Untech the Tech Talk: Empowering Small Businesses to Succeed

GEEK ~~not~~ GEEK

Building Resilient IT Systems:

A Guide for Small Business Owners

Introduction

Have you ever given real thought on the criticality of your technical systems and the role they play in the success of your businesses? It is probably not something that most business owners concern themselves about, because let's be honest, you have more important things to worry about, right? My goal is not to be condescending, but rather to emphasise that your technology systems are the foundations of your business and core to driving your success. Hence the importance of ensuring resilience throughout your critical systems. This article's intent is to help you understand some key aspects of making your IT systems more resilient.

Understanding IT Resilience

> IT resilience refers to the ability for your companies IT systems to withstand and recover from disruptions, through technical or human fault, or through cyber-criminal activity. Simply put, are you doing the right daily activities to ensure your systems are ready for an IT outage, and do you have systems and plans in place for WHEN an outage or interruption happens to ensure continuous operation? Note that I mentioned WHEN and not IF. This is because the assumption should always be that an outage will occur. IT Resilience encompasses both preventive measures to try and avoid outages and strategies for rapid recovery when outages do occur. The steps in this article will give you some high-level insight into the actions you need to take to improve your resilience.

Some Statistics

IT outages pose a significant and tangible risk to businesses, with 31% experiencing a major outage in the past year alone. These disruptions, often caused by hardware failures (45%), software failures (22%), human error (22%), and cyber-attacks (11%), lead to substantial financial losses.

From this Only 52% of organizations were able to restore their critical systems following a severe data loss event in 12 hours or less, and 29% needed a day or longer to get their systems up and running . Moreover, the complexity of hybrid and multi-cloud environments is escalating these risks, as 74% of IT leaders report. As cyber threats grow, proactive investments in IT resilience and advanced technologies like AI are essential to mitigate the frequency and severity of outages. The real and pressing nature of IT outages underscores the need for robust strategies to ensure operational continuity and security.

Asking the Right Questions

With that in mind, let’s talk about your systems and how you can make them more resilient to outages. Like insurance, IT systems and the support of those systems are really a grudge purchase for most, and just like insurance, no one thinks that this is money well spent until the day it is needed. And you would be right feeling that way as managing your IT systems and putting in plans are in fact an insurance policy. The same way you think of life insurance (What would happen if something happened to me?) is the same way you would think of the support of your IT ecosystem. The real consequences of an IT outage will only be felt when it occurs, but we can mitigate our risks by asking the below questions to assess the potential impact.

- How important is my technology systems to my business? Are we highly dependant on IT systems or can we run offline for a few days?
- What would happen if I had an outage, and can I afford it? Outages are multi-faceted and have a ripple effect on cost. Give some real though on the cause and affect of an outage.
- If an outage occurs due to a cyber-attack, what other damages can I expect? Outages are not only caused by system failures, but they are more likely to happen due to cyber-criminal activities which puts you and your business at even higher risk than just a standard outage.
- If I have a technology failure, how long would it take to get back up and running again?
- Lastly, are my systems currently efficiently managed to reduce the risk of outages?

Lee Child said, “Hope for the best, plan for the worst”

Planning for the worst by implementing strategies and pro-active daily operational activities, will reduce the risks your business may face.

Steps to Enhance Your IT Resilience

> There is so much to consider when looking at your critical and even non-critical systems that support your business. It is hard to find and focus on what is really going to make the difference, so we will be focusing on the three major steps you can follow to help you identify and assign risk, and then some steps on how to implement some mitigation strategies going forward. At a minimum, this would help you ask the right questions. If you have an IT team or a service provider, you should be empowered enough to make sure they are prepared for the worst.

Step 1: Conduct a Risk Assessment

We can not know what we dont know, so it is vital that we investigate our entire technology stack, from the critical to the less significant. To start, lets make a detaild list of all your IT assets. Once you have your list of assets at the ready, it is time to formulise the potential risks for each and assess the potential impact it could have on your business.

***Pro tip,** having a list of all your IT assets will not only help with risk but is also a very effective way to control and save costs on your IT.

