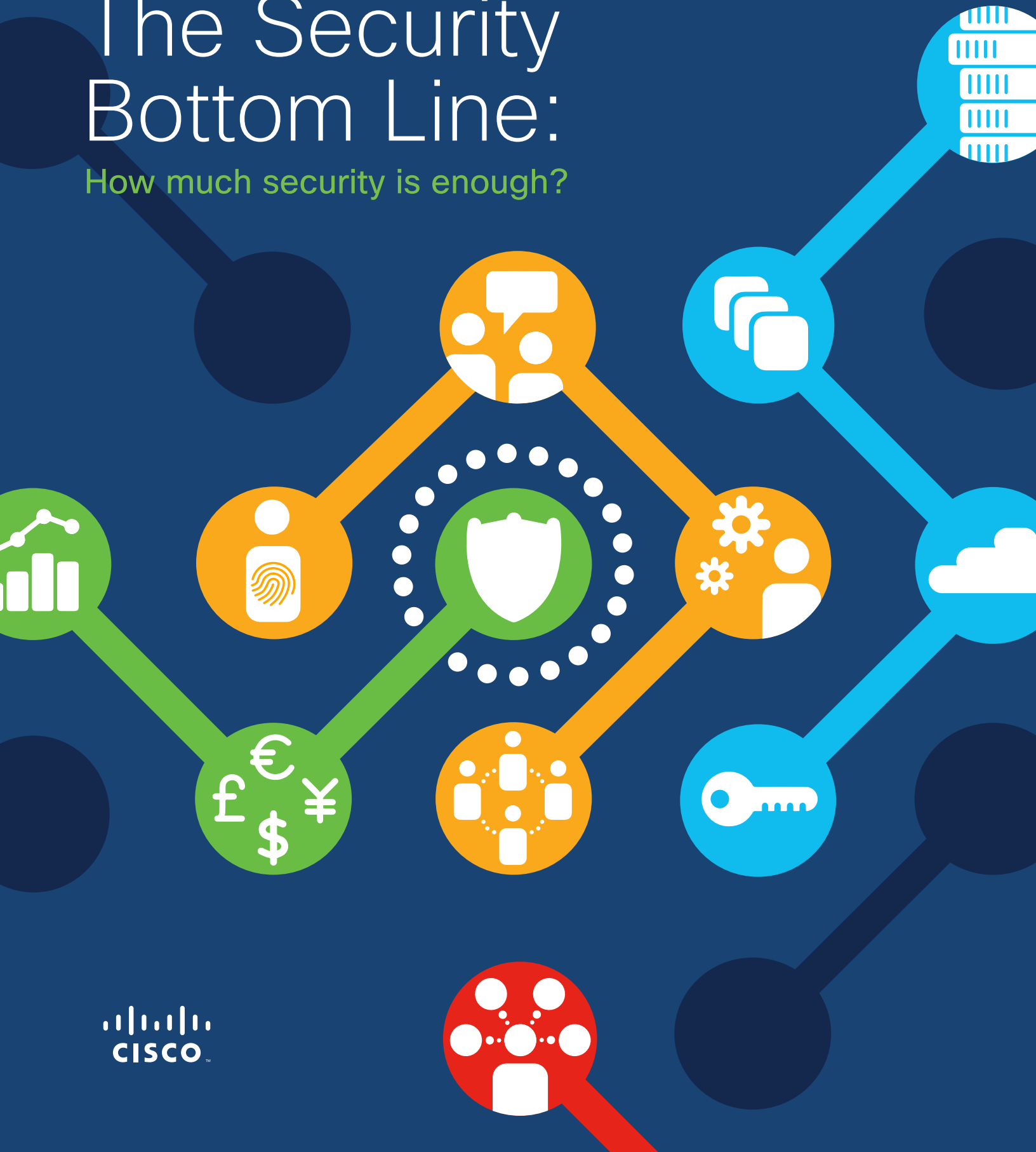
The Security Bottom Line:

How much security is enough?



