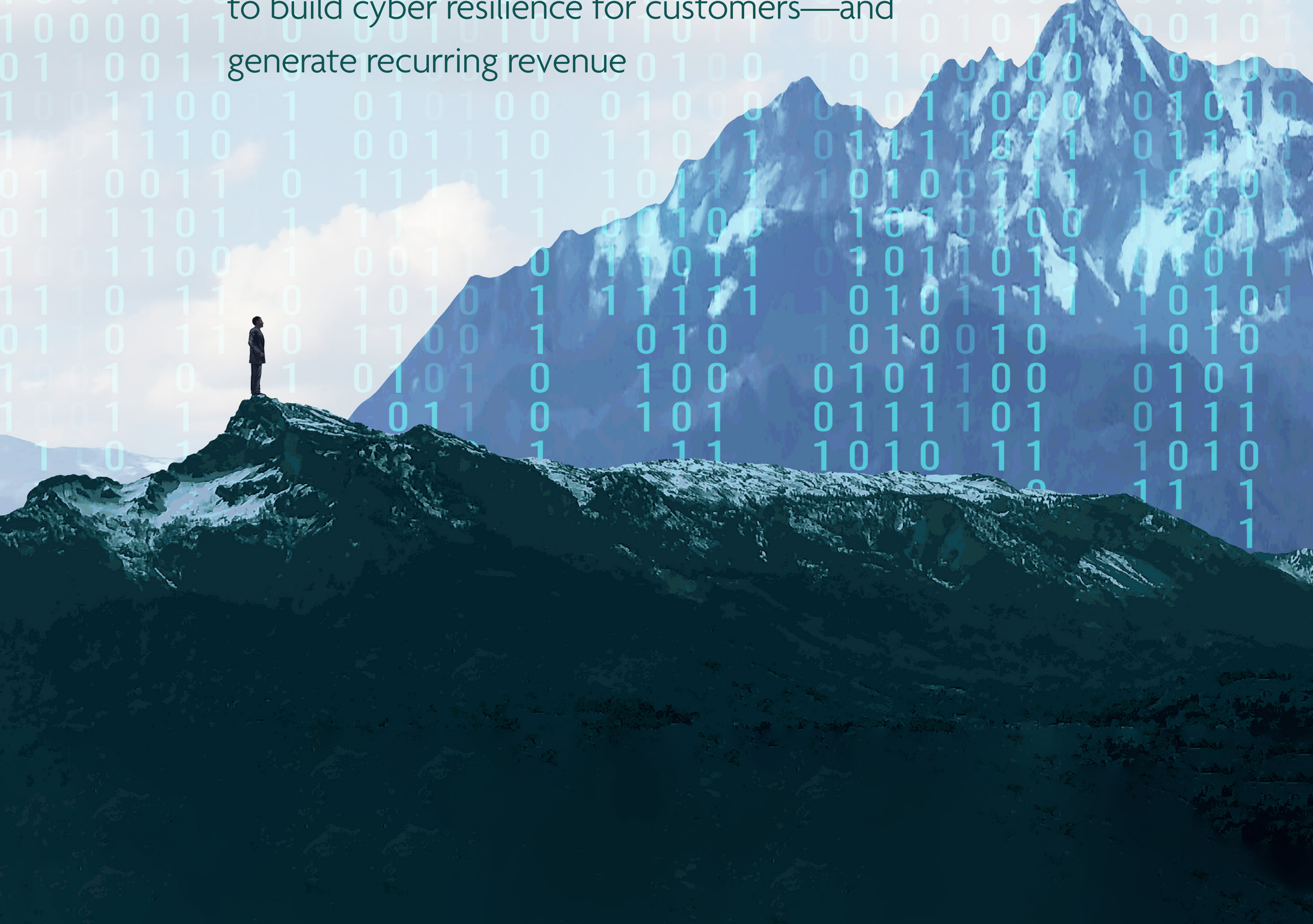
CONNECTSECURE

How to win business with cybersecurity assessments

For managed service providers, an opportunity to build cyber resilience for customers—and generate recurring revenue



INTRODUCTION

To fully understand the potential impact of leveraging cybersecurity assessments to grow your business, look no further than Karl Bickmore. The CEO of Snap Tech IT, a managed service provider (MSP), has made this topic central to any customer conversation.

Bickmore said, "We're winning a lot of deals. And our differentiator typically is that our assessment shows where the security needs are."

