CISCO CYBERSECURITY SERIES 2019 • CISO BENCHMARK STUDY
MARCH 2019

Anticipating the Unknowns

Chief Information Security Officer (CISO) Benchmark Study

Contents

Introduction: See No Evil, Block No Evil

Imagine if you could see deep into the future. And way back into the past, both at the same time. Imagine having visibility of everything that had ever happened and everything that was ever going to happen, everywhere, all at once.

And then imagine processing power strong enough to make sense of all this data in every language and in every dimension. Unless you've achieved that digital data nirvana (and you haven't told the rest of us), you're going to have some unknowns in your world.

In the world of security, unknown threats exist outside the enterprise in the form of malicious actors, state-sponsored attacks and malware that moves fast and destroys everything it touches. The unknown exists inside the enterprise in the form of insider threat from rogue employees or careless contractors – which was deemed by 24% of our survey respondents to pose the most serious risk to their organizations. The unknown exists in the form of new devices, new cloud applications, and new data. The unknown is what keeps CISOs, what keeps you, up at night – and we know because we asked you.

This is the 12th consecutive year we're publishing our findings around the cybersecurity landscape, and the fifth year we've conducted a benchmark study of thousands of security leaders. And this report is only the tip of the iceberg of data the survey generated. Over the coming year, we will publish more benchmark data by industry, geography, company size and job function, among other filters. To inform this report, we've surveyed more than 3,200 security leaders across 18 countries, asking questions in three categories:

1. **Set Up**: How do you set yourself up for success with training, budget, drills, best practices, and other core competencies?
2. **Architecture**: What is your approach to vendor/solution selection and alert management?
3. **Breach Readiness and Response**: How do you manage breaches in terms of what systems are affected, how much is lost, and how long does it take to recover?

Interview with Marisa Chancellor Senior Director, Security & Trust Organization, Cisco

You're defending 70,000 Cisco employees in 400 offices with hundreds of thousands of endpoints.

That's what I call my attack surface, and so as you can tell, there's a lot of stuff that people can try to get at. Yes – there are employees and data centers, but we also consume 600 clouds and so we have a true multi-cloud and hybrid cloud scenario to defend.

Tell us about your team's charter.

We are chartered to defend Cisco and we're focused on balancing the risk of Cisco as a business doing what it needs to get done, versus the risk of insider and outsider threats. And we focus on driving the right security architecture into our IT organization by looking at the incidents that come in that define the stability of our security posture.

(cont'd)

(cont'd)

What keeps you up at night?

Well I think for most people who are in security, what keeps us up at night is the unknown. When I think about what I must protect on a daily basis, we have a fantastic team and very capable technology, but we are focusing on the knowns, and the real threat is the unknowns.

We heard from CISOs about the number of alerts they have; do you think there are too many to manage?

That's true across the industry, but at Cisco on a daily basis, we look at 47 TB of network events on a daily basis and that all translates into about 22 incidents per day, which is impossible for a human to understand. It's coming at us from all over the spectrum, so we're having to figure out how to parse through all that information and how to get the technology to work for us. Being able to use machine learning and artificial intelligence to cull through a lot of those alerts allows us to hone in on the riskiest areas on which to focus. We don't have unlimited budget; therefore, how do we move at machine speed rather than human speed?

See more interview excerpts from Marisa Chancellor throughout this report.

We then compared performance across these areas to see whether, since we started tracking, you've made strides in building defenses, detecting cyber threats, and containing data breaches. This report sheds light on what actions are reaping results in strengthening organizational cyber health – so you can learn from your peers.

For example, when we asked, only 35% of you were able to confirm that, "It is easy to determine the scope of a compromise, contain it and remediate from exploits," suggesting that visibility into the unknown clearly is a key challenge. Maybe it was the "easy" part that threw you, as incidents are often not what they seem. Still, it means 65% of CISOs in the survey have room to improve. And yet we should take comfort from the 46% who said that they "have tools in place that enable us to review and provide feedback regarding the capabilities of our security practice". If you acknowledge when you can't see everything, at least you can measure and manage your ability to get better and see more.

While the good fight is far from over, it's also far from being all bad news. At least some respondents in our survey seem to be feeling good about their jobs. We asked whether you were experiencing cyber fatigue. We qualified this as having virtually given up trying to stay ahead of malicious threats and bad actors. Only 30% of respondents claimed to suffer from cyber fatigue this year. And while almost a third seems like a high number to be tapping the mat and raising the white flag, the drop from last year's figure of 46% is moving in the right direction and this is worth the fight.

If you consider the ability to see into both the future and past at once seems like a tall order, let's improve what we can see of the present moment, and look at some of the ways in which we measure up well, and not so well, today against previously reported data.

> “Our Security & Trust Organization is responsible for protecting Cisco; it’s as simple as that. But the flip side of that is - **how do we make sure that we can accelerate the business?** It doesn’t do us any good to lock down our entire environment where nothing is moving forward.”

Marisa Chancellor
Senior Director, Security & Trust Organization, Cisco

Look Back to Move Forward

Have CISOs become better or worse over the last year? We picked three areas that were hot-button topics last year and graded you according to your responses this year.