CISCO

Contents

Introduction: The Security Bottom Line

When organizations have dozens of security products installed, and yet still get breached, it begs the question: *How much security is enough?* How many products does an organization need? Which ones? How much should be spent on security? In other words, *where is the security bottom line?*

Security is something that organizations could spend infinitely on, trying to keep attackers at bay. But how much do they *need* to spend, and what do they *need* to do, to remain safe?

And it goes beyond money. Perhaps an organization has a substantial budget for security, but hasn't hired the right experts to execute its vision. Or maybe an organization has a reduced security budget, but has invested it wisely in the right people and technology – and on its most vulnerable or critical assets. Sometimes, much of an organization's security is managed by a third party, and it doesn't have the leverage to influence necessary changes or upgrades.

So yes, budget is important when it comes to security. But it's not everything. Where does your organization stand when it comes to security? Do you have the right people, processes, and technology in place to proactively defend your environment? Are you falling below the security bottom line, or rising above it?

In this report, we will outline key factors for security success, as determined by our industry experts, and a group of roughly 80 participants in a recent, double-blind survey of security professionals conducted by Cisco. And of course, it wouldn't be fair if we didn't provide at least a little guidance on how to take your security to the next level.

"There are many dynamics to security challenges beyond just money."

Wendy Nather, Head of Advisory CISOs, Cisco

The Numbers Don't Lie

It was telling to find in our recent survey that 56 percent of respondents (over half) have experienced a significant security event (breach, intrusion, malware infection, etc.) in the past year. Ninety-four percent of respondents said they know they have further to go to implement effective security. And 43 percent admit that they sometimes have to take shortcuts for dealing with security issues – such as completely wiping an infected endpoint rather than surgically removing the malware. (See Figure 1.)

Figure 1 How are today's organizations doing with security?
Percent of respondents, N=79

Source: Cisco 2019 Security Bottom Line Survey

But it's not all bad news. Ninety-five percent of respondents said they can efficiently identify which data and systems within their organization require the highest levels of protection – a good start! So why are they still struggling? Is it about the money? Or are other factors at play?

Cisco's Head of Advisory CISOs, Wendy Nather, calls out the following four factors that can affect security success:

- Budget
- Expertise
- Capability
- Influence

Nather famously coined the term "security poverty line" several years ago to initiate this discussion. She also authored two reports on the topic while serving as a research director at **451 Research**: "Living Below the Security Poverty Line" in 2011 and "The Real Cost of Security" in 2013.

"Based on my previous experience as a CISO in both the public and private sectors, I know there are plenty of organizations that struggle with security," says Nather. "There are many dynamics to security challenges beyond just money – such that an organization spending millions could still be doing poorly in security, while an organization with a smaller budget could have sufficient defenses based on its specific needs."

Factors for Determining Security Success

Money aside, there are other factors that can affect the security bottom line. Alongside budget, there's also expertise, capability, and influence.

Budget

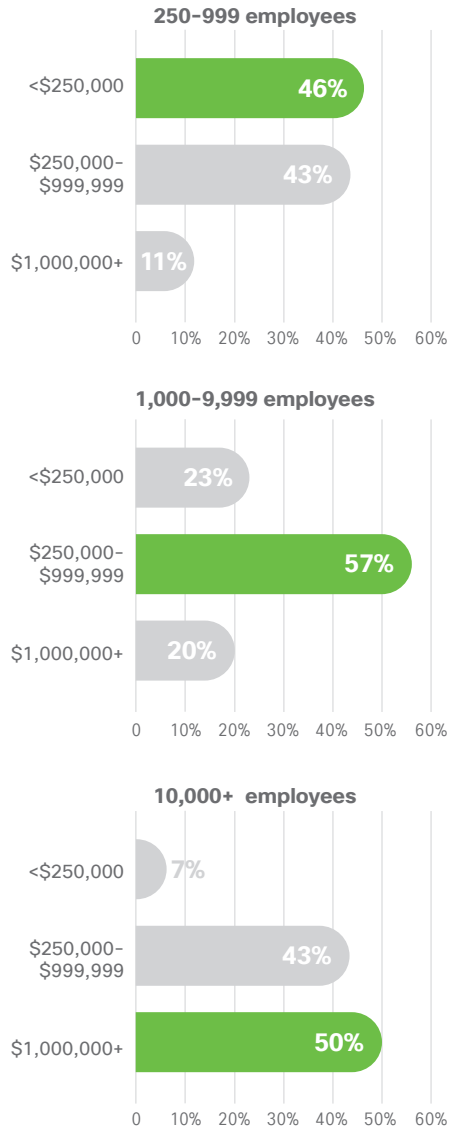
What are organizations spending on security?