Asset Identification and Classification

- Create a comprehensive inventory of all valuable IT assets.
- Rate each asset based on its sensitivity and importance.

Threat Identification

- Identify potential threats to your assets. List common threats such as system failures, natural disasters, human errors, and malicious attacks. Try and be as detailed as possible. It's vital that you try and accommodate for any eventuality, even things that are very unlikely.
- Rate the likelihood and potential impact of each threat.

Vulnerability Assessment

- Determine weaknesses that could be exploited by threats. Assess vulnerabilities in hardware, software, network configurations, and user practices. This is easy enough if you run an automated vulnerability scanning tool.
- Evaluate current security measures and identify gaps. This will probably already give you quite some action items to look at and I cannot stress this enough. DO THIS ASAP. Cyber Criminals are increasingly targeting small businesses, so you are a target.

Impact Analysis

- Understand the potential consequences of system outages and security breaches. The questions posed earlier in this document is a good starting point.
- Analyse the impact of possible incidents on business operations, including financial losses, downtime, legal consequences, and reputational damage.

Risk Scoring

By now, I am sure your list is as long as your arm and quite overwhelming so let's prioritise what can be done easily, fast and within your budget.

- Calculate risk levels using the formula: Risk = Asset Value (Value to the Business) x Threat Likelihood x Vulnerability.
- Prioritize risks based on their potential impact by assigning risk scores (high, moderate, low) and identify critical areas that require immediate attention.

And there you have it; a risk register you can work with. And now you can work on how you can fill those gaps and reduce your risk. However, getting yourself into a reduced risk state is only one part of the equation. You must also be implementing pro-active controls to ensure you stay on top of your newly improved resilient state.

Step 2: Take a Pro-Active Approach

You probably have a car, and if you don't, just join me on this journey and imagine you do. If you have a nice fancy car, you probably have a service plan, insurance, security systems and a MOT plan for it. You will take it in to be serviced regularly, make sure the MOT and insurance is up to date, wash it often and make sure you keep it clean on the inside. When you hear a funny sound, you will probably immediately take it to someone to look at and if a part breaks you will replace it very quickly. It must last you for years so you will look after it by being pro-active with its care and maintenance. I'm sure you get my point; Just like you fancy car, your IT systems can be an asset to you and your business if you choose the right technologies and pro-actively maintain them.

Adopt Cloud Solutions

> I am an advocate for using the right solution for you, so this is not me trying to sell more cloud to you. This is mainly looking at solutions that will improve your resilience and the truth is that most cloud providers have resiliency built into their platforms so that you don't have to worry about this. Now, if you cannot use the cloud for any reason, it doesn't mean that you are lost, it only means that the responsibility of building resiliency into your technology stack is on your shoulders and it will likely be a bit more expensive and complicated. Here are a few reasons why cloud is a viable option for resilient IT.

- **Geographic Redundancy**: Simply put, cloud providers have multiple failover locations making it easier to spin up a new service if something goes wrong. Be careful though. These are often not included and must be designed correctly, and they will often charge you for this service.
- **Redundant Systems**: Cloud infrastructures are designed with redundancy in mind, ensuring that multiple copies of data and resources are available to take over if one system fails.
- **24/7 Monitoring**: Cloud providers continuously monitor their own systems for issues, often detecting and addressing problems before they affect customers.
- **Pro-active Maintenance**: Regular maintenance and updates are performed by cloud providers, ensuring that systems remain secure and up to date without interrupting services.
- **Security and Compliance**: Cloud providers invest heavily in security, including physical security of data centres, encryption of data, and regular security audits.
- **Compliance with Standards**: Many cloud providers comply with industry standards and regulations (e.g., GDPR, HIPAA), ensuring that their infrastructure meets stringent security and data protection requirements.
- **Service Level Agreements (SLAs)**: Cloud providers typically offer SLAs that guarantee a certain level of uptime and availability. These SLAs provide businesses with assurances and potential compensation in case of service disruptions.

