CYBERSECURITY SPECIAL REPORT

SMALL AND MIDMARKET BUSINESSES

Small and Mighty

How Small and Midmarket Businesses Can Fortify Their Defenses Against Today's Threats

CISCO

53% of midmarket companies have experienced a breach

up to

5000

Average number of security alerts

Midmarket companies investigate 55.6% of security alerts

29% of midmarket companies say breaches cost them less than $100K. 20% say it costs $1,000,000–$2,499,999

Many small and midmarket businesses aspire to more effective cybersecurity practices just like larger counterparts. SMBs are dynamic – the backbone of innovation and the poster child of hardwork. They run even faster and work even harder than enterprise peers. And they are exposed to the same cyber threats.

In today's cyber threat landscape, every organization, large or small, is at risk for an attack. But increasingly, small/midmarket businesses are the focus of attacks[1] and often serve as a launch pad or conduit for bigger campaigns. Adversaries view small/midmarket businesses as soft targets that have less-sophisticated security infrastructure and practices and an inadequate number of trained personnel to manage and respond to threats.[1]

Many small/midmarket businesses are only beginning to realize how attractive they are to cybercriminals. Often, that realization comes too late: after an attack. Recovering from a cyber attack can be difficult and costly—if not impossible—for these businesses, depending on the nature and scope of the campaign. This report will give an understanding of the risks smaller organizations face, share an understanding of how smaller organizations stack up against their peers with respect to security and share a bit of guidance to bear in mind in 2018 and beyond.

Consider this finding from the Cisco 2018 Security Capabilities Benchmark Study: More than half (54 percent) of all cyber attacks result in financial damages of more than US$500,000 including, but not limited to, lost revenue, customers, opportunities, and out-of-pocket costs. That amount is enough to put an unprepared small/midmarket business out of operation—permanently.

A recent study by the Better Business Bureau (BBB)[2] helps to underscore how small/midmarket businesses can struggle financially to survive following a severe cyber attack. The BBB asked small business owners in North America, "How long could your business remain profitable if you permanently lost access to essential data?" Only about one-third (35 percent) said that they could remain profitable for more than three months. More than half reported that they would be unprofitable in under one month.

By the way, we see SMBs as companies with fewer than 250 employees and define midmarket as companies with 250–499 employees. Both segments are included in this report.

We analyze findings from SMB respondents in our 2018 Security Capabilities Benchmark Study, what we'll refer to merely as our Benchmark study. It offers insights on security practices currently in use, and compares the full results to the past three years.

Our SMB/midmarket data includes 1816 respondents across 26 countries.

1 Cyberthreats and Solutions for Small and Midsize Businesses, Vistage Research Center, 2018. Developed in collaboration with Cisco and The National Center for the Middle Market. Available at: https://www.vistage.com/research-center/business-operations/risk-management/20180503-22912/.

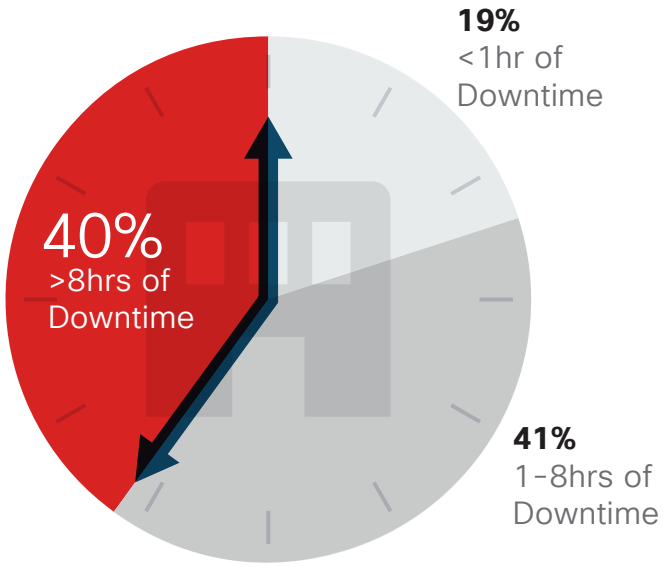
2 2017 State of Cybersecurity Among Small Businesses in North America, BBB, 2017: https://www.bbb.org/globalassets/shared/media/state-of-cybersecurity/updates/cybersecurity_final-lowres.pdf.