Technology

	You Said 2018	You Say 2019	We want to know more because...
Machine learning (ML) To what degree are you reliant on ML to reduce the level of effort required to secure the organization?	77%	↓67%	If anything, the negative trends in these first three questions probably stem from uncertainty and lack of confidence. Or that ML is not ready for prime time. Either way, we'd like to know more.
Artificial intelligence (AI) To what degree are you reliant on AI to reduce the level of effort required to secure the organization?	74%	↓66%	It could be that adoption is so widespread and integrated into your business processes that you don't feel it worth calling out.
Automation To what degree are you reliant on automation to reduce the level of effort required to secure the organization?	83%	↓75%	It's possible that you chose not to be "reliant," yet selectively automate. Even the largest organizations may not fully embrace automation.

Cost of a breach

	You Said 2018	You Say 2019	We want to know more because...
Thinking of the most impactful breach you experienced in the past year, what was the total cost?	8% said $5M+	8% said $5M+	Breaches remain a drain on resources and their impact is more than just financial.
	<$500K 47%	<$500K ↑51%	More than 50% of you are driving breach costs below half a million; excellent. Costs are down a little, or at least under control.
What improvements were made to better protect your company from security breaches?			
Separating IT and security functions	38%	↓35%	This is a controversial topic and the lack of a huge swing suggests you're equally divided as a group.
Increasing security awareness and training for employees	38%	↑39%	As long as people remain the weakest link, it remains an unknown just how much training is enough.
Implemented risk mitigation techniques	37%	↑39%	When you consider that this year, 20% of respondents claimed not to be very knowledgeable about risk and compliance, risk frameworks become standard operating procedure.
Increased investment in security defense technologies or solutions	41%	↑44%	Good, if paired with training and outcome-based measurement. Good for security metrics.

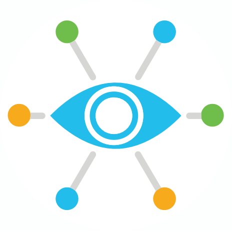
Cloud

	You Said 2018	You Say 2019	We want to know more because...
Moving security to the cloud has increased our efficiency, allowing our security personnel to focus on other areas	92% agree	↑93%	Continued adoption of cloud for the right reasons.
Leveraging cloud security solutions allows us to be more effective than operating with on-premises	91% agree	↑93%	A slight rise in cloud security confidence? We'll take it!
How challenging is it to defend cloud infrastructure from cyber-attacks	55% very	↓52%	A bigger drop in difficulty protecting cloud infrastructure? Even better!

Source: Cisco 2019 CISO Benchmark Study

State of the CISO

For some time now, threat hunters have talked about knowing the unknowns. It's time to expand that to the entire spectrum of cybersecurity: to users, apps, data, and clouds. You can't protect what you can't see.



You generally want to support the business, and not mire it down in bureaucracy. If you're going to be a bit more open, how are you mitigating control? This is going to be different for everyone. CISOs must deal with that balance of organizational culture while combatting the most critical threats. Sometimes blocking everything and locking everything down doesn't fit the culture of the enterprise. That might be right for a bank but not for a university.

The CISO faces several challenges managing cyberrisk – whatever their organizational model:

- Breaches create adverse impacts to financial profitability, brand reputation, customer data security, customer satisfaction, and continuity of business.
- Losses can be substantial and non-recoverable, creating a higher risk score for the organization on insurability.
- Over the years, vendor point solutions looked promising; however, each generates their own set of alerts. Many point solutions competing on alerts makes it difficult to identify those threats posing the highest risk to the organization, and becomes a resource drain.
- IT is usually siloed across the organization, making integration of securing the network, the cloud, and employee endpoints highly complex.
- Aggressive tactics to hire security IT personnel are required, as the specialized pool of candidates cannot sustain the magnitude of the problem across global organizations. The talent shortage is, however, out of control and not solvable by trying to fill all jobs.
- New threats appear daily, even hourly, and are employing more stealth and sophisticated methods. We recently reported on Emotet, Olympic Destroyer and other prevalent threats in Cisco's Threat Report 2019. Threat response as a category has to evolve and there is a need for tools to consolidate information and centralize remediation of infections and other incidents.

Additional technologies and processes for the the CISO to consider are:

- AI and ML, used right, are essential to triage the volume of work.
- The cost of a breach is falling – but don't get too excited yet.
- There is head room to realize obvious benefits in process improvement, e.g. training.
- There is more confidence in cloud-delivered security and in securing the cloud.

> **"You strive to understand how to get visibility into unknowns such as the new threats that are coming in – or even from within your own environment: unknown devices, apps, data. If you can't see it, you can't protect it. That's the biggest thing that keeps me up at night."**

2019 Findings

Our findings from the Benchmark Study revealed several areas that are critical to strengthening your organization's security posture. This section goes into detail on our findings of where and how CISOs and their peers are putting technology and processes in place (or not) to mitigate the damage that cyber breaches can have on their organizations, under the topics of best practices, architectural approach and breach readiness.

Set Up for Success?

What does it mean to be a CISO day-by-day? What is your charter? Our present survey revealed multiple areas that together determine your organization's cyber health, including: being practical about risk, setting criteria for budgeting, collaborating across divisions, educating staff, conducting drills, knowing how to track outcomes to inform investments, and being strategic on vendor and solution implementation.

Know your risk

Risk management is table stakes? Hardly. Understanding the risks of cyberattacks, and the compliance landscape that encompasses security breaches, is paramount to understanding how to defend and prepare for the worst. When asked who were very knowledgable about risk and compliance, only 80% of respondents were very knowledgeable. That leaves 20% of security professionals who could possibly use some of that training we discussed earlier. More unknowns – where you least expect them.