- **Rapid Deployment and Automation**: Cloud resources can be provisioned rapidly, allowing businesses to quickly recover and deploy new resources in response to outages.

*Please note that I am generalising on the above points. Not all clouds are the same, so make sure you investigate thoroughly.

Pro-Active Network and System Monitoring

> The goal is to catch things before they happen so that you can fix the problem before it starts, or atleast as soon as they happens, so that you can troubleshoot and get back online as fast a possible. Monitoring tools are very effective in identifying potential outages, especially ones who have AI capabilities, and well worth investing in. Having a watchdog looking at your network and systems pro-actively will reduce downtimes and prevent potential outages.

- **24x7 Monitoring**: Make sure that monitoring is coninuous. Issues happen while you are sleeping and the last thing you want is to come to work to a system outage or cyber-attack.
- **Alerts and Notifications**: Set up alerts to notify IT staff immediately when potential problems are detected. The alerts process should be defined in detail, including a well-defined change control process. This should map back to some of your risks to make sure you are continuously monitoring and managing those risks.

Daily Operational Excellence

> Pro-actively managing your systems on a daily basis is the same as taking that fancy car in for a service regularly, topping up the oil and just putting in petrol so it can run. Having good operational standards will help you ensure that you stay compliant and resilient to potential risks.

- **System Health Checks:** Monitor system and network performance. Review system logs for errors, warnings, and unusual activities and ensure that all critical services are running as expected. This will make sure you identify any potential issues before they happen.
- **Check Backup Status**: Verify that scheduled backups have completed successfully and periodically perform test restores to ensure data integrity.
- **Security**: Ensure that Anti-Virus scans are performed and up to date. Monitor and respond to security alerts from your security systems.
- **Patch Management**: Check for and apply critical security patches and updates.
- **User Accounts**: Ensure new accounts are created with appropriate permissions and regularly review and adjust user access levels. Also make sure to disable accounts for departed employees as soon as possible.
- **Networks**: Monitor network bandwidth and identify any unusual spikes. Check the status of routers, switches, firewalls, and other network devices and ensure network connectivity is in a good state.
- **Compliance and Policy Checks:** Ensure that daily operations adhere to company policies and compliance requirements.

- **Asset Management:** Monitor the status and health of hardware assets. Check software licenses for compliance and renewal status. Monitor resource usage and plan for future capacity needs.

Enhance Cybersecurity Measures

> We live in a world where criminal activity has reached pandemic proportions, and the internet has given criminals global reach at their fingertips and anonymity as their superpower. If you think you are not on their radar, you are wrong. Smaller businesses are now being targeted more than ever.

- **Firewalls and Anti-Malware**: Install and maintain robust firewalls and anti-malware software.
- **Regular Updates**: Keep all systems and software up to date with the latest security patches.
- **Employee Training**: Train employees on cybersecurity best practices and how to recognize potential threats.
- **Active Directory**: Implement a global user management system like Active Directory to manage user access.

*Very important note: this is oversimplification of what security measures are needed. I would highly recommend a professional engagement with a subject matter expert as Cyber Security is a vast and complex world.

Invest in Uninterruptible Power Supplies (UPS)

In a country where there is always power, this seems to be a mute subject, but power is a fickle beast. We don’t appreciate it because it’s always there, but something can go wrong and, in those cases, you would want a backup. Most laptops have at least two-hour battery life, but servers and networking equipment almost never have batteries included. For this reason, a UPS is good practice and would potentially save you an embarrassing conversation with your customers when they are still online, but you are not.

Leverage IT Support Services

> Leveraging professional nerds to help you with all of this is just good sense. As your business grows, so will the importance of your technology to your business and the complexity of your systems. This is why making a good choice on who will be looking after your IT will be a vital decision you will have to make. You have two options. One, hire your own internal team and two, outsources to a service provider. Each choice comes with its own pros and cons. Here are a few differentiators between the two.

