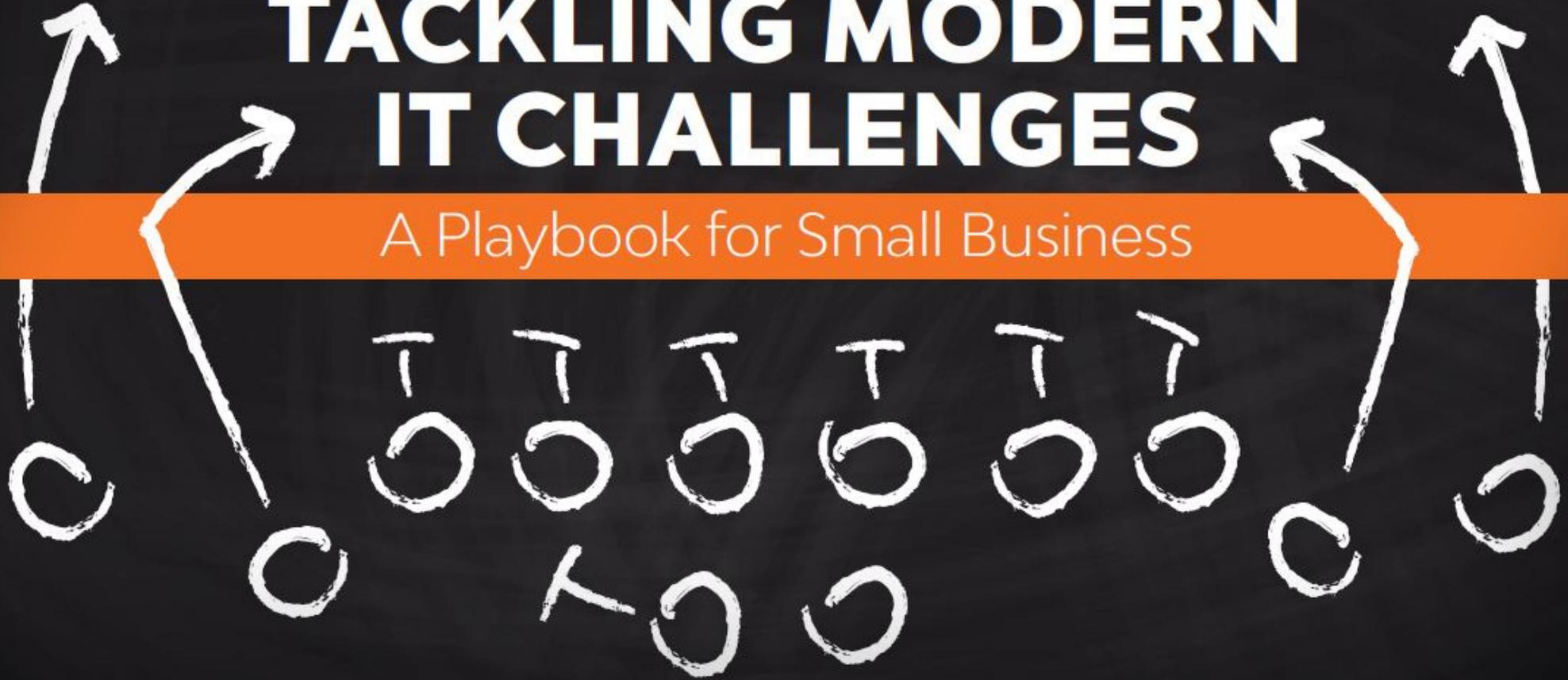


# TACKLING MODERN IT CHALLENGES

A Playbook for Small Business



**BULLETPROOF**

a GLI company

# Table of Contents

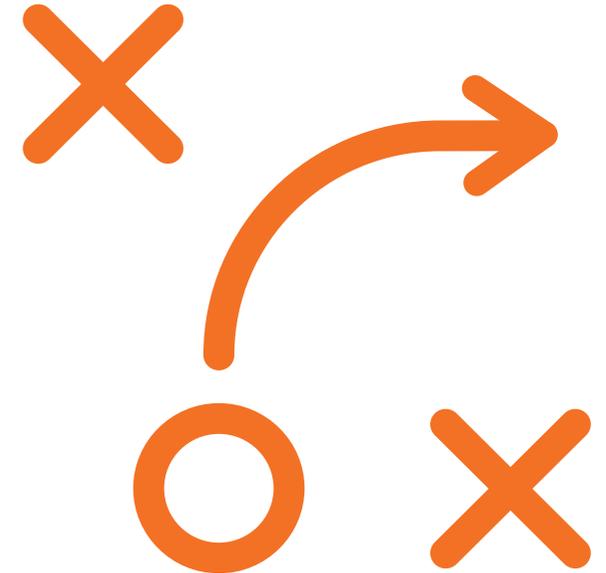
Introduction

**1** Chapter 1: The Way You Work Has Changed...Has Your Technology?

**2** Chapter 2: Why Hiring IT Talent is Harder Than Ever Before

**3** Chapter 3: Proactive IT Strategy in Uncertain Times

**4** Chapter 4: Why Outsourcing Your IT Makes Sense



# Introduction

Simply put, the way we work has changed. The businesses of today rely on technology for planning, productivity, execution and e-commerce, and information and data management.

Not every business leader is a technology expert. Nor should they be! But by leveraging Information Technology as a business enabler, not a cost center, and putting IT experts in charge where you can, you can focus on *your expertise*—your business.

One of my biggest takeaways from talking to small business owners and leaders is that many aren't taking advantage of all their technology stack has to offer and are missing out on critical efficiencies and information security best practices. Furthermore, many aren't aware of the explosion in cybersecurity threat frequency and severity that has taken place over the past few years.

Whether you're a team of 25 or 250, finding the time to properly leverage your technology tools, manage and maintain your infrastructure, and support the hardware and software needs of your team can be a challenge.

To help you tackle the modern IT challenges of today's business landscape, our team of experts has created this eBook covering the following topics:

1. Why Hybrid Work Makes Your Small Business a Big Target
2. Why Hiring IT Talent is Harder Than Ever Before
3. Proactive IT Strategy in Uncertain Times
4. Why Outsourcing Your IT Makes Sense

From one business leader to another, I hope this information helps to make this year your strongest and most productive ever. I'm happy to share my insights with you anytime – [click here](#) to connect with me on LinkedIn.

