Forbes INSIGHTS

2022 INTEL CYBERSECURITY OUTLOOK FOR SMALL AND MIDSIZE BUSINESSES

7 Realities Facing SMBs As They Enter A Future Of Increased Cyber Threats

COMMISSIONED BY INTEL CORPORATION

intel®

Table Of Contents

Introduction

For cybersecurity professionals, Covid-19 was a technological accelerant unlike anything else in modern memory.

When the world switched to remote work, new attack surfaces and threat vectors emerged essentially overnight. Every organization with digital assets—that is to say, most organizations—was suddenly more vulnerable.

Large enterprises, though far from impervious, were at least more likely to have the financial and human capital needed to augment their defense postures. For deep-pocketed IT departments, readiness was readily available in the form of cutting-edge security tools.

What of everyone else? How have small and midsize businesses (SMBs) fared during this unprecedented period of increased cyber threat, and what measures are they taking to keep their data and networks secure from future threats?

To find out, Intel, in partnership with Forbes Insights, surveyed more than 1,000 IT decision makers (ITDMs) at small and midsize businesses in November 2021. We asked about their experiences with cyberattacks during and after the pandemic; how, if at all, they intend to adjust their digital defense postures; and what tools they trust to protect their data and maintain operational continuity.

Respondents were evenly distributed in the U.S., the U.K., France, Germany, Australia, India, East Asia and Russia (see Methodology, below). The great majority (92%) are responsible for IT decisions at companies with more than 10 employees, and most (96%) posted less than $500 million in annual revenue for the most recent fiscal year.

Our findings reveal that SMBs are keenly aware of the threats they're facing, though they tend to underestimate their data's value to cybercriminals. And while most are keeping current with the latest cybersecurity tech, the survey exposed blind spots when it comes to hardware- versus software-based security solutions.

Finally, too few SMBs are using enterprise-grade cybersecurity tools, favoring consumer-grade products that may leave them vulnerable to ever-evolving attacks.

Methodology

- For the purposes of this survey, "small and midsize" businesses are defined as having no more than 500 employees. Most (92%) have more than 10 employees; most (96%) posted less than $500 million in annual revenue.
- All respondents are the IT decision makers within their organizations.
- Respondents evenly represent organizations in Australia, Canada, China, France, Germany, India, Japan, Russia, the U.K. and the U.S.
- The study was conducted across a range of sectors, including technology (21%), manufacturing (15%), professional services (14%), construction (9%), retail (9%), financial services (6%) and healthcare (5%).
- Forbes Insights conducted the survey in November 2021.

Key Findings

01 | Threat Analysis

- The great majority (87%) of IT decision makers working at SMBs understand that most cybercrime is committed for financial gain.
- Most respondents have already been targeted to some extent by malware (77%), ransomware (63%), data theft (63%), phishing attempts (75%) and focused hacks (67%). Of those who received ransomware demands, 29% report making payments to recover their data and/or network access.
- Despite that their organizations are "relatively small," most ITDMs see them as viable targets for cyberattack (60%). However, just one-quarter (24%) are keenly aware of their value as potential targets. Nearly one-third (30%) are unaware that multiple targets can be "bundled" together to make scaled attacks worthwhile to criminals.
- Likewise, while nearly all ITDMs (89%) believe their organization is exposed to cybersecurity risks, just 17% consider these threats to be "significant."

02 | Attacks On The Rise

- Half of those surveyed (50%) have seen increased cybersecurity attacks since the start of the pandemic. Those working in media (71%) and telecom (61%) saw the greatest spikes, while those in the beauty sector saw the smallest increase (29%).
- On average, SMB cyberdefenses earn a C-minus grade: Of the 76 average number of attacks reported over the past two years, an average of 22 "broke through" and required virus removal or other remediation. That's 71% cyberdefense effectiveness.

03 | Looking Ahead

- Six in ten (60%) are "extremely confident that [they] are maintaining leading-edge cybersecurity practices." Nearly two-thirds (63%) are "extremely confident" they can maintain operational continuity in the event of a cyberattack; that their data is secure (62%); and that their networks are protected against attack (61%).
- One-third of ITDMs (66%) agree that the pandemic accelerated the expansion of their overall digital footprint; three-quarters of those surveyed (75%) expect their digital footprints to continue to expand in the next one to two years.
- Most (64%) also agree that this expansion exposes their organization to greater cybersecurity risks. However, far fewer (36%) believe cybersecurity attacks will increase over the next year.

04 | Third-Party Risks

- Almost two-thirds of ITDMs (64%) agree that interfaces with partners, suppliers and vendors expose their organization to greater threats.
- Nearly half (48%) believe successful cyberattacks are more likely to result from external relationships; across the board, fewer than one-third are "very confident" in their suppliers', vendors' and partners' cybersecurity measures (28%, 27%, 30%).
- To address these concerns, they're collaborating closely with external partners (67%); conducting end-to-end cybersecurity audits (67%); and commissioning third-party audits (58%).

05 | Cyber-Hygiene

- ITDMs (85%) agree that human error is the most common cause of cybersecurity breaches.
- To solve for this, most (87%) have a specific person or specific people tasked with educating staffers on cybersecurity best practices.
- However, just one-third (32% "strongly agree") expressed the greatest confidence that their employees will follow these best practices.

06 | Hardware vs. Software

- More than one-third of ITDMs (37%) favor an even mix of hardware- and software-based cybersecurity measures. Further analysis shows that these mixed defenses were most successful against attacks (93%).
- Two-thirds (67%) agree that the "leading edge of cybersecurity" is moving toward more use of hardware-based measures. A slightly larger cohort (69%) agrees that hardware-based cybersecurity measures "are preferable to software-based measures."
- Most ITDMs (72%) are committed to increasing their investments in cybersecurity over the next year, though most (70%) would also prefer "security-enhanced hardware" that requires "little or no follow-investment."

07 | Consumer vs. Enterprise

- Nearly one-quarter (24%) of SMBs opt for consumer-grade security products over enterprise tools, and another third (36%) rely on a combination of the two.
- Why? Because consumer tools meet their needs (46%); they're convenient and easy to deploy (45%); and the price is right (40%).
- Many also believe their organization is "too small" for enterprise solutions (37%).

SECTION I

SMBs Know They Are Targets, Yet They Still Undervalue Their Data

Our survey confirms that IT decision makers at small and midsize businesses know intellectually that they're at risk of cyberattack.

In fact, most have already implemented security measures they believe to be sufficient. Yet our results also suggest these same leaders underestimate the value of their organizations' data and potential threat levels.

But first, it's worth examining the threats themselves. Who's targeting SMBs and why, and how has this changed in recent years?

"Financial gain is a common motivation for crimes, including cybercrime," says Amanda Ueno, strategic planner, Business Client Platforms, at Intel. "Financial benefit can be derived by either directly extorting the victim for ransom, selling data itself and/or using the data to enable other attacks that may lead to financial benefits."