In-House IT Team

If you already have a team, you will understand that they are on-hand and know your business intimately, but your cost commitment is high. Having our own IT team will be most beneficial if you need full control of your IT systems and you would probably be looking at implementing this when you grow into a corporate, as the governance and compliance requirements will become more specific to your business, and you would need to have that control in place. Here are a few pros and cons if you are thinking about hiring internally.

- **Pros:**
  - **Full Control**: Direct oversight of IT operations allows for customized solutions tailored to specific business needs.
  - **Immediate Response**: Faster response times to issues as the team is on-site.
  - **Deep Understanding of Business:** In-house teams are more familiar with the company's culture, processes, and goals.
- **Cons:**
  - **Higher Costs:** Not only are skills scarce, but they are also expensive and when you are hiring, you are committing to the annual salary for one person, including training and other activities that it costs you to onboard a new employee.
  - **Resource Limitations:** As with your technologies, you will need resilience in your people. For IT to be effective, someone always needs to be available.
  - **Limited Expertise**: One mind will never have the knowledge of that of a team. With so many technologies and solutions out there, one person will have potential gaps in specialized skills and expertise.
  - **Scalability Issues**: Difficulty scaling up quickly in response to sudden business growth or IT demands.
  - **Risks:** Risk of losing key IT staff, leading to disruptions and knowledge gaps.

Outsourcing IT Management

In a sea of IT service providers, you have many choices. I would say that you would need to be careful of jumping into bed with just any provider and you would need to make sure that you have asked all the right questions so you can feel confident that you have made the right choice. M Let's have a look at the pros and cons for outsourcing.

- **Cons:**
  - **Less Control:** Reduced control over IT operations and decision-making with dependence on the service provider for critical IT functions.
  - **Communication and Coordination:** With the wrong partner there are possible communication barriers and delays with challenges in ensuring the outsourcing partner fully understands and aligns with your business goals and culture.
  - **Service Quality:** Service quality may vary, and there may be issues with responsiveness and prioritisation. This is why it is vital that you ensure your provider has their own SLA's and not only back-to-back platform SLA's. They must hold themselves accountable.
- **Pros:**
  - **Cost Efficiency:** Reduced costs compared to maintaining an in-house team, including savings on salaries, benefits, and infrastructure with predictable expenses like fixed pricing models can make budgeting more predictable.
  - **Access to Expertise:** You will get access to a broad range of specialised skills and expertise.
  - **Wide Range of Technologies**: Providers often have access and knowledge to a wide range of technologies and best practices. Its their primary job after all.
  - **Scalability and Flexibility**: Easy to scale services up or down based on business needs with the ability to quickly adapt to new projects or changes in business direction.
  - **Focus on Core Business**: Allows you to focus on core activities while the outsourcing partner handles IT functions as there is less internal management required for IT functions.

Step 3: Implement Redundancy and Failover Solutions

When an outage happens, and it will, you will be happy that you have planned for it. So, lets plan for the worst and hope that it never happens.

Before we start, backup and Disaster Recovery (DR) are two different things. DR looks at recovering a system failure that is critical to the business where you would need back online as fast as possible. Backup is where you data is backed up at a point in time. This is securely done but you do stand to potentially lose data if a system outage happans and your last baackup point was a long time ago. It is good practice to always have backups and consider a disaster recovery solution if your business can not afford long downtimes. You will have to consider the risk of both options as the cost of DR can be quite high.

Start with Baking Up

> Backups are the first step in you recovery plan and a good way to ensure that you always have relianble data to revert back to in a case of data loss.

- **Backup Everything:** Backups are generally not on the heavy side of the cost scale, so it is worth having everything backed up. There are ways to manage the cost of your backups for lesser critical data, like playing around with how long you want to keep the backups and how often you want to do backups, but as far as you can, try and include as much as possible into your backups.
- **Automate Backups**: Schedule automated backups to ensure data is regularly and consistently backed up. Doing a backup manually might be simple but you don't want to add this to your to-do list. Most backup tools will also automate redoing a backup in the case it fails the first few times giving you time back and peace of mind that it is done.
- **3-2-1 Rule**: The rule of thumb is 3 copies of your data in two different locations, and one must be off site. This gives you the highest level of redundancy for most eventualities.
- **Test Restorations**: Regularly test backup restorations to ensure data can be recovered when needed.