*Steve Burns*



## About the Author

Steve Burns, President & Chief Operating Officer, Bulletproof

As the founder of Bulletproof, [Microsoft's 2021 Global Security Partner of the Year](#), Steve is passionate about helping businesses with their technology and security. With decades of experience, he is uniquely positioned to share his knowledge with business leaders who have varying levels of technical expertise.

# Chapter 1:

## The Way You Work Has Changed...Has Your Technology?

In 2020, small businesses scrambled to manage a sudden shift to remote work as provinces and states declared a state of emergency. Plans—and mistakes—were hastily made. Ad-hoc solutions were implemented and IT departments, if they existed, were stretched far beyond their limits.

As the dust settles after the largest public health crisis of our lives to date, many small businesses are realizing they are never going back to “normal.” Most organizations have concluded that instead of a full-time return to the office, a hybrid workplace is the best way forward.

According to the [Accelerating Digital Agility](#) report, **~57% of workers expect to be in the office 10 days or fewer each month**, and 98% of people believe future meetings will include remote participants.

### Hybrid Work Creates Security Risks

While a hybrid workplace is a necessary shift to meet the changing needs of the modern workforce, it can also create costly security risks.

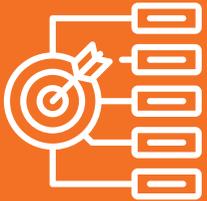
The most significant change organizations have experienced since pre-pandemic is that their data is now predominantly in the cloud rather than inside a firewall-protected data center.



## KNOW YOUR TERMS



**BYOD:** BYOD (Bring Your Own Device) is a policy or business philosophy where employees perform their work from personal devices (laptops, tablets, mobile phones) as opposed to company-issued ones.