He is not alone with this take. The rapidly evolving threat landscape has pushed cybersecurity to the forefront of priorities. Companies must shore up their cybersecurity postures or risk being put out of business, the MSP Expo cautions. This fact presents a business opportunity.

MSPs have everything to gain from embracing the relevant cybersecurity frameworks, like NIST, and identifying where they can make the greatest impact as IT Solution Providers.

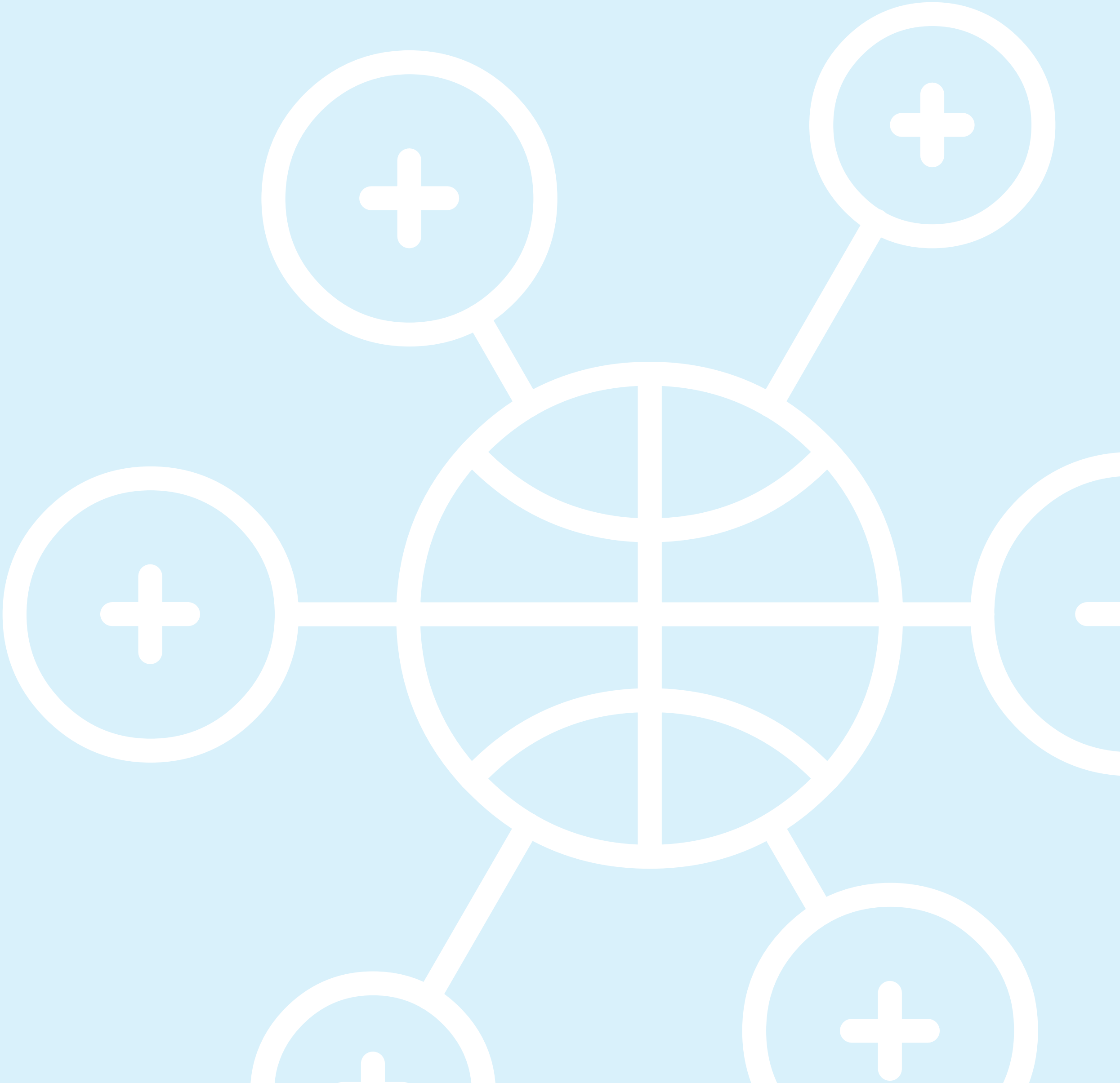
By bringing these insights — and the ability to remediate any vulnerabilities — to their clients, MSPs can effectively position themselves as the partner that every small to medium-sized business (SMB) needs to navigate the increasingly volatile security environment.

