EXECUTIVE SUMMARY

2019

IDG Security Priorities Study

Exploring the security projects organizations are focused on now and in the coming year

THE IDG SECURITY PRIORITIES STUDY, a survey of information security professionals, shows signs usually met with cheering in the field. Spending will rise next year (again). More security leaders report higher in their companies. These are signs of commitment, of taking security issues seriously.

On the other hand, respondents also indicate that communicating security's value remains a challenge — some even regard it as a distraction from more strategic work. And security pros' uptake of emerging tools, services, and approaches is measured, if not slow. As ever, these professionals face dueling challenges of emerging threats, budget and staffing pressures, and the need to find the meaningful signals in a very noisy field. The IDG Security Priorities Study provides insight into these and more details of what's happening with security budgets, organizational models, toolsets, and more.

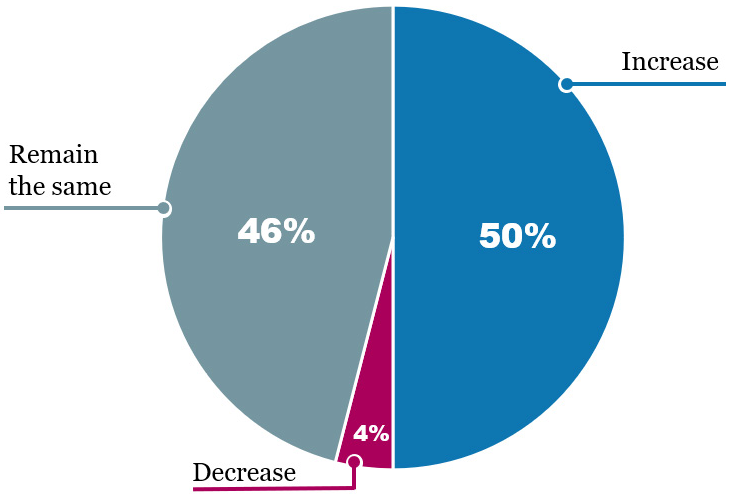
IDG surveyed 528 security-focused professionals worldwide who are involved in IT and security decisions in their organizations to gain a better understanding of the various security projects that organizations are focused on now, and in the coming year. The survey also provides insight into the issues that will demand the most time and strategic thinking from IT and security teams. Here are some of the key findings.

What's Driving Security Spending?

Fully half of respondents expect their security budget to grow in the next twelve months, while another 46% say theirs will remain flat versus last year.

The mix of their spending appears to be shifting gradually more toward operational expenses. Over the past two year, more respondents have seen an increase in OpEx (43%) than in Capex (34%), presumably reflecting the emergence of more as-a-Service options for security tools. Considering the speed of growth for overall IT cloud services — as one data point, Amazon Web Services revenue increased 41% year-over-year in the first quarter of 2019 — it could be argued that security is moving slowly in this regard.

EXPECTED CHANGE IN BUDGETS:



