Business System Solutions

THE BSS ADVISOR

Monthly Newsletter May 2025

Batten Down Your Security

Cybercrime historically increases by 40% during times of market instability or global disruption.

Illustration by Pixabay/Joe jplenio

by Anisa Williams, BSS Staff

In times of major disruptive events, most small business owners will slash spending and move into a holding pattern, hoping to ride out the swells of uncertainty. However, the last few downturns (both domestically and globally) have shown that cyber criminals ramp up their attacks, leading to a shocking three-fold increase in exploits and cyberattacks. This activity can last for weeks or months, depending on the nature of the world-altering event. The most common types of exploits include fraudulently impersonating legitimate websites, social engineering, phishing, and ransomware attacks.

While it may seem counterintuitive to fund increases in your IT security during a downturn, having a robust, secured, and solid infrastructure actually helps businesses survive. The best security takes a multifaceted approach, prioritizing cybersecurity and disaster recovery/backups while also focusing on employee education.

Invest extra when cutting budgets

Computers, networks, and internet connectivity are the backbone of doing business, regardless of your size and industry. We can't live without IT, but if your IT network is not secured from threats, you won't have a business to do.

(Continued on Next Page)

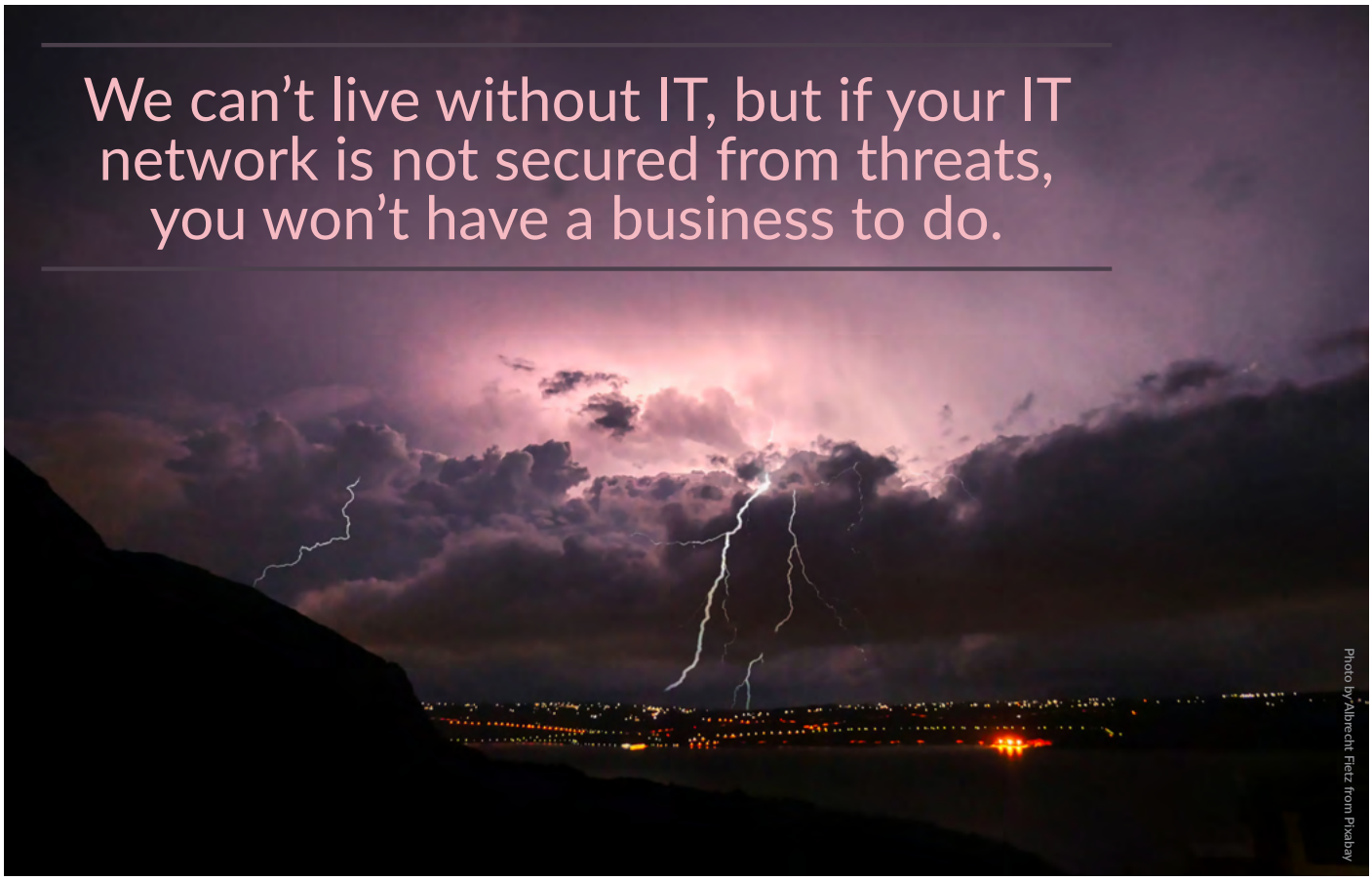
Business System Solutions is your IT Service Partner who provides peace of mind through guidance, education, and responsive support. Serving communities in Indiana, Tennessee, and Michigan.

