VOLUME 4

Securing Against Rising Threats

SMB dynamo

The People and Cisco Technologies Propelling Small and Medium Businesses

Technology Trends

Digital Journeys

Expert Perspectives

Story Links

Technology Trends

SMBs prioritize security as cyber attacks escalate

Why SMBs should start adopting "zero trust" security

How to make passwords more secure

Digital Journeys

What it takes to recover from a cyber attack

How to protect digitized production lines

Expert Perspectives

How to reduce cybersecurity insurance premiums

What you need to battle ransomware

Assessing your security like a hacker

If you want additional information about the technologies featured in this edition of *SMB dynamo* or have story suggestions for future editions, please contact us at dynamo@cisco.com.

The new forces shaping cybersecurity for SMBs

Running a small or medium-sized business is hard enough without trying to keep up with something as complex as cybersecurity. So, it's understandable why many SMBs choose to take only minimal precautions –at least until it's too late.

Unfortunately, more SMBs than ever are learning lessons the hard way. In fact, IDC now predicts one third of them will experience security breaches every three months; business disruptions will on average last one week.

Long gone are the days when only large enterprises were big enough for cybercriminals to bother hacking. Ransomware attacks are now largely automated and highly efficient, capable of profitably targeting businesses of all sizes. Smaller organizations, with their less mature security practices, can make for easy pickings.

This edition of *SMB dynamo* looks at how businesses can adapt to the forces shaping cybersecurity today: from the growing role of cyber insurance, the concept of "zero trust", and the move away from passwords; to how businesses can stop ransomware, as well as use an innovative tool to affordably identify potential vulnerabilities. We also examine what it took for one family-run Spanish manufacturer to recover from a pervasive malware infection.

Taken together, the costs of inaction have never been higher for SMBs. May *SMB dynamo* help illuminate a direction toward better protection for your business.

– *SMB dynamo* editorial team

Technology Trends

Repelling the onslaught

SMBs prioritize security as cyber attacks escalate

Cybersecurity is rarely a strength of small and medium-sized businesses. Only about two out of every five companies this size even have a full-time IT person (or equivalent) on staff, according to IDC's Worldwide Small and Medium Business survey, from February 2022. Of those IT employees that do exist at these smaller businesses, many are generalists with a host of responsibilities. The inherent complexity of security, as well as the fact that such safeguards don't drive revenue or attract new customers, often leads to security-focused projects getting pushed to the back burner.

But in the wake of the pandemic, that's changing. With cyber attacks like ransomware increasingly automated, SMBs are now a more profitable target.

"The widespread shift to remote work has been a boon for cyber attackers," says Katie Evans, SMB research director at IDC, noting the increased exposure and risk when employees access business-critical systems from remote locations, networks, and devices outside of offices with dubious safeguards. "SMBs are particularly vulnerable because their IT security capabilities are often less mature than large enterprises."

Based on its latest research, IDC predicts 33 percent of SMBs will experience IT security breaches on a

quarterly basis by 2024, resulting in at least one week of business disruption every three months. It's a wakeup call many are heeding.

"Half of the SMBs we've polled said increasing security is a technology priority over the next 12 months," says Evans.

The challenge is, how do they mount a better defense with minimal IT resources?

"IT specialists wear many, many hats"

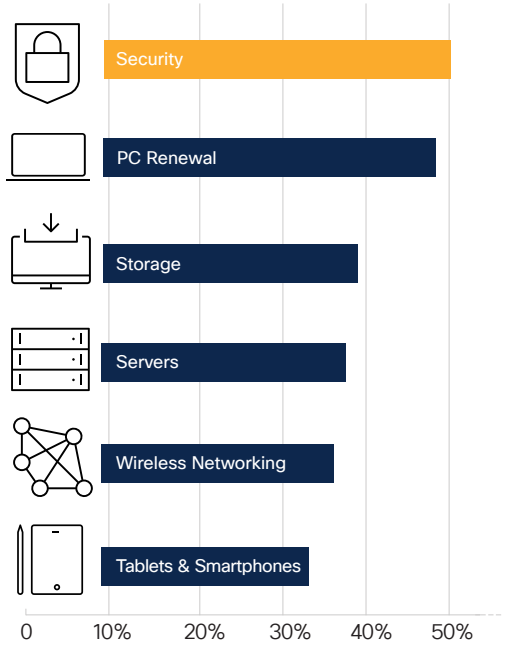
Small and medium-sized businesses are often mistakenly thought of as young, scrappy, technology-savvy startups. The reality is that many SMB entrepreneurs began building their businesses a decade or more ago, often with a different view of IT. IDC's survey reveals 34 percent of small and medium-sized businesses have been in business for 10 to 20 years, and another 36 percent have been in business longer than that. That suggests that at many of these older companies, technology in general, and cybersecurity in particular, may not be a core business priority.