**IT Governance:** The Information Technology function that aligns IT and business technology with the overarching objectives of an organization and defines the processes and parameters of an IT infrastructure. This responsibility often falls to the IT Manager or Director of an organization.



**MFA:** Multi-Factor Authentication (also referred to as two-factor authentication) is a best practice of organizational and information security. It requires two different forms of identification to grant access to an IT system. Typically, something you know (like a password) and something you have or are (like a smart phone or voice recognition).



**On-Prem:** Short for “on-premise” or “on-premises”, on-prem describes IT infrastructure and software that is installed and hosted on the physical premises of the people and organization using the software (as opposed to a remote facility like cloud-based software).

With data moving to the cloud and increased remote work, small businesses now have more mobile devices and employees are working from more locations. While that’s good news for employees who can access this data wherever they choose to work, it also means you have more points of risk to think about.

As teams work both remotely and in the office, the boundaries between work and home begin to blur. The reality is that some team members will also use home devices and networks for work purposes, which increases the number of endpoints that malicious actors can attack.

Personal devices are more likely to be lost and may have minimal security installed—or worse, none at all. Plus, phishing, ransomware, and social engineering attacks have become more sophisticated and harder than ever before to recognize.

### Hybrid Employees Need More Security Training

Organizations believe that if they invest in the right technology, their business and data will always be protected. However, the platforms you use will only work as well as your team has been trained to use them.

“

**Over 90% of all incidents can be traced back to mistakes such as clicking on malicious links or attachments in emails, entering organizational login information into a fraudulent website, not keeping software up to date and fixing security holes, or losing devices and equipment.**

”

Conducting training to change employee behavior, attitudes, and security habits is a necessary investment for all small businesses. This is more challenging in a hybrid workplace as **“1 in 3 remote workers admit they feel overwhelmed by the need to keep track of all their account credentials, it is easy to see how apathy, short attention spans, and bad cyber habits are the true adversary of a secure network.\*”**

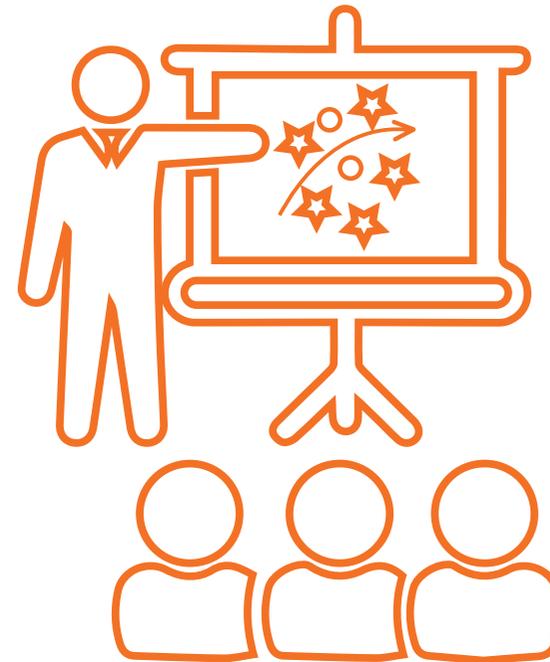
## Not Productive? Not Secure

For hybrid workers especially, security and productivity must go hand-in-hand. If remote work security policies cause frustration and wasted time for employees, they will simply work around them.

\*Source: Tech Radar

Without employee education and participation, even the most robust security methods aren't useful or effective. Employees working from home or from shared spaces like coffee shops, airports, or libraries must be able to stay compliant with security policies without interrupting their workflows.

Businesses that are serious about maintaining security when employees work both remotely and in the office must choose productivity software with built-in security with neither feature treated as an afterthought.



## Hybrid Workplace Software Checklist

If you're currently relying on a patchwork of software solutions, there could be dangerous gaps in your cyber defenses. This checklist can help you identify an all-in-one solution that can deliver productivity and peace-of-mind while eliminating the IT security problems you're facing today.