Coupled with demands for regulatory compliance by cyber insurance providers, cybersecurity assessments are becoming all the more critical to MSP success.

This white paper will explore the following:

Understanding the cybersecurity assessment

Call it the first law of cybersecurity: “You can’t protect what you don’t know.” In other words, companies that lack visibility into all assets can neither protect their environment nor reduce their attack surface.



As environments have grown well past networks and private hosted applications, the stakes have been raised. Organizations now have to contend with risks associated with everything from IoT and cloud applications to digital supply chains and more. A cybersecurity assessment is the first step to identifying potential risks and vulnerabilities as well as deploying the right tools to remediate them. This holds true both for MSPs and their clients.

What is a cybersecurity assessment?

A cybersecurity assessment examines an organization's ability to protect its information and information systems from cyber threats. The purpose of a cybersecurity risk assessment is to identify, assess, and prioritize risks to information and information systems.

NIST Cybersecurity Framework: The importance of the 'Identify' stage

All businesses can benefit from paying close attention to the NIST Cybersecurity Framework. NIST is the National Institute of Standards and Technology at the U.S. Department of Commerce, founded more than 100 years ago to advance measurement science, standards, and technology to enhance economic security and improve quality of life.

The NIST Cybersecurity Framework is designed to help businesses of all sizes better understand, manage, and reduce their cybersecurity risk and protect their networks and data. Although voluntary, no business that seeks to fully understand best practices for cybersecurity protection can overlook the importance of this source.

According to the NIST Cybersecurity Framework, the cybersecurity journey of any business starts with the **"Identify" stage** (the four other functions include: protect, detect, respond, recover), which establishes the foundation for future success in protecting an IT environment.

NIST

> “***The Identify Function assists in developing an organizational understanding to managing cybersecurity risk to systems, people, assets, data, and capabilities.*** *Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs.*”

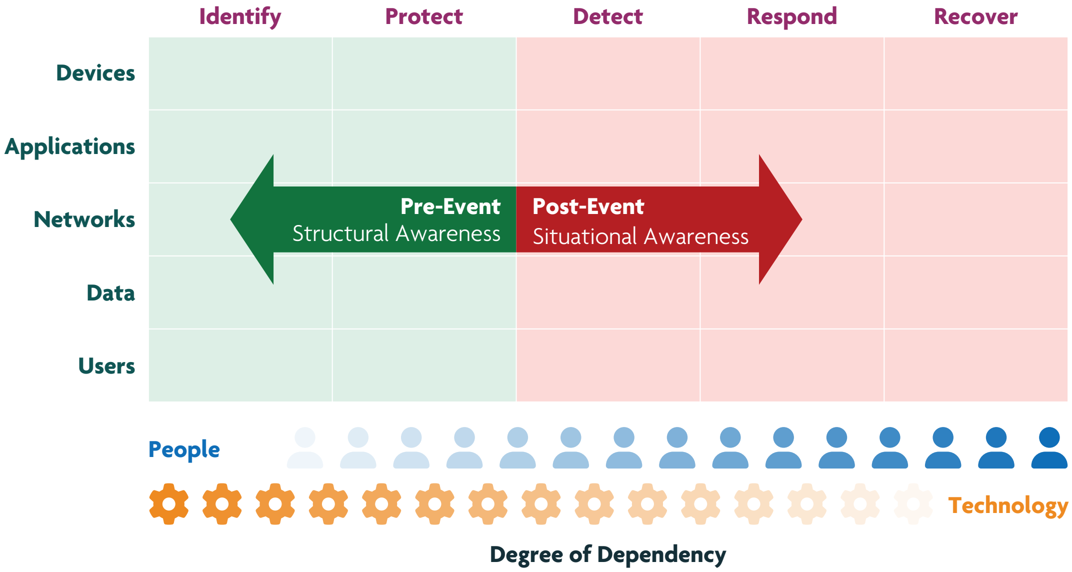
The Cyber Defense Matrix:

For MSPs that are just starting the process of building cyber resilience, the cybersecurity market may seem like a maze. How can a business possibly decipher which services and products it really needs?