How to spend budget

Almost half, or 47% of you, are determining how to control security spending based on organizational security outcome objectives. Measuring outcomes against investments is the best data-driven approach. What's more, 98% of you strongly or somewhat agree that their executive team has established clear metrics for assessing the effectiveness of their security program. 49% of respondents have metrics that are utilized by multiple areas of their companies to understand the risk-based decisions and improve processes to measure the security effectiveness throughout the organization.

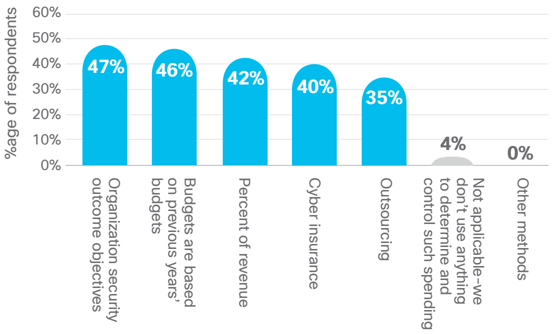
Back to the budget and, aside from outcome-based measurement, as shown in Figure 1 there are some less healthy options: Controlling security spending on previous years' budgets (46%) and percent of revenue respectively (42%) were both popular choices, but do not necessarily

> **"In some areas the risk is not as high because the organization has strong security practices; in other areas we have opportunities to shore up, minimize and close the gap on that risk. And that's how we make our investment as well as prepare for the next threats. We have to ask ourselves how we can build that foundational architecture to best prepare us for what's around the corner."**

correlate with better security. The breach landscape changes year-to-year, and your previous year's budget or percent of revenue may have little to do with what it costs to defend against future threats.

The fourth most relied upon approach to determining security spending is cyber insurance: **40% of you are using cyber insurance, at least partly, to set your budgets.** Taking this approach begins with a risk assessment to accurately identify your security risks and ensure they can be mitigated by insurance or protected by controls. It may be, for some companies that cyber insurance guidelines can play a role in technology selection and/or budget setting. Either way this merits further investigation in susequent reports.

Figure 1 Which of the following does your organization use to determine and/or control security spending?
Percent of respondents, N=3,259

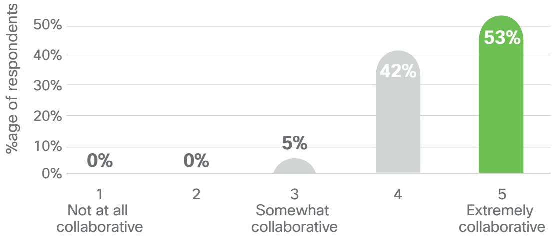


Source: Cisco 2019 CISO Benchmark Study

Collaboration not isolation

In past surveys, you've told us that you split security out from under IT and that you created the role of the CISO. Fortunately, you play well in the sandbox with your networking colleagues. Figure 2 shows us that 95% of you judge yourselves to be very or extremely collaborative between networking and security teams. You're not working in silos, and this has a tangible financial upside.

Figure 2 Respondents of different job titles reported on levels of collaboration between networking and security across the enterprise.
Percent of respondents, N=3,248



Source: Cisco 2019 CISO Benchmark Study

How much of a financial incentive? It turns out that **59% of those who were very/extremely collaborative between networking and security experienced a financial impact of their most impactful breach of under $100K – the lowest category of breach cost.**

This clearly merits further analysis and possibly points to greater need and possible development of more DevSecOps teams. The collaboration becomes not a matter of coincidence, but a must, especially in the age of Agile development.

And this is recognized at the highest executive levels. According to a recent CIO study published by IDG, "82% of CIOs expect their IT and security strategy to be tightly integrated in the next 3 years."*

*Source: A Secure Alliance: How the CIO-CISO Relationship Strengthens IT and Business, IDG, February 2019

Employee involvement: Drills and exercises

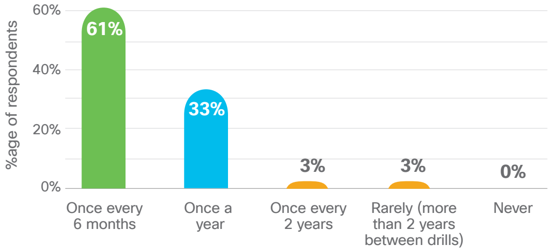
"What if we train our people and they leave?" goes the question. "What if we don't do it and they stay?" And the same applies from a security perspective. Yes, we focus on technology, but also we should spend equal time on process and on the people side of the business – because our people are the front-line of helping protect our organizations.

If people/users are cited as the weakest link in security, having a process that starts with onboarding new employees is common sense. Or so you'd think: only 51% rate themselves as doing an excellent job of managing human resources on security via comprehensive employee onboarding and appropriate processes for handling employee transfers and departures. It also seems counter-intuitive that the trend for training staff in the wake of an incident is flat year-on-year at only 39% of respondents.

A disaster striking can be perilous without proper preparations. Potentially there is room for improvement in this area when 61% of organizations perform a drill or exercise every six months to test response plans to cybersecurity incidents (Figure 3.) Drills can bolster the ability to have the proper controls in place to detect and respond as quickly as possible to mitigate damages.

