Cybersecurity TECHNOLOGY
NEWSLETTER

NETWORK PROVIDERS, INC.
JUNE 2023

Top 9 Benefits of Outsourcing Your Cybersecurity

BY JAY HILL
President & CEO

I'm excited to share more about my time with the Shark Tank. It's great when we can help each other. Robert Herjavec said "being an entrepreneur always comes at a price. The key is to use every challenge that comes your way as a source of motivation." He said it's important to always learn new skills to help your business grow. This keeps a business from becoming stagnant. He said to accept failures, but be resilient. "You can create your own success, and the only thing the world owes you is opportunity." This is great advice. Success takes action. Action takes change. Change is hard, but it's what moves us forward.

Sadly, my friend recently closed his business because he was afraid to make changes to meet market demands. This inspired me. I am conscientiously learning about technological advances to improve my business.

If you have any comments, please reach out.

When it comes to protecting your business from cyberthreats, having the right tools and technology is only half the battle. You also need the expertise, controls and processes to manage and mitigate these threats effectively. That's where a managed security service provider (MSSP) comes in.

Think of an MSSP as your outsourced cybersecurity department, ensuring your technology is safe, secure and compliant.

In this article, we discuss the benefits of outsourcing your cybersecurity to a trusted MSSP partner. From enhanced security posture to cost savings, you'll learn how collaborating in cybersecurity matters can help protect your business from cyberthreats while streamlining your IT operations.

Although there are a lot of benefits to outsourcing your cybersecurity, we're listing the top nine below:

Enhance Business Outcomes

Partnering with an MSSP can help you enhance your business outcomes by reducing downtime, increasing productivity and improving customer satisfaction. You can focus on growing your business and achieving your strategic goals by mitigating cyberthreats and keeping your IT systems secure.

Fill IT Gaps

An MSSP can help fill IT gaps by providing the expertise, controls and processes to manage and mitigate cyberthreats. Whether it's managing vulnerabilities, implementing security controls or responding to incidents, an MSSP can help you bridge the gaps in your IT security.

Lower Costs

Outsourcing your cybersecurity to an MSSP can also help you lower costs. Instead of investing in expensive cybersecurity tools and technologies, you can leverage an MSSP's expertise and infrastructure to achieve the same level of security at a fraction of the cost.

Access to Specialized, Experienced Security Experts

An MSSP has a team of specialized, experienced security experts who can provide the support and guidance you need to manage and mitigate cyberthreats effectively. These experts have the knowledge and expertise to rapidly implement advanced security solutions and respond to incidents.

Advanced Security Solutions

Partnering with an MSSP also gives you access to advanced security solutions that may otherwise be unavailable. From threat intelligence and hunting to endpoint protection and cloud security, an MSSP can provide you with the latest security solutions to keep your IT systems safe and secure.

Rapid Incident Response and Remediation

In the event of a cyberattack, an MSSP can provide rapid incident response and remediation services. Their experts can quickly identify and isolate the threat, contain the damage and restore your IT systems to full functionality, minimizing

Continued from pg. 1

downtime and reducing the impact on your business.

Ongoing, Continuous Protection
Cyberthreats are constantly evolving, so it's essential to have ongoing, continuous protection in place. An MSSP can provide you with the 24/7 monitoring and management needed to detect and mitigate cyberthreats in real-time, ensuring your IT systems are always protected.

Threat Intelligence and Hunting
An MSSP can also provide you with threat intelligence and hunting services, which involve monitoring and analyzing threats in real-time to identify potential vulnerabilities and prevent attacks before they occur.

Compliance Support
Finally, partnering with an MSSP makes meeting your compliance requirements easier. An MSSP can provide the support and guidance needed to comply with industry-specific regulations, such as HIPAA, PCI DSS and GDPR, and ensure that your IT systems are always compliant and secure.

Outsourcing your cybersecurity needs to an MSSP is an investment to secure the future of your business. The benefits of enhanced business outcomes, filling IT gaps, lower costs and more make it a wise choice for any organization looking to strengthen its security posture.

By partnering with an MSSP like us, you'll get the expertise and experience to protect your business from ever-increasing, sophisticated cyberthreats. Don't wait until it's too late.

Contact us now to bolster your cybersecurity.

Become Better At Hiring And Coaching

By Avoiding These 3 Mistakes

Leaders make common mistakes with job descriptions when hiring and reviewing performance. The consequence is an increased probability of hiring mistakes or providing someone with useless performance feedback. Leaders often fall into this trap to avoid accountability or because they fear a performance expectation is flawed.

Most of these errors are entirely preventable. Here are three mistakes every leader should watch out for.

Describing A Job In Vague Terms

"Supporting the marketing team in promoting our products" is too vague. What does that mean? What level of performance is considered poor, good or great? Watch out for "-ing" verb tenses, as they are often too vague. Instead, consider a more specific statement of the job, such as "To help our customers modernize their inventory management systems by increasing sales of existing customers by 20% per year through new product introduction." We would consider that an essential statement of the role's mission, which is a high-level but specific explanation of why the job exists.

