, not at all.

Phishing emails can also contain ransomware infected attachments (Graphus). In 2021, the FBI's Internet Crime Complaint Center received 3,729 complaints identified as ransomware averaging losses of more than $49.2 million (FBI). 2022 is already seeing an increase.

SMBs: THE FALLEN

Colorado Timberline – Five-year-old (as of Feb. 2011) supplier's files were encrypted by ransomware and hackers did not offer unlocking software, despite the company paying the ransom. Ultimately, after being acquired by a private equity firm, declared bankruptcy (ASI)

The Heritage Company – Ransomware brought down this 61-year-old telemarketing company (PrivacySavvy).

United Structures of America – After paying the ransom, this $100,000,000 company didn't get its data back and eventually declared bankruptcy. The time from infection to bankruptcy was about 2 years (National Law Review).

Wood Ranch Medical – Ransomware encrypted all patient data, which led to bankruptcy (PrivacySavvy).

2 HACKERS: THEIR METHODS

What else do hackers do to your data and systems in 2022?

Phishing
What hasn't changed much over the years is that over 92% of cyberattacks, including ransomware, still start with phishing emails of some kind (KnowBe4). Phishing emails are up 600% since the pandemic began (Boston.com).

Spear Phishing
These emails are sent to specific people at a company or organization. The hacker/scammer has done his research on the person and customizes the message to the receiver. This can lead to BEC, a very lucrative hack (see below).

Whaling
The crooks target C-suite executives and administrators. Oftentimes, this also leads to BEC (below).

Business Email Compromise
BEC attacks use spear phishing or whaling to gain access to an organization's email accounts. The attackers quietly maintain their presence in the network to spy on email communications, learning names and processes to use in the scam. Then, impersonating a C-suite executive or manager, they draw in lower level employees in financial departments to send funds to them. The impersonators can also steal confidential data or IP. In 2021, the FBI's Internet Crime Complaint Center received 19,954 BEC complaints with losses at nearly $2.4 billion (FBI).

Malware attacks
Malware attacks saw a decrease in 2021, with a -4% change—but there were still a total of 5.4 billion malware attacks (FBI).

WHY CAN'T HACKERS BE CAUGHT?

With this kind of brazenness by attackers, you may ask why authorities can't locate them:

- Extradition treaties for hackers operating in China, Russia, North Korea, Iran or other countries may not be in place. Dealing with the criminal laws of another country can be difficult and rogue nations can support the hackers inside their countries.
- An IP address can be hidden through malware, and botnets can run without human intervention, after an initial click on a phishing email
- (Bloomberg Law).
- Gathering legal evidence can be difficult in the end. Log files are not reliable in a court.
- Digital forensics are critical to maintain chain of custody, i.e. to never lose possession of a compromised computer; it can possibly be considered an active crime scene (Bloomberg Law).

ANATOMY OF THE HACKER

So who are the threats to your network and data? Hacking is a serious business on the dark web. With so much money being made each year--about $6 trillion--cybercrime is more profitable than all illegal drug trades combined. This is projected to be $10.5 trillion in 2025(Cybersecurity Ventures).

And hacking tools are available for free or for as low as $50 on the dark web (Mission Critical Magazine). Some hackers use "exploit kits," sets of programs used for compromising networks and systems, in order to compromise their targets.

Hackers and hacker gangs can control botnets to bring down websites or use command-and-control (C2) computers to initiate and control attacks on targets. The attackers can use the C2 system to load ransomware or other malware onto a target system.

Call centers can offer tech support to help victims get their payment to the criminal group (Gov Info Security). Phishing emails are often the origin of infection.

When hackers steal your data or ransom you, they will more than likely be out of the reach of the law (see sidebar).

The Risks Are Too Great

So you can't rely on law enforcement and you're responsible to customers to protect their data. And if you survive the financial costs of a cyberattack, the reputation and legal costs could be even greater. And when you do report it, you may not see your data or systems restored. If you are hacked and customer data is ransomed or exfiltrated to a hacker's machine, you could be legally responsible.