> **"A lot of what catches people, when they get phished, is an emotional response and that's what hackers do; they try and provoke an emotional response, and so that's what we try and do in our phishing simulations with our employees. It's all context based, and so when an email apparently tells you there's a package waiting for you, who doesn't want to send or get a whole lot of packages?"**

Figure 3 How often (if ever) does the organization practice a drill or exercise to practice its response plan to a cybersecurity incident?
Percent of respondents, N=3,321



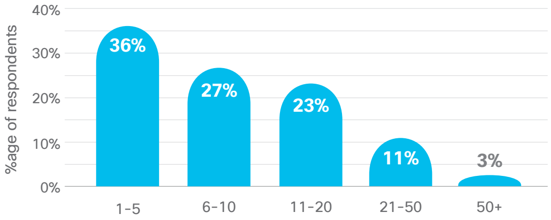
Source: Cisco 2019 CISO Benchmark Study

Architecture: Navigating the Vendor Buffet

As the need for an all-encompassing approach to protect from cyber threats has grown, organizations have rushed to acquire multiple point solutions. We know this because in 2018, 21% of respondents had more than 20 vendors and 5% had more than 50. This year that has fallen to 14% and 3% respectively. We're finding the trend for number of vendors and solutions going down; but as multiple vendor solutions aren't integrated, and therefore don't share alert triage and prioritization on limited dashboards, our survey found that even those CISOs with fewer point solutions could better manage their alerts through an enterprise architecture approach.

To better manage alerts, one best security practice is to reduce the number of vendors and point solutions. In 2018 there were 54% of respondents with 10 or fewer vendors in their environment, whereas now this number has risen to 63% (Figure 4.) This means more respondents have fewer vendors; vendor consolidation, for a variety of possible reasons, is real and measurable.

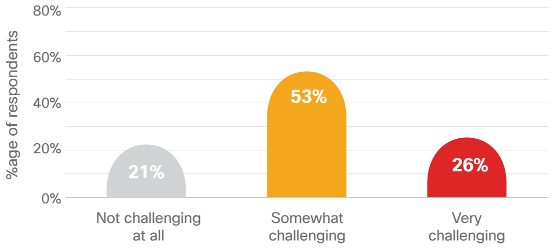
Figure 4 Number of security vendors (brands & manufacturers).
Percent of respondents, N=3,248



Source: Cisco 2019 CISO Benchmark Study

Don't just take our word for it. This multi-vendor approach (instead of an integrated approach) causes the persistent challenge of alerts to continue: 79% of respondents said it was somewhat or very challenging to orchestrate alerts from multiple vendor products, compared with 74% in 2018 (Figure 5.) Thus, while security professionals are attempting to address vendor sprawl and its attendant issues, managing it has not become easier and needs further improvement to optimize resources. This is where security analytics, machine learning, and AI can greatly help by automating the initial stages of alert prioritization and management. Too bad adoption rates for these new technologies seems to have wobbled slightly this year.

Figure 5 Managing alerts from multiple security vendors.
Percent of respondents, N=3,248



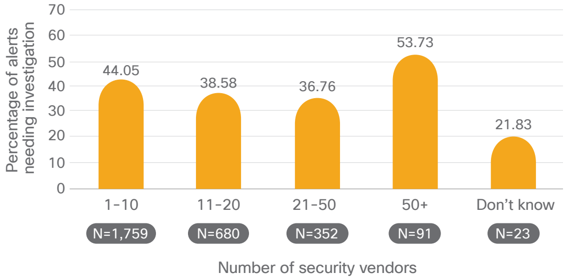
Source: Cisco 2019 CISO Benchmark Study

> **"If we can reduce the vendor footprint and have a more integrated architecture, that helps us significantly. I would rather have more automation on the back-end through an integrated architecture than having to slap something on top of it and write some new scripts to bring it all together."**

Although the size of your organization may certainly contribute to your numbers of alerts and vendors, data tells us that fewer vendors can make alert management more efficient (see Figure 6.) At the top end of the funnel, 63% of organizations with only 1-5 vendors and 42% of organizations with 6-10 vendors saw fewer than 5,000 alerts per day. Of course it also might tell us they have alerts turned off.

And reducing the number of vendors you have to manage helps your teams focus on more important work like remediation. Those with fewer than 10 vendors had a higher average response rate, remediating 44% of legitimate alerts, rather than 42%. You gain efficiency by lowering the number of security vendors as shown in Figure 6.

Figure 6 The contrast of how many alerts that need to be investigated by security vendor footprint.
Alerts, N=2,905



Source: Cisco 2019 CISO Benchmark Study

Finally, we found that 65% of organizations that are very up-to-date, and constantly upgrading with the best technologies available, more often experienced a lower count of daily security alerts (up to 10,000 per day). The next best option – to replace or upgrade security technologies on a regular cadence (but not necessarily be equipped with the latest and greatest tools) – had a 60% chance of receiving up to 10,000 alerts per day.

> **“At the end of the day it is about culling through all the alert information, and this is where we have set Plays to look at information. So, if we start to see a certain type of event this is what's going to trigger an incident for us.”**

Alert management challenge: You don't know what you don't know

Talking about too many alerts to anyone in security is like talking about the challenge of traffic to anyone in a major city. It's bad, we get it, move on. But you generally do something about it: car pool, avoid rush hour, work from home. And alerts are also the key to the unknown and cannot be ignored. Buried in that pile of information is the 1% of threats that get through even the best layered defense.