What's a day of lost business between colleagues?

Said no IT admin ever. System downtime, which undermines productivity and profitability, is a significant issue for businesses following a cyber attack. Research from the Benchmark Study found that 40 percent of respondents (250–499 employees) experienced eight hours or more of system downtime due to a severe security breach in the past year (Figure 1). Cisco saw similar results for larger organizations in the study sample (those with 500 or more employees). The difference, though, is that larger organizations tend to be more resilient than small/midmarket businesses following an attack because they have more resources for response and recovery.

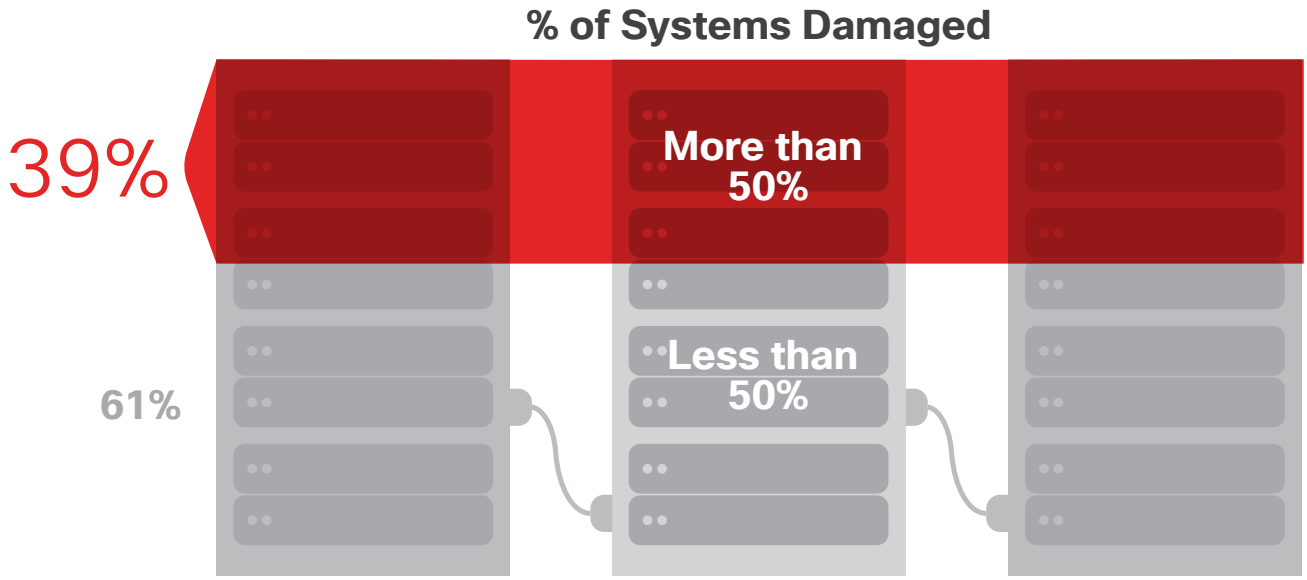
Also, 39 percent of respondents reported that at least half of their systems had been affected by a severe breach (Figure 2). Smaller businesses are less likely to have multiple locations or business segments, and their core systems are typically more interconnected. When these organizations experience an attack, the threat can quickly and easily spread from the network to other systems.