"IT specialists at small companies wear many, many hats," says Evans. "They're tasked with addressing employee technology needs and issues, web presence, server and cloud infrastructure, finance and payroll systems, communication and collaboration tools, sometimes point of sale, sometimes marketing automation, you name it."

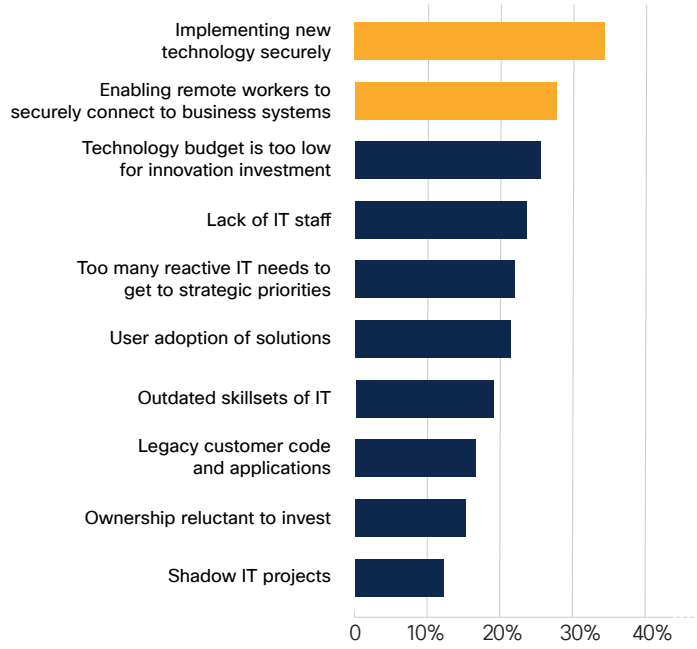
IT security a top priority for SMBs

By 2024, **33%** of SMBs will experience security breaches **every 3 months** resulting in at least **1 week** of business disruption

Which of the following Infrastructure & Device areas will be technology priorities for your company in the next 12 months?



What are the largest technology challenges in achieving your business priorities?



Source: IDC, 2022 Worldwide Buyer Behavior Snapshot, Doc # US49058522, May 2022

In fact, IT security is often seen as a prime barrier to achieving business goals. When IDC asked SMBs about their largest tech challenges in achieving business priorities, the top two concerns relate to security: implementing new technology securely; and enabling remote workers to connect securely to business systems.

Insurance driving security requirements

Despite these challenges, the costs associated with mitigating business risks are pushing SMBs to get their arms around cybersecurity. Skyrocketing cyber insurance premiums have put a clearer ROI on taking action. (See "A roadmap to cybersecurity insurance," page 17.)

Cisco Secure cyber expert Wolfgang Goerlich hears this regularly. "Insurance is a hot topic," he says. "In previous years, security was driven by regulatory requirements or customer requirements. Now, for the first time ever, insurance companies are the ones driving this. Insurers have been really strong at encouraging good controls and maintaining security hygiene." (For more from Goerlich, read "How SMBs can adopt "zero trust" security," page 8.)

Integrating security solutions

All of these trends provide SMBs with ample reasons to review the IT security measures they have in place.

> "In previous years, security was driven by regulatory requirements or customer requirements. Now insurance companies are the ones driving this. Insurers have been really strong at encouraging good controls and maintaining security hygiene."
>
> **Wolfgang Goerlich**
> Advisory CISO,
> Cisco Secure Access by Duo

The good news is most SMBs already have some form of security, whether it's antivirus software, network firewalls, or cloud-based backup and recovery.

And the bad news? These tools are typically a collection of independent solutions that make monitoring cybersecurity difficult for a single SMB IT person to take on in addition to his or her other duties. An often-staggering number of alerts ultimately get ignored because of the time, effort, and skill required to investigate and validate them.

"It's easy to become overwhelmed with tools and alerts," says Albert Salazar, the director of product management at Cisco SecureX. "SMBs need an easy-to-use platform that brings together the security solutions they already have."

> "SMBs are seeing the threats, and they know they need a strategy for protecting their business and responding in the event of an attack."
>
> **Katie Evans**
> SMB research director, IDC

Included with every Cisco Secure product, Cisco SecureX addresses this need, combining multiple, otherwise disparate sensor and detection technologies into a single platform. It delivers unified visibility across Cisco Secure and third-party security solutions, as well as intuitive automation controls.

"SecureX provides the simplicity SMBs need to identify, prioritize and respond to threats within their environments," Salazar explains. "If you have one of our security solutions, you have access to it, and you'll see how helpful it is to have information from multiple tools all in one place."

Learn more about SecureX

To experience SecureX with your Cisco Secure product, click on the banner in your dashboard.

As the complexity and costs of cybersecurity threats rise, many SMBs are taking a hard look at how they protect their businesses.

"They're seeing the threats and understanding the risks," says IDC's Evans, "and they know they need a strategy for protecting their business and a plan for responding in the event of an attack." ■

Understand the benefits of zero trust security, and how to get started:

Attend a zero trust workshop

How SMBs can adopt "zero trust" security

A conversation with J. Wolfgang Goerlich, advisory chief information security officer for Cisco Secure Access by Duo

SMB dynamo: What is "zero trust" and why does it matter to SMBs?

Wolfgang Goerlich: Zero trust sounds like another IT buzzword, but it represents a new approach to protecting an organization's devices and applications. Zero trust is a security architecture that expands protection beyond a company's firewall, which is important in the age of mobile devices and the cloud. It establishes a perimeter wherever and whenever access is required, so ideally, all users and devices are continuously validated as they connect to applications and data. For SMBs, the technical details are less important than knowing that U.S. federal government departments and agencies are beginning to adopt this strategy. These kinds of regulations start with the agencies, but sooner or later, they move down the supply chain and affect smaller companies.

SMB dynamo: Is there value in SMBs adopting a zero trust approach in the near term?

Goerlich: Some business owners will say, "I will worry about that later." I've had conversations with others who say that having these security controls in place will give them an advantage when competing for contracts. The growth in cyber insurance coverage is also starting to drive this. Most cyber insurers are already saying they won't renew coverage without MFA [multi-factor authentication], which is one component of zero trust, and they've begun asking about zero trust practices. This suggests in a couple of years, insurance will be requiring zero trust as well.

"These kinds of regulations start with the agencies, but sooner or later, they move down the supply chain and affect smaller companies."

Wolfgang Goerlich
Advisory CISO, Cisco Secure Access by Duo

SMB dynamo: What does a zero trust strategy look like for an SMB?

Goerlich: While creating a zero trust architecture is not a simple undertaking, SMBs can take early steps. They can start by asking their security vendors and managed service providers, 'What is your zero trust story? What is my clearest, quickest path to success?" Broadly, there are five areas to address: people, devices, network, application workloads, and data. If you have a product like Cisco Secure Access by Duo, which was created to make zero trust easy and accessible to companies of any size, it's a matter of enabling the features, then rolling it out to your workforce, devices, and applications. The other domains, such as networks and application workloads, will still need to be considered. The good news is SMBs have time to prepare. ■

3 Takeaways

1. Cyber insurers are beginning to ask about zero trust practices
2. Multi-factor authentication is one component of zero trust
3. Start by asking whether IT has good coverage of all people, devices, and applications

Solving a problem like passwords

How SMBs can get smarter about verifying that only the right users have the right access

Passwords have long been a necessary but faulty form of security. According to Verizon's 2022 Data Breach investigations report, about half of all breaches involved stolen or weak credentials.

The risks passwords pose only intensified during the pandemic. "Once remote work took hold, so many more businesses moved more applications to the cloud," says Omar Zarabi, founder and CEO of Port53 Technologies, a Cisco Partner. "Many small and medium-sized businesses focused on enablement first and security second. The password jungle grew and became unwieldy."

A higher volume of passwords exacerbates other issues. The biggest is that users have a hard time remembering all of them—51 percent of them forget or reset a password every week, according to research by Duo Security, a division of Cisco Secure—which leads to 57 percent of them reusing the same password on multiple sites.

At the same time, cybercriminals have been finding more insidious ways to steal company passwords,

whether through phishing or targeting insecure home and public Wi-Fi network connections. Combine that with more automated ransomware attacks, and SMBs become profitable, low-hanging fruit.

Passwords have now become a dangerously weak link in the chain. “Companies typically had to worry about attacks to their networks. Now they have to worry about attacks on identity and access,” says Zarabi. “As a result, IT has to find a way to protect everywhere, all the time.”

Securing passwords with context

While replacing passwords altogether would be ideal—instead establishing a user's identity through biometrics, security keys, or a mobile device, for example—the reality is that for many SMBs, passwords will remain a vital part of effective cybersecurity.

“Even though passwords are problematic, they are important,” says Zarabi. “To secure them, it’s important to layer on other access control techniques or contextual understanding.”

Multi-factor authentication (MFA) is one critical technique. MFA uses a second, separate form of identity validation before granting access to data and applications. This combines something a user knows (the password) with something only they have, like an alert on their phone. Combining passwords with MFA helps to ensure that only the right people have access to the right types of company data.

“Identity is the new perimeter,” says Ted Kietzman, Product Marketing Manager at Cisco Secure Access by Duo. “Previously, if you authenticated once onto the network, you were trusted. Now companies need to get more granular than that by verifying identity and devices.”

This kind of security practice is increasingly required through industry regulations and insurance. “Cyber liability insurance is driving a lot of our MFA conversations,” says Kietzman. “Companies need to have MFA in place to get a lower premium.”

Taking steps towards MFA

The good news is that many SMBs often already use some MFA for certain applications or platforms, and most of their employees are familiar with it through their consumer devices. The challenge is ensuring that MFA is used consistently across your IT environment, whether in the cloud or otherwise.

Learn how passwordless authentication can benefit organizations of any size:

Duo Passwordless: Expert Tips and Your Questions Answered!

Zarabi recommends three key steps:

Step 1: Understand the scope — Begin by auditing what applications are in use, which require login credentials, and which users use them. Also, are those applications provisioned by IT or are they being used personally? Gaining an understanding of login activity can help you identify where MFA can mitigate vulnerabilities.

Step 2: (Re)gain control — If you determine passwords in your organization are like the Wild West, with little to no oversight, consider a tool that can help IT retake control through automated management.

Step 3: Implement easy-to-use MFA — The most effective security tools are the easiest to use—for both IT and especially users—so there’s little incentive to work around them. Look for MFA solutions that are straightforward to deploy on-premise, in the cloud, or a hybrid of the two; simplify enrollment of current staff and new hires, ideally with a self-service option; and offer a range of second-factor authentication methods, in particular push notifications to a mobile device.

For better or worse, passwords will likely remain as one weapon in SMB’s security arsenal. Fortunately, new techniques are now readily accessible to bolster your password programs to better verify user identities and mitigate your business risk. ■

Digital Journeys

Like fighting air

How one Spanish manufacturer recovered from a cyber attack

Enrique Villaverde knew his company's network was not performing correctly. Employees at Megablok, his family-owned manufacturer of lockers based in Zaragoza, Spain, often lost connections on their desktops. Some were so frustrated that they asked to work from home, where connections were more reliable.

"We spent many months with complaints and discomfort," says Villaverde, CEO of the 25-year-old company with 80 employees and no full-time IT staff. "It's infuriating because you don't know what you're fighting, nor how to find it. We expanded the broadband, re-verified the cabling, but the problem continued. It was like fighting the air!"

Then, just as the pandemic was forcing Spain into lockdown, the already bad situation turned much worse. Customers started receiving fake invoices that appeared to come from Megablok but included a different bank account number for sending payment.

"Now it wasn't just a problem of our productivity slowing down," says Villaverde. "Now our image was being damaged. That was when the alarm bells sounded."

Thousands of malicious connections

For help, Megablok turned to Orbe Seguridad, a Cisco Premier Partner also located in Zaragoza.

Daniel Sánchez Yuberto, director of engineering and technology at Orbe, was surprised by what they found. "In these cases, our incident response team first deploys Cisco Umbrella to monitor all DNS outgoing traffic," he says. "We observe all connections established by all the endpoints and block all malicious connections serving malware, phishing, cryptomining, or command-and-control."

The situation was more serious than either Villaverde or Sánchez could have imagined. "It was incredible," says Sánchez. "Thousands of connections to malicious domains had been established."

Curing the infection

Although shocking, the cyber attack on Megablok was not particularly unique. Through the first two years of the pandemic, security risks quickly grew for many companies as more employees began working from home, often on unsecured networks or personal devices. Many organizations also rapidly adopted new technologies to automate operations, improve safety procedures, or allow remote access. Given their limited resources and lack of IT expertise, SMBs were often easy targets.

Fortunately, Megablok had Orbe to help recover before its business suffered irreparable harm. Sánchez's team worked quickly to identify the endpoints and the

users who were unknowingly originating the malicious traffic. “Within a day, Megablok network outages were gone,” says Sánchez.

More security challenges remained, however, including the hundreds of phishing emails Megablok received each day. Employees were unsure of which emails were legitimate, and this had begun to negatively impact customer relationships.

And those fake invoices? They were likely the result of a so-called “man in the middle” attack, in which cybercriminals steal the credentials of some company employees. They read the victim’s email and can then respond with an email that uses a domain name very similar to the victim’s, display it as an alias, and effectively communicate as if they represented Megablok.

To protect Megablok inboxes, Orbe deployed cloud-based Cisco Secure Email and urged all users to update their credentials. Almost overnight, the volume of phishing e-mails dropped dramatically. Suddenly users could trust their email again and focus on the business at hand.

Finally, Orbe also had to scrub the malware that had infected many endpoints. “We configured and deployed Cisco Secure EndPoint,” says Sánchez, “and integrated all of the solutions into Cisco SecureX, so we were able to easily investigate threats, isolate infected endpoints, and remove installed malware.”

Funding the recovery

The improvements to Megablok’s operations were immediate: connectivity issues disappeared and Villaverde gained peace of mind knowing its infrastructure was better protected.

As with any smaller business with limited resources, the cost of achieving such protection required careful consideration. “We knew we needed to adopt the new technology in order to recover from the attack and help the business remain productive,” says Villaverde. “But as a smaller, family-run business, evaluating the costs felt overwhelming.”

Orbe connected Villaverde with Cisco Capital, which in turn worked with global vendor financier DLL to find a flexible payment solution that worked best for Megablok. As a result, the company was able to streamline the total cost of the project, bundling Orbe’s managed services into a predictable payment, and avoiding any upfront costs.

“Knowing that we were able to make set payments over time meant we didn’t have to make cuts to other areas of the business and could better manage budgets,” says Villaverde.

Now that Megablok has recovered from the security breaches, Villaverde and his employees can once again work without worry. “Now we can get back to taking care of what we really need to be doing: production manufacturing,” says Villaverde, “and running the family business that my parents, sister, and I created 25 years ago.” ■

Learn more about how Orbe Seguridad managed cybersecurity services protect SMBs.

Watch the full video:

Orbe Seguridad's 4-step recovery plan

1. Address the network outages – Monitor all DNS outgoing traffic with **Cisco Umbrella** to observe all connections established by all the endpoints
2. Protect email as a critical communication channel – Deploy **Cisco Secure Email** and update all access credentials
3. Clean the malware from endpoints – Configure and deploy **Cisco Secure EndPoint**
4. Integrate on one platform – Implement **Cisco SecureX** as a single security management system for easier ongoing monitoring

Learn more about Cisco IOT and how Vem Sistemi helps SMBs manage and mitigate cyber risks.

Securely connecting smarter factories

How manufacturer DECO Industrie protects its digitized production lines

Upgrading phones, laptops, and printers is one thing. Modernizing industrial machines that have been in place for decades is quite another.

DECO Industrie opened its first factory in 1951. The Italian manufacturer has grown slowly but steadily since then, expanding its focus from household detergents to food and cosmetic products. Today, the company has six production plants, all of which are being modernized with technologies built for big factory settings but with a price tag and simplicity that make them attainable for SMB manufacturers.

"We've always kept an eye on new technologies that enable us to grow in new markets, monitor quality, keep costs under control, and improve productivity," says Antonio Campri, president of DECO Industrie.

Real-time industrial data

The company recently upgraded the machines on its production lines so they could connect to the internet and each other, all tied together with a Cisco IoT network designed for rugged industrial environments. For the first time in its 71-year history, DECO Industrie has a birds-eye view of its factory floors, with real-time data that helps inform and optimize business operations.

"DECO understood the more data they get from their production plants, the more they can drive efficiency and quality," says Marco Bubani, head of innovation at Vem Sistemi, DECO Industrie's IT services provider and Cisco Gold Certified Partner.

Securing connections

But with connectivity comes vulnerability, so the company made sure to reinforce its industrial network and machines with a number of security solutions. Cisco Identity Services Engine (ISE) is helping monitor and control who can access the network and when. Cisco Industrial Network Director (IND) is providing full visibility of factory automation devices and processes. And Cisco Industrial Security Appliances (ISAs) protect every machine from malicious or unwanted actions.

"A general-purpose network infrastructure couldn't support DECO's digitization journey," Bubani explains. "They needed a factory-focused network infrastructure that is designed for industrial environments, devices, and applications."

The IoT network is fully separated from DECO Industrie's corporate network, he explains, with an "industrial DMZ" that allows secure data exchange between the company's factory environments and business offices.

"We cannot miss the chance technology offers us to make it possible for machines to dialog with humans," Campri says. Finding ways to securely deploy the latest technology in support of smarter manufacturing are the kind of strategies that will help this 70-year-old company continue growing for another seven decades. ■

Expert Perspectives

A roadmap to cybersecurity insurance

How to maximize protection and minimize premiums

In Ed Zarrell's recent conversations with business owners, the same topic keeps coming up: cybersecurity insurance. "By now most leaders have, at the very least, heard stories of companies they know being attacked by ransomware or data breaches," says Zarrell, sales director at Cisco partner LA Networks in Los Angeles. "The apprehension this creates, and knowing that ransomware is not going away, is driving interest in cybersecurity insurance."

Concern is warranted. Small businesses suffered 40 percent more ransomware attacks in 2021 than the previous year, according to cyber insurance provider Coalition, which comes in the wake of a 2020 ransomware tsunami as SMBs shifted to remote work. The average cost of a cyber insurance claim in 2021 rose 56 percent.

Large organizations were once the primary victims of cybercrime, but attacks today are increasingly automated, turning vulnerable small and mid-size businesses into profitable targets. As Zarrell notes, "No organization is immune."

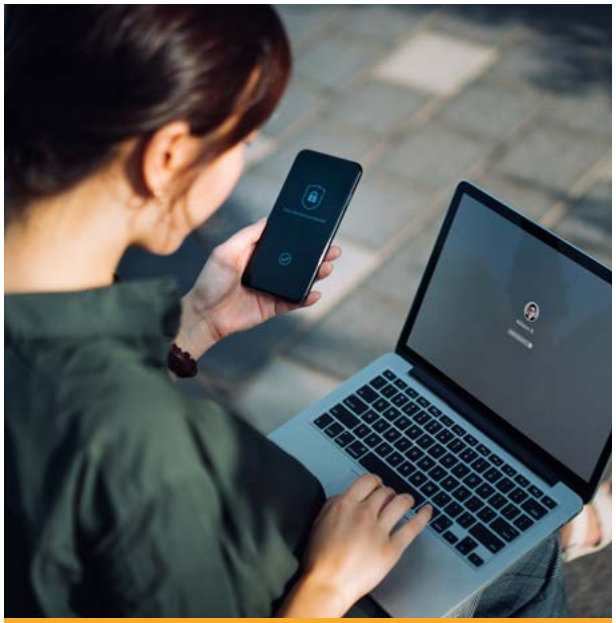
In the event of a cyber attack, having the right insurance policy can provide peace of mind by mitigating potentially crippling financial payouts and covering costs such as business disruption, legal fees, forensic analysis, and more. However, purchasing coverage comes with its own challenges.

Pricey premiums, but even pricier if you get hit

SMBs who seek cybersecurity insurance often feel sticker shock. Premiums have skyrocketed as insurers struggle to forecast risk amid spiraling claims.

According to Cole Haney, an assistant vice president in the cyber practice at insurance broker Brown & Brown, premiums have more than doubled in recent years due to the rise in ransomware. Despite the higher price tag, insurance still buys many SMBs peace of mind that they won't get hacked out of business. But to even qualify a company for coverage, insurers are now also requiring that they implement higher IT security standards to prevent attacks from occurring.

"If you're struggling to qualify for cyber insurance, being offered higher-than-average premiums, or seeing a long list of coverage exclusions," says Haney, "that's a strong sign you need to assess your security posture and consider tools and controls that could make it stronger."



5 essential security measures required by cyber insurers

1. Multi-factor authentication
2. Endpoint detection and response
3. Data backup and recovery strategy
4. Secure remote access
5. Next-generation firewall

Start with MFA

Haney says the simplest yet most effective tool to lower premiums—and increasingly a requirement to even qualify for coverage—is multi-factor authentication (MFA). Mandating two or more types of identity verification to access applications and IT systems, often using a phone or token as with a tool like Cisco Secure Access by Duo, can prevent up to 90% of cyber attacks, according to US national security cyber chief Anne Neuberger. "Insurers consider MFA the single most important aspect determining an organization's ability to qualify for coverage," Haney says. "Without it, you're essentially leaving the doors to your network unlocked."

But MFA is only one cybersecurity cornerstone that insurers require. Haney notes three other key elements that a business needs: Endpoint detection and response, which identifies threats across an IT environment; data backup and recovery plans with regularly scheduled backups; and a Remote Desktop Protocol that is not exposed outside the company firewall.

To assess risk and price their coverage, insurers require SMBs to complete an exhaustive evaluation, which Haney says can also help SMBs identify security gaps. "They're assessing the level of employee training, such as how aware your staff are of phishing techniques," says Haney, "as well as your software patching cadence, and whether you have tools like privileged account management and email filtering."

Read LA Networks' approach to cybersecurity insurance

Watch the webinar, Cybersecurity Insurance and MFA: What You Need to Know

Security that pays for itself

Working with the right partner can help simplify what steps to take. LA Networks has developed a cybersecurity assessment tool of its own to gather comprehensive information about a customer's security profile, identify vulnerabilities, and create a roadmap for addressing them over the short and long term. "With the right approach, even small businesses can get to a point where they have an extremely secure, multi-layered security stance," says Zarrell. (A mini-assessment sample is available on its website.)

While business leaders can feel overwhelmed by cybersecurity requirements, Zarrell contends that the right tools ultimately pay for themselves: not only do they dramatically reduce the likelihood of a costly cyber attack, they also help a business access much better insurance rates.

"If you have, for example, Cisco Secure solutions such as Duo for MFA, Cisco Umbrella for DNS web security, a next-generation firewall, and effective anti-virus protection," says Zarrell, "with these easy-to-implement tools you're putting your business in a much better position to qualify for cyber insurance and get a relatively low premium." ■

Battling ransomware

Why you need both a first and last line of defense

Learn how simple it is to secure your organization:

Cisco Umbrella

Small Business Endpoint Security

Cisco SecureX

By Eric Howard, Cisco Security Technical Leader

Ransomware attacks now move faster than ever before. Research from Cisco Secure shows that attackers, by using increasingly automated processes, can infect your system, encrypt your data, and deliver a hostage letter all in a matter of hours, if not minutes.

How can a small business protect against something that moves so fast? It helps to first understand how these attacks work.

Anatomy of an attack

Ransomware is the result of a multistage infestation of IT systems. Several components are involved in an attacker gaining access to a system and locking away files until payment is made.

It starts when a user clicks on a malicious web link (often in an email), which triggers the delivery of a weaponized file that might look like a Word doc or PDF, but in fact contains code that 1) steals information, and 2) gives attackers control of the device.

But one device is never enough for a ransomware payout. So the attack utilizes that device to execute further exploits across other devices and go deeper into your network, possibly gaining access to Active Directory domain controllers or main servers.

