TAYLORED

Advisor

GET THE MOST OUT OF YOUR IT SPEND:

ENTERPRISE-QUALITY NETWORK AND SERVER SECURITY SOLUTIONS ON SMB BUDGETS

TABLE of CONTENTS

WHY IT DOESN'T PAY TO SKIMP ON NETWORK AND SERVER PROTECTIONS

In today's threat climate, businesses face increasing — and increasingly sophisticated — network and server threats. Small to medium-size organizations that may have previously been too small to be noticed by dangerous threat actors are now facing many of the same risks as large, enterprise-level corporations, with fewer resources to combat them and lower budgets to implement cutting-edge solutions.

COMMON THREATS FOR SMBs

A lack of awareness about potential cybersecurity threats puts small to medium-size businesses at risk of dire consequences when not prepared with the tools to combat and defend against them. The most prevalent network and server security risks for SMBs in today's technology landscape include:

Ransomware. This is a form of malware that encrypts a business's files and/or IT systems and demands a ransom from the business with the promise of restoring data and function. Even if businesses pay the ransom, the return of their files and system functionality is not guaranteed.

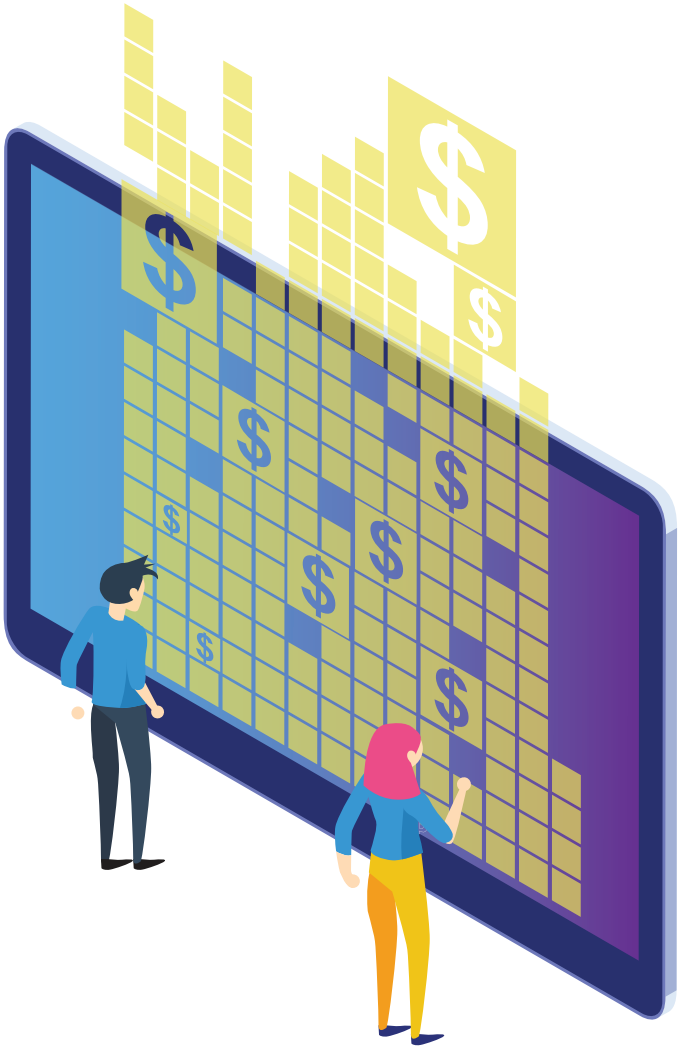
Phishing emails. These are online scams in which criminals impersonate legitimate businesses, people or organizations via email in order to steal data and other sensitive information. This data theft is usually accomplished via a link in an email that takes the user to a seemingly legitimate website, which then prompts them to enter private information such as SSN, credit card information, banking information and more.

Contrary to popular belief, the risks of these threat actors are very real no matter the size or scope of your business. No business is safe without the proper precautions, tools and remediation techniques.

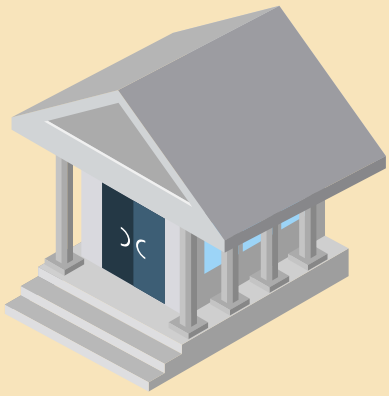
THE REAL COST OF A NETWORK OR SERVER SECURITY EVENT

One of the primary reasons that SMBs do not invest in proper network and server security is cost. A common misconception is that the cost of precautionary tools and solutions is much higher than that of the traditional break/fix method typical in many SMBs' approach to IT. In truth, the real cost of a network or server security event such as ransomware, phishing scam or other cybersecurity attack can be devastatingly expensive — if not impossible — to fix.