Cue the Cyber Defense Matrix, a framework developed by Sounil Yu, a renowned cyber strategist, to help organizations identify gaps in their security posture. The matrix was created to cut through the jargon and inconsistent terminology in favor of clearly articulating product capabilities. By evaluating products and services in accordance with the Matrix, businesses can minimize duplication and assure optimal coverage.

The basic construct of the Cyber Defense Matrix starts with two dimensions:

The first two functions—Identify and Protect—both serve to minimize vulnerabilities, unlike Detect, Respond, and Recover which define what the response to an attack looks like once it occurs. By focusing on Identify and Protect, a business will reduce the number of episodes that require activation of the next three steps.



Five operational functions of the NIST Cybersecurity Framework	
Identify:	Inventorying assets and vulnerabilities, measuring attack surface, prioritizing, baselining normal, threat modeling, risk assessment
Protect:	Preventing or limiting impact, patching, containing, isolating, hardening, managing access, vulnerability mitigation
Detect:	Discovering events, triggering on anomalies, hunting for intrusions, security analytics
Respond:	Acting on events, eradicating intrusion, assessing damage, forensic reconstruction
Recover:	Returning to normal operations, restoring services, documenting lessons learned, resiliency

Five assets classes to be secured	
Devices:	Workstations, servers, phones, tablets, storage, network devices, IoT infrastructure, etc.
Apps:	oftware, interactions, and application flows on the devices
Networks:	Connections and traffic flowing among devices and apps, communication paths
Data:	Content at rest, in transit, or in use by the resources to the left
Users:	The people using the resources listed to the left

The current state of MSPs' cybersecurity practice

The vast majority of MSPs that service SMBs are in the beginning of their cybersecurity journey. But the onslaught of increasingly sophisticated hacks and ransomware attacks is quickly turning considerations into action. Consequently, many MSPs have started to evaluate vulnerability management tools and the possibility of using them for cybersecurity assessments tailored to regulatory frameworks, such as HIPAA, PCI, and FFIEC.

So, what may hold MSPs back? Lets take a look at a few factors that tend to stand out.

Many MSPs suffer from tool fatigue. The sheer number of products and services that they have adopted in recent years tend to make MSPs understandably weary of adding another feature to their portfolio.

Point solutions drive up the price. The patchwork of solutions that MSPs often use comes at a cost, creating an impression that it may be challenging to profitably leverage cybersecurity.

Busy schedules get in the way. The lack of time and bandwidth to perfect their own cybersecurity practice make some MSPs apprehensive about speaking to its benefits with customers and prospects.

Why market dynamics favor cybersecurity assessments

In the past few years, the environment in which MSPs operate has dramatically changed. While the “cobbler’s children go barefoot” mentality may have worked in the past, **the current threat landscape calls for an Assumed Breach mindset**. The assumption that cyber attacks will happen reshapes cybersecurity protection strategies, turning the focus on identifying and addressing vulnerabilities before they are exploited, thereby minimizing the Incident Response (Detect/Response/Recover) cycles the MSP either needs to manage or participate in.

MSPs now have to treat themselves as their first customer, ensuring their own practice is airtight in order to lead credible conversations with prospects and clients about the benefits of using cybersecurity assessments to identify, assess, and remediate vulnerabilities.

Just as endpoint detection and response (EDR) and antivirus software have become second nature to MSPs and their customers, market forces have put vulnerability management next in line for mass adoption. Specifically, the growing importance of cyber insurance for SMBs is prompting questions like, “How are you securing your RMM?” Only this time, it’s the customer seeking an answer from the MSP.

The role of cyber insurance in driving adoption

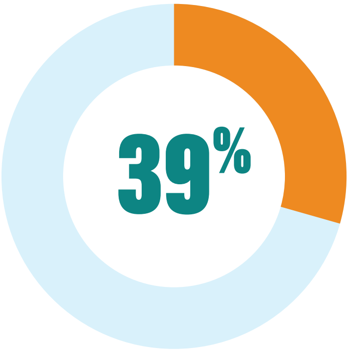
Cyber insurance, also called cyber liability insurance or cybersecurity insurance, is a relatively new and emerging industry. Although a limited number of insurance companies began offering cyber coverage 20 years ago, their share has rapidly increased, from 26% in 2016 to 47% in 2020, according to the U.S. Government Accountability Office (GAO).

The global cyber insurance market is projected to see significant growth over the next few years, from $7.60 billion in 2021 to $36.86 billion in 2028. Fortune Business Insights point to the remote work trend and the notable rise in cyberattacks as driving factors behind projected increase.