Coordinate your defenses

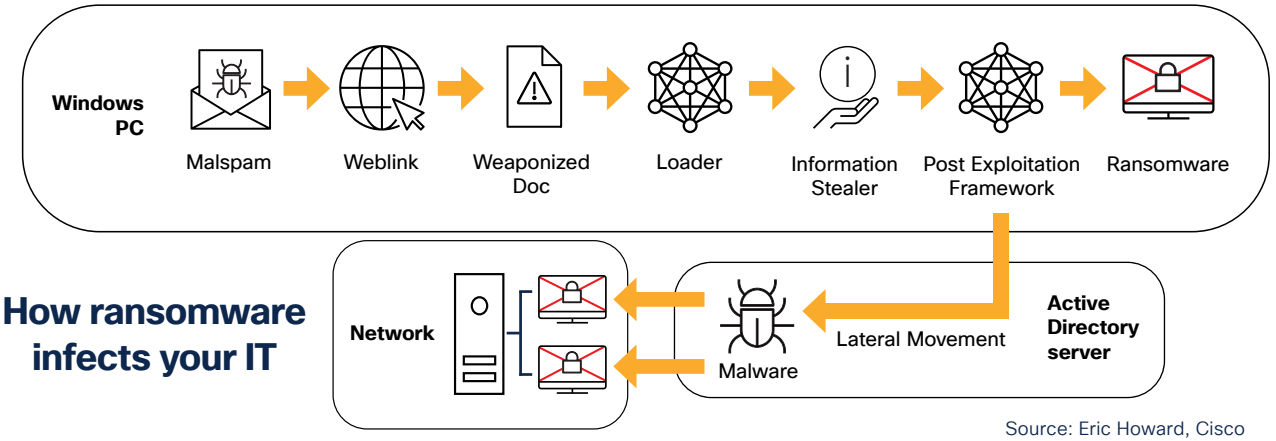
Your first line of defense is to monitor and ideally block web traffic to malicious links. DNS (domain name system) is an Internet protocol that maps domain names to IP addresses. A DNS lookup is the very first step of any attempted connection: before a device can connect to any IP and receive data from it, a DNS lookup has occurred.

DNS exploits are often woven into ransomware attacks, either to infect or to control. By using DNS monitoring—forwarding all your DNS lookups through a security solution like Cisco Umbrella—threats can be blocked earlier before a connection is ever made back into a device on your network.

Your last line of defense is endpoint security, which monitors the potentially malicious processes running on devices connected to your network.

By layering both DNS monitoring and endpoint security together using Cisco Secure X, which also offers automated workflows, your security professional or Partner can efficiently connect the dots between suspicious web traffic and the devices that initiated the DNS lookups in the first place.

With fast-moving ransomware, these two critical security tools provide the information needed to isolate a fast-moving ransomware infection before it spreads. ■



How ransomware infects your IT

Source: Eric Howard, Cisco

Learn how Port53 penetration testing services help maintain a proactive security posture.

Assessing your security like a hacker

How a new online tool promises affordable penetration testing

"You don't know what you don't know until you know it."

This idiom certainly applies to cybersecurity. Because a company's vulnerabilities and risks will persist—and likely be exploited—until they are identified and mitigated.

But how do you know how exposed your company's systems and data really are? One proven strategy is to authorize a simulated cyber attack and see what happens.

This is the approach many large enterprises take. Armed with technology specialists and ample financial resources, these companies continuously assess and fortify their security through routine penetration testing. But for small and medium-sized businesses, these advanced "pen tests" are often out of reach.

"SMBs know they need to perform deeper, more frequent assessments to identify security gaps," says Omar Zarabi, founder and CEO of Port53 Technologies, a Cisco partner based in San Francisco that helps small businesses leverage enterprise-grade, cloud-delivered security solutions. "But traditional pen tests are highly manual, take up to six weeks, and can be prohibitively expensive."

As a result, most SMBs avoid security assessments altogether. Those that are required to validate their cybersecurity protection—for compliance, insurance, or legal mandates—typically do so with fast, infrequent vulnerability scans that provide a limited amount of information.

"A vulnerability scan is like making sure all of the doors and windows on your house are locked. A penetration test goes much deeper to determine what can be compromised if something gets in," Zarabi explains. "Both are vitally important, so we need to make them more accessible for SMBs."

It's not lip service.

Port53 will soon release a cloud-based, highly automated tool that performs both external vulnerability scans and internal penetration tests. According to Zarabi, the tool will integrate with Cisco SecureX to automate the deployment of fixes and patches for newly identified security gaps.

"It's fairly revolutionary to have these tests automated and delivered from the cloud," Zarabi says, noting the tool performs vulnerability scans using IP addresses and penetration tests over a secure connection. "Once you take humans and tedious manual processes out of the equation, frequent, in-depth testing becomes much more viable for SMBs. And it's always better to have a continuous, comprehensive understanding of your vulnerabilities than a snapshot in time that only reveals part of the picture."

After all, you don't know what you don't know until you know it. ■