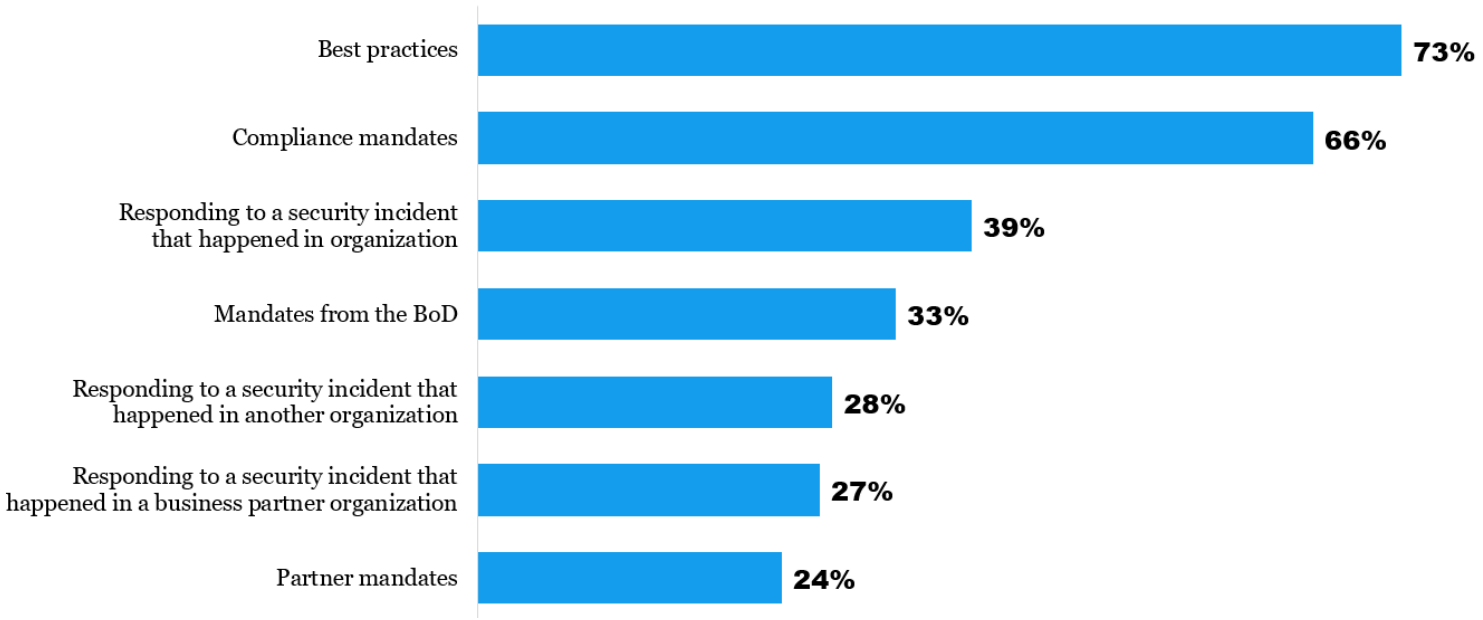
What is behind the increase in overall spending? The threatscape is dynamic, and large-scale data breaches continue to hit the headlines. 2019 thus far has seen news such as an estimated 885 million record breach at First American Corporation. However, this is a cadence of headline breaches stretching back through Target to Choicepoint, and malware from WannaCry and Stuxnet back to Slammer — and so on, for decades.

Now, survey respondents indicate that news-driven security prioritization is relatively less common in their organizations. Instead, the biggest drivers by far are best practices (73%) and compliance mandates (66%). Both of these answers have often-debated drawbacks. Experts note that even well-established best practice frameworks from NIST and COBIT are limited and organizations can struggle to implement their directives in each unique context, and with the greatest possible effect.

Compliance as a driver of budget and priorities is perhaps even more problematic. Survey respondents listed compliance mandates as one of their biggest distractions from executing more strategic security plans.

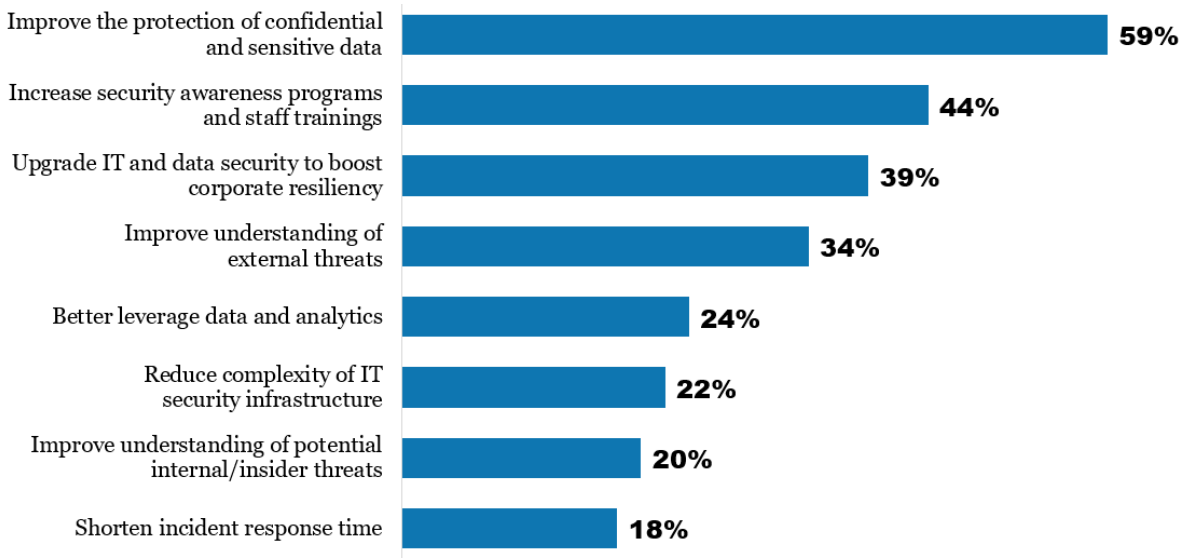
"No matter how many times security pros say 'compliance isn't security,' there are auditors and regulators who think it is," said Pete Lindstrom, VP of Security Strategies at research firm IDC (a sister company of IDG Communications).