There is no magic number when it comes to security spending. The amount any given organization should spend on security depends on several factors including: size, industry, risk appetite and posture, and so on. However, we have broken out the annual security spend of our survey respondents (based on organization size) to serve as a rough benchmark for other organizations. As Figure 2 illustrates:

- Among **mid-market organizations (250-999 employees)**, 46 percent are spending under $250,000 annually on security, and 43 percent are spending $250,000 to $999,999 annually. (Only 11 percent are spending $1 million or more annually.)
- The majority (57 percent) of **enterprise organizations (1,000 – 9,999 employees)** are spending $250,000 to $999,999 annually on security. (Only 20 percent are spending $1 million or more annually, while 23 percent are spending less than $250,000 annually.)
- Fifty percent of **large enterprises (with over 10,000 employees)** are spending $1 million or more annually on security, with 43 percent spending $250,000 to $999,999, and just seven percent spending under $250,000.

While these numbers provide some basic insight on the ratio of size of organization to security spend, it's important to note that the size of an organization isn't everything when it comes to security spending. The number of employees alone doesn't necessarily correlate with the amount of revenue or funding available, or even the amount of risk that the organization faces. For example, a hedge fund may be managing billions of dollars with a small team, and a large state government agency with lots of employees may have a thin and fluctuating budget.

Figure 2 How much does your organization spend annually on security?



Source: Cisco 2019 Security Bottom Line Survey

Another popular yardstick for gauging security spend is taking a percentage of the IT budget. However, percentages don't help when the numbers involved are very large or very small. If a bank can afford to spend 10 percent of a billion-dollar IT budget on security, it can buy a lot more than a startup that gets 10 percent of a $50,000 IT budget to spend on security. When enterprises are setting spending levels for security, they are better off pricing out the specific security capabilities they need instead of simply picking a percentage of the IT budget at random.

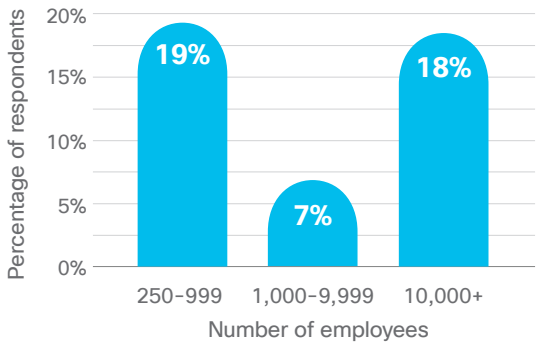
Can organizations afford the security they need?

An astounding eighty-four percent of survey respondents said they were able to afford some, but not all, of the *minimum* amount of security they needed to defend their infrastructure. Interestingly, we found that it was organizations with 1,000 – 9,999 employees that seemed to be struggling most when it comes to affording what they need – with only seven percent of these organizations saying they were able to afford all of the minimum security they needed. (See Figure 3.)

Comparatively, 19 percent of smaller organizations (250-999 employees), and 18 percent of larger organizations (over 10,000 employees) said they were able to afford all of the *minimum* security they needed. It appears that as organizations grow, security budgets do not always grow proportionately (until a very large number of employees is reached).

"The interesting question is why it's not the smallest organizations that most often rate themselves as being unable to afford the minimum security they need," says Nather.

