CompuCom® | MANAGED IT as a SERVICE

7 Big IT Risks **You Can't Afford to Ignore**

Problems with your company's IT – and how it's managed – may be costing you more than you think. Here are 7 IT concerns you should consider addressing.

Many business owners are focused on growing their operation, but growth is a double-edged sword. As you expand, your organization becomes more complex, as do your technology and IT management needs.

You may hire additional employees who need onboarding onto your network and various systems, add new locations that need IT oversight and management, and adopt new technologies and solutions to run your business more strategically and productively. Managing that growth and technical complexity can be an uphill battle – and it comes with numerous risks.

But how do you know which ones are worth addressing? When looking for possible vulnerabilities, be aware of these seven IT risks that are most likely to cost your company significant time and money:

Sometimes an employee just needs to visit the wrong website or click on the wrong pop-up box, and ***malware is automatically downloaded on their device.***

Risk #1: Your network security coverage has cracks.

Beyond having a firewall and antivirus software, many companies lack the protective tools and protocols that can prevent significant damage from a cyberattack. For example, modern cybercriminals increasingly use social engineering and "**phishing**" email or text-messaging scams that con unsuspecting employees into handing over payment card information, account numbers, passwords, and other personal or business information. They send malicious attachments through email, tricking employees into opening them and then locking down business systems using ransomware. Sometimes an employee just needs to visit the wrong website or click on the wrong pop-up box, and malware is automatically downloaded on their device.

Companies can reduce the risk of a cyberattack through ongoing network and device monitoring services, including those that proactively scan all emails for malicious attachments before employees even open them, says John Knox, Director of Engineering and Project Management for CompuCom. But businesses should also incorporate other strong practices for avoiding and mitigating attacks, such as making sure all software upgrades are made promptly across all employee devices in the organization, and that a routine data backup process is in place to ensure valuable assets and data can still be accessed if a cyberattack does take place.

Knox recalls one company that prided itself on its cybersecurity measures, including enacting a strong employee password policy. However, the company suffered a data breach due to a virus that infected them through a commonly used – and seemingly harmless – business software program that hadn't been updated for over a decade. "The attackers took advantage of a security vulnerability in the free app," Knox says. "It's incredibly important to make sure your software stays up-to-date."

Certain remote cybersecurity monitoring solutions offered by a full-service **managed IT services provider (MSP)** can continually check for software updates and security patches across an organization's devices to ensure all programs are current and secure.

Risk #2: Ex-employees still have access to your data.

When an employee leaves – whether voluntarily or not – many employers forget to cut off access to all of the internal databases and key business solutions that person may have been connected to, such as software programs, customer databases, and social media accounts. This means the former employee could still be logging into those programs and spying on or stealing data.

Knox recalls one California doctor who left a large practice to start his own. He was able to access his former employer's patient contact information and use it to solicit business for his new practice. "He simply made a copy of all the data, and started emailing everyone," Knox says.

Given the real risk of ex-employee espionage, create and adhere to strict protocols for promptly disabling access to the company's network and all software, tools and solutions once an employee no longer works for you.

Risk #3: Hardware and software malfunctions are causing significant disruption and low productivity.

Technology is supposed to make your operation more efficient and your employees more productive, but it does the opposite if there are system delays or frequent downtime.

Your first goal should be to choose technology with a good reputation that is intuitive to use, reducing the time spent training employees on how to use it. Beyond that, though, you need to make sure you have round-the-clock IT support that is readily available to help you and your employees handle technology slowdowns and disruptions before they affect your business.

You can reduce the productivity drain of hardware and software disruptions by working with an MSP that offers vendor management services that include contacting vendors when a problem arises with their products or services, says Ken Jackowitz, CompuCom's Senior Vice President, Product, Marketing, and Digital Services. The MSP should have experienced technicians that know who to reach out to and can more quickly resolve technical frustrations.

