Here's A Service We Offer: IT Security Services

Cyber security threats pose a serious risk to businesses of all sizes. With new sophisticated hacks emerging every day, you can no longer take a "set it and forget it" approach to IT security.

Unfortunately, the owners of many small and medium sized businesses take the perspective that they won't be breached because they are small. Their logic is that hackers and cybercriminals are only focused on stealing from the biggest and most successful companies. Unfortunately, that's far from the reality.

Unless your business is secured by 24/7 network monitoring, intrusion detection and advanced threat management (at a minimum), you are leaving yourself vulnerable.

Protecting your digital assets — from servers, applications, all the way down to individual files — is multi-layered and complex. Your IT security needs will look completely different from another company's. That's why we audit your IT infrastructure and current security protections before devising and implementing your unique IT security plan. With custom IT security services from Connectability, you get the attention and level of protection your business needs at an affordable monthly cost.

Give us a call at (647) 492-4406, if your are interested in IT Security Services for your business.

October 2021

This monthly publication provided courtesy of Ted Shafran, President of Connectability

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 businesses.

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 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

Continued from pg.1

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.

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

"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."

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.

Complete these steps, and you can ensure that your business will survive any data disaster that comes your way.

Shiny New Gadget Of The Month:

The LINK AKC Smart Collar

The world can be a dangerous place for a pooch who doesn't know any better; so, it's best to know how to keep tabs on your canine companion in case they bolt. That's where the LINK AKC smart collar comes in.

This smart collar is a comfortable and safe tracking alternative for your pooch. The LINK AKC smart collar comes equipped with several other useful features, including but not limited to:

- Activity monitoring and sound training specific to your dog's breed
- Temperature alerts if your dog is too hot or cold
- A place to digitally store vet records
- Waterproof features for up to 30 minutes in water

If you want your dog to be the best, highest-tech boy or girl out there, this collar is for you!

Top tips when selecting an MSP for your business

Technology underpins nearly every aspect of modern business processes. Managing it, however, can be complex and tedious. This is where managed IT services providers (MSPs) can help. Whether your company needs software solutions, network infrastructure management services, or cloud technology, MSPs can provide all this and more.

Selecting the best MSP

While there are numerous MSPs out there, not all of them are equipped to meet your company's unique needs. You can only achieve optimum IT results by selecting the right MSP.

Here are some criteria to keep in mind:

Depth of skills and experience – An MSP should have the skills and experience that go beyond basic software installation, maintenance, and upgrades. They should also have strong expertise in advanced IT functions, such as database management, cloud technology, security, and cross-platform integration, so they can keep pace with your company's growing IT requirements.

Financial stability – With IT being the backbone of your business operations, you need an IT partner who will be there for the long haul. Assess their stability by checking how many clients they have and their customer retention numbers. Also, read customer reviews and testimonials.

Competitive service level agreement (SLA) – An SLA is a contract that dictates the standards that your MSP must meet. It should be able to answer these questions: Do they offer 24/7 support? Can they conduct remote and on-site support? What are their guaranteed response and resolution times? If they fail to meet their committed service levels, do they offer rebates or money-back guarantees?

Third-party vendor partnerships – Pick an MSP with an ongoing relationship with the technology vendors (e.g., Microsoft, Oracle, Salesforce) whose products you already use in your IT environment. Verify the partnership the MSP has with those vendors. The higher the partnership level, the more vendor certifications the provider has, which means they can provide plenty of expertise to your business.

Choosing the right provider is a crucial decision that will impact your business's performance and success. If you want to learn more about how MSPs can support your business, contact us today at (647) 492-4406.

Tech Connect Video Series:
Beware Of Phishing Attacks!

You probably spend a lot of time emailing clients, vendors, partners and colleagues. It's your main tool to communicate. Unfortunately it's also a hacker's prime target. Hackers use a method called "phishing" to convince their victims to open malicious links or attachment, send funds to random bank accounts, or provide confidential information about themselves or their companies. Cybercriminals can then get your passwords, install programs on your computer and network, and steal your confidential data.

Cybercriminals are working diligently to get into your computer, infect your backups, and install Ransomware across your network. That's why your business needs to stay up to date on the latest solutions and training to help your team spot phishing attacks, and prevent them from arriving in your inbox to begin with.

If you would like to learn more about improving your security and preventing your business from becoming a victim of a phishing attack, watch this video NOW! You will learn 3 tips to improve your email security. To find out more, go to **YouTube**, look up **Connectability IT Support** and find the video "**Beware Of Phishing Attacks! 3 Tips To Improve Email Security**" OR go to our website at www.connectability.com, hover over "Resources & Videos" and select "Videos".

3 Digital Disruptions That Affect WFH Employees And How To Avoid Them

As more employees work from home, the risk of cyber-attacks grows. In 2020, between the months of March and July, nearly half of all businesses dealt with some sort of digital disruption. Some of the most common digital disruptions were:

Worker Productivity Losses

When hackers infiltrate company computers, they might steal employee identities. This won't hurt your business directly, but it will indirectly, as workers have less time for work while they grapple with their identity being stolen.

Internet Of Things Infiltrations

Now that so many "smart" devices can be hooked up to a central server, there are more avenues than ever for hackers to gain access to sensitive company data.

Ransomware Attacks

Businesses of all sizes are falling victim to ransomware attacks, but it's the small and mid-size ones on a tight budget that really suffer from the fallout.

To stop these kinds of attacks, educate your workforce on best practices for avoiding hackers and make sure their systems are up-to-date with good cyber security software. Nothing is bulletproof, but you can do a lot to protect your company.

5 Tips For Millennial Entrepreneurs From A Millennial Entrepreneur

Millennial entrepreneurs are more diverse than entrepreneurs of any other generation, with a greater portion of them being women and people of colour than ever before. But what does it take for a millennial to succeed in this brave new world of business?

1. Remember that although older business owners may have valuable insights, they might not understand how entrepreneurship works in the digital age.
2. Know how to do every job in your business; after all, you'll have to do them all when you start out!
3. Find a mentor, someone who is where you want to be one day, and learn from their successes and failures.
4. Don't take advice from people who haven't been where you are – even if the advice is well intentioned and from people you care about.
5. Do not let people judge you for your age. Being in the know about the latest tech – because of your age – is a tremendous advantage in today's marketplace.

Who Else Wants To Win A $25 Gift Card?

You can be the Grand Prize Winner of this month's Trivia Challenge Quiz! Just be the first person to correctly answer this month's trivia question and receive a $25 gift card to Starbucks. Ready? Call us right now with your answer!

Where did Google founders go immediately after getting their first investment check?

a) Burger King
b) Wells Fargo
c) BMW Dealership
d) Disneyland

Call us right now with your answer!
(647) 492-4406

This month we will be donating to **The Salvation Army**.

Founded in 1882 in Canada, The Salvation Army is one of the largest non-governmental direct providers of social services. They are committed to giving hope and support to vulnerable people in 400 communities across Canada, and more than 130 countries across the globe.

The Salvation Army's focus is to provide aid for children and families, by offering necessities of life. The organization is dedicated to fighting homelessness and providing rehabilitations to those with addictions. The organization goes above and beyond to not only meet the needs of the individuals they serve, but to offer additional social and community service programs that focus on nurturing capacities, skills and strengths of the individuals.

If you want to contribute to The Salvation Army, we would love your help! Email: info@connectability.com or call (647) 492-4406.