Figure 3 My organization is able to afford all of the minimum security it needs.
Percentage of respondents who agree



Source: Cisco 2019 Security Bottom Line Survey

"Is it because they feel they're less of a target, and therefore don't need as much security? Does the perceived security risk grow in relation to other growth factors of an organization? Or does an enterprise come onto the radar of attackers after it achieves a certain profile, only to be faced with a security imperative that it realizes it hasn't met?"

Does a bigger budget increase security confidence/capability?

Twenty-seven percent of organizations spending $1 million or more annually on security said they were able to afford all of the minimum security they needed, versus only nine percent of those spending $250,000 to $999,999. So it seems logical that, yes, increased spending does make some difference in security capability.

However, organizations across all security budgets still feel they have further to go to implement effective security. Ninety-four percent of those spending $1 million or more annually said they have further to go, while 95 percent of those spending $250,000 to $999,999 said so, and 92 percent of those spending less than $250,000 said they have further to go.

Among organizations with 1,000 – 9,999 employees, only 23 percent said they rely most on internal staff for security expertise. This once again speaks to the finding that organizations of this particular size are struggling most when it comes to affording the security capabilities they need.

So while budget definitely helps, it's not everything when it comes to security. What other factors come into play?

Expertise

Do organizations have the appropriate staff and skills to effectively secure their environments?

When asked who they rely on *most* for security expertise, only 37 percent said internal staff. Almost as many respondents (28 percent) said they rely most on professional networks. This speaks to the widespread skills shortage in cybersecurity. According to **research by (ISC)²,** we have a shortage of nearly 3 million cybersecurity professionals around the world today.

While it's good that organizations feel they can turn to outside resources for security expertise, there is also critical business knowledge for which they should be able to rely on their internal security staff. This includes knowledge surrounding user experience and process design, risk analysis, and incident response.

"There are many security risk calls that need to be made, and a lot of incident response work that can only be done if you have institutional knowledge of an organization," said Nather. "So even when you have external incident responders, they still have to rely on internal professionals who know what's going on within the network."

We also uncovered that 34 percent of respondents are learning about security vulnerabilities and incidents that affect their organization from the media. This highlights the ongoing need for reliable journalists and expert bloggers to fill the cybersecurity situational awareness gap for many enterprises.

Capability

What additional factors are hindering organizations from achieving strong security?

Even if an organization has the expertise to know what it needs to do in its security program, that doesn't necessarily mean it has the capability to execute on it. For example, conventional wisdom holds that network segmentation is a critical cybersecurity control, but a complex legacy network run by multiple providers may be too difficult and costly to disentangle with available resources.

Additionally, security teams can't always dictate their requirements to outside groups or organizations. For example, when a manufacturer has to meet dozens of country-specific operational standards and regulations, it can take years for it to clear and distribute a software update for its control systems.

Capability is an important factor in the bottom line. Sometimes also referred to as "security maturity," capability rests on fundamental functionality that organizations need before they can move ahead with more sophisticated projects. This includes (see Figure 4):

Figure 4 Security Maturity Pyramid

1. **Knowing what you have and what it's doing.** Keeping an asset inventory up to date isn't as easy as it sounds in today's dynamic environment. Many application ecosystems are so complex that no one person may know what data is being shared, for what purposes, and through which interfaces. User audits generally uncover accounts that are critical but undocumented.
2. **Being able to initiate (and prevent) changes to resources.** If you don't control a resource, you have to be able to get the owner to change it in a timely fashion to fix a vulnerability. Likewise, you need to make sure that changes only happen when they are approved, and that they take technology dependencies into account as well.
3. **Understanding your security risks.** What are your most critical assets, and what are they worth to criminals? You should know what kinds of threats are most likely to target your resources, how to recognize them, and how to block them. Otherwise you may spend time and money on assets that don't matter, while ignoring the ones that do.
4. **Being able to install and operate security technology.** Once you've mastered the first three capabilities, you will be able to make effective use of products and services.

Which technologies are most commonly being used in security programs?