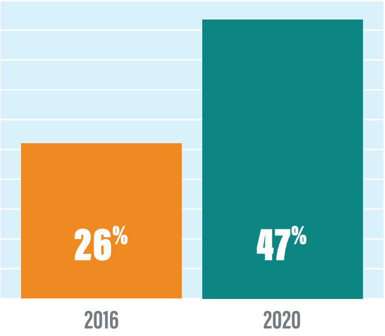
The average cost of a data breach also continues to grow, reaching a median cost of $21,659, although most organizations can expect their costs to rise as high as about $650,000, according to the 2021 Verizon Data Breach Report. When a single breach can take such a financial toll, it gives companies all the more reason to invest in cyber coverage. (39% of all data breaches stemmed from web application compromise)

So, where do MSPs fit in?

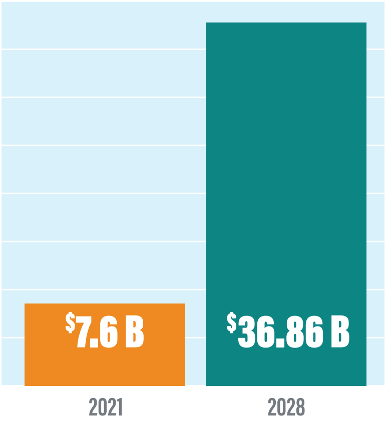
Insurance carriers require policy holders to meet certain criteria to qualify for cyber coverage. And that's where MSPs have a crucial role to play. In their role as managed service providers, they are uniquely situated to drive revenue through security.



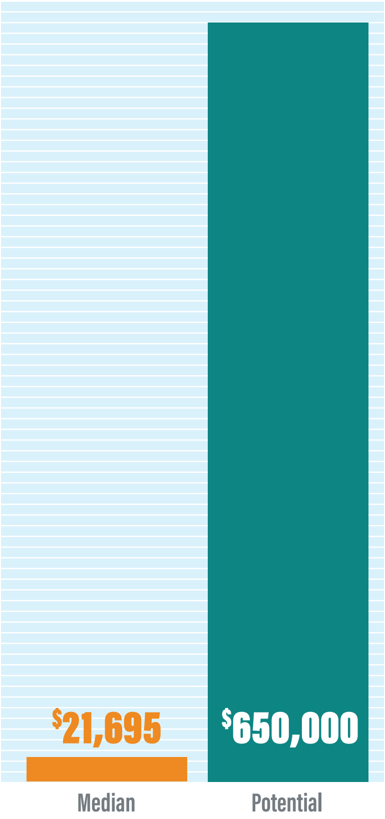
of all data breaches stemmed from web application compromise