"Contacting vendors when a problem arises with their products or services is a real time killer for businesses," Jackowitz adds. "Experienced IT technicians can save them time by knowing who to talk to when issues come up, and getting an answer quicker."

Risk #4: "Guests" are using your Wi-Fi to snoop on your data.

Many businesses have Wi-Fi networks that aren't properly segmented to protect their sensitive information and data. You don't want people visiting your facilities to be able to break into your internal network through your guest Wi-Fi access.

Knox recommends organizations have at least one separate guest Wi-Fi network exclusive to any non-employees who visit the business. This shields the internal network from the risk that a visitor could snoop on your internal network activity. But many companies should also consider segmenting their Wi-Fi even further if they have additional cybersecurity concerns, such as protecting certain hardware or business information, he adds.

Businesses should also consider having all of their guests sign into their Wi-Fi network using a registration or "splash" page, Knox adds. Not only does this provide an additional layer of security, but the right sign-in tool can also provide businesses with data about who is visiting their facilities. "The customer analytics one can glean from guest Wi-Fi usage may be valuable to certain businesses," he says.

> *"... many companies should also consider segmenting their Wi-Fi even further if they have additional* ***cybersecurity concerns****, such as protecting certain hardware or business information."*
>
> — **JOHN KNOX**
> Director of Engineering and Project Management for CompuCom

Risk #5: Outdated software kills employee productivity.

Beyond the security risks, outdated software can also greatly hurt employee productivity. Many software makers add new features and capabilities when they upgrade programs that make them easier to use and more useful to the end user. Outdated software is more prone to stalling and causing hardware slowdowns, which only wastes valuable time – and money – needed to keep your business running, Knox cautions.

"Every time they're sitting there looking at an hourglass spinning, you're paying them for that," he points out.

Risk #6: Not maximizing your technology – and missing out on its full potential.

You may be spending money on comprehensive or high-end solutions and hardware, but getting only a fraction of their total value. It's a common problem. Many companies acquire solutions for specific purposes, but then don't realize the full potential of those solutions within their organization.

A common example: A business may buy customer relationship management (CRM) software to keep better track of customer data. That software, however, may offer a wide range of additional features that could make the business smarter and more efficient about how it tracks and uses data – but the business doesn't use those features.