These are the top 15 security technologies being used by our survey respondents:

1. **Firewalls/Security Policy Management**
2. **Email Security**
3. **Network Malware Protection**
4. **Cloud Threat and Workload Detection/ Protection**
5. **Data Loss Prevention**
6. **Encryption**
7. **VPN**
8. **Secure Internet/Web Gateway**
9. **Security Information & Event Management (SIEM)**
10. **Network Access Control**
11. **Cloud Access Security Broker**
12. **Endpoint Security/EDR**
13. **Web Application Firewall**
14. **Network Threat Detection/Network Traffic Analysis**
15. **Threat Intelligence Platforms**

> **“The more products you have, the more work you’re trying to do to connect all of that information together. When you think about security, you have to take a holistic approach, not just a pillar-by-pillar strategy... With automation built in, you can start to take action without having to grow your team significantly.”**

Marisa Chancellor, Senior Director, Information Security, Cisco

Taken by itself, the top 15 technologies listed above make up a substantial portfolio, requiring a large number of people with heavy expertise to configure, maintain, and monitor it all. The implication is that the personnel cost of the security bottom line is higher than many organizations realize when they are trying to plan out what they need.

"In my previous role as an industry analyst, I polled security professionals on which technologies they thought CISOs needed to buy to properly secure their organizations," said Nather. "The answers I got were really across the board – indicating that there is no standard blueprint. Some named as few as four technologies, while others called out more than 31 different tools."

"Many respondents to this poll simply said that what an organization needs depends on various factors, including what kind of data it has, what industry it's in, whether it is geographically dispersed, and so on," Nather continued. "If we can't create a one-size-fits-all answer for the CISO – and the closest thing we have is a compliance standard for a tightly scoped, well-understood risk case such as PCI-DSS – then we can't expect every organization to know with confidence what it actually needs. And if it doesn't know what it needs, then it also doesn't know whether it can even afford security."

While there are some technologies most organizations will choose to have, such as firewalls and endpoint security, the rest really depends on an organization's specific situation. And it may require substantial research and a cybersecurity audit before an organization can determine what exactly it needs or can afford.

Kelley Misata, PhD, is the founder and CEO of Sightline Security. Sightline is a new cybersecurity company and 501(c)(3) nonprofit that is partnering with other nonprofits to assess, prioritize, and improve their security.

Cybersecurity for Nonprofits

Why is an organization like Sightline needed today?

Misata: Several reasons, but here are the top three. One, nonprofits don't know what they need yet. They're navigating cybersecurity without a map. With all the complexities in security today, that's really difficult – particularly when you have limited time, staff, and money. And rightfully so when you are focused 200% on your mission of helping others!

Two, commercial security solutions aren't designed with nonprofits in mind. Yes, nonprofits have similar business functions, but they also have nuances that make how they manage security different.

Three, nonprofits aren't well versed in the language of security, and frankly security professionals can sometimes make it a bit complicated for non-security people to understand what we are talking about. Nonprofits attend security conferences and find that they can't bridge what's being said or align the solutions being offered to their business. Sightline's mission is to be the bridge, translator, and advocate for these organizations. We are building assessment tools and a security community solely for nonprofits.

Influence

Can organizations effectively influence vendors, partners, and other third parties to provide the security they need?

Third-party supply chain security is a major concern for CISOs today. With services, hardware, and software coming from dozens or hundreds of different sources, organizations don't stand a chance when it comes to exerting complete control over their security.

And it's no surprise that the more employees and budget organizations have, the more likely they are to be able to influence vendors and partners to help them with security. For example, 86 percent of organizations with 10,000+ employees are learning about security vulnerabilities and incidents that affect their organization from the affected vendors/partners before they are public, versus just 60 percent of organizations with fewer than 1,000 employees.

And 38 percent of organizations spending $1 million or more annually on security said they were always able to add security-related terms and conditions to a vendor/partner contract, versus only 17 percent of organizations spending less than $250,000 annually on security. This indicates that larger organizations with more spending power are better positioned to negotiate with outside parties.