Insurance Companies Offering Cyber Coverage



Global Cyber Insurance Market Growth

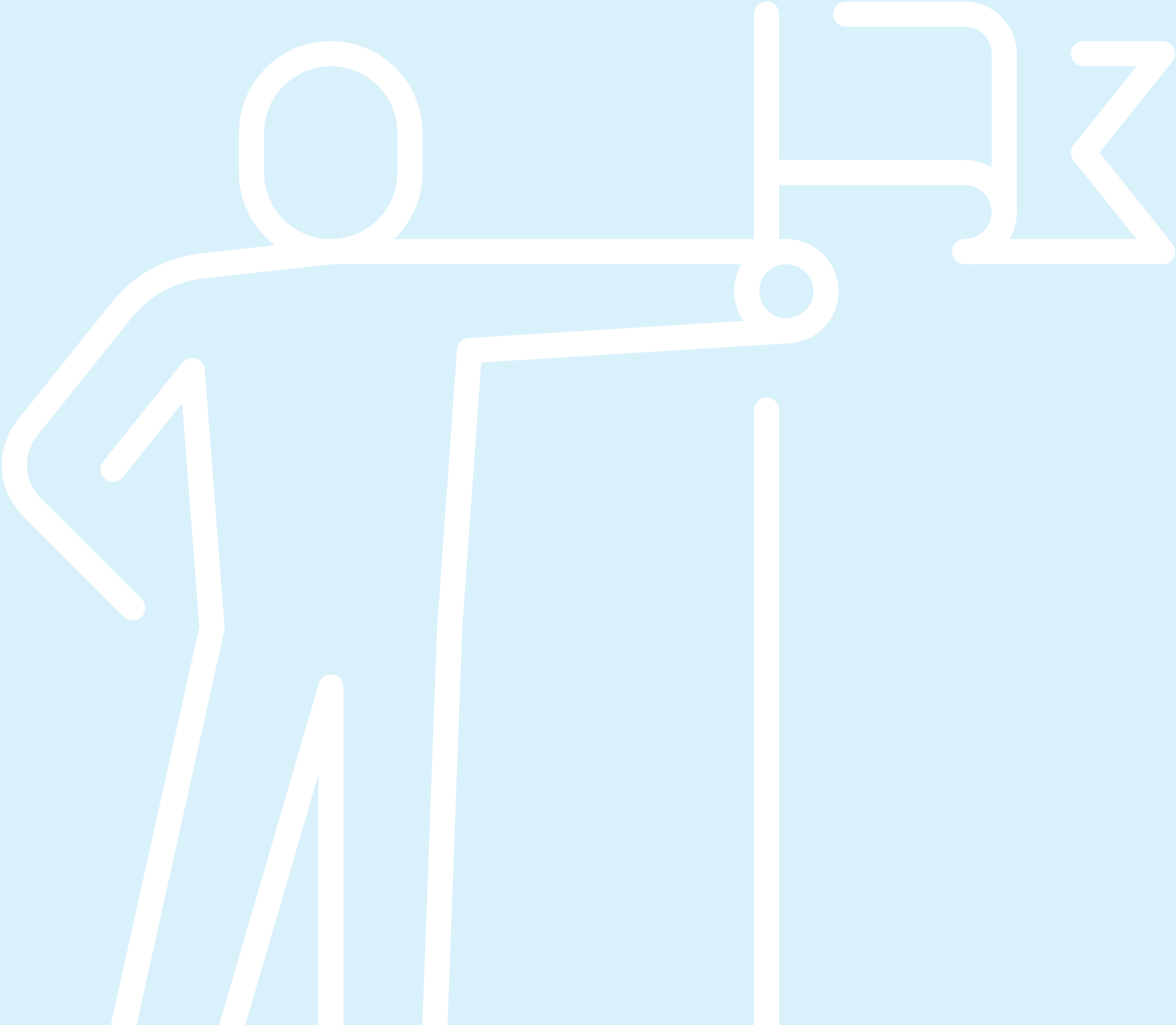


Average Cost of a Data Breach

What MSPs can gain from adopting cybersecurity assessments

Cybersecurity assessments empower MSPs to edge ahead of the competition. By adding this service to their portfolio, MSPs position themselves as credible, trustworthy partners in a volatile threat landscape.

Let's take a look at the reasons why.



It builds credibility

SMBs look to insured MSPs with their own house in order. Customers want their MSP to be an expert partner, mastering specific details on all IT assets. With the help of cybersecurity assessments, an MSP will know exactly what comprises the customer environment and how vulnerable those assets might be. The end result is the customer sees that insight and visibility are being applied, not guesswork, thereby improving trust and positioning the MSP as an indispensable partner to the business.

It meets demand

Cybersecurity assessments signal the MSP is forward-thinking and fully aware of the demands of modern businesses. As outlined above, customers will increasingly need MSPs that can help them check a number of boxes required to get cyber insurance, such as vulnerability management, configuration management, and Active Directory monitoring and management.

The right vulnerability management tool gives MSPs the ability to relay important information during the insurance provider's due diligence process with the customer. This is a critical feature for MSPs that vye for the business of companies most likely to acquire cyber insurance — primarily those that create, store, and manage electronic data online, such as customer contacts, customer sales, PII and credit card numbers.

It enables cyber resilience

MSPs are like patient zero. Building up their own defense and response protocol also means protecting the end customers. In other words, the MSPs reap the benefits of assessing their own cybersecurity practice — and remediating any vulnerabilities — while assuring their customers enjoy the same optimal protection.

It opens up sales conversations

Cyberattacks present an existential threat to SMBs. Yet, a recent CNBC survey showed 56% of small businesses are not concerned about being hacked. But, as Tech Channel writes, executives who believe their companies are too small to merit the attention of bad actors fail to see how t he landscape has changed. In 2020, for instance, 43% of cyberattacks targeted small businesses, according to a Verizon report.