As for who's targeting SMBs, Todd Cramer, director of business development, security ecosystem, at Intel CCG, Business Client Platforms, has some ideas: "Nation-state-sponsored e-crime syndicates are the most innovative in developing new [attack] techniques. Then an interconnected ecosystem scales attacks using automated services, such as ransomware-as-a-service, credential access brokers and crypto-based monetization schemes."

At the dawn of the digital age, criminally motivated cyberattacks were typically directed at banks and other financial institutions. After all, that's where the money is.

As data itself became the "new oil"—an increasingly valuable resource—cybercriminals found new and novel ways to monetize other digitized information: credit card numbers, trade secrets, customer profiles, location data, employee salaries and so forth.

"The data has value as long as some entity or individual, including the [data's owner], is willing to pay for access to or return of the data," Ueno says.

Criminals also created new tools and techniques for waging these attacks (see sidebar "A Glossary Of Common Attack Techniques"). Cybercriminals are nothing if not inventive.

"Hacking has truly become an industry," Cramer says.

For much of the modern digital age, IT professionals working at smaller businesses didn't share the same security concerns as their peers at larger companies. Why would cybercriminals waste their time going after a local manufacturer or a regional radio station or a small chain of restaurants? Surely, they believed, their data wasn't worth the time and trouble.

Not so, says Cramer. In fact, because larger organizations tend to encrypt, segment and distribute sensitive records across different networks, it's "tougher for attackers to get a complete spectrum of customer data."

"SMBs present a 'soft underbelly' [and] access to a broader spectrum of customer account or personal identifiable information," he says.

Not only is SMB-sourced data often more robust—and therefore more valuable on cyber black markets—SMB network defenses are typically easier to defeat.

"If you're an attacker and you're looking to steal [data], you're going to look for the easiest way, [not] the hardest way," says Ueno. "Attacks on a bunch of small companies may not draw as much scrutiny and attention from media and law enforcement as one on a large enterprise with a potentially similar payout."

The good news: As our survey reveals, most IT decision makers at small and midsize businesses are aware of these scenarios.

The great majority (87%) understand that most cybercrime is committed for financial gain. They consider their "relatively small" organizations as potential targets (60%) and they (62%) understand that their organizations' data could have value to hackers.

Nine in ten (89%) SMBs are already exposed to cybersecurity risks. Specifically, most respondents have been targeted by malware (77%), ransomware (63%), data theft (63%), phishing attempts (75%) and focused hacks (67%). Of those who received ransomware demands, 29% made a payment to recover their data or network access.

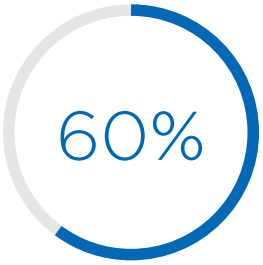
In response, most of those surveyed have implemented antivirus protection (79%), firewalls (76%) and network security (64%).

Here's the bad news: Nearly one-third (30%) are unaware that multiple small and midsize targets can be "bundled" together to make scaled attacks worthwhile to criminals; one-quarter (26%) are likewise unaware that these scaled attacks constitute their "main" cybersecurity threat. Just one-quarter (26% "completely agree") share the most serious concerns over these potential attacks. Even fewer (17%) believe that the cybersecurity risks they face are "significant."

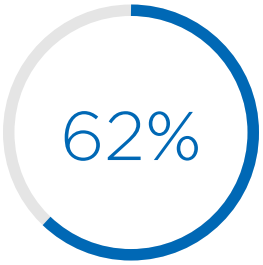
Does this disconnect suggest overconfidence? Indifference? Lack of awareness?

A Glossary Of Common Attack Techniques

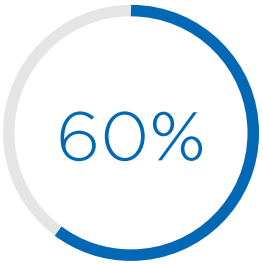
- **Brute Forcing:** Attempting to guess passwords and other user credentials by submitting large databases of character and word combinations to the security system
- **Cryptojacking:** Assuming control of a target's computer for the purpose of mining cryptocurrency in the background, leaving the victim unaware
- **Denial-of-Service (DoS)/Distributed Denial-of-Service (DDoS):** Making a target's computer, network or website unavailable to users by disrupting its credentials or connection to the internet
- **Malware:** "Malicious code" that compromises an application, computer or network to steal the target's data or disrupt their operations
- **Man-in-the-Middle:** Inserting a monitoring device or malicious code between an authorizing service and its users to collect credentials and other valuable data
- **Phishing:** Tricking victims into revealing sensitive information such as user credentials, network details and other useful data
- **Ransomware:** A type of malware that cryptographically encrypts a target's computer, network or storage device until a ransom is paid
- **SIM Jacking:** Taking control of a target's phone by fraudulently convincing their cell phone provider to move the victim's account to another device
- **Social Engineering:** The psychological manipulation of a target to convince them to share confidential information or divulge sensitive data
- **Spoofing:** Digitally masquerading as someone known to a target in order to extract sensitive data or convince them to take a desired action
- **SQL Injection:** Inserting malicious commands into a back-end database to gain control over an application, website or network
- **Zero-Day Exploit:** A software vulnerability that's unknown to the owners and/or developers and that represents a short window of opportunity for cyberattack



of respondents agree that though they are a relatively small business, they are a viable target for cyberattacks.



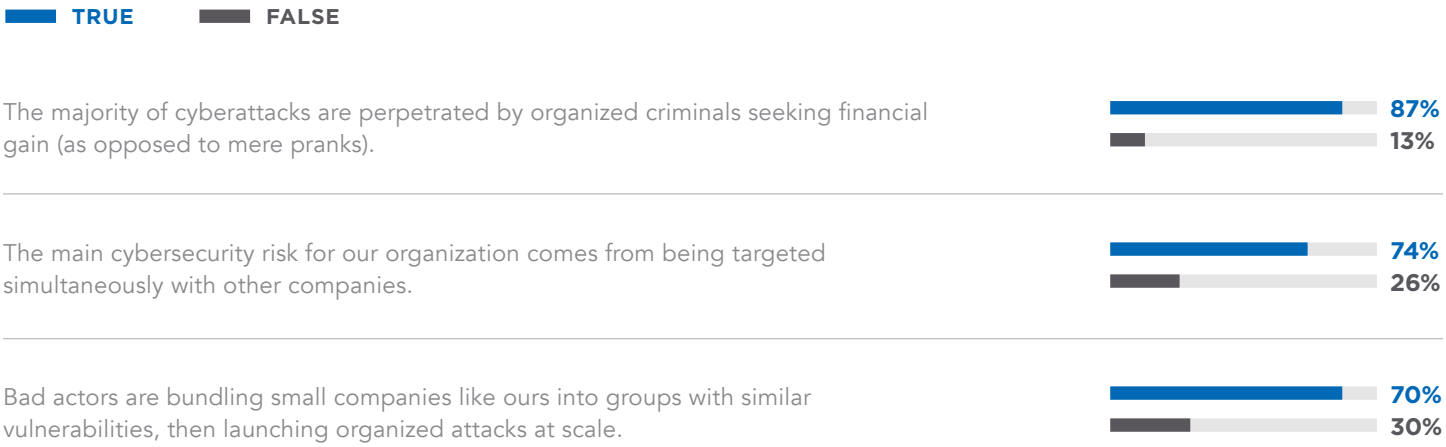
have personal and operational data that would be of value to a hacker.