Where does this leave smaller organizations, who may be even more dependent on external partners? "Their best option may be to band together with peers to wield more influence over shared providers and suppliers," says Nather. "For example, industry associations, regional cybersecurity forums, or information sharing and analysis centers (ISACs) enable members to organize requests and responses to security issues. Finding or creating this influence is part of the CISO's job today, which makes networking even more important."

(Cybersecurity for Nonprofits, cont'd)

What are some of the particular security challenges that nonprofits face?

Misata: First, nonprofit businesses run very lean – meaning they don't have time or money to waste on anything that doesn't directly support their mission. For many nonprofits, cybersecurity is seen as expensive, overwhelming, and not needed until something bad happens.

Second, many nonprofits haven't identified which of their assets might be attractive to attackers. So how can they know what to protect? Many nonprofits today are led down the path of spending money on solutions before understanding what they need.

Third, one of the biggest challenges for nonprofits is that no one person in the organization is squarely focused on security. Even though they're very energized and know that security (particularly cybersecurity) is important, their attention is pulled in many directions.

The great news is that despite all of this, nonprofits are stepping up and are no longer seeing themselves as immune to an attack; they recognize that they have assets and data of value. But they often have minimal influence over vendors and service providers – they are far behind the curve. Through our work with Sightline members, we are now able to gather data and insights about the state of security in nonprofits so that we can start to bring them into the fold.

Key Takeaways

Overall, organizations do not think they can afford the security they need, no matter what size they are or how much they're currently spending.

Organizations in the middle with 1,000 to 9,999 employees are struggling the most to adequately secure their environments.

There is no single answer when it comes to which security products an organization should be using, or how much should be spent on security. It depends largely on the size and type of organization, the criticality of its assets, and what it can actually afford. This makes it more difficult for enterprises to figure out what their security programs should include.

Increased spending does not always translate into greater security capability/confidence. Other factors must be considered, such as expertise and influence.

Organizations should be sure that their internal staff continues to build expertise in both security overall and in their specific environment and risk profile. There are some aspects of security that only insiders are equipped to handle.

Capability plays an important role in the security bottom line. Factors such as whether or not a security team has control over certain resources can greatly impact its ability to execute on a defense strategy – even with the required budget and expertise on hand.

The bigger the organization, the easier it is to influence third parties that affect its security posture. Smaller organizations may need to leverage the power of associations to get the same influence and economies of scale.

Recommendations for Elevating Security

Regardless of where your organization falls in relation to the security bottom line, here are some recommendations for solving the main challenges raised in this report.

1. Figure out what's right for your organization

Organizations should take a close look at where their security spending is going. In this industry, there's a lot of pressure to keep up with peers. *"What is everyone else buying? Do I need that new technology?"* Of course, it's always good to keep an eye on the industry and evaluate what others are doing to increase their defenses. However, as we've confirmed in this report, security is never one-size-fits-all.

Before you go shopping for more technology, look at your expertise in relation to the security maturity pyramid in our capability section. As the old saying goes, "You can't secure what you don't know you have." And a vulnerability scanner won't help you if you can't fix what it finds.

Knowing which threats are not just possible, but *probable*, will help you focus on the right priorities when you can't cover everything. Consider conducting a **cyber risk assessment** either in house or via a third party to get you started on the right path.

2. Get more from your investments

An unfortunate trend over the years has been to always seek out the latest and greatest security products. This is good in theory for making sure you're protected from constantly evolving threats. However, for many organizations, it's created a complex mess of disjointed point products that are difficult – if not impossible – to manage. If you're getting too many alerts from disparate technologies and have to spend all day going back and forth between different applications to figure out what's going on in your environment, your security will suffer.

Instead, it's time to invest in security technologies that work for you – instead of the other way around. Cisco takes a **platform approach to security** – meaning, we don't just sell firewalls or email security or anti-malware technology. We provide an open and broad portfolio of security technologies that all work together to defend your network. If a threat is found in one area, we give you the ability to automatically block it everywhere else. Automation and integration can go a long way in minimizing complexity and making sure you get the most out of your security technologies and personnel.