Figure 1 System downtime following a severe breach



Source: Cisco 2018 Security Capabilities Benchmark Study

Figure 2 Percentage of systems affected by a severe breach



Source: Cisco 2018 Security Capabilities Benchmark Study

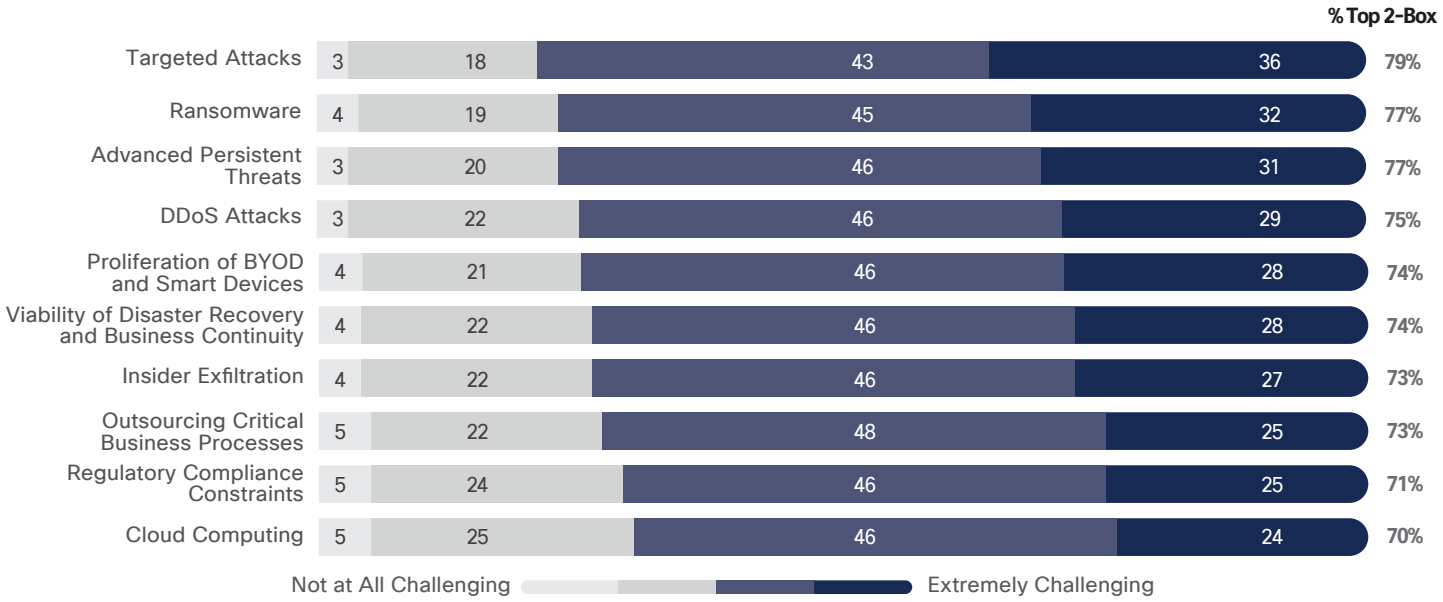
Sleepless security nights

When asked about the biggest security challenges they face, respondents are most concerned with three things:

- Targeted attacks against employees (think well-crafted phishing)
- Advanced persistent threats (advanced malware the world hasn't see before)
- Ransomware

Ransomware (interestingly not cited as a "top 3" concern of large enterprise)—is, as you surely know by now, malware that encrypts data, usually until affected users pay a ransom demand. It can create severe disruption and system downtime for small/midmarket businesses. Ransomware is also costly in a different way for these organizations: Cisco security experts explain that small/midmarket businesses are more inclined to pay ransoms to adversaries so that they can quickly resume normal operations. They simply can't afford the downtime and lack of access to critical data—including customer data. (See Figure 3.)

Figure 3 Top security concerns for midmarket businesses[5]



Source: Cisco 2018 Security Capabilities Benchmark Study

Other Threats SMBs Can't Ignore

Despite worries about ransomware, Cisco security experts suggest it is a diminishing threat as more adversaries shift their focus to illicit cryptocurrency mining ("cryptomining"). The appeal of this activity is threefold: It can be highly lucrative, payouts can't be traced, and adversaries can worry less about the potential for criminal liability for their actions. (For example, there is no risk of patients being deprived of critical care because a hospital's systems and essential data are locked up by ransomware.) Adversaries can also deliver mining software ("miners") through various methods, including email-based spam campaigns and exploit kits.[3]

3 Ransom Where? Malicious Cryptocurrency Miners Takeover, Generating Millions," Cisco Talos blog, January 31, 2018: https://blog.talosintelligence.com/2018/01/malicious-xmr-mining.html.