Focusing Only On Actions, Not Results

Some leaders make the mistake of wording their expectations in terms of only actions, not results. "Contact at least 20 existing customers per week and conduct an account review with at least five customers weekly." That is a perfect expectation of an "input" or an "action," but it is insufficient if all expectations are just actions, with no eye for the expected results. The risk is that people go through the motions of doing prescribed actions without feeling the urge to deliver a specific outcome. And your organization succeeds or fails based on results in critical areas, not actions.

Solely Focusing On Results, Not Actions

Other leaders make the mistake of wording their expectations in terms of big-picture results without regard to the actions that are likely to achieve them. "Grow revenue at least 15% per year" is a very specific "what." But to make that expectation more achievable, you must also list several actions that are expected to help achieve that result.

Instead of creating job descriptions, I encourage colleagues and clients to follow a practice called writing a "scorecard." A scorecard has a clear mission for the role. It identifies 5–7 outcomes you expect a person to achieve by a specific date. The outcomes are a mixture of actions you want the person to take and the results you expect them to achieve. This makes it easy to "score" whether someone has achieved the outcomes. Using a scorecard will improve your ability as a leader to hire and coach people to embody the organization's purpose and take actions that achieve results.

Building Better Client Relationships in a Remote Setting

Do you work with clients you've never met in person? If so, you might have wondered how you could build more meaningful long-term relationships with your clients. In most cases, it all boils down to communication. Your clients want clear and consistent interactions with you and your team, so be transparent and up-front when talking with them. You should also find out how your client prefers to communicate. Some may exclusively want to talk through e-mail, while others might prefer text or phone calls.

If you really want to exceed your clients' expectations, be proactive. Don't wait for them to contact you for every little thing; reach out weekly or monthly to ensure you're meeting all of their needs. People want to work with someone they can trust and rely on. Don't give them a reason to doubt working with your business. By improving communication, you'll have a much easier time building strong, long-term relationships with your clients.

3 Steps to Zero Trust Cybersecurity for Businesses

Cyberattacks have become rampant and have also grown in sophistication. A simple lapse in your network security could lead to a chain of events that could prove catastrophic for your business. You can avoid this by implementing a robust cybersecurity framework such as zero trust.

Zero trust asserts that no user or application should be trusted automatically. It encourages organizations to verify every access while treating every user or application as a potential threat. Zero trust is a great starting point for businesses that want to build formidable cybersecurity. It can not only adapt to the complexity of the modern work environment, including a hybrid workplace, but also protect people, devices, applications and data irrespective of where they are located.

However, zero trust should not be mistaken for a solution or a platform, regardless of how security vendors market it to you. You can't just buy it from a security vendor and implement it with a click of a button. Zero trust is a strategy — a framework that needs to be applied systematically.

As you begin your journey to implement a zero-trust framework to bolster your IT security, there are three core principles that you must remember:

1. Continually Verify
You should strive to implement a "never trust, always verify" approach to security by continuously confirming the identity and access privileges of users, devices and applications. Consider implementing strong identity and access (IAM) controls. It will help you define roles and access privileges — ensuring only the right users can access the right information.

2. Limit Access
Misuse of privileged access is one of the most common reasons for cyberattacks. Limiting access ensures that users are granted minimal access without affecting their day-to-day activities. Here are some common security practices that organizations have adopted to limit access:

- **Just-in-time access (JIT)** – Users, devices or applications are granted access only for a predetermined period. This helps limit the time one has access to critical systems.
- **Principle of least privilege (PoLP)** – Users, devices or applications are granted the least access or permissions needed to perform their job role.
- **Segmented application access (SAA)** – Users can only access permitted applications, preventing any malicious users from gaining access to the network.

3. Assume Breach and Minimize Impact
Instead of waiting for a breach, you can take a proactive step toward your cybersecurity by assuming risk. That means treating applications, services, identities and networks — both internal and external — as already compromised. This will improve your response time to a breach, minimize the damage, improve your overall security and, most importantly, protect your business.

We Are Here to Help

Achieving zero trust compliance on your own can be a daunting task. However, partnering with an IT service provider like us can ease your burden. Leverage our advanced technologies and expertise to implement zero trust within your business — without hiring additional talent or bringing on additional tools yourself.

Don't Trust These Zero Trust Security Myths

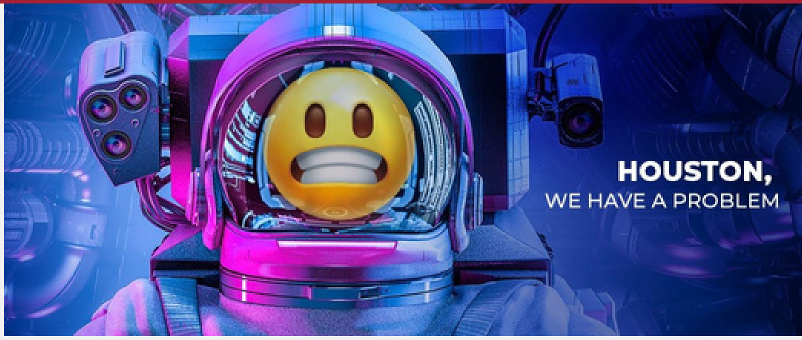
In today's threat landscape, businesses are constantly at risk of being targeted by a cyberattack. Adopting a zero trust security model could be a wise decision from a cybersecurity point of view.