Here are five findings related to the alert landscape as you related to us:

1. There has been a year-on-year shift towards respondents seeing fewer alerts, which should mean less to manage, and in theory an easier time getting to the alerts that matter. The group with the lowest volume of alerts sees 10,000 or less per day, and 59% are in this group, versus 50% in our previous year's survey.
2. Ten thousand daily alerts are still too many? Sure, but when you consider that 41% see more than 10,000 and that some claim to see more than 500,000 alerts (admittedly only 1%), the figure of 10,000 is at least moving in the right direction.
3. The good news is over. You're responding to 50.7% of alerts compared with 55.6% in 2018. This suggests that while some of you are seeing fewer alerts, which feels like it should make the job easier, many are actually responding to fewer of them.

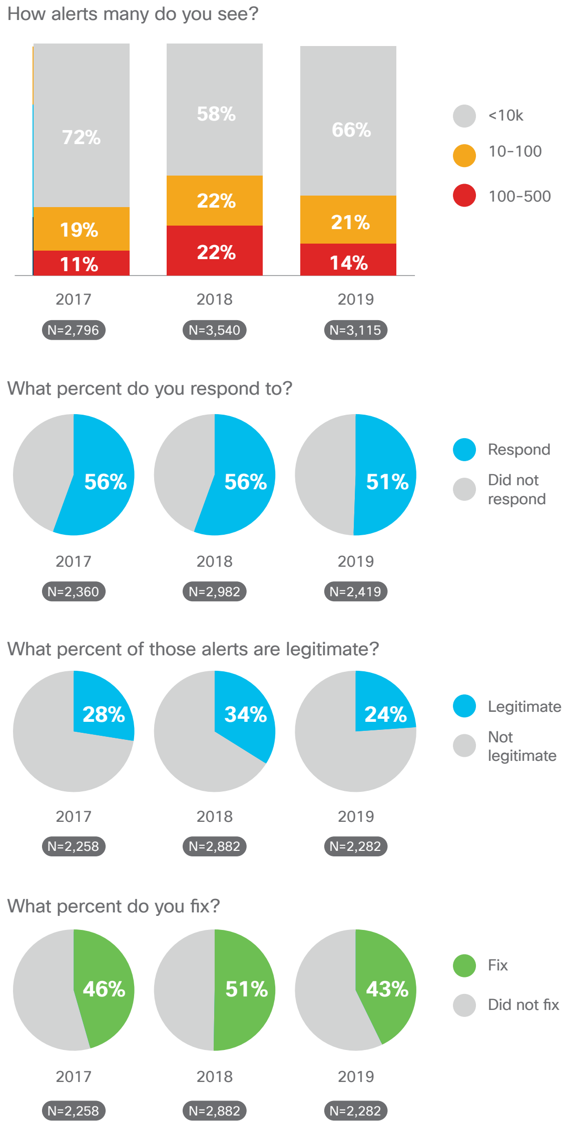
4. Only 24.1% of alerts that were investigated turned out to be legitimate, down from 34% in 2018. This shows that the accuracy of the tools used to determine which alerts should be investigated are not doing their jobs.
5. There's worse news still when we look at alert remediation: there is a dramatic drop from the 2018 survey in the number of legitimate alerts that get remediated – from 50.5% to 42.8% this year.

Put another way and illustrated in Figure 7: if you are one of the organizations that faces up to 10,000 alerts per day, that leaves 1,000 legitimate alerts unattended. Every single day. And that's just the half (50.7%) you investigated. The case has never been stronger for security threat response tools that can ingest broad data sets, provide visibility into that big data, and provide a means to rapidly take action.

Manage what you measure

This drop in remediation is crucial given that many of you are moving towards remediation as a key indicator of security effectiveness. The number of respondents who use mean time to detection as a metric decreased from 61% (2018) to 51% (2019) on average. Time to patch has also dropped in focus from 57% (2018) to 40% (2019). The biggest shift is in respondents who focus on ***time to remediate*** (48%) as an indicator, which rose from 30% in 2018. This shows a new focus on remediation as a security professional's KPI to measure their security posture. *When you contrast this with the rise in the number of legitimate alerts not being remediated, a drop in investment in machine learning and a slow rise or steady rate in the amount of training, it appears we are in need of more innovation in alert management.*

Figure 7 Comparison from survey results of how many alerts are seen, what percentage are responded to, which percentage of those alerts responded to are legitimate, and what percentage of incidents are remediated.



How alerts many do you see?

What percent do you respond to?

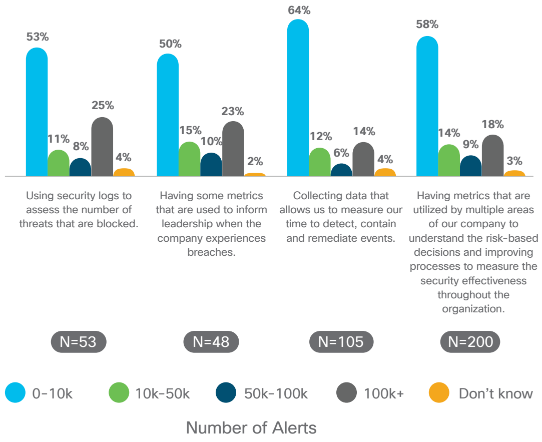
What percent of those alerts are legitimate?

What percent do you fix?

Source: Cisco 2019 CISO Benchmark Study

The survey data also revealed that 64% of those that collect data that allows them to measure their time to detect saw 10,000 or fewer daily alerts – the highest cohort in this matrix (see Figure 8.)