**The right secure remote work software solution for forward-thinking businesses will:**

- ✔ Include advanced threat protection and security features that help stop phishing and ransomware attacks, enable multi-factor authentication and conditional access, and restrict the movement of sensitive data.
- ✔ Give you (at least) these basic essentials: email, calendaring, mobile document creation and collaboration, team communication, and file storage and sharing.
- ✔ Work from anywhere that your employees choose to work, and from a range of devices for companies with bring-your-own-device (BYOD) policies.
- ✔ Provide built-in tools for managing and authenticating users, including role-based access control.
- ✔ Enable multi-factor authentication for enhanced remote work security.
- ✔ Help protect users from phishing and business email compromise (BEC) attacks.
- ✔ Help protect users from malware attacks.
- ✔ Allow for the implementation of a data loss prevention (DLP) policy that can help monitor the transmission of sensitive information and prevent it from ending up in the wrong hands.
- ✔ Give users advanced collaboration tools, including video conferencing, whiteboarding, team chat, direct calling, recording and automated transcription options for meetings, and real-time document co-authoring.
- ✔ Provide all of the tools your business needs with a layer of embedded security that doesn't inhibit productivity.

# Chapter 2:

## Why Hiring IT talent is Harder than Ever Before

If you're a small business leader, you may be familiar with how challenging recruiting and retaining IT team members can be. More often than not, IT positions are expensive and difficult to fill.

However, starting in early 2021, the hiring dilemma for IT became even more difficult as "The Great Resignation" began. Coined by Professor Anthony Klotz of Texas A&M University, the term represents an economic trend in which employees are voluntarily resigning from their jobs at a significantly higher rate than normal.

The Great Resignation has amplified the skills gap in the IT labor market, meaning there are now more open IT positions than there are professionals to fill them.

**"With the pandemic providing the spark for companies to increase their tech workforce, 80% of businesses are currently in need of IT workers, and 70% of all businesses are having a difficult time finding candidates with the right skillsets."**

— Tech Salary Guide 2022

The average cost of an IT resource is skyrocketing, and the turnover rate is at an all-time high.

Information Specialist is one of the jobs with the fastest-growing demand, according to LinkedIn, and tech positions were among the top 10 roles across every country LinkedIn looked at in their recent analysis of The Fastest Growing Jobs Around the World.



– LinkedIn Data Insights

Even if you can recruit IT talent, we're approaching an inflection point where the cost of IT resources is so expensive that insourcing simply no longer makes sense for small businesses. Salaries have been rising in the Information and Communication Technology job sector since 2021.

And now, we've reached a tipping point. We've hit a time where the cost and difficulty of recruiting IT resources, combined with the inevitable gaps in security posture created by a forced adjustment to hybrid work, leaves organizations vulnerable (not to mention at a time when cyberattacks are at an all-time high).

## IT Requirements for Small Businesses Have Changed

Today's SMB IT environment is challenging. Now that so many more employees work remotely, file and data management, access management, and digital collaboration have become crucial functions—and they all need to be cloud- and mobile-compatible.

If your IT resources felt pressure before, COVID-19 introduced a force multiplier effect as they had to deploy cloud-based collaboration services and allow employees outside the office to access corporate data. This quick adjustment to support a work-from-home environment had IT teams stretched to their limits; and realizing that their tech stack may not be operating as smoothly as they thought.



# Chapter 3:

## Proactive IT Strategy in Uncertain Times

Several changes in the IT technology landscape are causing uncertainty for SMBs. The pressure of soaring cybercrime, hybrid work environments, staff shortages, and small IT team capacity constraints make it difficult to prioritize tasks.

IT teams are finding themselves in a constant state of reacting—to software bugs, hardware failures, issues stemming from user error. This is a strategy that leaves the doors open to a costly disaster such as a breach in data privacy or employees getting locked out of work systems causing a complete productivity standstill and potential service disruption. In organizations where the IT team is a team of one—or no one at all—the risk is all the higher.

By underinvesting in IT, SMBs should expect to stay in a reactive state. When there is always a fire to be put out, you risk making bad IT decisions that could lead to a company-wide halt in productivity.