Disaster Recovery

> Start by chosing the correct target location of where your disaster recovery environment will live. You have several options available to you when choosing your target destinations. Just always ensure that these target locations are geographically apart, even if you are in the cloud.

- **Hosting On-Prem**: If you are hosting your servers on-prem or colocation datacentre, you can choose to duplicate your hardware and host them somewhere else. The second option is to replicate your environment into the cloud.
- **Hosting in the Cloud**: If you are hosting in the cloud, it should be a little simpler as most cloud providers offer geographic redundant datacentres. If you want to ensure you have vendor security, you can always choose to host your disaster site in a different cloud provider. This might be a little more complex but very doable.

Continuity solutions

> Now that you have chosen the right target for your disaster recovery solution, it is time to look at the solution options that you have. Your uptime will be the main factor in choosing your solution and must be considered very carefully. The cost of highly available DR solutions could be very high so don't be sold on the sales pitch, but rather calculate the rate of cost for the solution against the rate of loss in the case of a disaster. If the rate of loss is higher than the rate of cost, then a highly available (Most expensive) solution would be for you. Below is a comparison of different DR options starting at the lowest for with the longest recovery times to the highest cost but likely to give you almost 100% uptime guarantees.

- **Pilot Light:** A minimal version of the environment is always running in the cloud, ready to scale up in the event of a disaster.
  - **Use Case:** Suitable for systems that require faster recovery times but can tolerate some downtime**.**
  - **Pros:** Reduced cost compared to full-scale replication, faster recovery than basic backups.
  - **Cons:** More complex than simple backups, still involves some downtime.
- **Warm Standby:** A scaled-down version of the production environment runs in standby mode and can be quickly scaled up in a disaster.
  - **Use Case**: Suitable for applications that need to be up and running quickly after a disaster but can tolerate brief downtime.
  - **Pros**: Faster recovery times, moderate cost.
  - **Cons**: Ongoing costs for running a partial environment, complexity in scaling up.
- **Hot Standby (Active-Passive):** A fully functional replica of the production environment is maintained and can take over in the event of a failure but not always kept online to lower cost.
  - **Use Case**: Suitable for mission-critical applications that require minimal downtime.
  - **Pros**: Very fast recovery times, minimal data loss.
  - **Cons**: High cost requires significant resources for maintenance.

- **Active-Active (Multi-Site):** Two or more fully operational environments run simultaneously, sharing the load and providing immediate failover capability.
  - **Use Case**: Suitable for applications where continuous availability is essential.
  - **Pros**: Continuous availability, immediate failover.
  - **Cons**: Very high cost, complex to implement and manage.

Develop a disaster Recovery Plan

> Once you understand the solution that you will require, it is time to plan for the eventuality of a disaster. Here are some high-level points that you must implement to manage you DR effectively.

- **Develop a Disaster Recovery Plan:** Create a detailed disaster recovery plan outlining the steps to take in the event of an outage.
- **Roles and Responsibilities:** Define clear roles and responsibilities for staff members during a recovery process.
- **Regular Drills:** Conduct regular drills to ensure everyone knows their role and the plan is effective.
- **Implement a Communication Plan**
  - **Internal Communication**: Develop a plan for communicating with employees during an outage to keep them informed and coordinated.
  - **External Communication**: Prepare templates and protocols for informing customers, partners, and stakeholders about the outage and expected recovery time.

Conclusion

Making IT systems resilient to outages and criminal attacks is crucial for small businesses to ensure continuity and maintain customer trust. By conducting thorough risk assessments, implementing redundancy, and developing comprehensive disaster recovery plans, you can significantly enhance your IT resilience. Regularly updating and testing these measures will help maintain their effectiveness, allowing your business to navigate any disruptions with minimal impact.

SME ONE

CONNECT WITH US

BUZZBOX@SMEONE.CO.UK
+44(0) 33 335 5676
WWW.SMEONE.CO.UK