Cisco threat researchers explain that malicious actors using the new business model of illicit cryptomining "are no longer penalizing victims for opening an attachment or running a malicious script by taking systems hostage and demanding a ransom. Now, [they] are actively leveraging the resources of infected systems."[4] For small/midmarket businesses unwittingly aiding illicit cryptomining operations, slower system performance might be the only red flag signaling they've been compromised—unless they have the right technology in place to detect when cryptomining activity is present.

The 0.5% insider threat: 100% too high?

As respondent companies move more data and processes to the cloud, they must also take steps to manage another potential threat: rogue insiders. Without tools to detect suspicious activity (such as downloading of sensitive customer information), they are at risk of losing intellectual property, sensitive financial and client data through corporate cloud systems.

A recent investigation by Cisco threat researchers highlights the risk: From January to June 2017, they examined data exfiltration trends using machine-learning to profile 150,000 users in 34 countries who were using the cloud. Over 1.5 months, researchers found that 0.5 percent of users made suspicious downloads. Does half a percent seem bad? Put another way, this means two employees at a 400 person firm would be insider threats. That is 100 percent too high. Specifically, those users downloaded, in total, more than 3.9 million documents from corporate cloud systems. That's an average of 5200 documents per user during a 1.5-month period.[5]

Cisco 2018 Security Capabilities Benchmark Study

This special report features select data findings from the Cisco 2018 Security Capabilities Benchmark Study. The research involved more than 3600 respondents across 26 countries. For more insights on security practices currently in use by organizations of all sizes, and a comparison of results from Cisco's previous studies, download the *Cisco 2018 Annual Cybersecurity Report* available at: https://www.cisco.com/c/en/us/products/security/security-reports.html.

4 Ibid.

5 For more details, see "Insider threats: taking advantage of the cloud" in the Cisco 2018 Annual Cybersecurity Report, available at: https://www.cisco.com/c/en/us/products/security/security-reports.html.

Challenges

The best defense against the threats described earlier—requires coordination and orchestration of IT resources. Those resources are most commonly the people, processes, and technology that businesses can amass to deter attacks.

However, even more so than their larger counterparts, smaller businesses are challenged to coordinate these resources in ways that yield insights into threats and stop or mitigate attacks before they cause damage. The perennial lack of security talent that affects enterprises impacts smaller counterparts even more.

SMB security tech trends

Moving forward, smaller organizations indeed seek to address the cybersecurity challenges that threaten their organizations with new tools to stop threats.

Benchmark Study respondents said that if staffing resources were available, they would be more likely to:

- Upgrade their endpoint security to more sophisticated advanced malware protection/EDR – the most common response at 19 percent.
- Consider better web application security against web attacks (18 percent)
- Deploy intrusion prevention, still seen as a vital technology to stop network attacks and exploit attempts. (17 percent). (See Figure 5.)

As organizations consider new technologies, a challenge is determining how well their products interoperate to keep businesses protected. The management burdens of combing through many consoles to respond to threats or security incidents should not be underestimated.

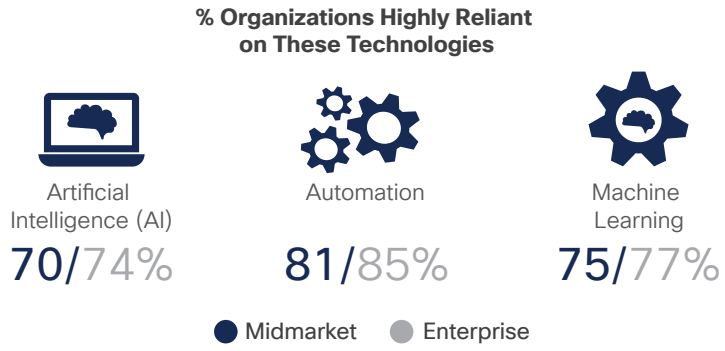
"Many people think that if they go with a multivendor, best-of-breed approach, it will protect them better," says Ben M. Johnson, CEO of Cisco partner Liberty Technology in Griffin, Georgia. "But what we see is that it's harder to manage, costs more, and decreases security effectiveness overall."