FACTORS THAT DETERMINE PRIORITY OF SECURITY SPENDING



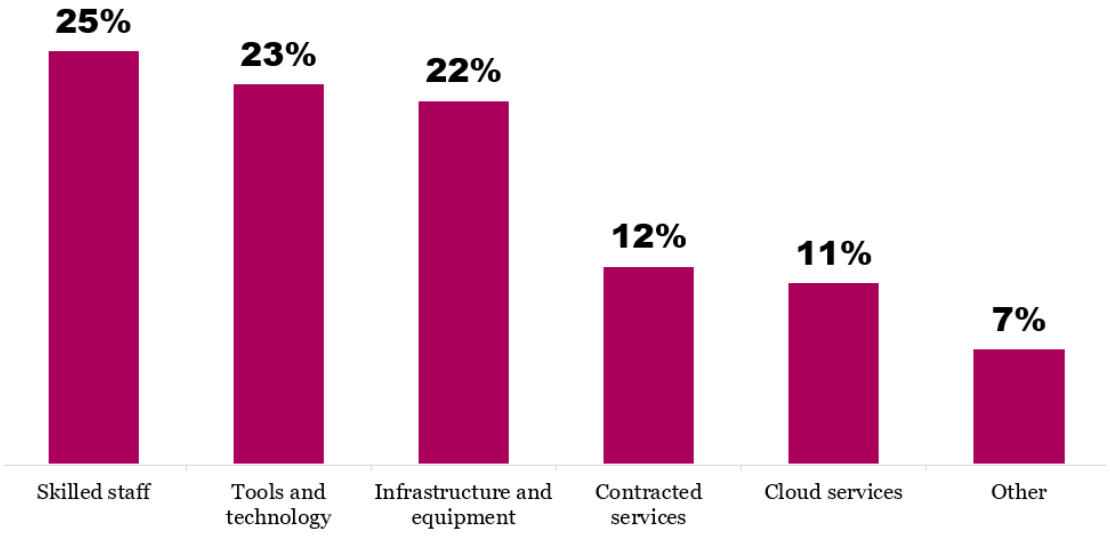
Top priorities include the usual suspects - but internal and external threat intelligence and better use of analytics show significant interest as well.

TOP PRIORITIES FOR THE COMING YEAR



New to this year's study, respondents were asked how their annual IT security budget will be allocated to services over the next 12 months. Staffing, tools, and infrastructure each absorb roughly similar amounts of the security budget. Outsourced and cloud services get less.

SECURITY BUDGET ALLOCATION OVER THE NEXT 12 MONTHS



Who's In Charge?