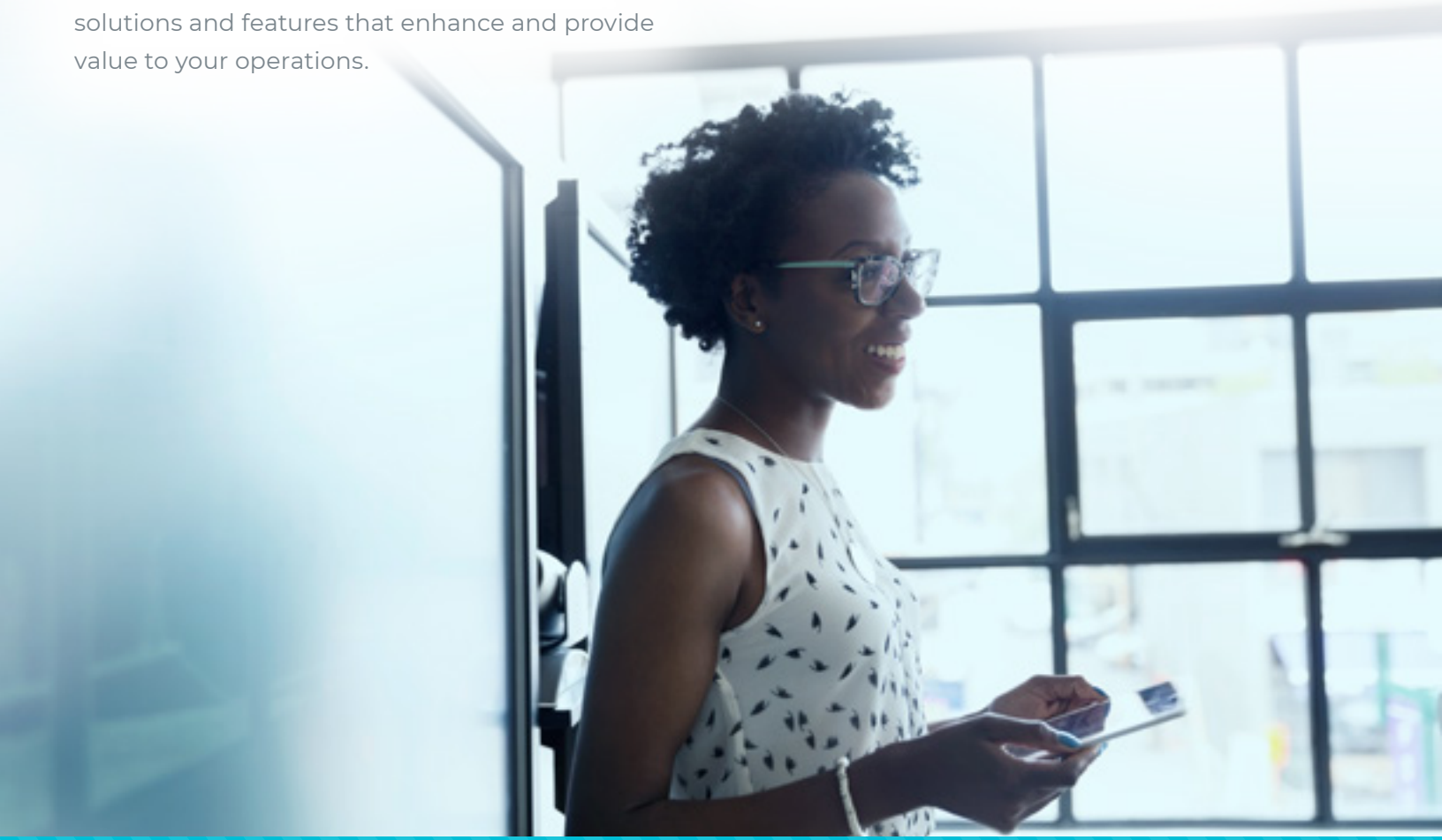
It's important to understand the full potential of every piece of software and hardware your business invests in. Because many of today's solutions offer so many features, a full-service MSP with experienced technicians can consult you on the solutions and features that enhance and provide value to your operations.

Risk #7: Your physical technology security is lacking.

Think your security risks are only of the cyber sort? Think again. Businesses need to be vigilant about their physical security as well. Beyond just, say, locking your premises, that also means locking down your technology so that a thief can't, for example, steal a thumb drive or log into an employee's laptop.

"Physical security is an issue that many companies overlook," he says. "It could be a cleaning person who uses a USB drive to log onto your network. It could really be anyone who has access to your facilities or your devices."

You can teach your employees best practices for protecting their work devices and data when working remotely, such as locking down their devices and using hard-to-crack passwords. But you should also deploy tools that prevent a thief from gaining access to your network and data even if they manage to steal a device, Knox says.



A Partner to Keep You **Productive**

As your company grows, it's only natural that your IT operations will become more complex – and potentially even overwhelming. By partnering with a full-service, national managed services provider like CompuCom, you gain peace of mind through advanced security solutions and proactive, 24/7 support. We remotely monitor your network for potential threats, manage your vendor relationships, help with employee onboarding and offboarding, and offer a robust suite of additional services, allowing you to shift your focus back to your core business.

CompuCom also supports your existing IT staff and leaders by offloading much of the risk and day-to-day burdens they face, allowing them to concentrate on more strategic tasks, such as launching new technology initiatives and addressing the high-impact needs of the business.

Want to learn how CompuCom's Managed IT as a Service can help your business? Call us today at **1-800-300-0983** or visit us at **smb.compucom.com**.

5.20.2019

CompuCom® | MANAGED IT as a SERVICE