Figure 8 How does your company measure your security effectiveness, compared to the number of alerts you experience?
Percent of respondents, N=3,259



Source: Cisco 2019 CISO Benchmark Study

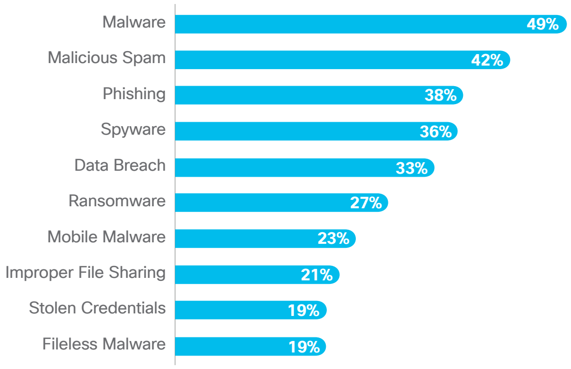
Breach Readiness and Response: When the Unknowns Comes Calling

Attacks seen in the past year

For the first time this year, we got specific in asking about the types of attacks that CISOs have experienced and we asked about a set list of common attacks. While some have seen highly specific variants of malware such as WannaCry (11%) or threat categories such as wiper malware (15%), the most oft-cited attacks are malware and variants such as ransomware.

> **“Today 90% of our incidents are still related to malware, or the evolution of malware such as ransomware and similar attacks. And it's those advanced persistent threats where we don't quite know what that threat vector is yet.”**

Figure 9 Which security incidents/attack types have you encountered in the past year.
Percent of respondents, N=2,909



Source: Cisco 2019 CISO Benchmark Study

As shown in Figure 9, two of the top three are issues with email security; that remains the #1 threat vector. Whether you are investing in protecting the move to Microsoft Office 365 or trying to better protect against Business Email Compromise (BEC) using DMARC, email is still an area to focus on. That two of the top 10 are insider threat issues (file sharing and stolen credentials), shows that you must look at what's happening inside as much as outside, and be aware that some criminals can log in rather than break in. This drives the need for better multi-factor authentication (MFA). Nowhere is the need more apparent for balancing the need for security (letting the right people in) with supporting seamless business (not hindering the people you do let in with a clunky user authentication experience).

And as concern with other areas remains high but manageable (such as the move to the cloud), concern about user behavior (e.g., clicking malicious links in email or websites) remains high and is now the top concern for CISOs. When asked about the challenge of defending various parts of their infrastructure, the highest concern was user behavior. This perception of vulnerability has held steady for the past three years between 56 to 57% of respondents.

We also asked which of these types of attacks resulted in some level of breach (loss of data) and received this priority of responses:

1. Malware (20%)
2. Data breach (19%)
3. Spyware (14%)
4. Phishing (13%)
5. Ransomware (13%)
6. Malicious spam (13%)

Interestingly, the perceptions of risk varied among security-related roles. For instance, the Risk and Compliance Officers consider the biggest vulnerability to be "Targeted Attacks" – these executives are well-aware of the dire consequences a fatal attack could have on continuity of business.

To learn more about what breaches are threatening your organizational stability, read Cisco's Threat Report 2019.

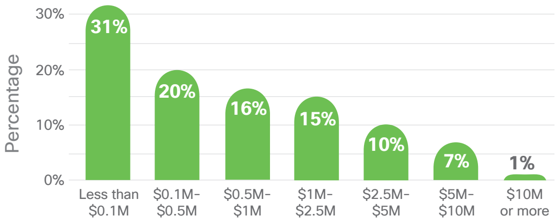
Cost of a breach: More than just money

We're all aware of the potential consequences of a breach: financial loss (see Figure 10), brand and reputational setback or ruin, shaken stockholder confidence, loss of valuable data, regulatory and non-compliance penalties, and the list goes on. Looking at the year-on-year comparison of data, there is a clear shift towards issues of perception and sentiment; there's no let up on the need to keep operations running, but customer experience and brand reputation both jumped up as key concerns (Table 1.)

Table 1 Top concerns due to breaches.

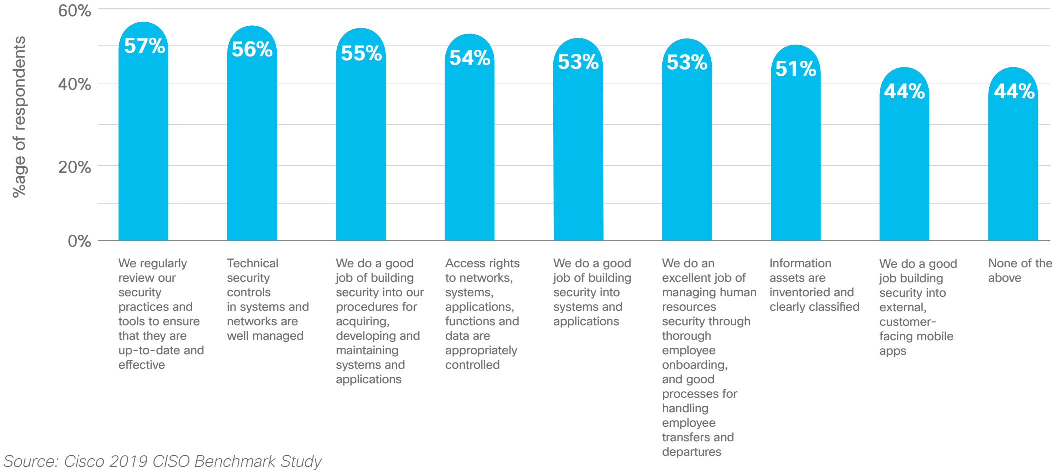
Concern Due to Breach	You Said: 2018	You Say: 2019	
Operations	38%	36%	A marginal shift downwards in operational concern is overshadowed by customer-facing worries.
Customer retention	26%	33%	Continued negative sentiment around data breaches and the prevalence of malware such as ransomware makes consumers wary.
Brand reputation	27%	32%	Household names become synonymous with a large attack for years; we're not naming any here but think customers will quickly build a list.