You must prepare your SMB or organization for an attack. It's not a matter of whether you get compromised, but a matter of when. You have to respond to risk appropriately and regularly. Risks can also change as your business changes and grows.

HACKERS: THE STATS

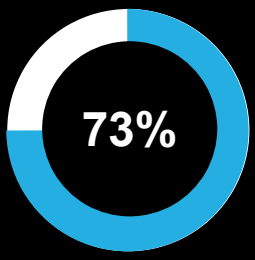
Hackers learn company weak points and their business processes. Here are some other alarming cyber stats:

- Hackers attack every 39 seconds and steal 75 data records every second (on average) (Web tribunal).
- You can buy American citizenship for $6000, medical records for about $250(SecureLink), credit cards for $5 and social security numbers for as little as $1 on the dark web (Trustwave).
- Hackers create 300,000 new malware each day and greater than 6,000 criminal marketplaces sell malware, such as ransomware (Web tribunal).
- Thirty-two percent of malicious hackers say access to privileged accounts are how they hack into systems (Web tribunal).
- Fifty-two percent of SMBs experienced a cyberattack in 2021; ten percent were hit with more than 10 attacks (Help Net Security).
- The global average cost of a data breach for SMBs was about $2.98 million in 2021. The highest cost was on the healthcare industry (AccountabilIT).

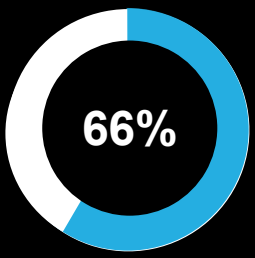
The big guys usually recover, but not without significant costs. Sixty-six percent of organizations were hit with ransomware in 2021, while 37% were in 2020. Forty-six percent of those organizations still paid the ransom in 2021 (increasing five-fold to $812,360 on average), even though the FBI advises victims to not pay (Sophos).

But again, **60% of SMBs that suffer a cyber attack are out of business in six months**.

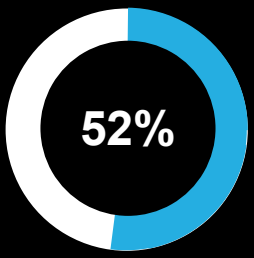
HACKER STATS



Seventy-three percent of malicious hackers say legacy firewalls and anti-malware software are irrelevant or obsolete (Web tribunal).



Sixty-six percent of organizations were hit with ransomware in 2021.



Fifty-two percent of SMBs experienced a cyberattack in 2021.

3 IS YOUR INTERNET DOWN?

Contrary to popular misconception, your IT support are not the people monitoring your cybersecurity. If you have a network outage, password problem, printing problem or internal server issue, then IT are your guys. But if you want to talk about threats to your systems, inside and outside, and the risk that vulnerabilities bring to your company, then you need a cybersecurity expert. Relying on IT support is the opposite of a strategic approach to cyber security called “zero trust,” which involves securing an organization by eliminating the unexamined trust of vendors processes and services and continuously validating every stage of business (Palo Alto Networks).

Cybersecurity experts also implement operational “controls,” like practices and procedures, in every prepared business.

IT support generally is concerned with availability, i.e. helping you get your internet connection working again when you need it and access to networks, hardware and software. It’s not a swipe at IT; that’s just what they were trained for. When someone asks for connection assistance at a company, the “IT guy” is generally called.

Meanwhile, cybersecurity focuses on CIA: protecting computer systems, digital devices and data from unauthorized access or change. IT is about the systems data is stored on. Cybersecurity is concerned with protecting the data on those systems, handling online threats and controlling users’ access to company systems.

TECHIE STUFF: DON'T RELY ON IT SUPPORT. KNOW THE CIA TRIAD

To understand more about the differences between IT and cybersecurity, we need to look at the cybersecurity objectives in the CIA Triad. The Triad is comprised of three objectives (CompTIA CySA+ Study Guide):

Confidentiality involves protecting the privacy and security of data for approved persons when needed. Cybersecurity experts implement security "controls" such as firewalls, access control lists and encryption to maintain confidentiality.

Integrity involves keeping data from unauthorized corruption or change. Cybersecurity experts implement security controls such as hashing and integrity monitoring to maintain data integrity.

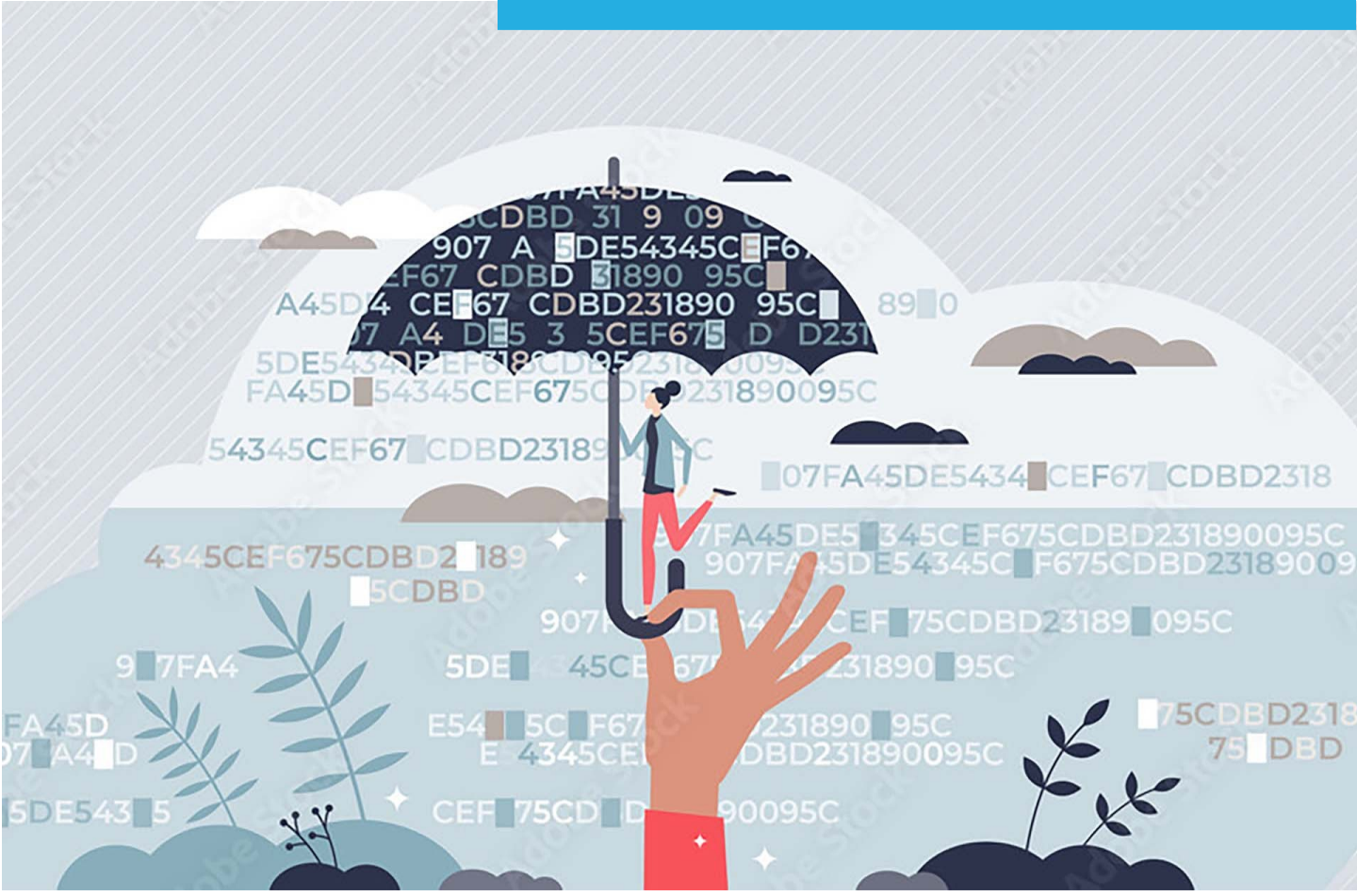
Availability involves keeping data accessible for those who need the data when they need it. Cybersecurity experts implement security controls such as load balancing and backups to maintain availability.

4 KNOW YOUR CYBERSECURITY INSURANCE

So you can't rely on law enforcement or IT, but what about cybersecurity insurance? Did you know 91% of SMBs do not have it? Perhaps they don't see the urgency. Insurance can cover things like breach investigations, legal defense, judgments and settlements, repairs, business losses and other costs (JDSupra.com). When it comes to recovery, the policies generally allocate a set amount to remediation and recovery. (Data breach costs rose from $3.86 million to $4.24 million--the highest average total cost in the 17-year history of IBM and Ponemon Institute's 2021 report (IBM).) Insurance may provide coverage for much of the recovery, but not all.

However, cyber insurance is also becoming more costly and more difficult to get. Policy costs rose 74% in 2021 to a total cost of $5 billion. Increases in premiums were due to higher risk, more litigation, greater demand and other costs. Renewal rates have been going up every year since 2019. Your insurer may also require specific actions to be taken: implementing multi-factor authentication (MFA), installing anti-malware software (one-in-five SMBs don't use computer and device security), correctly backing up data and making disaster recovery plans (51% of SMBs lack an security incident response plan) (Bloomberg Law).

Make sure that your policy includes the specific protections that you are looking for because coverage disputes could arise. Ninety-four percent of those with cyber insurance said that their experience of getting it has changed over the last 12 months, with higher demands for cybersecurity measures, more complex or expensive policies, and fewer organizations offering insurance protection (Sophos).



ASK THE RIGHT QUESTIONS ABOUT CYBER INSURANCE

Your cybersecurity experts can help you ask the right questions when shopping for the right insurance policy for you:

- What is covered?
- Will you be covered if you are found negligent and did not adhere to policy requirements?
- What you are required to do in the event you are breached?
- What do you have to document to show you took sufficient measures and followed correct protocols?

The main question to ask is, will insurance help you be in a better position to restore your systems and recover business operations and profitability? Most brokers will not know the answer to these questions. Having help with preparing your company to buy a policy and asking the right questions of an insurer is something your cybersecurity experts can help you with.

5 RESPONDING TO RISK

In the end, an insurer can't help you protect your data. You'll get some financial restitution, but you may not be able to restore your customers' valuable data--nor their trust in you. For the best protection, you need to know your risks and how you should respond to the loss of your data's CIA if you are hacked.

1. What Do You Have?

You have to know what you have in order to protect it. Look at physical and virtual assets: data, hardware and software that have a "positive economic value"–things that cost money.

How critical are these assets? How much revenue do they affect or generate? What would happen if the asset was no longer available? You should label assets in the analysis on a scale of importance.

2. What are your vulnerabilities?

What are your organization's structural flaws and weaknesses? You need to uncover these vulnerabilities in your current security. How effective are your current safeguards? What weaknesses still exist despite them? You need a complete picture of your networks and data's security.

Every asset should be measured for multiple vulnerabilities and your cybersecurity tested with industry-standard tools. Your cybersecurity experts should have diverse backgrounds and experience to enable them to consider all the weaknesses specific to your organization. (cont.)

TECHIE STUFF:
Your cybersecurity experts should use the well-known equation Risk = Threat x Vulnerability.
A risk results when both a threat and a vulnerability are present (LIFARS).

Many SMBs are using software based on legacy code from 15 to 20 years ago. The recent zero-day vulnerabilities (vulnerabilities that are exploited before experts even know about them) using Log4J is a case in point.

The initial vulnerability was only the first of an eventual four that required patches. Software vendors don't go out of their way to update their software with these new patches—and the results can be devastating. The Log4j vulnerability is so dangerous because of how ubiquitous the Log4j library is: "It's present in major platforms from Amazon Web Services to VMware, and services large and small. The web of dependencies among affected platforms and services means patching can be a complex and possibly time-consuming process" (Dynatrace). You need to be on top of vendor software like this as well.

3. What Threats Are Out There?

What malicious forces are out there? What are the human or environmental threats to your assets? What types of attackers might there be? The human threat actors are the most widespread and employees the greatest addition to this threat.

4. And What Would It Cost If…?

So when you look at the vulnerabilities and threats, you can determine what dangers an asset may face. Both a threat and a vulnerability must be present in order for them to be a "risk" to your organization. What is the likelihood that the vulnerability would be exploited? What would happen to your organization if the attack occurred? You should assign a likelihood that the exploit will occur and impact ratings for the risk. Then you can see your total risk with a "risk rating."

WHAT WOULD IF COST IF…?

Your cybersecurity experts should perform their risk assessment after every change to your networks and systems, as well as at the end of every quarter. Vendor systems should also be assessed. As an objective third party, your cyber experts may also find risks you have overlooked and perform security compliance audits as well. They should monitor the latest cyber threats from information-sharing forums. (cont.)

KNOW THE LIKELIHOOD AND IMPACT OF RISKS FACING YOUR SMB OR ORGANIZATION

5. What To Do About The Risk?

So, what to do about the risks? Responding to risk could include:

- **Treating –** Mitigating the risk should include using security and operational controls.
- **Tolerating –** Accepting the risk retains it, but by proven acceptance criteria.
- **Transferring –** Sharing and outsourcing the risk, e.g. sending residual risk to an insurance provider.
- Though **"termination,"** which involves avoiding the risk by ending or changing the activities carrying the risk, is an option in risk management in some other industries, it's not really possible to go offline in today's world.

(Security+ Guide to Network Security Fundamentals)

Also realize that not every risk can be entirely eliminated or transferred. You should be involved in procuring the best cybersecurity possible instead. As mentioned, insurance is not and should not be all you rely on. Sometimes the question is, how much risk can you tolerate? Time and money are involved; some risks must also simply be accepted.

Your cybersecurity experts should know the likelihood and impact of the risks they find and how to respond. Then they will develop a custom set of hardware, software, practices and configurations to bolster your security and reduce your risk to acceptable levels. (cont.)

10 THINGS YOU CAN DO TO RESPOND

Here are some sample risk mitigation steps that can make you a harder target. Just make sure this checklist isn't the "end-all" of your security:

1. Create or enhance user training
Create a culture of cyber awareness at your business. Over ninety-two percent of cyberattacks start with email. A careless employee could put your entire business at risk by clicking a phishing link or being scammed. You know how to stop most attacks: cyber education. Also, perform background checks of each employee.

2. 24/7 monitoring
Have personnel to monitor networks for infiltration by threats and exfiltration of data. Protect company WiFi from unwanted connections.

3. Protect data and do backups right
Training on how to handle customer or company data is critical. You may also want to institute data loss prevention software. Create and store backups on a separate network segment or on an air gapped (non-connected) network. Air gapping supplies the best protection, especially for storing backups. Only give access to backups to relevant and educated employees.

4. Patch/update
Administrators need to create processes for installing updates and patches, and for doing them as soon as possible.

5. Change default passwords
Vendor-supplied, default passwords should be changed on all network routers, firewalls, and intrusion detection and prevention systems. And if you think passwords don't matter, the SolarWinds attack was possibly due to a weak password: "solarwinds123" (CNN).

6. Remove dead accounts and privileges
When an employee leaves, remove their account and remove administrative privileges that were temporarily given to that user. Practice the principle of least privilege, i.e. only give employees the minimum rights they need. Administrator privileges can also be used for malware installation. Keep accounts locked down.

7. Install and update anti-malware protection
Though no longer the only thing needed for security, anti-malware software is still needed. Scan each computer.

8. Decrease the "attack surface"
Install firewalls and anti-malware software, shut down unused ports, and isolate systems on appropriate network segments. Use different vendors for network products. This will help with creating "layered security," where if one layer fails, another takes its place.

9. Create a secure supply chain
Get on the phone with your suppliers and partners. Ensure you are on the same page on cybersecurity.

10. Use multi-factor authentication
Whenever possible use MFA to create a secondary login protocol. 68% of malicious hackers say MFA and encryption are their biggest obstacles (Web tribunal). This is not a foolproof method, but it should be used.

And don't forget! Create and practice an incident response plan.

6 WHAT IS YOUR CYBER SECURITY POSTURE NOW?

Impeding an attack and detecting it should be a goal: if you cannot stop a hack, you want to mitigate it and slow it down through the ability to detect and respond effectively.

The pandemic shift to remote work has seen an increase and evolution in a number of kinds of attacks. It has created more responsibility: unsecured remote network access, confusing security protocols and recession-driven budget concerns. Many SMBs and organizations weren't prepared for the migration of business to the internet.

Your SMB or organization previously may not have had more than a static website. Now maybe you've expanded with an online store, customer database and new compliance regulations--not to mention remote employees who resisted the Great Resignation. Remote workers have only compounded the problem (The SSL Store).

Don't let your unattended weaknesses become a problem. You could lose everything and recent history has shown that many companies do lose everything.(cont.)

Hacking prevention begins with training for every employee and you should conduct regular phishing email drills for them. That will foster a culture of cybersecurity at your workplace where everyone needs to be onboard with security in your company.

You should proactively plan and initiate security conversations. While IT is not the ultimate answer, your cyber people need to be in partnership with IT.

Cybersecurity-as-a-service from a managed service provider is designed to help organizations deal with risks. Oftentimes, the MSP operates side-by-side with a company's IT staff.

Finances are the thing with which you as a business owner or board member are, rightly, concerned. Even if your company does not end up bankrupt, your business could be saddled with immense costs. Day-to-day operations could be disrupted: employee daily workflows, customer service, and regulation and compliance requirements. You may even incur substantial fines and lawsuits over a data breach.

A Vision for the Future

You saw a vision for the future, innovating, expanding, attracting new customers, generating new business, keeping valuable employees, attracting new, diverse talent, and creating a well-known brand. But with a data breach, your plans for the future could be threatened. Your reputation could be damaged and you can't attract new customers or employees with a bad rep.

You need to prepare. Fight for what you love and built. One careless employee or vendor is all it takes to lose your customer data. You have money to mitigate it now; don't wait until it costs much more. Manage and mitigate the red flags.