Machine Learning: Security Help or Hype?

We've all heard about machine learning given its recent hype. It turns out midmarket businesses rely about the same amount as larger peers on behavioral analytics solutions that can effectively detect attacks. Solutions using machine learning and automation are relied on slightly less heavily by midmarket businesses when compared to organizations with more than 1000 employees (Figure 4).

Machine learning is most effective when it is an additional detection layer in an already deployed product as opposed to buying a separate product in order to "do machine learning." This way teams gain the benefit of machine learning to detect anomalies and threats at machine speed without any new team burdens.

Figure 4 Midmarket businesses are less reliant on automation and AI tools



Source: Cisco 2018 Security Capabilities Benchmark Study

Mobile Midmarket

Businesses also recognize that their security approaches must meet the demands of the modern work environment—in particular, the shift to mobility and the embrace of mobile devices. Fifty-six percent of respondents said that defending mobile devices from cyber attacks is considered very challenging or extremely challenging.

Midmarket and the Cloud

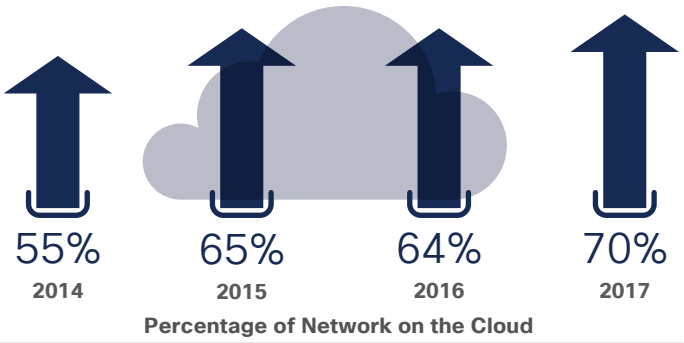
In recognition of their security challenges, many respondents are looking to the cloud to bolster defenses without adding people or straining existing resources. The question is whether moving security to the cloud is enough of a strategy to ward off attacks. Also, businesses can't simply offload security responsibility by moving data to the cloud: They must still be knowledgeable about the security controls imposed by cloud providers as well as how potential breaches in the cloud might impact on-premises resources.

The adoption of cloud services among midmarket businesses is clearly on the rise, based on Cisco's research. In 2014, 55 percent of these businesses said they hosted some of their networks via a form of the cloud; in 2017, that number increased to 70 percent (Figure 5).

Many respondents believe that the cloud can help close some gaps in their defenses as well as resolve some shortcomings in their infrastructure and the abilities of their staff. In fact, according to Cisco's research, midmarket businesses' top reason for hosting networks in the cloud is the belief that it offers better data security (68 percent); the second most popular reason is that the business lacks enough internal IT workers (49 percent). (See Figure 6.)

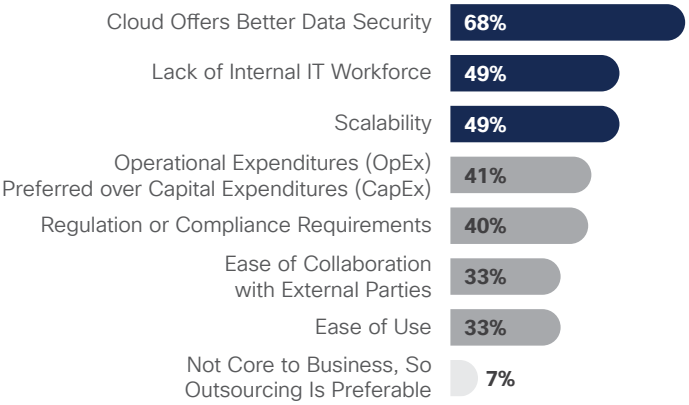
Midmarket businesses also favor the cloud because of its scalability—that is, reducing the business' reliance on its internal resources—and the flexible shift to operational expenditures instead of capital expenditures (Figure 6).