Financially speaking, the cost of cybercrime is extremely high and is only expected to increase. According to Cybersecurity Ventures, the cybercrime impact is expected to reach $6 trillion in 2021 and nearly double that by 2025. This means that, depending on the type of threat actor, SMBs could face unprecedented costs using the break/fix method.



In addition, many of the losses associated with cybersecurity breaches are not immediately calculable but can ultimately take a toll on a business's productivity and long-term success. Some of these losses include:



Downtime, lost productivity and time diverted from other initiatives.
In terms of ransomware alone, the cost of downtime to businesses is 24 times higher than that of the ransom amount, and the average downtime associated with ransomware is 19 days (Datto's Global State of the Channel Ransomware Report 2020).

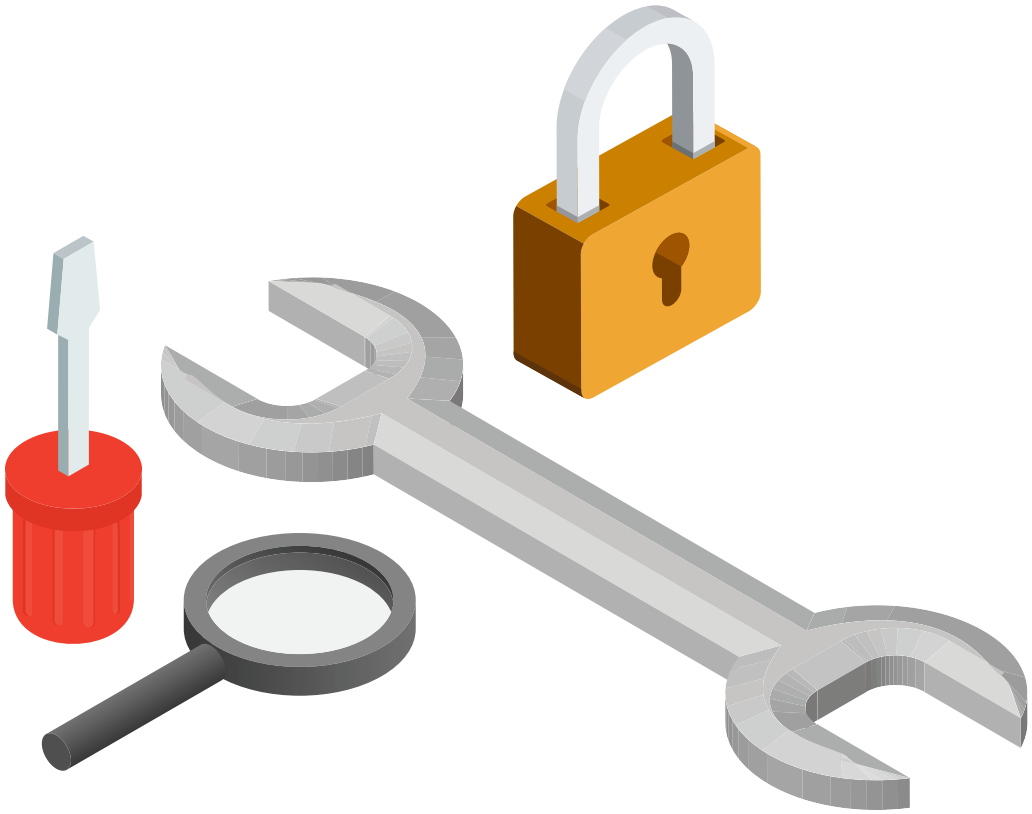
Damage to reputation.
A significant majority (59%) of buyers say they would avoid companies that suffered a cyber attack in the past year (Arcserve 2020 Data Attack Surface Report).

Potential legal implications.
As of April 2020, 52% of legal and compliance leaders were concerned about cybersecurity risks (Gartner). Compliance is particularly important for industries such as government, banking (PCI) and healthcare (HIPAA), in which businesses are subjected to massive fines if found to be in breach of these regulations.

Bankruptcy and going out of business.
Within six months of a cybersecurity attack, 60% of SMBs go out of business (Inc.).