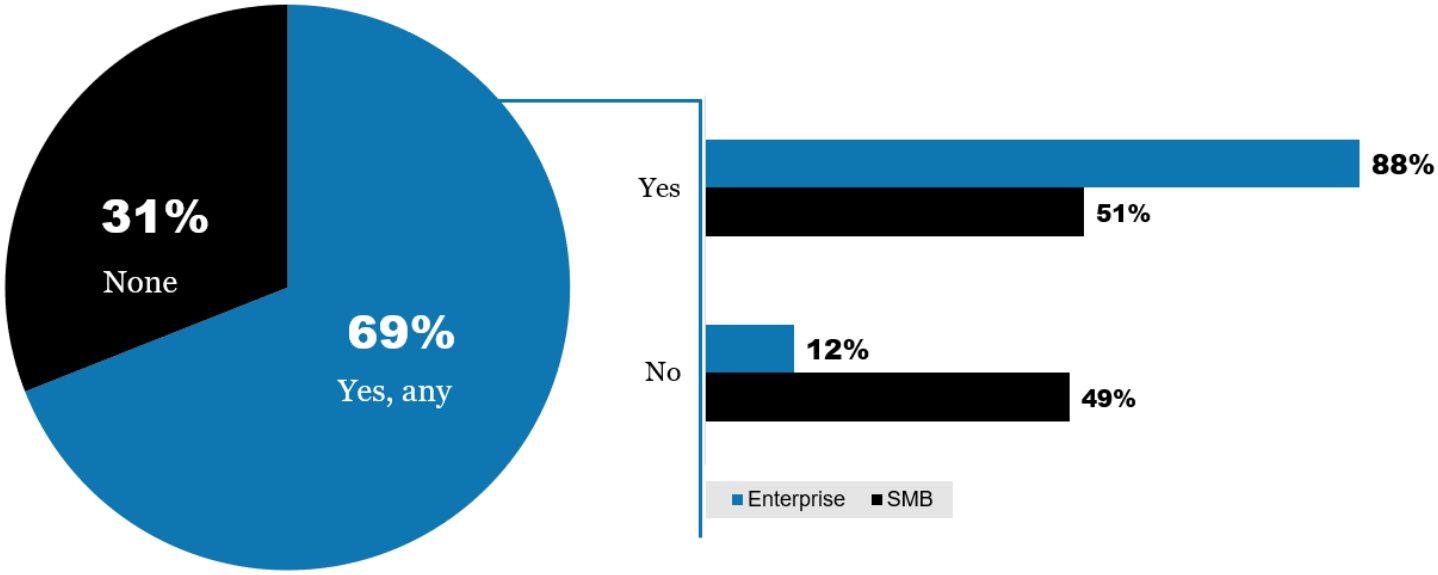
For years, some experts in the security field have championed reporting outside of the IT organization. One argument is that the security department needs independence from the CIO to make sure necessary controls, which can sometimes slow business systems and processes, are nevertheless put in place. Another argument is simply that reporting to the CEO shows that the business takes risk seriously.

This year's survey results show that more than two-thirds of responding organizations (69%) have a CSO, CISO or other designated top security leader. Of those leaders, 31% report to the CIO, while 29% report to either the CEO or the Board of Directors.

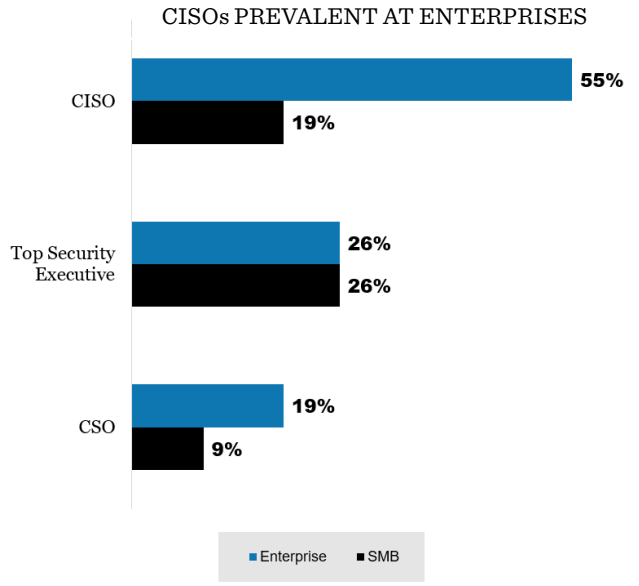
Predictably, titles rise with company size. Breakout data shows that large enterprises are more likely to have a top security executive than small or midmarket organizations.