Caretakers of Your Productivity.

"And God is able to bless you abundantly, so that in all things at all times, having all that you need, you will abound in every good work."

2 Corinthians 9:8

(Continued from page 1)



Cutting cybersecurity initiatives shouldn't be done lightly. Attackers expect businesses to cut IT needs and actively target Small and Medium sized Businesses (SMBs) because of that. Over 61% of SMBs are the target of cyberattacks, with 82% of ransomware attacks against companies with fewer than 1,000 employees and 37% with fewer than 100 employees.

Considering the cost of recovery from a ransomware or data breach averages $2.73 Million (excluding tha ransoms), many SMBs are irreversibly damaged and 60% close their doors within six months of an attack. Those that stay open have an uphill climb to regain reputation and deal with long-term recovery struggles.

Insider risks grow during layoffs

Employees stealing data or caring less about following security procedures are a bigger threat during times of economic instability and layoffs. When employees feel insecure or betrayed, DTEX Systems' Insider Risk Report noted that 56% of companies were subject to data theft when employees resigned or were laid off.

Most businesses who were able to effectively stop insider threats are because they have invested in security measures in advance to notify and interrupt exfiltration of company data.

Identify risks to show ROI

Simply, organizations that slash IT resources will be less protected. Identifying gaps in your security, tools, processes, and backups will ensure you are able to fight off and recover more quickly from a cyber-attack.

Even if your company is not subject to compliance regulations, performing an IT Security Audit* will help you identify the easy and quick things you can do to shore up your infrastructure. This will also help to demonstrate the value of your cybersecurity and disaster recovery programs to prevent budget cuts in IT.

(Continued from page 2)

New technologies in both hardware and software can help companies be more secure when business needs are getting leaner, allowing smaller staff to do more with less. Additionally, adding a cyber insurance policy can help SMBs recover more quickly without fear of financial ruin.

Outsource to stay focused on your business

Outsourcing your IT to a Managed Service Provider (MSP) is a cost-effective way to dramatically increase your cybersecurity and get leading edge tools, often for less per month than it costs to keep an internal IT person.

Many MSPs, like BSS, offer flat rate monthly fees with no surprise invoices, that help you navigate market fluctuations with stability and scalability. Trusting a team of IT experts allows you to stay focused on your business while they do what they do best: keep you safe and educate your employees on security best practices.

BSS clients get leading edge Managed Detection and Response, a cybersecurity software designed to detect intrusions and unusual behaviors before it escalates into a breach. Additionally, we insist on hourly and daily secure backups that can get you back up and running in hours or a few days, versus the average downtime of 21 days from cyberattack.

Companies that don't have robust policies and tech in place to protect themselves are under the greatest risks for closures. Awareness is the first step: knowing that cybercrime increases greatly during instability means that you can put measures in place today. Investing in prevention now means the less expensive it will be in the long run. From that place of strength, you'll be able to wait out the storm, regardless of what the cybercrime world throws at you. □

Sources

https://solcyber.com/securing-your-business-during-economic-uncertainty/
https://www.darkreading.com/cybersecurity-operations/the-importance-of-recession-proofing-security-operations
https://www.strongdm.com/blog/small-business-cyber-security-statistics
https://www.weforum.org/stories/2024/02/why-cybercrime-spikes-in-times-of-global-crisis/
https://ponemon.dtexsystems.com/
https://www.perforce.com/blog/pdx/ransomware-costs-downtime
https://go.crowdstrike.com/2025-global-threat-report
https://www.sophos.com/en-us/press/press-releases/2024/04/ransomware-payments-increase-500-last-year-finds-sophos-state

Phishing Forms

Phishing, or impersonation of a company or person to gain personal information or access to accounts or resources, can come in many different formats.
Be Suspicious! If the message has a sense of urgency or seems strange, it's probably a Phish.


WEBSITES


LINKS


VIDEO


EMAIL ATTACHMENTS


TEXTS


PHONE CALL


POP UP ADS


SOCIAL MEDIA

Threat actors are using AI filters and voice imitation to impersonate others in phone and video calls. Be more cyber-savvy than them: STOP and THINK before sharing your precious information.

Business System Solutions

Return Address:
601 3-Mile Road NW, Suite C
Grand Rapids, MI 49544

The BSS ADVISOR

info@bssconsulting.com

North-Central Indiana Office
1211 Cumberland Avenue
West Lafayette, IN 47906
(765) 742-3440

Middle Tennessee Office
1026 West College Street
Murfreesboro, TN 37129
(615) 819-0600

West Michigan Office
601 3-Mile Road NW, Suite C
Grand Rapids, MI 49544
(616) 776-0400

6 Years in a Row!
2019-2024 Winner
Channel Futures.
Leading Channel Partners Forward
MSP 501

HELP THE OWNER GET TO CYBER-SAFETY!

Avoid Viruses and Hackers to find the path to the BSS Cybersecurity Fortress