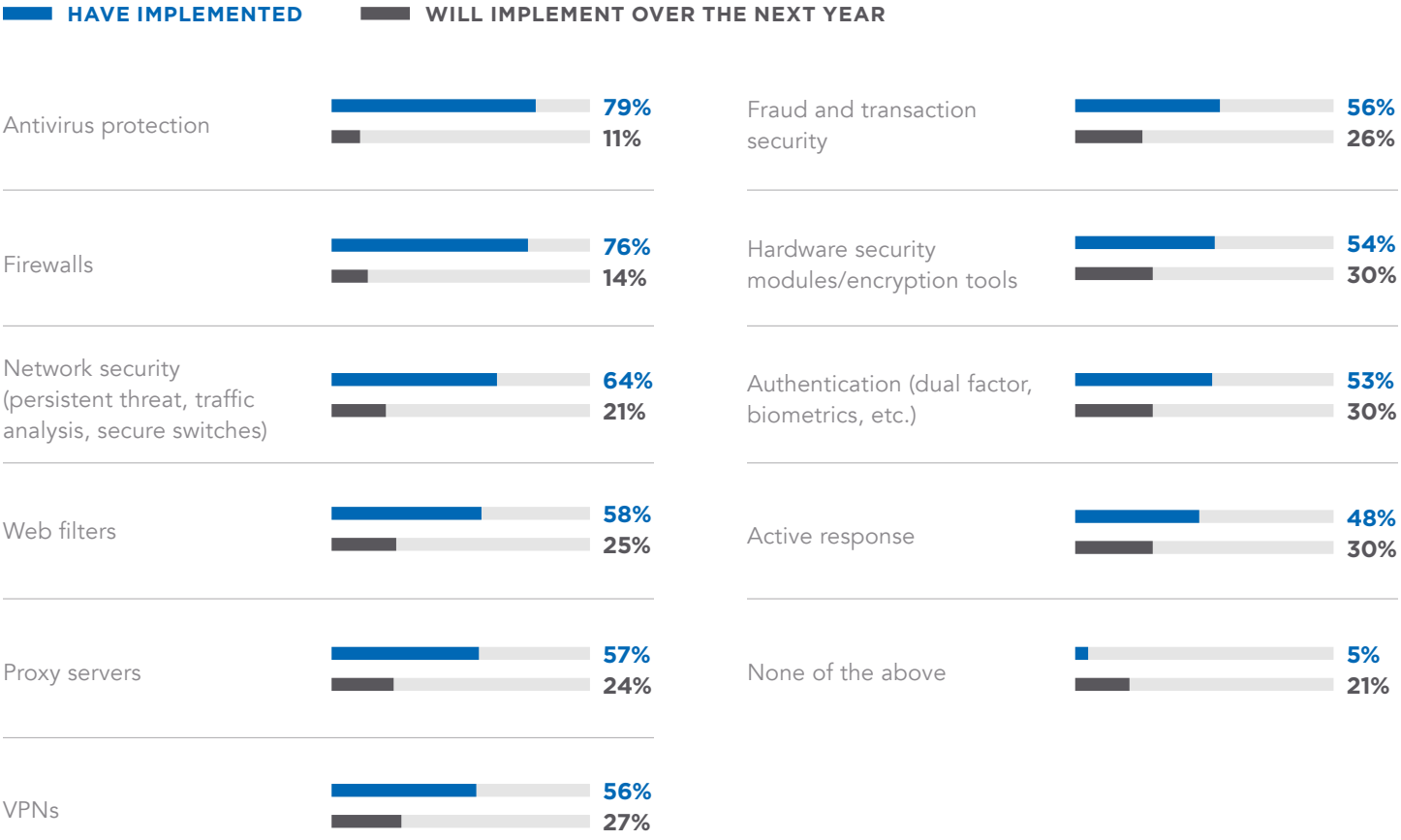
are extremely confident that they are maintaining leading-edge cybersecurity practices.

*Percentages represent the number of respondents who agreed or strongly agreed (4's and 5's on a 1-5 scale, where 1 = Not at all and 5 = Strongly agree).

In your opinion, are the following statements about cybersecurity attacks true or false?



Which of the following cybersecurity tools have you implemented? Which ones are you planning to implement over the next year?



SECTION II

The Pandemic Created More Ways To Breach SMB Networks

By some estimates, cyberattacks grew more than sevenfold during the pandemic, due largely to the near-universal shift to work-from-home.

SMBs found themselves especially vulnerable. As Ueno explains, many small business networks are managed by "an IT of one." That is, one person who's tasked with overseeing the company's technology. Or, she notes, "maybe it's not managed at all."

In the best of times, single-handedly securing a business network is no easy task. Now consider that the pandemic sent everyone home to work on less-secure personal computers and consumer-grade Wi-Fi connections. This is the stuff of cybersecurity nightmares.

"All the practices you put in place while everyone was in the office? They worked well in that environment," Ueno says. "But now you're in a different environment [and] that opened up a new set of scenarios where the business may or may not have … ensured that security is up to date."

Cybercriminals were quick to recognize this, and they wasted no time going after SMBs. Of the 1,000-plus IT decision makers surveyed, half (50%) report increased cybersecurity attacks since the start of the pandemic. Those working in media (71%) and telecom (61%) saw the greatest spikes, while those in the beauty sector saw the smallest increase (29%).

This disparity across industries makes sense to Cramer. "Obviously, sectors that handle sensitive personal identifiable information (PII), or financial, healthcare or account data, are high-value targets," he says. These companies are also more likely to have cyber insurance, he notes. If necessary, they can afford to pay a ransom to avoid the risk of a serious data breach that might damage their brand.

But still, as outlined earlier, no business should believe itself to be off-limits to cybercriminals. Even for companies that don't deal with PII or other data with obvious black-market value, successful cyberattacks can be catastrophic.

"Businesses may be on the hook for expenses such as credit monitoring for affected customers," Ueno explains. "If there is no, or inadequate, insurance coverage, huge unplanned expenses could negatively impact the business cash flow."

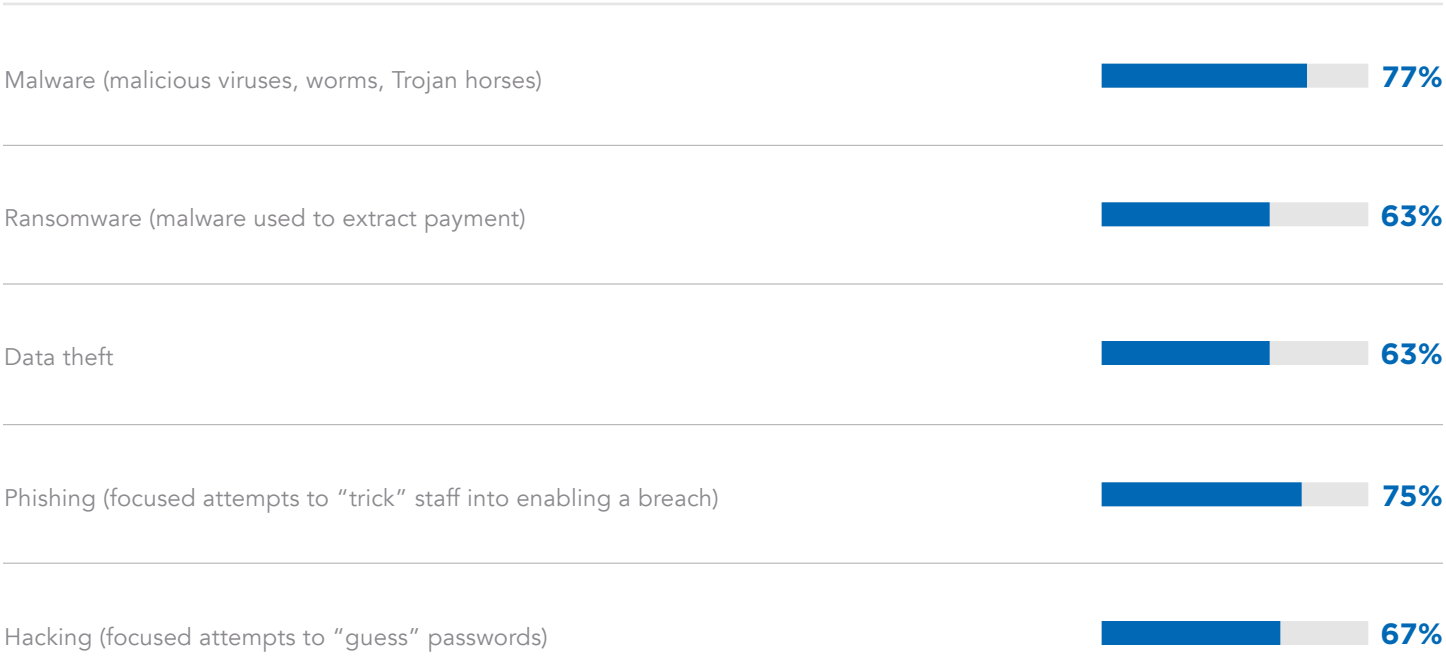
On other networks, such as within Internet of Things systems or industrial sectors, successful breaches may not involve customer data. But their effects are no less disastrous. "The ability to [shut down] operational networks … can cause huge havoc to customers in the form of service outages," Cramer says.

How effective were SMB defenses? Good, but not great. Of the 76 average number of attacks reported over the past two years, an average of 22 "broke through" and required virus removal or other remediation. That's a 71% defense rate.

With cybersecurity known to be so important to their operations, why are SMBs willing to accept C-minus results?

Have you been experiencing the following sorts of attacks?

*Percentages represent the number of respondents who indicated they have experienced attacks to some extent (3's, 4's, and 5's on a 1-5 scale, where 1 = Not at all and 5 = To a significant extent).



How many total intrusions have you successfully detected/prevented over the past two years?

Average number of intrusions **54**

How many total intrusions broke through your defenses, leaving you needing to deal with them (e.g., virus removal; other remediation) after the fact?

Average number of intrusions **22**

SECTION III

Many SMBs Don't Know What They Don't Know

Despite failing to prevent three of ten inbound attacks, most of the SMBs surveyed are evidently pleased with their efforts.

Indeed, 60% are "extremely confident that [they] are maintaining leading-edge cybersecurity practices." Nearly two-thirds (63%) are "extremely confident" they can maintain operational continuity in the event of a cyberattack; that their data is secure (62%); and that their networks are protected against attack (61%).

Asked about specific threats, most IT decision makers can "confidently point to specific, proactive and effective defenses" that are relevant for the following functions: data loss prevention (66%); intrusion detection (67%); intrusion prevention (64%); security incident reporting (67%); event management (63%); and phishing attack prevention (59%).

How do we reconcile such displays of confidence with an average failure rate of 29%?

By our analysis, SMBs may be disguising a sense of helplessness. They're doing everything possible to prevent cyberattacks; they're following best practices; they're making the right investments. Yet they still fail three times out of ten.

There's another contradiction in the data worth examining: Two-thirds of ITDMs (66%) agree that the pandemic accelerated the expansion of their overall digital footprint; three-quarters of the ITDMs surveyed (75%) expect their digital footprints to continue to expand in the next one to two years. Most (64%) also agree that this expansion exposes their organization to greater cybersecurity risks.

And yet far fewer—just 36%—believe cybersecurity attacks will increase over the next year. Only those working in the insurance sector were markedly more concerned about increased attacks (50%).

66% of respondents agree that the pandemic has accelerated the expansion of their digital footprint.

64% believe that their expanding digital footprint exposes them to greater cybersecurity risk than in the past.

75% believe that their digital footprint will continue to expand over the coming 1-2 years.

*Percentages represent the number of respondents who agreed or strongly agreed (4's and 5's on a 1-5 scale, where 1 = Not at all and 5 = Strongly agree).

We don't detect helplessness here. We see overconfidence.

"SMBs think securing the network is all that's needed," Todd Cramer explains. There's "a mentality that a firewall plus single-sign-on ID authentication plus antivirus software equals safety. In fact, there are many more layers to protect to get true defense in depth. ... SMBs don't even know what they don't know" (see sidebar "What Is 'Defense In Depth'?").

Jen Larson, director, Security Product Line and Security Marketing, Business Client Platforms at Intel, sees yet another dynamic at work. "People can get overly focused on a certain type of attack based on what they're hearing in the news [and] based on the headlines," she says.

High-profile ransomware attacks, for example, may inspire IT directors to ramp up those particular defenses at the expense of, say, VPN fortification and installing routine patches.

This piecemeal approach can become problematic. Cybersecurity "is not just whack-a-mole," Cramer explains. "If you're in the security industry, you know there are targeted attacks at all the layers. This notion of 'defense in depth' is critically important for an SMB."

What Is "Defense In Depth"?

"Defense in depth" is an IT strategy for creating multiple layered defenses against cyberattacks. If one line of defense is compromised—user authentication, for example—other fortifications, elsewhere in the network, are expected to detect and prevent further intrusion.