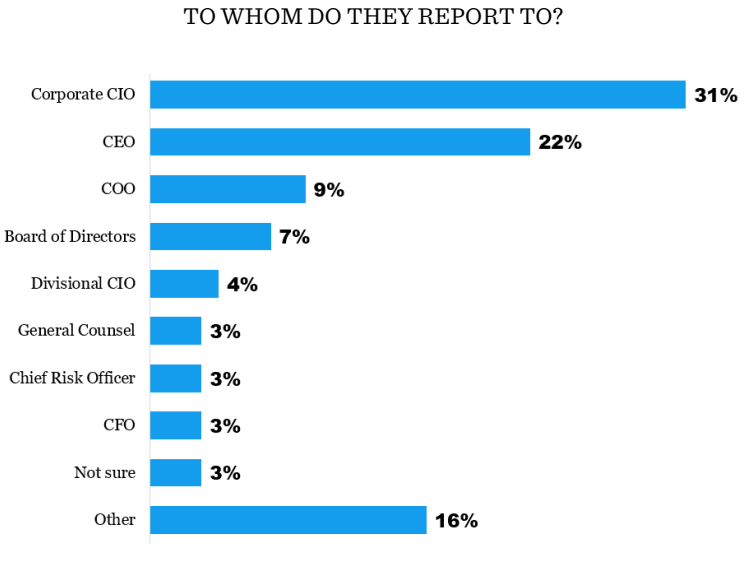
Turnover at the CISO level is often attributed to the difficulty of the job and the likelihood of this executive suffering the consequences of a data breach. However, this survey's results show another side of turnover: high demand for skilled leaders. Nearly one quarter of respondents said they have been approached about other security jobs six times or more during the past 12 months.

ROUGHLY 1/3 OF ORGANIZATIONS LACK A DESIGNATED SECURITY EXECUTIVE



SECURITY EXECUTIVES & REPORTING STRUCTURE





Technologies and Processes — More of the Same?

A certain set of familiar security technologies have achieved wide adoption. These technologies scored the highest level of in-use (either in production or being upgraded) among respondents - anti-virus/malware (83%), firewalls (82%), endpoint protection (76%), patch management (73%), and security education/awareness training (72%). This year's data finds that organizations are actively researching zero trust technologies (47%), deception technology (40%), behavior monitoring & analysis (39%), and cloud data protection (38%). Last year's results showed more interest around blockchain (58%), while this year only 50% of respondents are interested in the technology.

The challenge is that the ever-evolving threats create an arms race for security professionals — and simply buying more of the same kinds of tools may not let them keep up. As more digital business processes come online and more data flows through these companies, real innovation in security is necessary. That includes not only technology innovation, but also new thinking, processes, organizations, and more.

Respondents indicate a number of areas where they feel their security program falls short. Factors include failure to address security during application development (35%), inadequate employee training and awareness (31%), lack of involvement prior to implementing new