Figure 5 Midmarket businesses show a steady increase in cloud adoption



Source: Cisco 2018 Security Capabilities Benchmark Study

Figure 6 Midmarket businesses choose the cloud for security and efficiency



Source: Cisco 2018 Security Capabilities Benchmark Study

People: Finding staff to strengthen security

The good news is that the Benchmark Study shows that 92 percent of midmarket businesses have an executive responsible and accountable for security. (See Figure 7.)

Given ample staff resources, midmarket businesses would be willing to add more security tools such as advanced endpoint protections or web app firewalls.

Midmarket has something in common with larger counterparts: a shortage of IT staff hindering the ability to shore up defenses. There simply aren't enough people in-house to manage tools that could improve security, according to Cisco's research.

For that reason, many small/midmarket businesses look to outsourced assistance to gather the talent they need to increase their knowledge of threats, save money, and respond to breaches more quickly. The desire for unbiased insight was the most common reason given by midmarket businesses for outsourcing their security tasks (Figure 8), followed by cost-effectiveness and the need to respond to security incidents promptly.

Outsourcing help is a good way for businesses to make the most of limited resources. But these companies can run into trouble if they assume that an outsourced provider or a cloud partner will provide all of the capabilities that they lack in-house.

Chad Paalman, CEO of NuWave Technology Partners in Kalamazoo, Michigan, a Cisco partner, finds that many small/midmarket businesses are unaware of exactly how much (or how little) analysis and monitoring their outsourced security providers offer.

Figure 7 Executives responsible and accountable for security at midmarket businesses

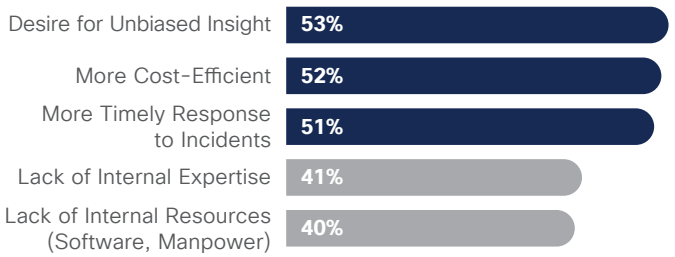
92%
Have an Executive Responsible for Security

Title of Executive Responsible for Security

42%	(CISO) Chief Information Security Officer
24%	(CSO) Chief Security Officer
10%	(CEO) Chief Executive Officer
8%	(CIO) Chief Information Officer
3%	(COO) Chief Operating Officer
5%	(CTO) Chief Technology Officer
6%	(SVP or VP) Senior Vice President or Vice President of IT
2%	(CRO or CCO) Chief Risk Officer or Chief Compliance Officer

Source: Cisco 2018 Security Capabilities Benchmark Study

Figure 8 Midmarket businesses use outsourced help to overcome lack of internal resources



Source: Cisco 2018 Security Capabilities Benchmark Study

"Many business leaders are not educated about their networks. They assume that if they have a firewall, then they have a padlock on the door and no one can get in. They also assume that if their security has been outsourced to a managed service provider (MSP), log monitoring is happening, or the service includes intrusion detection."

Chad Paalman, CEO of NuWave Technology Partners

The bottom line, however, is that small/midmarket businesses count on their outsourced partners to deliver:

- Outsourced advice and consulting services (57 percent),
- Incident response (54 percent),
- Security monitoring (51 percent).

However, they are less likely to outsource tasks such as threat intelligence (39 percent). (See Figure 9.)