At Intel, Jen Larson explains, "Intel offers a foundational set of security capabilities for businesses called Intel Hardware Shield to create a defense-in-depth approach which starts deep in the silicon. Intel Hardware Shield is an umbrella of capabilities [organized] in three separate categories—below-the-OS protections; application and data protection; and advanced threat protections."

"On Intel systems the security capabilities we align within each of those categories are designed to help deliver unique attack surface protections against a broad range of attacks. It's the summary of these approaches that delivers defense in depth and also shrinks the attack surface," Cramer says.

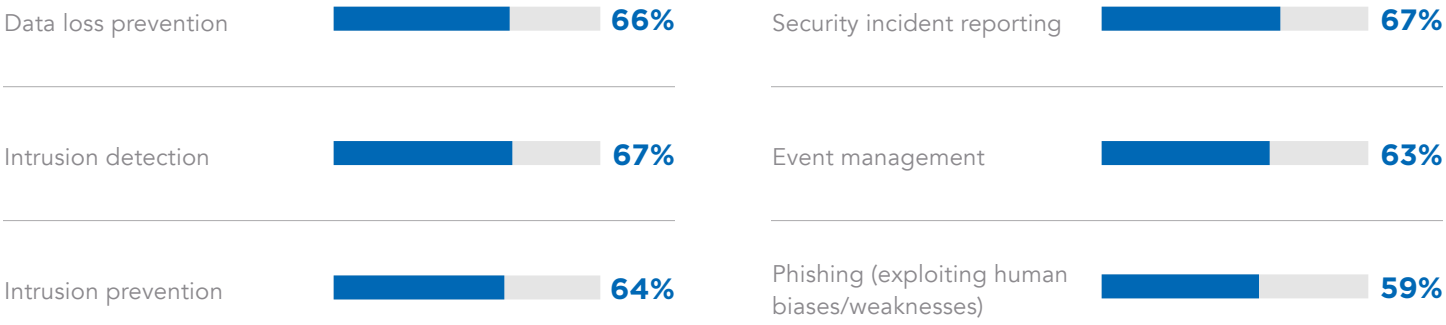
Whether SMBs manage their own cybersecurity or work with a managed service provider or some combination thereof, defense in depth is a must-have.

Since the beginning of the pandemic, have you seen the number of cybersecurity attacks increase, decrease or remain about the same? What is your expectation for the number of cybersecurity attacks your company is likely to face over the next year?

	Increase	Decrease	Remain the same	Not certain
Since the pandemic	50%	12%	32%	6%
Over the next year	36%	18%	34%	12%

Are you able to confidently point to specific, proactive and effective defenses against the following?

*Percentages represent the number of respondents who indicated they can point to examples (4's and 5's on a 1-5 scale, where 1 = Not at all and 5 = Yes, absolutely).



SECTION IV

Supply Chain Attacks Put SMBs At Greater Risk

Another concern for SMB cybersecurity is the increased use of managed service providers, or MSPs.

For smaller companies without large IT budgets, MSPs offer affordable, turnkey technology solutions such as network storage, application hosting and event monitoring.

MSPs also accept responsibility for their clients' data security and privacy. This is very useful for SMBs. "Outsourced managed security [is] more professional," Cramer says. Taking cybersecurity out of the business's hands "is an important trend that all SMBs are moving toward."

This trend has also created new opportunities for cybercriminals. By breaking an MSP's top-level security, so-called "supply chain attacks" can expose hundreds, if not thousands, of valuable data sources.

"Software supply chain attacks are newer techniques that present real problems for everyone," Cramer says. "When attackers hit these providers, their malware, ransomware and other malicious code may be distributed across the MSP's fleet of servers and PCs. … By targeting the provider [they] can get down into the software of many places."

In fact, many of the most prominent security breaches in recent years have been supply chain attacks.

Our research shows that SMBs are aware of the risks posed by digital connections to third parties, including MSPs. Two-thirds of the IT decision makers surveyed (67%) agree that partners, suppliers and vendors expose their organization to the greatest threats; nearly half (48%) believe successful cyberattacks are more likely to result from external relationships.

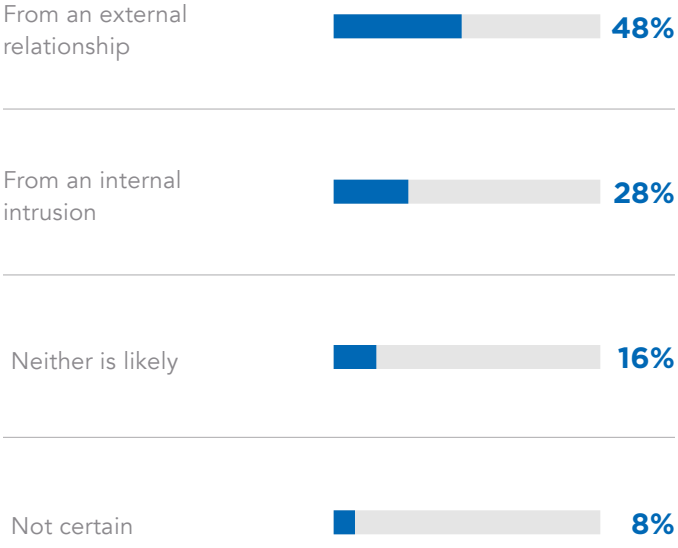
A minority are "very confident" in their suppliers', vendors' and partners' cybersecurity measures (28%, 27%, 30%).

Short of cutting all digital contact with third parties (a practical impossibility), how can SMBs improve their security postures in this regard? Most (67%) say they're collaborating closely with external partners; they're conducting end-to-end cybersecurity audits (67%); and they're commissioning third-party audits (58%) (see sidebar "'Least Privilege' And 'Zero Trust Security' Explained").

This is precisely the right idea, Cramer says. More than anything else, he urges SMBs to do their homework before working with any third party. When considering MSPs in particular, IT decision makers should look for software and hardware packages that are "truly defense in depth and best in class," he says.

And, Cramer adds, they should ask themselves: "Are [MSPs] providing the 360 of everything I need [for my] business and security?"

Which is more likely: a successful cyberattack resulting from an external relationship or from your own internal operations?



"Least Privilege" And "Zero Trust Security" Explained

When asked how SMBs can mitigate risks by exposing their networks to third parties (an unavoidable necessity for most companies), Amanda Ueno recommends "least privilege with zero trust security combined with regular auditing."

What exactly are "least privilege" and "zero trust security"?

"The concept of least privilege is to grant the only minimal level of rights needed by an individual, device or software," Ueno says.

For example, an individual responsible for the company's IT may not need access to personnel data. Least privilege therefore dictates that that individual not get it. Should a cybercriminal gain access to this individual's credentials, the personnel data stays safe.

"Zero trust security" is the constant evaluating of users and devices to determine security risk and whether they should be granted access to networks or network assets.

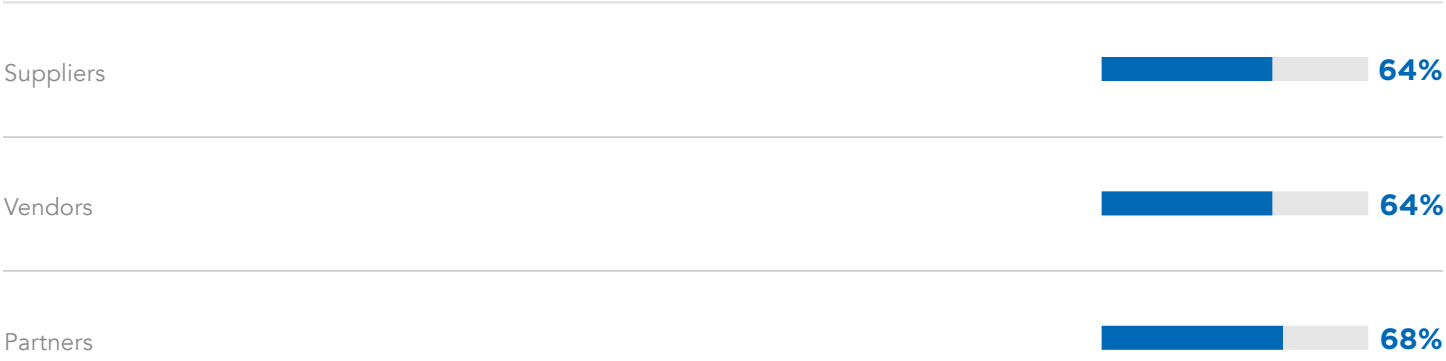
In practice, Ueno says, zero trust might start with, at a minimum, granting certain users access to their company email only when they're also logged into a recognized device that's compliant with the latest security policy.

To what extent do you believe your networks and data are exposed to cybersecurity risks stemming from interfaces with external relationships such as partners, suppliers or vendors?

Not at all				To a significant degree	Not certain
1	2	3	4	5	
2%	9%	22%	37%	27%	3%

Are you confident in the cybersecurity measures in place amid your external relationships?

*Percentages represent the number of respondents who indicated they are confident (4's and 5's on a 1-5 scale, where 1 = Not at all and 5 = Very confident).



SECTION V

More SMBs Must Practice Better Cyber-Hygiene

Even just one innocent keyboard slip can undermine the most sophisticated digital defense.

Indeed, IT decision makers at SMBs (85%) agree that human error is the most common cause of cybersecurity breaches. With that in mind, most (87%) already have a specific person or specific people tasked with educating the staff on cybersecurity best practices.

And yet, just one-third (32% "strongly agree") expressed the greatest confidence that their employees would follow these best practices.

One solution? Requiring better cyber-hygiene—a set of standard, companywide practices and protocols that ensure your data and networks remain secure. Examples: requiring strong passwords from users and forcing periodic password updates; and educating employees about common phishing scams (see sidebar "Cyber-Hygiene 101").

Already, most (59%) IT decision makers are confident in their defenses against phishing attacks. That's a good start. But Cramer advises them to dig deeper. He also believes SMBs should create two sets of hygiene protocols: one for internal risks, another for external.

"For example," he says, "insider threat can be mitigated with a least-privilege approach to defining roles and [granting] rights that only give internal users access to what they need." IT should also build "a logging framework that can determine who did what and when, should an internal breach occur."

Externally facing cyber-hygiene protocols, on the other hand, might include multifactor authentication for any third parties who access sensitive data. Ultimately, Cramer says, "good cyber-hygiene that focuses on defense in depth across all attack surfaces and techniques does the best job [and it] does meaningfully deter attacks."

As Larson further notes, effective cyber-hygiene needn't be complicated. "It's paying attention to your passcodes [and] making sure they're strong, training your employees to look out for suspicious links and content. It's buying the right devices [because] hardware actually does matter … and keeping your systems backed up and updated. If you did those things, you'd have a great start. Ideally, it's about starting to build a defense-in-depth security program from there."

Cyber-Hygiene 101

Understanding that data security relies heavily on their employees' knowledge of best practices, Intel suggests that SMBs train their employees to:

1. Appreciate the importance of good cyber-hygiene as the first line of defense against cybercriminals
2. Recognize social engineering scams, such as phishing and domain spoofing
3. Fully understand those data security regulations that affect their industry
4. Use strong, unique passwords and change them regularly
5. Be prepared to react if they accidentally click on a malware link or otherwise compromise the business's data or network
6. Update software and systems in a timely manner when patches are made available

This is baseline. As Ueno notes, "Depending on the types of internal threats, additional security measures may be needed in addition to the best-known methods for addressing external threats."

85%

of respondents agree that the most common cybersecurity breaches are the result of human error.

89%

are confident that their employees are following the best cybersecurity practices.

87%

have a specific person or persons who are charged with continuously educating their staff on procedures to prevent human error-enabled cyberattacks.

*Percentages represent the number of respondents who somewhat agreed, agreed or strongly agreed (3's, 4's and 5's on a 1-5 scale, where 1 = Not at all and 5 = Strongly agree).

SECTION VI

Software- or Hardware-Based Security? SMBs Are Split

Ask average employees about protecting their personal computers and they'll probably mention antivirus software—and not much else.

That's perfectly acceptable. Quality antivirus software (and strong passwords) will keep most of us safe from most hackers.

This is not true for business networks, the servers, routers and even individual PCs of which require protection at the software and hardware levels.

Most SMBs are aware of this. When asked to describe their current cyberdefenses, they indicated that both hardware and software were more or less equally represented.

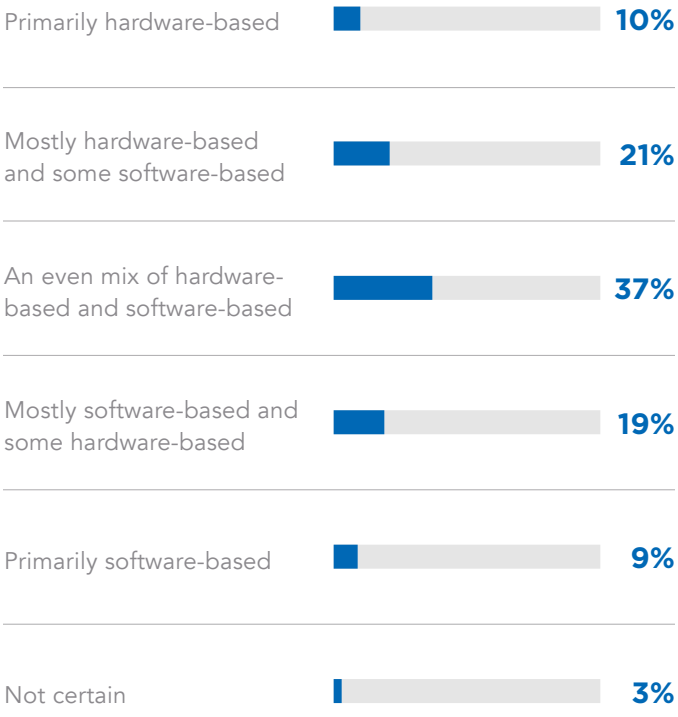
One in five SMBs (21%) prefers "mostly hardware-based measures and some software-based." The converse cohort is roughly the same size: 19% prefer "mostly software-based and some hardware-based" (19%). At either end of the data, about one in ten (10%) relies primarily on either hardware and software.

The largest cohort of SMBs—a bit more than one-third (37%)—favors an even mix of hardware- and software-based cybersecurity.

According to the survey data, these mixed measures saw the greatest success rate: Separately, hardware- and software-based defenses prevented an average 39 (of 67 total) and 25 (of 40 total) attacks in the past two years, respectively. SMBs using an even mix of each were successful against 76 in 82 total attacks.

That's a 93% success rate—or grade-A work.

What is the approximate mix of hardware-basis versus software-basis for your cybersecurity measures?



For the time being, at least, it seems that evenly mixed cyberdefenses are meeting the needs of most SMBs. But both Cramer and Ueno expect hardware-based defense measures to become more important as threats accelerate and evolve.

"With defense in depth, it's about starting with a secure foundation," Cramer says. "Hardware security has a long-recognized role [in this]."

For Ueno, hardware solutions serve a vitally important function that software cannot handle alone: "[Software] is dependent on what's available, exposed and visible to the operating system, [but] the OS does not necessarily have the capability to see everything that's going on across the platform," she says. Underlying hardware-based tools can detect data that may be hidden from the operating system and its applications, then send it back upstream for software-based analysis.

Cramer and Ueno agree that this type of relationship between hardware and software provides the best protection.

Ueno is most concerned for those 9% of SMBs who expect software alone to protect their organizations.

"There isn't one tool or solution that will address all types of threat. Different tools could be focused on different security risks or threats," she says. However, "if you only rely on a software-only solution, you could likely have blind spots."

Upkeep Is Vital, And Needn't Be Expensive

According to our survey, two-thirds of SMBs (67%) agree that the "leading edge of cybersecurity" is moving toward hardware-based measures, and a slightly larger cohort (69%) believes hardware-based cybersecurity measures "are preferable to software-based measures."

Why aren't more of them implementing hardware-based solutions? Upkeep costs, perhaps.

While most respondents (72%) are committed to increasing their investments in cybersecurity solutions over the next year, they (70%) would also prefer "security-enhanced hardware" that requires "little or no follow-investment."

"It may not be just the upfront expense of acquiring a solution, but also concerns over the knowledge and/or infrastructure required to deploy and use these solutions," Ueno explains.

This needn't be the case, she says.

"From an Intel perspective, we recognize that [concern]. We have worked very hard to make it such that [hardware] is out of the box as much as possible. … There's nothing extra that you, as an SMB, have to do to make it work."

But, she stresses, "make sure that you're up to date when the patches come through."

In this regard, SMBs seem to be doing it right. Asked how often they update their tools, the most common answer was one year (38% hardware, 37% software). Nearly one-third (30%) report twice-yearly updates for their hardware, and more than one-third (37%) update their software on this same schedule.

67% of respondents agree that the leading edge of cybersecurity is migrating toward greater use of hardware-based measures.

69% believe that hardware-based cybersecurity measures—an environment that prevents attacks and can be continuously updated by the manufacturer—are preferable to software-based measures.

72% believe that over the next year they will be increasing their investments in cybersecurity solutions.

70% would increase their current cybersecurity budget if they were confident that security-enhanced hardware could be kept current with little or no follow-on investment.

*Percentages represent the number of respondents who agreed or strongly agreed (4's and 5's on a 1-5 scale, where 1 = Not at all and 5 = Strongly agree).

SECTION VII

Enterprise Tools Are Mistakenly Considered Out Of Reach

For all their differences, most SMBs have one thing in common: It's not easy to find the time, money or workforce necessary to mount and maintain top-notch cyberdefenses on their own.

"They can run the tools themselves," Cramer says. But, he admits, "that's the odd case." The investments in time and training are out of reach for most.

Most SMBs also don't think they can afford the enterprise-grade tools that protect larger organizations. Instead, they turn to off-the-shelf, consumer solutions to keep their data and networks safe. Our survey shows that nearly one-quarter (24%) of SMBs opt primarily for consumer-grade security products over enterprise tools; another third (36%) rely on a combination of the two.

For better or worse, consumer tools are widely believed to meet SMB needs (46%); they're convenient and easy to deploy (45%) and the price is right (40%). Additionally, 37% of SMBs who employ consumer-grade cybersecurity tools believe their organization is too small for enterprise solutions.

Perhaps not surprisingly, SMBs posting less than $1 million in revenue are more likely to feel this way (43% vs. 37% overall).

Unfortunately, our analysis reveals dramatically diminished efficacy when these products are used by SMBs. In the past two years, consumer-grade cyberdefense measures were successful just 55% of the time; those who rely on a mix of consumer- and enterprise-grade successfully defended their networks 69% of the time.

Meanwhile, enterprise-grade cybersecurity measures posted an 86% defense rate—just 10 successful breaches against 71 total attacks on average.

Why are enterprise-grade tools so much more effective? At Intel, at least, it's because developers are dedicated to ongoing security assurance. Larson explains: "We're not only looking at new capabilities, new innovations [and] those things that are on the platform. We're also looking to protect that platform after purchase. We're looking for issues in our products tirelessly through our red teams and bug bounty programs. ... That's how we approach security for businesses."

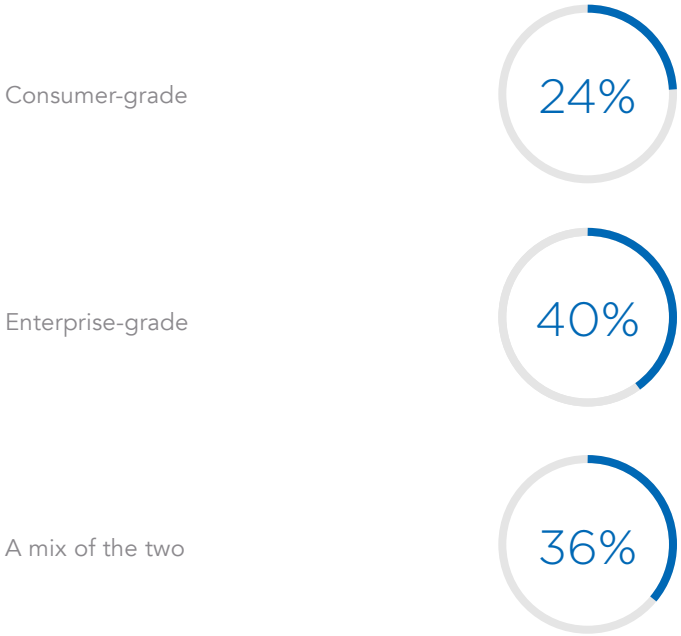
Surely any defense is better than no defense, but compromising with consumer-grade tools isn't necessary. Most cybersecurity providers offer modified enterprise packages that are designed to meet the needs of small and midsize businesses.