Zero trust works on the premise that everything — humans, machines or applications — poses a risk to your network and must prove trustworthy before accessing your organization's network or data. By insisting on verification and authentication at every step, zero trust makes it difficult for a hacker to gain access through a compromised user account or device.

With the increasing acceptance of the zero trust framework, there has also been an increase in misinformation surrounding it, fueled mainly by security vendors vying to sell their products. We will discuss the top zero trust myths and how an IT service provider can ease the transition toward zero trust security.

Top Zero Trust Myths Busted

Let's take a quick look at the four common myths surrounding the zero trust framework and dispel them with facts:



Myth #1: I can achieve zero trust for my business by using a zero trust product.

Fact: There are no miracle zero trust solutions. Zero trust is a security strategy that needs to be implemented systematically. However, you can use solutions and tools to support the framework. Consider getting help from an IT security provider to identify and implement the solutions best suited for your business.

Myth #2: Zero trust is too complicated for me to implement.

Fact: It can be challenging for businesses with limited knowledge or resources to achieve a zero trust security framework. If you lack expertise, consider partnering with a

Continued from pg. 3

PROMOTE Your Services, Products and Brand

Come and Be Part of Utah's Business Community!

We are launching a brand new, regional magazine designed to give business owners tips, industry insight, connection, and the inspiration entrepreneurs and small businesses owners need to grow and make an impact. This isn't just another magazine; this is a publication WE (a local small business) are curating for OUR CEO peers that will be distributed every quarter.

Limited Offer: Ad cost will range from $500 full page, $350 1/2 page, $150 1/4 page.
Submission Deadline: June 12, 2023

If you would like to receive a media kit and insertion form, please contact the Marketing Department at elvecia@networkprovidersinc.com or call her at 801-849-0521 xt.108. Please make sure to leave your full details: name, company, number and email.

Just like a father works to keep his family secure and protected, having the right defense practices in place can keep your business thriving.

Find out how we can help you stay protected.

trusted IT service provider who can help you understand your business's risk profile and develop a realistic roadmap to implement a comprehensive and effective zero trust security strategy.

Myth #3: Zero trust will make it difficult for my employees to do their jobs and will negatively impact productivity and morale.

Fact: Zero trust enables better user experience and promotes increased collaboration. While increased friction and decreased efficiency due to additional security layers could surface, an IT service provider can certainly help. By suggesting user-friendly policies and easy-to-use solutions that balance security with convenience, your employees can perform their jobs seamlessly.

Myth #4: Implementing zero trust is too expensive.

Truth: Implementing zero trust can be expensive, but that cost is still lower than the fortune you may have to shell out in the event of a major cybersecurity incident. You may have to deploy additional resources and tools to get the best out of a zero trust security model.

Fortunately, you can control expenses and increase efficiency by opting for the help of an IT service provider.

The time to act is now!

By now, it should be clear that zero trust is an effective security framework that can help protect your business against cyberattacks while ensuring business continuity in the event of a breach. With that said, implementing zero trust on your own can be a challenge. That's why partnering with a specialist like us is the best option. Reach out to learn how you can leverage our expertise to implement an efficient zero trust model with minimal effort.

5 Reasons

Why It's Important to Update Your Systems Regularly

It is important to install Windows updates to protect your computer from malicious attacks. Updates add new features and fix known bugs or vulnerabilities to help keep users and computers systems secure. It also finds security loop holes that are discovered in outdated programs. Below are five reasons to have the latest updates in Windows:

Enhanced Security Protection
Old and outdated software is vulnerable to hackers and cyber criminals as updates keep you safe from exploitable holes into your organization.

Improved Software and Hardware Compatibility
When new software and upgrades are made available, existing systems and software may not always remain compatible, so it's important to consult with an IT professional to ensure this process runs seamlessly.

Reduced Costs
The cost of disruption caused by unstable systems and software can very quickly escalate to more than it would cost to invest in an upgraded system.

Happier Staff and Customers
Out-of-date technology gives your business the reputation of being behind the times. Offer your customers a better experience and give staff a chance to increase productivity and efficiency.

Increased Efficiency
Software updates provide new and improved features and speed enhancements to make the end-user experience better.

Below are dates of versions of Windows that will no longer be supported by Microsoft:

Windows 7 as of January 14, 2020

Windows 8 as of January 12, 2016

Windows 10
- **Supported until October 14, 2025**

Windows 11
- **Supported from October 4, 2021 - Present**

If you have old versions of Windows and would like to know what options are available for your systems, give us a call. We can help!