Figure 10 Thinking of the most impactful breach your organization has experienced over the past year, what was the financial impact?
Percent of respondents, N=2,386



Source: Cisco 2019 CISO Benchmark Study

Figure 11 Which practices are being employed to safeguard the organization?
Percent of respondents, N=3,223



Source: Cisco 2019 CISO Benchmark Study

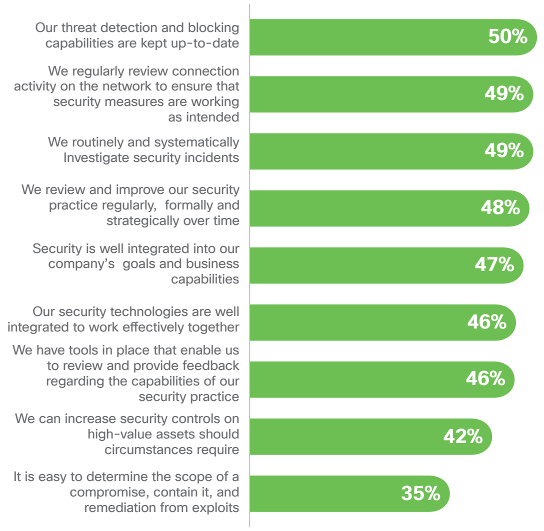
What you are doing to address the threat of a breach

We asked our security professionals to what extent their organizations took precautions to put people, process, and products in place to safeguard their organizations.The results are shown in Figure 11.

Further, we asked what approaches are taken to mitigate security risks, and those results are shown in Figure 12.

And from even more data, we found that although 85% of respondents were very knowledgeable about policies and practices regarding infrastructure security and protection, only 74% were very knowledgeable about business continuity and disaster recovery. Only 75% percent of respondents were very knowledgeable about incident response. This is a problem. 100% of anyone involved in security should be knowledgeable about incident response; and in fact, this can be extended to all employees within an organization. This is where training becomes so vital, and its lack of prominence in this year's results continues to stand out.

Figure 12 Security postures: Approaches taken to mitigate security risks.
Percent of respondents, N=3,248



Source: Cisco 2019 CISO Benchmark Study

Dealing with the Unknowns

The bridge between finding unknown threats and acting upon the right ones lies in an effective security posture. Here are practical recommendations we devised based on our survey findings for you to consider:

- Base security budgeting on measured security outcomes with practical strategies coupled with cyber insurance and risk assessments to guide your procurement, strategy, and management decisions.
- The only way to understand the underlying security needs of a business case is to collaborate across siloes – between IT, Networking, Security, and Compliance groups.
- There are proven processes that organizations can employ to reduce their exposure and extent of breaches. Prepare with drills; employ rigorous investigative methods; and know the most expedient methods of recovery.
- ML, AI and more automation should be able to boost security efforts exponentially – and next year we need to see more respondents in the "completely reliant" phase of implementation and practice. Cisco employs machine learning technology in various security products including Advanced Malware Protection, Umbrella, Stealthwatch and Cisco Threat Response.
- Build a security operations Center (SOC) to manage breach response in organizations of all sizes.
- Cloud security can help with the unknown. Ninety one percent agree that utilizing cloud security increased visibility into the network. Cisco Umbrella is cloud-delivered security that blocks users from connecting to known and suspected malicious domains, IPs, and URLs, whether users are on or off the enterprise network.
- Secure data centers and multi-cloud ecosystems with integrated solutions such as the Cisco Secure Data Center solution featuring visibility, segmentation, and threat detection from Tetration, Stealthwatch, and the NGFW.
- Address the number one threat vector with phishing protection, advanced spam filtering, and defense against Business Email Compromised with DMARC; check out Cisco Email Security.
- Endpoint security helps address unknown threats on user devices; try Cisco Advanced Malware Protection for Endpoints also available on our web, email, cloud, and network security solutions, creating an environment of products that work together for more effective and efficient threat protection.
- Gain fast threat detection, highly secure access, and software-defined segmentation with Cisco's Network Visibility and Segmentation which combines Cisco Stealthwatch Enterprise, the Cisco Identity Services Engine, and Cisco TrustSec technology.
- Trusted access is a critical component of security. Duo verifies user trust (confirming a user is who they say they are) using its best-in-class adaptive multi-factor authentication (MFA) solution.

> **“It can seem an arms race at times to figure out how to keep in front of malicious hackers, but the way I look at what's coming around the corner is that you follow where the business is going in terms of new techniques and technology, and that's where you are going to see the gaps.”**

“Sometimes CISOs have used fear to drive some of the budget investment. What we prefer to look at is: What is the risk to the business? There are all levels of acceptable risk, and so we focus on where there is the highest risk to the company. We’re very fortunate that Cisco takes security very seriously and invests in that foundational architecture to best prepare us.”