Your business can make smart decisions about how you tackle modern IT challenges.

### Getting Ahead: Moving Away From a Reactive Strategy

To escape a constant cycle of reactivity, SMBs must consciously adopt a proactive strategy and take immediate steps to achieve it. Strategic planning is integral to the success of any SMB organization, and IT should not be excluded. To formulate a proactive IT strategy, you must plan for when things go well and when they don't.

IT roadmapping is a type of planning designed and ideal for organizations with modern IT structures and teams. This type of planning helps IT teams focus on key milestones to guide their decision-making. Specifically, this type of roadmap determines the timelines, actions, and resources needed to accomplish goals that impact the organization's internal systems and processes. An IT roadmap includes detailed IT-specific projects such as updating software or migrating data.

Inefficient processes and undeployed or underused software are all realities when a proactive IT strategy is not used. You may think you are preparing for growth by investing in a variety of products when in fact you could be wasting budget on underused software that may not even be deployed until it is outdated, or that doesn't serve your IT goals.

Although the decision is yours to move to a proactive approach, all of the planning does not have to land on the (already full) plate of your IT team. In these times of hybrid work models, SMBs have learned that outsourcing IT support and management can alleviate a lot of pressures placed on small teams, IT planning included.

## Add Certainty to Your Budget

Outsourcing your IT planning will help you manage the transition from a reactive approach to a proactive IT strategy. Additionally, outsourcing will help control your budget by reducing recruitment costs, management resources, and overhead.

IT teams are not immune to soaring inflation prices—the costs of tech talent, training, equipment, and software have all increased in recent years.

By choosing a managed IT service provider to fully manage or augment your current IT capabilities, costs will be predictable and you'll have access to service desk support, IT infrastructure management and monitoring, and human resources that could cost an exorbitant amount to handle in-house.

Productivity loss is another potential cost of a reactive approach to IT. Managed IT service providers (MSPs) assist employees with technical challenges and push for a timely resolution, reducing interruptions to their productivity and any impacts to end users.

A knowledgeable, trusted MSP can even provide expertise and guidance to SMBs when making decisions about scalable software and hardware solutions that best fit their needs and budget at any given time.



## Scalable Resources—Ready to Grow When You Are

Planning for the future often means being prepared for change. Growing your team, deploying more features from your software, increasing productivity, and better supporting remote employees are on the to-do list of many SMBs. But when you're a small business owner or leader just trying to keep up with what's in front of you, growing and implementing changes such as these are the last things on your mind.

With a managed IT service provider, you have a full team of experts that are ready and prepared to support your growing business. The reliability of outsourcing to a scalable IT service provider truly allows you to plan and act proactively versus reactively, knowing there are resources you can depend on for scenarios accounted for in your IT roadmap.

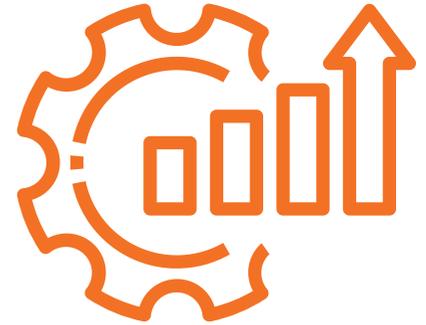
Small IT teams also require software solutions that are scalable, so that the technology being used by employees will enable them to stay connected and productive as the company grows. Microsoft's technology is designed to grow with you—when you're ready.

## Increasing Productivity with Microsoft

Bring your IT roadmap goals to life with a proactive IT strategy. Using a single Microsoft technology stack, you'll have the tools to create work process efficiencies and increase productivity.

Whether your employees are working on-site, remotely, or both, the level of data protection and productivity will not differ. In fact, Microsoft is designed to add security features without making it harder for employees to do their jobs.

Bulletproof has helped SMBs protect their data, devices, and people since 2000. As Microsoft 2021 Global Security Partner of the Year winner and 5X Microsoft Canada Impact Award winner, Bulletproof has over two decades of experience effectively implementing IT processes, procedures, software, and support, allowing SMB leaders to do what they do best: focus on their business.