BASIC SECURITY TOOLS FOR NETWORKS AND SERVERS

With the true costs of cybersecurity incidents in mind, business owners can better understand the value of investing in the proper network and server security tools and solutions. But before we discuss how to maximize ROI on IT security initiatives, let's take a look at some of the most effective security protections and why you need them.



THE TOOLS

As with any solution, the right tools are key to both helping prevent cybersecurity issues and solving them when they occur. At a minimum, SMBs should consider the following network security tools.

SERVER-SIDE TOOLS

Server-side tools work at the server level to protect against cybersecurity threats before they wreak havoc on business systems. Essential server-side tools include:

Antivirus protection. The basics of cybersecurity protection, antivirus protection searches for and removes malware.

Viable backups. Local and off-site backups help to protect against cyber threats and allow for businesses to restore data in the event of an incident. Full backup and disaster recovery solutions are ideal and not limited to enterprise-level businesses. Backup solutions at an SMB budget level can still offer comprehensive protection by backing up data and systems to the cloud — enabling the business to restore functionality at any time.

Email protection. To protect against spam, scams and phishing, email protection monitors, identifies and removes potential threats. Ironscales is a great example of a thorough email protection software.

FIREWALL

An SMB needs not only a robust, next-gen firewall but also that firewall to be configured properly. It should inspect each data packet that comes into a network individually and ensure there's nothing nefarious about it. A firewall can also be configured to keep logs of all information so that in the event of a cybersecurity breach it's easier to identify the point of intrusion entry and what led to the intrusion occurring in the first place.

SOFTWARE

By layering the right kinds of software, such as antivirus, firewall filtering and email filtering, SMBs can have comprehensive and collaborative forces working together to help prevent cybersecurity threats at the source. An experienced network and server security provider can recommend the right types of software for your business's needs and budget.

WHY SMART SECURITY ISN'T PLUG-AND-PLAY

As with any business solution, it's important to remember that simply purchasing the right tools is not enough. When investigating your security options, it's essential to confirm that they can be implemented in the best possible way. This will not only maximize the tools' efficacy but also ensure optimum ROI.

Configuration: All cybersecurity protection tools need to be configured properly so that you know they're operating at optimal performance and achieving the goals they're meant to.

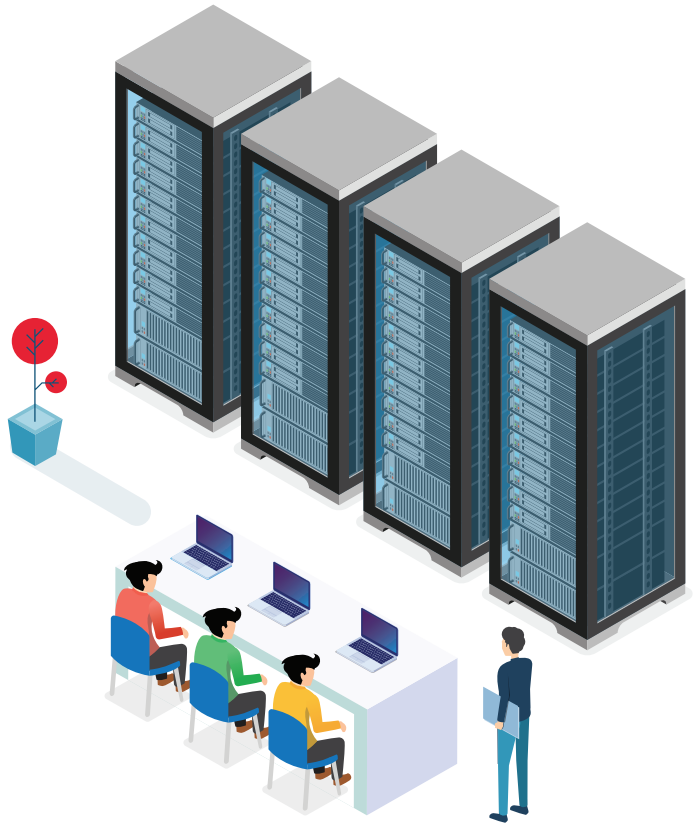
Layered security: Never rely on a single solution or tool to do the job. All of your solutions should work together to ensure that there are no holes in security and that every aspect of your network and/or servers are fully protected.