The good news is that midmarket businesses appear to be setting aside some of their limited resources for understanding and responding to threats for things like bolstering threat intelligence and incident response.

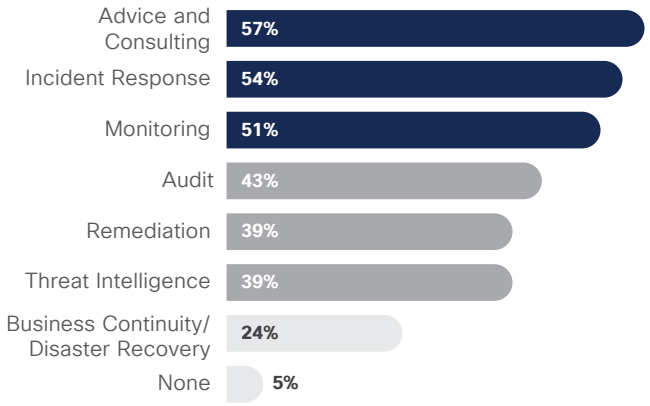
Processes: Regular check-ins for managing security

Comprehensive, regular security processes—such as controls for high-value assets and reviews of security practices—help organizations identify weaknesses in their security defenses. Such processes are not as prevalent in small/midmarket businesses as they should be, perhaps owing to the lack of staffing.

For example, according to the Cisco 2018 Security Capabilities Benchmark Study, midmarket businesses are less likely than larger organizations to agree that they review security practices regularly, that they have tools in place to review security capabilities, and that they routinely investigate security incidents (Figure 10).

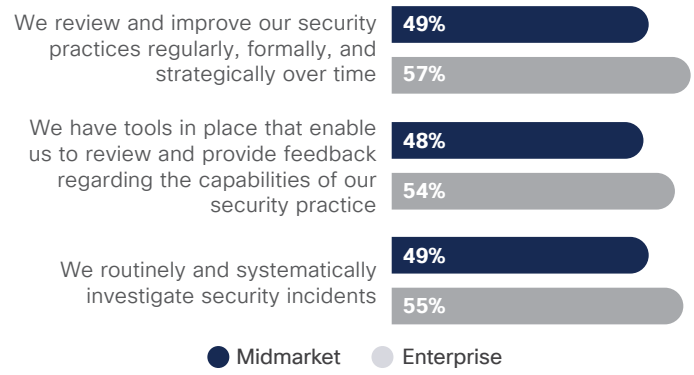
On a positive note, 91 percent of midmarket businesses said they conduct drills to test their incident response plans at least once a year. However, as with their reliance on the cloud and outsourced partners, the question is whether such incident response plans are adequate to push back on increasingly sophisticated attackers.

Figure 9 Midmarket businesses outsource advice and consulting as well as incident response



Source: Cisco 2018 Security Capabilities Benchmark Study

Figure 10 Midmarket businesses less likely to strongly agree on the use of operational processes



Source: Cisco 2018 Security Capabilities Benchmark Study

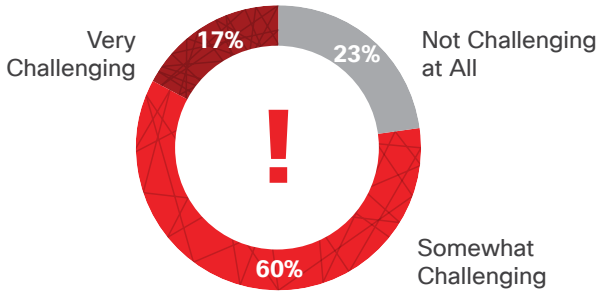
Connecting people, processes, and technology: The orchestration challenge

If small/midmarket businesses add more security products and vendors to their defenses—and shift IT resources to managing these products—will their organizations better manage security? The opposite may be true, at least in terms of understanding and orchestrating security alerts.

Most small/midmarket businesses today recognize that as they create a more complex product and vendor environment, their responsibilities increase. For instance, 77 percent of midmarket businesses found it somewhat challenging or very challenging to orchestrate alerts from these many solutions (Figure 11).