## Seeing the Full Picture

Having a proactive IT strategy should account for every scenario that could arise so you and your team know exactly what to do in the event something does go wrong.

For example, if you are migrating your servers from on-premises to the cloud, who is responsible? Will there be any system downtime? How could it impact your employee productivity, or your customers? These are the types of questions that need to be considered and planned for so that you can optimize your technology with minimal disruption.

Or say your employee switches from working from the office to working from home and can no longer access the materials they need to perform their work. Who should that employee contact for help? How can that employee get their technology back to full function so that productivity doesn't suffer? Everybody in your organization should understand who to turn to when things go wrong, and you should feel confident that issues will be resolved swiftly, without impacting organizational efficiency.

Our Managed Services team has decades of experience handling all kinds of system migrations and has the project management expertise to make sure your migration goes off without a hitch.

## Change is Certain

Your plan is not going to change from your current reactive approach to a proactive one overnight; organizational buy-in and behavioral changes are required to achieve adoption. There will be a necessary transition time as people and processes adapt. If you are outsourcing your IT services, you have access to top-level expertise to guide you to best-in-class training and change management solutions.

Additionally, the plan will need to be iterated on as environmental factors influence IT processes. If one thing is certain, it's change—so how are you going to prepare and adapt for it?

Planning, training, and executing an IT roadmap is a great start to taking a proactive approach to IT strategy. Having the expertise from Bulletproof to help guide your roadmapping to match your goals and the existing capabilities of your team gives you scalable options and peace of mind knowing your IT strategy is strong and secure.

The benefits to SMBs of outsourcing IT services reach beyond the planning and transition stages. It could be the solution your organization needs to relieve many modern issues in these uncertain times.

# Chapter 4:

## Why Outsourcing Your IT Makes Sense

Even with whispers of an economic recession on the horizon, it's a job seeker's market in the tech industry right now, and it's making recruitment difficult and expensive. Additionally, it's taking longer to find the right hire than it has before. North American companies are taking between 54 and 60 days on average to hire a successful IT candidate.

Coupled with the quickly changing cybersecurity landscape, organizations without proper network monitoring are leaving the door wide open to cyber threats.

For small and medium-sized businesses (SMBs), these issues can be serious burdens on security and productivity.

### **Are You Training Your Team to Know Everything?**

When new talent is secured, training and retention are continuous. This is necessary to reduce gaps in skillsets and prevent security risks. With a growing number of cybercriminals preying on remote

workers, gone are the days of a firewall and a password being adequate network security.

With any size team, training is important to equip staff with the knowledge they need to effectively manage their work. Training is another cost layered onto the recruitment process and salary of your new hire. It's not a one-and-done event, it takes continuous training to keep your team thinking ahead of cybercriminals and ahead of technology advancements.

Despite continuous training, there are only so many hours in a day that a small IT team can apply the knowledge they've learned to catch up with the evolving landscape while balancing a daily workload and monitoring an expanding virtual network. It's a matter of time before exhausted IT employees miss something important such as a technology deployment or cyber threat that puts your entire network at risk.

## Productivity Relies on IT More Than Ever

Half of North America's private-sector GDP is driven by small- to mid-sized businesses. With smaller individual workforces that generate big results for the economy, can SMBs like yours afford to miss a beat?

Almost everything we do during the day relies on technology. That means almost everything we do during the day relies on who is managing your IT network. That is a heavy burden for a small internal team—and for the team responsible for hiring those positions.

Companies that are outsourcing their IT operations not only have eyes on their network at all times, but they also have access to robust disaster recovery should a cyber threat find its way into the network.

## Thinking Outside the Cubicle

With 3.6 million tech-related job postings in the US last year, it is certainly an uphill battle for SMB organizations like yours to compete for and keep IT talent.

Just because there are vacant cubicles in the IT department doesn't mean they have to be filled by expensive hires. There are several areas of expertise required in an IT team, making it difficult and out-of-reach for you to try to fill every gap or expect a small team to take on all the work.