Marisa Chancellor
Senior Director, Security & Trust Organization, Cisco

About the Cisco Benchmark Survey

The double-blind survey, conducted by an independent research partner, covers many industries including retail, transport, manufacturing, financial services, as well as government and higher education. Participants are full-time employees working in mid-market (250-999 employees), enterprise (1,000-9,999), and large enterprise (10,000+) organizations.

Respondents fill a variety of roles including Chief Information Security Officers (CISO), Chief Information Officers (CIOs), and other senior titles. They are knowledgeable about security policies and procedures and involved in setting security strategy. A majority hold titles of CISO, Director/Manager of IT and/or CTO, and 99% of survey respondents have a team in their organization dedicated to cybersecurity.

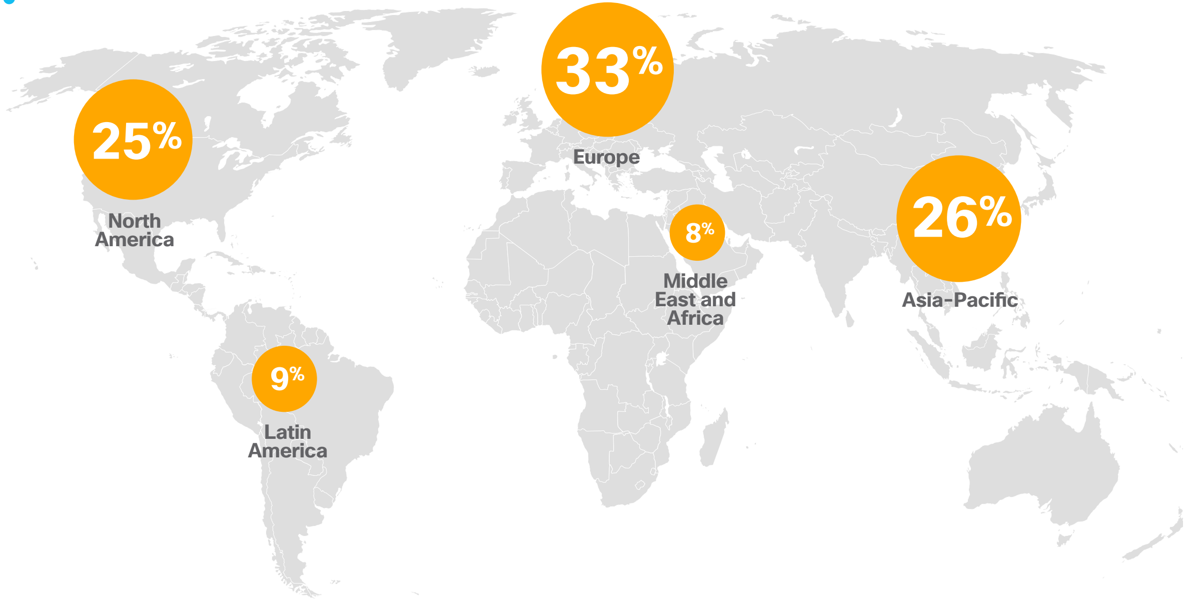
Respondents come from all continents and 18 countries including the USA, Canada, UK, France, Germany, Australia, Japan, and China (Figure 13.)

Qualified Respondents

The following criteria were used to qualify respondents:

- Adult (25 or older) who passes screening for sensitive/competitive employment.
- Works on a full-time basis for a for-profit company, government, or higher education that has 250+ full-time employees and a formal IT department.
- Is involved in IT Security beyond approving budgets.
- Is very knowledgeable about security policies and practices.

Figure 13 Respondent distribution by region, rounded up to nearest percent.
Percent of respondents, N = 3,259



Source: Cisco 2019 CISO Benchmark Study

The Cisco Cybersecurity Series

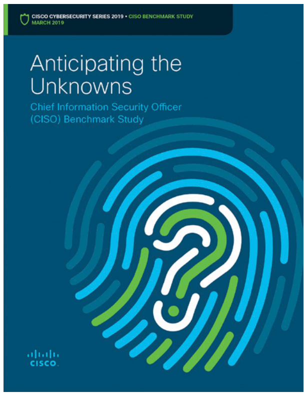
Throughout the past decade, Cisco has published a wealth of definitive security and threat intelligence information for security professionals interested in the state of global cybersecurity. These comprehensive reports provided detailed accounts of threat landscapes and their organizational implications,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

In our new approach to our thought leadership, Cisco Security is publishing a series of research-based, data-driven publications under the banner, Cisco Cybersecurity Series. We've expanded the number of titles to include different reports for security professionals with different interests. Calling on the depth and breadth of expertise in threat researchers and innovators in the security industry, the collection of reports in the 2019 series include the Data Privacy Benchmark Study, the Threat Report and the CISO Benchmark Study, with others to come throughout the year.

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

CISCO CYBERSECURITY SERIES 2019 • DATA PRIVACY
JANUARY 2019
Maximizing the value of your data privacy investments
Data Privacy Benchmark Study
cisco

CISCO CYBERSECURITY SERIES 2019 • THREAT REPORT
FEBRUARY 2019
Defending against today's critical threats
February 2019 Threat Report
cisco


CISCO CYBERSECURITY SERIES 2019 • CISO BENCHMARK STUDY
MARCH 2019
Anticipating the Unknowns
Chief Information Security Officer (CISO) Benchmark Study
cisco

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 March 2019 CISO_01_0319_r1

© 2019 Cisco and/or its affiliates. All rights reserved.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Adobe, Acrobat, and Flash are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries.