PALMTECH
I.T. Solutions For Business

THE PALMTECH TIMES

PalmTech Computer Solutions September 2021

"I DIDN'T KNOW"

Unfortunately, That Excuse Doesn't Replenish Your Bank Account, Resolve A Data Breach Or Erase Any Fines And Lawsuits.

It's coming ...

- That day a hacker steals critical data, rendering your office useless ...
- That day when your bank account or credit card is compromised ...
- Or that day when your customers' private lives are uprooted ...

Cybercriminals are constantly inventing NEW ways to infiltrate your company, steal your assets & disrupt your life. The ONLY way to STOP THEM is by CONSTANTLY EDUCATING yourself on how **to PROTECT what's yours!** We can help! Sign Up for our "Cyber Security Tip of the Week". You'll receive byte-sized quick tips via email packed with solutions to stay one step ahead!

www.palmtech.net/resources/cyber-security-tip-of-the-week/

This monthly publication provided courtesy of Chuck Poole, CISSP, CEO of PalmTech Computer Solutions.

Our Mission

To equip small and midsized businesses in the West Palm Beach area with a smooth running and seamless IT platform that enhances productivity, improves efficiency, and creates a competitive advantage.

Protecting Your Business From Data Disasters

Data is everything to a small business in this day and age – which means if you lose access or control of your data, you lose everything.

As dramatic as that might sound, the data backs that up. According to several sources, 93% of companies, no matter how big they are, are *out of business within one year* if they suffer a major data disaster without having first formulated a strategy for combating it. And since 68% of businesses don't have any sort of plan for that worst-case scenario, that means losing data would be a death knell for most of the businesses in the country.

Fortunately, your business does not have to be one of them. By taking the following steps, you can ensure that you have a rock-solid disaster recovery plan in place.

Step 1: Know How A Disaster Recovery Plan Is Different From A Business Continuity Plan

The main difference between these two types of plans is that while business continuity plans are proactive, disaster recovery plans are reactive.

More specifically, a business continuity plan is a strategy by which a business ensures that, no matter what disaster befalls it, it can continue to operate and provide products and services to its customers. A disaster recovery plan, on the flip side, is a strategy by which businesses can back up and recover critical data should it get lost or held for ransom.

So, now that we have a clear, concise understanding of what constitutes a disaster recovery plan, we can dive into the steps necessary to create one.

Step 2: Gather Information And Support

In order to get the ball rolling on your disaster recovery plan, start with

continued on page 2

executive buy-in. This means that everyone, from the CEO to the entry-level employees, needs to be brought in on executing the plan in case your company suffers a data disaster. When everyone is aware of the possibility of a data disaster, it allows for cross-functional collaboration in the creation process – a necessary step if you want to prevent breaches in all parts of your systems.

You need to account for all elements in your tech systems when you're putting together your disaster recovery plan, including your systems, applications and data. Be sure to account for any issues involving the physical security of your servers as well as physical access to your systems. You'll need a plan in case those are compromised.

In the end, you'll need to figure out which processes are absolutely necessary to keep up and running during a worst-case scenario when your capability is limited.

Step 3: Actually Create Your Strategy

When everyone is on board with the disaster recovery plan and they understand their systems' vulnerabilities, as well as which systems need to stay up and running even in a worst-case scenario, it's time to actually put together the game plan. In order to do that, you'll need to have a good grip on your budget, resources, tools and partners.

> **"93% of companies, no matter how big they are, are out of business within one year if they suffer a major data disaster without having first formulated a strategy for combating it."**

If you're a small business, you might want to consider your budget and the timeline for the recovery process. These are good starting points for putting together your plan, and doing so will also give you an idea of what you can tell your customers to expect while you get your business back up to full operating capacity.

Step 4: Test The Plan

Even if you complete the first two steps, you'll never know that you're prepared until you actually test out your disaster recovery plan. Running through all the steps with your employees helps them familiarize themselves with the steps they'll need to take in the event of a real emergency, and it will help you detect any areas of your plan that need improvement. By the time an actual data disaster befalls your business, your systems and employees will easily know how to spring into action.

So, to review, these are the quick actions that you and your employees will need to take in order to make a successful, robust disaster recovery plan:

- Get executive buy-in for the plan.
- Research and analyze the different systems in your business to understand how they could be impacted.
- Prioritize systems that are absolutely necessary to the functioning of your business.
- Test your disaster recovery plan to evaluate its effectiveness.

For assistance with your strategy, contact us at 561-969-1616. If you'd like information on our Disaster Recovery Assessment which will reveal how quickly your business could be back up and running after a disaster, server crash, etc., visit: www.palmtech.net/data-tragedy/.

Are Your Employees' Credentials For Sale On The Dark Web?

Visit www.palmtech.net/darkweb/ For A Free Scan!

If You Think Your Password Is Secure, You Should Think Again!

The National Institute of Standards and Technology (NIST) created many of the password best practices you probably loathe, including using a combination of letters, numbers, and special characters. The NIST now says those guidelines were ill-advised and has changed its stance. Find out why and what this means for you.

The problem

The issue isn't that the NIST advised people to create easy-to-crack passwords, but their previous advice inadvertently made people generate weak passwords using predictable capitalization, special characters, and numbers, like "P@ssW0rd1."

Such a password may seem secure, but the string of characters it's made up of could easily be compromised by hackers using common algorithms.

Furthermore, while the NIST also recommended that people change their passwords regularly, they did not specify how and when to change them. Without proper guidance, many people assumed that this meant adding or changing one or two characters every year or so.

The NIST essentially forced everyone to use passwords that are hard for humans to remember but easy for a hacker's algorithm to crack.

Eventually, the institution admitted that their recommendation creates more problems than it solves. The NIST has then reversed its stance on organizational password management requirements, and is recommending banishing forced periodic password changes and getting rid of complexity requirements.

The solution

Security consultant Frank Abagnale and Chief Hacking Officer for KnowBe4 Kevin Mitnick both see a future without passwords. Both security experts advise enterprises to implement multifactor authentication (MFA) in login policies.

MFA requires a user to enter one or more valid credentials aside from a password to gain access to an account. This could be a physical security key, a login prompt on a mobile device, or a facial or a fingerprint scan. Without the additional security requirements, hackers' attempts to crack passwords would be futile.

Moreover, Mitnick recommended implementing long passphrases of 25 characters or more, such as "recedemarmaladecrockplacate" or "cavalryfigurineunderdoneexalted." These are much more difficult to guess and less prone to hacking. Simply put, passwords should be longer and include nonsensical phrases and words that make them almost impossible for an automated system to crack.

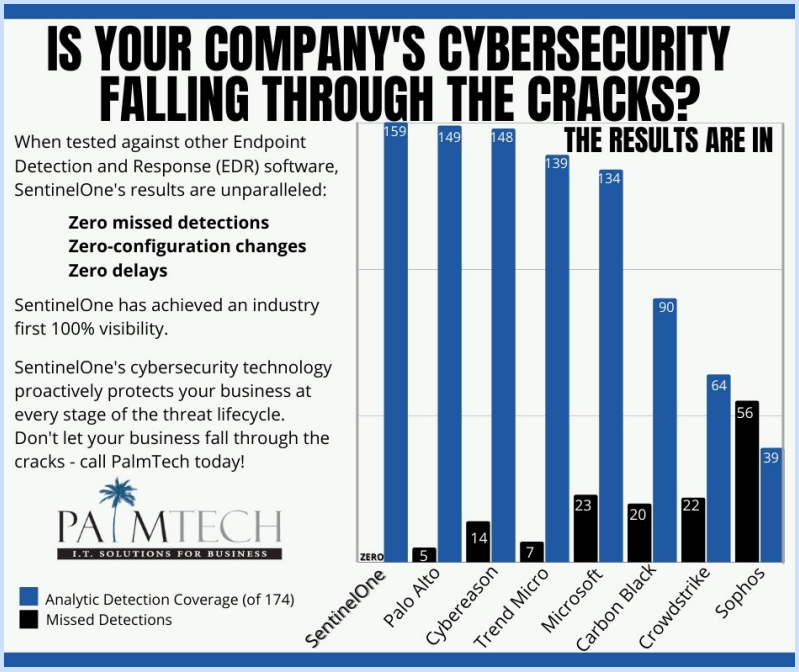
What's more, the NIST recommends making screening of new passwords against lists of common or compromised passwords mandatory. This is because a complex, 25-character password is already considered weak the moment it has been compromised.

Finally, you should also enforce the following security solutions within your company:

Single sign-on – allows users to securely access multiple accounts with one set of credentials

Account monitoring tools – recognizes suspicious activity and locks out hackers from the network OR keeps hackers from accessing the network.

When it comes to security, ignorance is your business's kryptonite. If you'd like to learn about what else you can do to remain secure, call us at 561-969-1616.



Why Is Having A Business Continuity Plan Important?

Many small- to medium-sized business (SMB) owners fail to prepare for major crises like flood and ransomware attacks. Disaster events can cause downtime, which can result in lost revenue and lower profits. In addition, SMBs that fail to recover quickly from disruption face the risk of losing their customers to their competitors. To prevent this from happening to you, it's important to have a business continuity plan (BCP) in place.

What Is a BCP?

A BCP is a predefined set of protocols on how your business should respond in case of an emergency or natural disaster. It contains contingency plans for every aspect of your organization, including human resources, assets, and business processes.

Key Threats To Business Continuity

Various types of threats can affect SMBs such as:

Natural disasters: These are natural phenomena such as floods, storms, earthquakes, and wildfires.Man-made disasters: These include cyberattacks, intentional sabotage, and human negligence.Equipment and utility failures: These include unexpected power failures, internet downtime, and disruption of communication services.

How To Build an Effective BCP

If your company does not have a BCP in place, now is a good time to create one. These steps will help you formulate an effective BCP that will ensure your company keeps running even during a major crisis.

Perform a Risk Assessment

To create an effective BCP, it's important to identify the risks to prioritize. Start by identifying potential threats that may impact your daily operations. List down as well industry risks, geographical area, rising trends, and issues that your stakeholders may encounter. Next, categorize the risks based on the level of impact, likelihood of occurrence, or other criteria.

Once risks have been identified and a plan has been developed, carefully identify any possible gaps.

Collaborate with your team to identify any weak points in the plan, and make changes as necessary.

Perform a Business Impact Analysis (BIA)

A BIA will help you determine how a disruption can affect your company's current functions, processes, personnel, equipment, technology, and physical infrastructure. IT will also help you calculate the potential financial and operational loss from each function and process affected.

Identify Your Recovery Options

Identify key resources for restoring your business to minimum operational levels. Some recovery options you can take include using data backups, allowing employees to work from home or operating from a secondary location.

Document The Plan

Make a record of the BCP and store the document in a secure location, preferably an off-site one to reduce the risks of loss or damage in case of a disaster.

Test and Train

Once your BCP is in place, your continuity team needs to perform tests regularly to identify gaps and make necessary changes to ensure the plan's effectiveness. They also need to conduct regular employee training so that everyone knows their respective roles should a disaster strike.

Having an effective BCP is a great way to ensure your business can quickly recover after a major disaster. **If you're thinking about creating a BCP for your company but don't know where to start, give us a call today at (561)969-1616.**