There are more efficient solutions available that include management or augmentation of IT operations—for a fraction of the cost to build an in-house team.

Choosing to outsource means you know you're hiring experts who bring resources to the table that you wouldn't otherwise have access to. It also means that you are hiring trusted professionals who have been vetted by an experienced company, removing the risk of a bad hire or having to deal with employee turnover (which happens to be at an all-time high among IT roles).

*Unhappy and overworked IT staff who are unable to keep up with increasingly advanced and high-volume demands of business today could pose as much a threat to a network as external threats do.*

## Raising the Bar—Not the Tension

The expanding role of an IT professional is making it difficult to manage the workload with a small team. The rise in cybersecurity risks alone is a lot to keep on top of, and no business is too small to be immune to online threats.

More SMBs are outsourcing IT operations for many reasons—ultimately because it relieves them from significant financial and operational stress. It allows them to skip the costly steps of recruiting and training new talent while gaining the expertise of professionals. This outsourced model enables you to reduce overhead and take control of your budget and IT operations at the same time.

How much time and money have you spent recruiting for IT?

Fixed costs are essentially converted into variable costs when your IT is outsourced. Pay-as-you-go allows you to scale your business up and down so you pay for what you really need day-to-day. Outsourced IT professionals can provide strategic consultation and IT roadmap planning to help prevent cyber threats and optimize your network.

Outsourcing enables businesses to access a full team of IT experts along with their software and equipment, unlocking IT support and operational efficiency without the significant capital investment required to set up an always-on network operations center.

**Bulletproof is an IT management company that has been successfully reducing the stress on SMBs throughout North America for over 20 years.**



## Identifying and Choosing a Managed Service Provider (MSP)

Modern IT teams at small and mid-sized businesses are faced with a host of time-consuming issues and ongoing staffing problems that make Information Technology management and operation infeasible. Enterprise-grade solutions exist, but simply scaling them down doesn't meet the unique needs of SMBs.

SMBs need a solution developed to solve their specific issues—a solution that provides employee education, 24x7 IT support, and protection against cyber threats—without making it harder for users to do their jobs.

By outsourcing IT to a trusted MSP, SMBs can often choose to augment current IT operations or an on-premise IT department. Choose a provider that will protect your data and help you improve productivity through:

- Proven Information Technology expertise at all levels
- Advanced security protection
- Seamless integration with your existing processes

Outsourcing IT makes sense for SMBs because it enables them to keep their network up and running and manage risks associated with the cloud, without interrupting productivity.



## Protect Your Data and Productivity With Bulletproof

Bulletproof has been helping SMBs protect their data and productivity for over 20 years. Our experts are fully trained in the Microsoft tech stack. This sets us apart from other IT service providers that support a variety of tech but are not as knowledgeable in Microsoft technology.

At Bulletproof, our skilled team provides enterprise-grade solutions without the enterprise price. We will be your trusted IT service partner while saving you all the expensive hassle that comes with hiring and training your own in-house team.

Explore how we can help your organization reduce IT headaches and labor costs while protecting your network from advanced cybersecurity threats. [Learn more about our Bulletproof 365 services.](#)

# Schedule A Complimentary SMB Technology Briefing

Whether you're a new small business or a growing organization, there is no denying that technology will be an essential part of how you do business. Make smart, strategic decisions when it comes to your IT software, hardware, and security with help from an experienced Managed Services Provider.

Be proactive with your IT planning and take advantage of the support a partner with decades in the business can provide.

Our SMB Managed Services experts can help you understand your position in today's technology landscape and how you can **leverage your tech and streamline your processes to grow efficiencies, output, and profit.**

**No cost, no obligation – just the facts.**



## Sources

<https://hired.com/state-of-tech-salaries/2022/>

<https://www.computerworld.com/article/3542681/how-many-jobs-are-available-in-technology.html>

<https://www.firewalltechnical.com/the-risks-of-hiring-an-in-house-it-support-department/>

<https://www.cyberstates.org/>

<https://www.linkedin.com/pulse/tech-issues-explained-cybersecurity-skills-gap/>