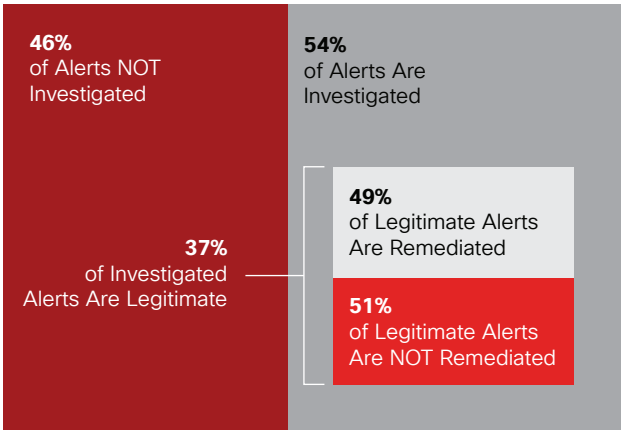
When businesses try to analyze these alerts, the combined challenges of people, processes, and technology can cause many alerts to be left uninvestigated, as the benchmark study found (Figure 12):

Figure 11 Midmarket businesses less likely to strongly agree on the use of operational processes



Source: Cisco 2018 Security Capabilities Benchmark Study

Figure 12 Percentage of security alerts that are not investigated or remediated



Source: Cisco 2018 Security Capabilities Benchmark Study

Recommendations for the future

Technology

As organizations consider new tools, ideally, they can avoid adding to the number of vendors they manage and alerts they must respond to.

With that in mind, are products built with openness in mind? How will they integrate with others in terms of sharing data and threat intelligence? Is there management console integration?

If a vendor says products are built to fit and work with others – does this happen out of the box or will the buyer have to do considerable API work?

Machine learning, while surrounded with hype, has its place in security. However, look for machine learning as a detection layer inside already deployed products versus a stand-alone product from another vendor that adds another product to manage.

People and Process

To put it plainly, develop a strategy to improve cybersecurity. Only 38 percent of small/midmarket businesses have an active cyber-risk strategy in place, according to the Vistage Research Center, a resource center for business leaders.[6]

Does your planning include end users receiving appropriate training? Do your insurance policies cover the loss of business stemming from a cyber attack? How about creating business continuity and crisis communication plans to enable faster recovery and help prevent reputational damage.

Also, IT leaders must explain in clear terms what business management really wants to know with respect to breaches:

- What is the impact to the organization?
- What measures the security team is taking to contain and investigate the threat. How long it will take to resume normal operations.?[7]

"By adopting a set of security platforms and tools that all work together, versus disparate pieces that may actually conflict with each other, you get an amplification of security effectiveness, as well as a simplification of management."

Ben M. Johnson, CEO of Liberty Technology

"Small/midmarket businesses should assess these risks and develop response plans before a breach—not after."

Chad Paalman, NuWave Technology Partners

6 Cyberthreats and Solutions for Small and Midsize Businesses, Vistage Research Center, 2018. Developed in collaboration with Cisco and The National Center for the Middle Market. Available at: https://www. vistage.com/research-center/business-operations/risk-management/20180503-22912/.

7 Cisco 2017 Midyear Cybersecurity Report: https://www.cisco.com/c/dam/global/es_mx/solutions/security/pdf/cisco-2017-midyear-cybersecurity-report.pdf. 13 Ibid.

Conclusion

A final recommendation for small/midmarket businesses to drive improvements in cybersecurity is to recognize that incremental change is better than no change. In short, they should not let a desire to be "perfect" in their security approach get in the way of becoming "better." Perfect, as in all things, does not exist.

Small/midmarket businesses also must understand that there is no "silver bullet" technology solution to solve all of their cybersecurity challenges. The threat landscape is too complex and dynamic. The attack surface is always expanding and changing. And, in response, security technologies and strategies must continually evolve as well.

To learn more about Cisco's threat-centric approach to security, visit cisco.com/go/security.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Published July 2018