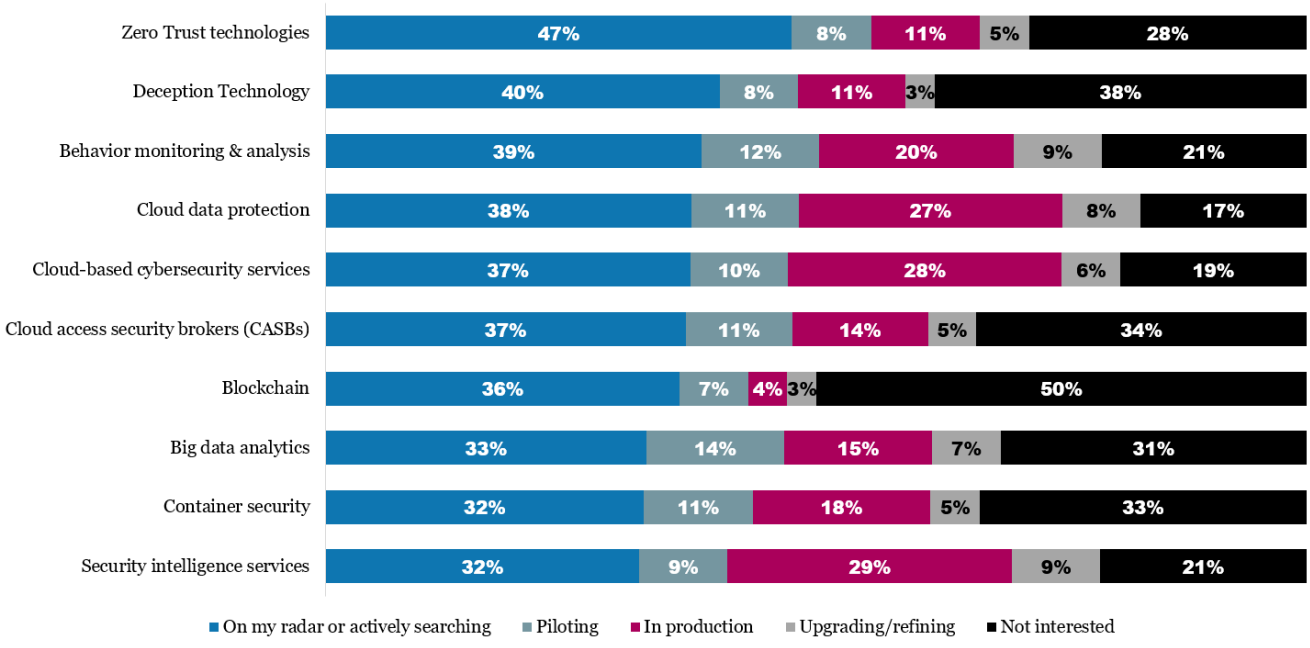
technologies (30%), lack of proactive strategy (27%), and inadequate communication between security and lines of business (27%). Those are process problems. But technology portfolios need updates, too, said Lindstrom.

"Just doing the basics in cybersecurity — which I've been promoting for 25 years — hit diminishing marginal returns years ago. We need to move on to newer methods like deception and resilience to protect enterprises," Lindstrom said.

The survey results show mixed uptake for some tools and approaches that could be considered new or a departure in some meaningful sense from security-as-usual. These include zero trust technologies, DevSecOps, deception technologies, and big data analytics, which form the basis for emerging applications of machine learning and, eventually, artificial intelligence.

Lindstrom said Zero Trust concepts in particular show potential, although the industry tosses around the term, making the specific meaning ambiguous. The term was coined by John Kindervag at research firm Forrester, and refers to the use of micro-segmentation of the network and other techniques to verify permissions to access any resource, rather than trusting any user "inside the perimeter" by default. Lindstrom also noted the role that security vendors and their marketers can play in helping security professionals find the right innovations to continue reducing risk and combating emerging threats. The most important adjustment, he said, is "to do a better job of describing the value proposition of their stuff in more specific terms."

SECURITY TECHNOLOGIES BEING ACTIVELY RESEARCHED



When every product's marketing message is pushed up the ladder and defined in broad, allegedly strategic terms, those claims lose meaning. And with that, the products (and their marketers) lose credibility. This contributes to the cautious pace security teams take in evaluating possibly useful new technologies.

"There's such a dearth of credibility these days, the most important thing you can tell a prospect is something that you don't do," Lindstrom said. The survey results suggest security teams will have more money to spend next year. The challenge will be to spend it in the most efficient way, with the greatest impact.

About the Survey

IDG's 2019 Security Priorities Study was conducted among the audience of IDG brands (CIO, Computerworld, CSO, InfoWorld and Network World). The survey was fielded online to gain a better understanding of the security projects organizations are focused on now and in the coming year. The research also looks at the issues that will demand the most time and strategic thinking for IT and security teams, as well as the services that are held in-house versus outsourced. Results are based on 528 respondents who are involved in IT and/or corporate/physical security decisions.