Cybersecurity assessments allow MSPs to open up a discussion about risk. Whether they want to offer a comprehensive assessment or a one-time vulnerability scan to take the conversation to the next level, it gives the providers an opportunity to earn customer confidence while expanding sales.

It adds value (not work)

Cybersecurity solutions that operate in the Identify and Protect segments allow MSPs to automate functions, adding value to the end customer without increasing their heavy workload. The ease of use and automation will help MSPs move along their cybersecurity journey, and provides a "road-map" on how to help the client.

Meet two companies that leverage cybersecurity assessments to win business

snaptech iT

Ask Karl Bickmore about the importance of risk assessments and he'll give a straight answer: they're everything. The CEO of Snap Tech IT, an MSP offering next-generation security services, said the company has turned them into an engine for business growth.

In fact, Snap Tech IT prominently displays risk assessments on the homepage with a direct appeal to heavily regulated industries and their need to ensure compliance standards and best practices around NIST, CMMC, GLBA, SOX, and more. A key feature of the service is the ConnectSecure Vulnerability Manager™, the only tool of its kind designed and priced specifically for MSPs and MSSPs to support their SMB clients.

"We're providing better reporting, better data, better planning, and it's helping us win more deals — like significantly more deals — and our sophistication on what has gone up," Bickmore said.

"It's really up to our needs," he continued. "I can get out there and just run an ad-hoc scan, and there's no additional licensing to happen. It provides us an easy way to have confidence that our tools are working, that we're catching everything in the network and that we're seeing devices and their vulnerabilities — not just computers and servers — but the switches, the infrastructure items…"

And the clients approve, like this VP of technology operations at an advertising agency, "The assessment helped us confirm a lot, more than anything, to provide me a roadmap of what to do to get a security foundation in place. It provided me with support with my CEO to say this is what we need to do and this is what it costs. She loved that! It helped her sleep better at night."

watsec CYBER RISK MANAGEMENT

If there's one phrase that Dennis Houseknecht returns to in his interactions with clients, it's this: "What about the things you don't know?" Houseknecht is the CTO of Waterloo Security (WatSec), a cyber risk management firm, which has made employee security training and ongoing network assessments core components of its service packages.

WatSec has developed the Intelligent Cyber Resilience (ICR) assessment to help business clients quickly understand and resolve cyber exposures, achieve compliance requirements, and maximize return on their cybersecurity investment. The company partners both with MSPs and their clients. After trying a variety of tools, Houseknecht said the ConnectSecure Vulnerability Manager came out ahead because of its "all-in-one" capabilities.

"We're bringing that in as part of our vulnerability assessment and it's giving us a big differentiator from tools we used in the past, which were much more focused on just given vulnerability data," Houseknecht said. "It enables us to provide information to our co-managed IT teams that they either don't have or would have to spend a lot of time and effort to get — and we're basically serving it to them."

Another benefit?

"A lot of our clients really like the fact we have a third-party set of eyes that can come in and validate what the MSPs are doing. We provide what we like to call it oversight. We're also able to give MSPs an independent set of data, so they're not grading their own homework."

What to look for in a vulnerability management solution

At the heart of any cybersecurity assessment is the right vulnerability management tool. But how do you know which vulnerability management solution is right for you — and your clients?

Let's look at few features stand out.

Ability to discover — and perform recurring scans of all IT assets

Gartner points out vulnerability assessment is a function that can be delivered via active scanning, agents and passive monitors, and recommends that organizations leverage a combination of all of the above for complete coverage. Although Gartner tends to focus on enterprises, the importance of breadth of coverage holds true for MSPs and their small-to-medium-sized clients (SMBs) too.

Any asset discovery process and vulnerability assessment must achieve full visibility; in other words, the solution needs to identify and continuously scan all assets in your environment to eliminate any risk of blind spots.

This means the solution must take into account the growing number of people working from home on a full- or part-time basis. External scans show weaknesses in a network that could lead to a potential incident by helping to detect open ports, protocols, and named vulnerabilities in public-facing network equipment such as web servers and firewalls.

At the heart of this process is the vulnerability scanner which should have the capability to discover systems running on your network or that connect via remote access solutions, including:

- **laptops and desktops**
- **virtual and physical servers**
- **databases**
- **firewalls**
- **printers**
- **routers**
- **access points**
- **switches**
- **IoT devices**

Once detected, the scan probes each system for attributes, such as operating systems, open ports, installed software, user accounts, file system structure, system configurations, and more. In order to determine whether they are vulnerable to attack, the information is run through several databases of publicly known vulnerabilities, such as NIST's National Vulnerability Database (NVD) and OEM sources. The results determine what actions should come next (see more below).