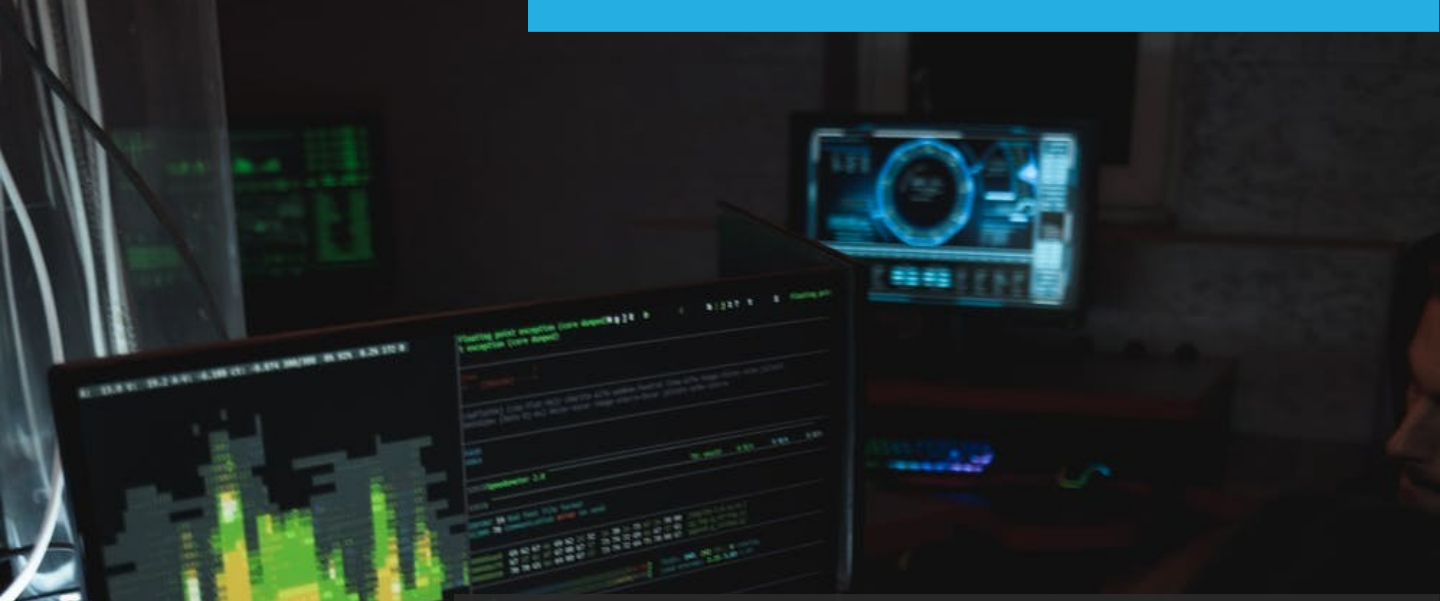
Prepare Now

You can continue the process: write down the plans, policies and procedures, educate your employees, and get cybersecurity experts who can help you as they've helped other small to medium sized businesses and organizations to fight for your security.

CYBERSECURITY BUYER'S GUIDE

Your solution should:

Implement defense-in-depth using multiple, overlapping firewalls and network devices from different vendors, and network segmentation.	Y
Identify and remediate security problems and weaknesses, including pentesting your networks and websites.	Y
Implement enterprise-grade endpoint security.	Y
Maintain user privacy and account management.	Y
Root out insider threats.	Y
Identify unnecessary, stolen, rogue or compromised computing devices and resources.	Y
Protect against business email compromise, ransomware and other cyber threats.	Y
Prevent emerging and zero-day cyberattacks.	Y
Perform critical monitoring of your organization's networks and systems to enable compliance with its applicable regulatory requirements, such as PCI-DSS regulations for credit transactions or HIPAA regulations for PHI in health care organizations. It should also establish a baseline for future audits.	Y
Implement incident response plan, including use of best practices for data loss prevention and recovery for accidental and malicious events.	Y
Protect roaming Bring Your Own Device and Choose Your Own Device business devices.	Y
Provide cyber training for employees and internal policies.	Y



WHY YOU SHOULD WORK WITH TECH KAHUNAS

So are you ready to prepare for the future? Tech Kahunas can start with a 15 minute phone consultation where we'll talk about your IT and security needs and concerns. Then we'll partner with you on a risk assessment to guide you on your journey to cyber strength.

Call 1-858-777-0040 to schedule now.

Tech Kahunas understand technology. We've had 13 years meeting the needs of San Diego's businesses with computer support and security.

Tech Kahunas work with nonprofits, manufacturers, schools, accounting firms, and government and law offices with 10-200 employees that may not have dedicated technology staff in-house. With us you can look for increased profits, reduced downtime, reliable IT performance and fast incident response, pivoting on a dime.

Tech Kahunas have years of this.

CONTACT US

Tech Kahunas
858-777-0040
info@techkahunas.com