Redundancy: Because of the ever-changing landscape of cyber threats, even the most sophisticated and effective solutions have the potential to fail. For this reason, it's important to have a reliable and comprehensive backup and recovery plan so that you can get back to work quickly in the event of a network or server security event. A backup and disaster recovery plan ensures that data, assets and systems are consistently and properly backed up, allowing SMBs to restore files and functionality as needed.

Choosing and implementing tools and solutions that are the right size for your business and tailored specifically for your needs requires extensive experience and typically far more resources than most SMBs have internally. With this in mind, SMBs looking to maximize their network and server security solutions should partner with a reliable, local provider who can not only optimize solutions but also boost ROI with proven strategies.

STRATEGIES FOR BOOSTING SECURITY ROI

By far, the best strategy to boost network and server security ROI for most SMBs is to partner with an IT solutions provider that has experience with the right tools. An experienced IT provider can provide comprehensive network and server security protection with high-level tools, expert configuration and client-specific customization — all without a massive investment in internal labor and infrastructure.



SPECIFIC BENEFITS OF PARTNERING WITH AN IT PROVIDER INCLUDE:

Custom solutions.
The right partner will become familiar with your environment, specific strengths and weaknesses, and network and server security goals in order to build custom solutions unique to your business. An IT provider should take the time to learn what's really important to you. For example, does your business need to focus on network security or the protection of data files? Knowledgeable providers can help you determine where your investment is best spent and what aspects of IT security you might be able to save on. This makes for more flexible pricing, as you can balance your needs with your budget.

Convenience.
Having a reliable IT provider makes managing network and server security easy, as you have a single place to take any issues.

Expertise.
IT providers have a larger knowledge base to draw from, and they are able to offset the high investment costs related to staying on top of technology. Even if SMBs have an IT staff, one person can never replicate the knowledge of an entire team of professionals dedicated to various aspects of IT.

Savings and capacity.
By working with an IT provider, SMBs don't need to hire a whole team of IT staff, which is often cost-prohibitive. With a third-party IT provider, businesses can get the best of both worlds — savings and expert ability to handle a wide array of IT issues.

Access to the latest technology.
When you hire an IT provider to monitor or manage servers, you're not just getting IT experts, you're also getting best-in-class tools such as antivirus protection, cutting-edge software and state-of-the-art security solutions. These investments are typically too expensive for SMBs to implement on their own. But through an IT provider, SMBs gain access to tools without the massive investment.

Monitoring.
For SMBs managing network and server security without an IT provider, it can be difficult to know when a breach or other incident arises. With constant monitoring and advanced software, IT providers know immediately when there's a problem, resulting in less downtime and damage associated with the incident.

Increased resources and peace of mind.
All SMBs are working with limited resources. Even if your SMB has an IT staff, employees need time off and have other work responsibilities to handle on a daily basis. An IT provider gives you access to a team of on-call professionals who can handle any issues that occur at any time.

TAYLORED IS HELPING SMBS LIKE YOURS GET THE MOST OUT OF THEIR SECURITY INVESTMENT

With more than three decades of experience creating customized technology solutions, Taylored knows what it takes to get SMBs the most for their money. With our one-on-one approach to providing IT solutions, we help SMBs just like yours streamline their approach to network and server security while also implementing innovative solutions for optimal performance and protection — all at a cost that works within your budget.

We do so by assessing your business's unique needs and creating a network and security plan that prioritizes the things that matter most to you. Whether your primary concern is phishing emails or a data backup and disaster recovery system, our team of IT experts can help your business make the most out of your IT security budget. Our goal is to meet your needs, not to sell you unnecessary products and services.

In addition to saving SMBs money, our approach to IT security offers an unparalleled level of service, expertise and support. With our team of network and server security experts, you can rest easy knowing that you, your employees and your customers are protected not only by industry-leading tools but also by IT professionals who are there to help at any time.

Our experience serving our local community in the Indianapolis area has helped establish Taylored as the go-to for all things technology, specifically network and server security. We have a wide range of long-term clients throughout industries such as banking that value security as a cornerstone of a successful business. We're committed to ensuring that all of our clients feel safe and protected, no matter where the ever-evolving world of technology takes them.

THANK YOU FOR READING!

As business owners ourselves, we know how valuable your time is. We'd like to thank you for reading about the importance of network and server security, and we hope this information is helpful in addressing the IT security needs of your business. If you're interested in learning more about how Taylored Systems can help your organization, please contact us at your convenience.

TAYLORED SYSTEMS

ADDRESS:
14701 CUMBERLAND RD, SUITE 100,
NOBLESVILLE, IN, 46060

PHONE:
317-776-4000