"[SMBs] need right-sized security, [since] their networks and systems are not as broad an attack footprint," Cramer says. For example, Intel's "vPro Essentials SKU is more affordable for SMBs and it comes with the right-sized security. SMBs should focus there."

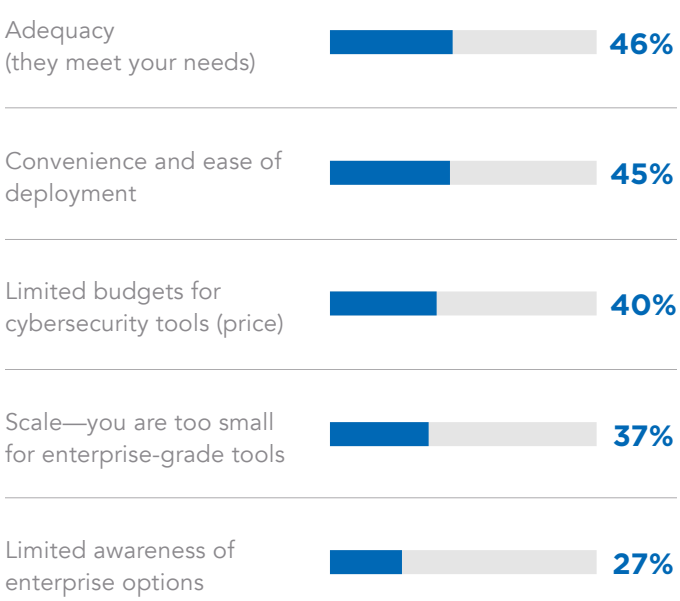
Whether they're implementing cybersecurity measures for the first time or looking to upgrade their current systems, Cramer has one last piece of advice for SMB IT decision makers.

"Most security software vendors offer three package tiers: consumer, SMB and enterprise," he says. "Hitting the middle spot is probably best. … Don't run consumer-grade security software. … Go for the SMB package that's not quite enterprise-grade but provides enough [protection]."

Which of the following best characterizes the security products you are employing?



Why are you opting for consumer-grade tools?



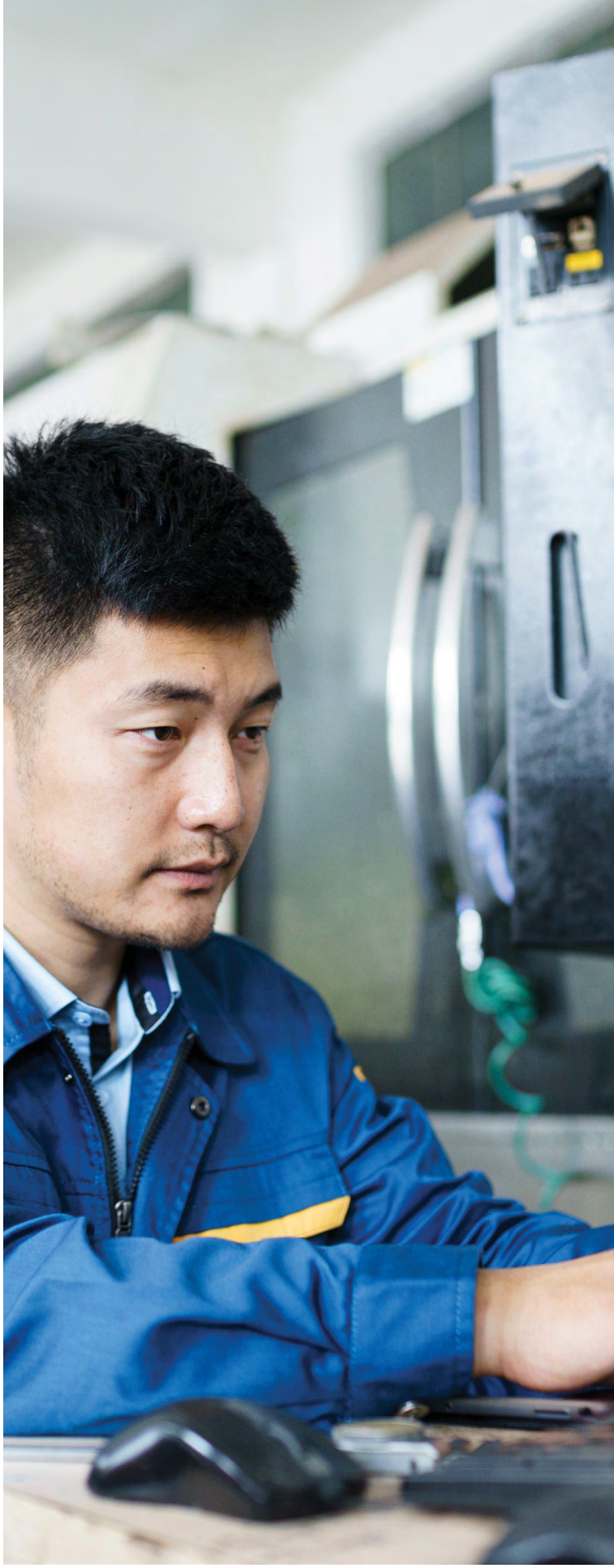
Conclusion

Covid-19 changed fundamental customer behaviors and expectations, forcing many business owners to evolve rapidly.

Modern cybersecurity, too, must evolve. Local or global, brick-and-mortar or virtual—every commercial operation will find itself under greater attack from cybercriminals. For small and midsize businesses, the stakes have never been higher. Just one data breach can permanently destroy a hard-earned reputation among customers.

Deciding how to defend one's digital assets is not simple. As Cramer explains, "SMBs are in different stages." Some opt to be self-sufficient and run their own cyberdefenses; this can become expensive and resource-intensive. Others place their trust in managed service providers, which presents its own risks.

Whatever path to cybersecurity they choose, "awareness is crucial for IT decision makers at SMBs," Cramer says. The worst decision, after all, is an uninformed decision.



Forbes Insights is the strategic research and thought leadership practice of Forbes Media, a global media, branding and technology company whose combined platforms reach nearly 94 million business decision makers worldwide on a monthly basis.

By leveraging proprietary databases of senior-level executives in the Forbes community, Forbes Insights conducts research on a wide range of topics to position brands as thought leaders and drive stakeholder engagement. Research findings are delivered through a variety of digital, print and live executions, and amplified across Forbes' social and media platforms.

JEFF KOYEN

Report Author

499 Washington Blvd., Jersey City, NJ 07310 | 212.367.2662 | https://www.forbes.com/forbes-insights/