"I look at security as an ecosystem. The more things work together, the better. If I have to spend time and energy integrating technologies on my own, it's less time I can spend actually doing security."

Steve Martino, SVP/CISO, Cisco

And when it comes to your vendors, be sure to take advantage of everything they offer – a lot of it for little to no cost. Attend those free webinars. Call on technical support. Attend vendor events. Join those customer advisory groups. Participate in vendor trainings. By all means, if you've invested in technology, your security staff should know how to use it effectively.

3. Adopt a zero-trust approach to security

Today's threats are coming at your organization from all angles. They are targeting users, applications, your network, the cloud, IoT devices, and the list goes on. This expanded attack surface makes it critical for organizations to take a **zero-trust approach** to security.

Zero trust requires organizations to:

- Obtain visibility into all areas of the network
- Adopt controls to ensure that only the right people, devices, and applications can operate in the organization's environment
- Have an effective means of blocking suspicious behaviors to prevent the spread of attacks

With these steps, organizations can more effectively protect their workforce, workload, and workplace.

By moving beyond basic security measures and taking a more layered, holistic approach to security, you can make it harder and more expensive for attackers to compromise your assets – which certainly helps your security bottom line!

4. Increase your training

Since many of our respondents are relying on outside sources for security expertise, it seems more training should be in order. Make sure that once you hire your talent, you continue to invest in their skills and understanding of your environment.

Allow them to attend conferences and workshops. Conduct internal training sessions. Encourage them to access free resources like the **Cisco Security Blog** and **Cisco Talos threat intelligence page** to stay up to date on the latest threats. Let them pursue more certifications. In short, make sure they're not just simply doing their jobs, but are becoming true experts in the process – not just security experts, but experts in your business as well. A third party will never understand your particular security needs and constraints as well as your own people.

5. Consider outsourcing

If you're running a bunch of old legacy systems, chances are your IT team is spending too much time managing and updating them, while getting ineffective security in return. Migrating from complex legacy systems to outsourced SaaS applications for well-known, non-core business functions such as email, office applications, payroll, and others can greatly help with security in those areas, so that you can concentrate on securing your core assets and processes.

For security products that require more dedicated staff than you have available (due to cost), outsourcing the management of those technologies through an MSSP is an option

as well. Realize that it's sometimes best – and more cost-effective – to get help with security than to try to do everything on your own.

6. Join forces

As our section on influence indicated, there's certainly power in numbers when it comes to security. If your organization is too small to assert influence over your suppliers, consider banding together with other organizations through professional networks or industry groups to build more clout. Being able to get timely bug fixes and updates from your vendors and partners is critical for effective security. And it is harder for them to say no to fifty small companies versus just one.

Visit cisco.com/go/security to find out how we can help protect YOUR environment.

Methodology

Our data for this report is based on an online, double-blind survey among approximately 80 IT decision-makers located in the U.S. who were asked security budgeting and planning questions. Respondents are full-time employees in mid-market (250-999 employees), enterprise (1,000-9,999 employees), and large enterprise (10,000+ employees) organizations; working for a for-profit, government, or higher education institution with a formal IT department. They are knowledgeable about security policies and procedures, involved in setting security strategy, and are spending at least 40 percent of their time on security.

About the Cisco Cybersecurity Series

Throughout the past decade, Cisco has published a wealth of definitive security and threat intelligence information for security professionals interested in the state of global cybersecurity. These comprehensive reports have provided detailed accounts of threat landscapes and their organizational implications, as well as best practices to defend against the adverse impacts of data breaches.

In our new approach to thought leadership, Cisco Security is publishing a series of research-based, data-driven publications under the name "Cisco Cybersecurity Series." We've expanded the number of titles to include different reports for security professionals with various interests, including the Data Privacy Benchmark Study, Threat Report, CISO Benchmark Study, and more.

For more information, and to access all the reports and archived copies, please visit: www.cisco.com/go/securityreports.

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 October 2019 BTTM_01_1019