Alignment with the NIST Cybersecurity Framework and other important compliance standards

As outlined earlier, the cybersecurity journey of any business starts with the "Identify" stage, which establishes the foundation for future success in protecting an IT environment.

The quickest way to detect vulnerabilities and secure networks? Run an assessment that scans your own and your customer's IT infrastructure for this common compliance standard.

While you can introduce the benefits of NIST compliance to your end customers, the right vulnerability management solution gives you the ability to support other standards as well. Depending on which industries your clients are in, they will benefit from your support for compliance standards like PCI DSS, HIPAA, GDPR IV, NIST 800-53, NIST 800-171, CIS, CIS 8.0, ISO 27002, Cyber Essentials and Essential Eight.

Ease of use and easy-to-understand reporting that clearly articulates risk to the business for end customers

Whether you want to build customized reports with a user-friendly drag-and-drop editor or have data automatically presented, your vulnerability management solution should not make you choose. **Easy-to-understand reporting is essential to busy MSPs**. The ability to clearly articulate business risk is a key piece of how you can bring value to your end customers; and an actionable and intuitive dashboard that shows what needs to be addressed can help you achieve that goal.

The ease of reporting should cover every aspect of the Identify stage of the NIST Cybersecurity Framework, allowing you to present a range of reports in standard Microsoft Office formats (Word, Excel, PowerPoint), such as:

- **Asset reports**
- **Vulnerability reports**
- **Compliance reports**
- **Remediation reports**
- **Security posture reports**
- **Build your own**
- **Active directory reports: identifying misconfigurations, weak policies, and privilege user access**

TechTarget

> “*A vulnerability management tool must be easy to deploy and use, reliable, nonintrusive and safe — that is, it poses few conflicts for an existing IT environment. A product that is cumbersome to navigate or presents confusing dashboard information won’t be used, at least not to its fullest potential.*”

Key features of an easy-to-use solution include, for instance:

- **Integration to industry standard PSA systems**
- **Availability of a one-time scan which opens an opportunity to talk about risk with your customer**
- **Multi-tenant view to all MSP clients**
- **Strong role and access-based security for co-managed clients**

Ability to prioritize remediation of vulnerabilities

Just showing customers their vulnerability risk exposure is no longer sufficient. As important is having the ability to mitigate those risks. Not all vulnerabilities, however, bring the same risk of exploitation. Therefore, consider a solution that, once you have identified the vulnerabilities, lets you categorize them based on their potential impact if you were to face a cyberattack.

Ratings and scores, such as Common Vulnerability Scoring System (CVSS), an open framework for communicating the characteristics and severity of software vulnerabilities, inform the evaluation and determine which vulnerabilities should take priority. The scores are not a catchall but one of many factors that contribute to accurate vulnerability identification with low false positive rates. Given the broad data sets analyzed, **effective prioritization is crucial to addressing risks with the highest likelihood of exploitation in the near future**.

Look for a solution that includes an Application Patching feature that helps remediate vulnerability by patching third-party Windows applications. This greatly helps reduce risk exposure and serves to safeguard the network from external actors. To cite Gartner, organizations that leverage risk-based vulnerability management will suffer 80% fewer breaches.

CONCLUSION

As the threat landscape grows more complex, MSPs have an unprecedented opportunity to introduce the importance of building cyber resilience to their SMB customers. Just as using firewalls and virus software have become second nature to businesses, vulnerability management will be an indispensable feature of the future. The cost of leaving business networks vulnerable to exploitation is simply too high.

By gaining a prioritized view of their SMB clients' vulnerabilities, MSPs gain just the selling leverage they need — it becomes their ticket to winning business.

CONNECTSECURE

About ConnectSecure

ConnectSecure is a cybersecurity company exclusively focused on serving Managed Service Providers (MSPs). Founded by MSP industry pioneers, ConnectSecure leverages a collaborative model for product development that integrates MSP insights. The ConnectSecure purpose-built, multi-tenant, all-in-one B2B cybersecurity platform allows MSPs to build cyber resilience and drive business by uncovering and remediating vulnerabilities of their small to medium-sized business clients.