

EXCLUSIVE RESEARCH FROM



EXECUTIVE SUMMARY

2017 IDG ENTERPRISE SECURITY PRIORITIES STUDY

The Architecture of Security: Understanding the Role & Strategy

Small organizations still struggle to stay on top of threats and keep their networks and IT assets safe, even as larger organization lay the groundwork to tackle future challenges, a new survey of security and IT decision-makers reveals.

THE SECURITY OF CORPORATE DATA and networks is a top priority for companies of all sizes, but the security practices of SMB (<1,000 employees) and enterprise (1,000+ employees) organizations are distinct and, in some areas, divergent. That, according to the 2017 IDG Enterprise Security Priorities survey of security and IT decision-makers.

Enterprise organizations are far more likely to have retained a chief security officer (CSO), along with having a dedicated security group. They are also more likely to have deployed security technologies like two-factor authentication or data loss prevention tools than SMB organizations, which struggle to fend off threats from outside including malware and denial of service attacks.

These are among the conclusions of the latest IDG Enterprise Security Priorities Survey, which sampled the opinions of 694 security and information technology decision-makers to better understand their thoughts and priorities for 2017. The survey sampled the opinions of security and IT professionals

and executives from across industries to assess their concerns and priorities for the coming year. Respondents ran the gamut, from CSOs (16% of respondents) down to rank and file IT workers (5%). The majority (70%) of those we surveyed were manager level employees working in security, information technology, or networking.

Recent studies have suggested that security is a top priority and often the top priority for information technology groups. But our survey found that security-driven hiring and organizational structures are more common among larger organizations than smaller ones. In fact, enterprises are almost three times as likely as SMBs (66% vs. 24%) to have a CSO/CISO position. Overall, fewer than half (47%) of survey respondents reported having a dedicated CSO or Chief Information Security Officer (CISO) at their firm .

47%

have a dedicated
CSO or Chief
Information
Security Officer
(CISO) at
their firm

ENTERPRISE 66%
SMB 24%

Additionally, CIO's 2017 State of the CIO survey tells us that security is becoming more tightly integrated into their overall IT strategy. More than half (51%) said that security and IT strategy and roadmaps are tightly integrated. That is a noticeable jump from last year, when just 37% of CIOs described their IT security strategy as tightly integrated with their overall IT strategy. And closely linked IT and IT security strategies are the norm in industries like financial services (64%) and healthcare (68%). Eight in 10 CIOs we surveyed

said that they expect IT security and IT to be tightly integrated within the next three years.

66%

of organizations with a CSO/CISO say IT security is responsible for managing insider threats.

55%

of organizations without a CSO/CISO say IT is responsible.

Many Hats Make for Hard Work

That may sound like an arbitrary measure, but we found that it was one manifestation of a broader pattern. Namely: the growth of information security as an area of specialization within enterprises, compared to SMBs continued reliance on IT generalists, which keeps information security as just another functional area within a broader portfolio of security.

For example, at organizations lacking a CSO or CISO, information security issues are escalated to the Chief Information Officer (CIO) or CEO in about equal measure. At organizations where a CSO/CISO is present, that individual typically takes primary responsibility for a wide range of security is-

ssues, including insider threats, incident response, vulnerability management and security awareness training.

Similarly, when we asked respondents what kinds of security decisions they are involved with at their organization, 48% of respondents overall said that they contribute to decision-making on both corporate (i.e. physical) security as well as IT security. However, just 40% of our enterprise professionals said they are required to be involved in both physical and IT security, compared to 56% of respondents who worked for SMBs. Looked at the other way: almost half of enterprise respondents (48%) said they focus solely on IT security decisions, compared to one third (33%) of SMB respondents.

It shouldn't be surprising that employees at smaller organizations are required to wear more hats in their day to day work. But it is also true that wearing many hats, in this way, can make it more difficult to strategize and plan for the long term.

In an interview with CSOonline.com, Lorna Koppel, Director of Information Security and CISO at Tufts University, said "On one half, you're trying to think about the threats, all of the vulnerabilities. But at the same time, you have to step back and think what is really important to the business and how can I enable those activities in an appropriate manner."

“ On one half, you're trying to think about the threats, all of the vulnerabilities. But at the same time, you have to step back and think what is really important to the business and how can I enable those activities in an appropriate manner.”

Lorna Koppel
*Director of Information
Security and CISO
Tufts University*

That was the consensus of responses to a question we asked this year about the kinds of security challenges that were forcing our survey respondents to “redirect time and focus away from strategic tasks.”

Among the bright, shiny objects that are pulling at our security and IT pros and becoming a source of distraction are cyber threats from outside the organization . But just 22% of organizations with a standalone security department listed this as a top distraction, while organizations where IT and security are

part of the same department (that is: there was no separate security function), a third said such attacks are a top distraction. Similar percentages were reported among respondents who worked for organizations with a designated CSO, reinforcing the connection between practices and priorities that we see elsewhere.

For companies that maintain a standalone IT security function, the biggest distraction wasn't cyber threats, but regulators. Thirty-eight percent said meeting governance and compliance regulations forced them to take their time away from strategic planning. That, compared to just 23% of companies

where IT and security were managed together. Financial organizations also notice a hindrance from governance and compliance regulations – 40% say these regulations are a challenge that takes time away from security strategy.

A Detection Gap

One possibility as to why external threats are a larger issue for SMB organizations may be because they have fewer tools to detect and combat them compared to enterprise organizations. On that count: our survey revealed notable differences between large and small companies' account of what tools and

technologies they are using versus those that they are still evaluating or simply considering.

STATUS OF SECURITY SOLUTIONS IN PRODUCTION

Incident response	56% ENTERPRISE 37% SMB
Network monitoring	53% ENTERPRISE 30% SMB
Data loss prevention tools	43% ENTERPRISE 22% SMB

Enterprises, for example, are almost twice as likely to have deployed data loss prevention (or DLP) technology than smaller businesses, with 43% of enterprises claiming they have DLP in production, compared to just 22% of SMBs .

Network monitoring (53%) and incident

response technologies (56%) are far more likely to be in production at enterprises than SMBs (30% and 37% respectively). These technologies have been shown to help identify security compromises early and to limit the damage caused.

Other security industry studies have revealed a similar disconnection between large and small firms in areas like threat detection and blocking. The 2017 Verizon Data Breach Investigation Report found that 61% of data breach victims were businesses with fewer than 1,000 employees.

“The specter of super-sophisticated hackers can be paralyzing,” said Sara Cable, the Assistant Massachusetts Attorney General for Customer Protection, in an interview with CSOnline.com. “But companies can protect critical data and assets by first understanding where their sensitive data and IT assets are and what behaviors characterize their use.”

Phishing Drives Identity & Access Investments

Given the scourge of phishing and DDoS attacks that have ravaged businesses in recent years, it shouldn't be surprising that stronger identity management and access controls are a top priority for security and IT professionals regardless of the size of the company that employed them.

The combination of phishing attacks that lure employees, followed by sophisticated malware infections are a one-two punch that has knocked out even some of the most sophisticated firms in the world in recent years. Malware installation followed successful phishing attacks 95% of the time, Verizon reported, while weak passwords or stolen passwords were linked to 80% of hacking related breaches. And, with 14% of employees falling for phishing emails during awareness exercises carried out for firms, hackers have plenty of opportunities to bypass corporate security protections.

What challenges are taking time away from security strategy?

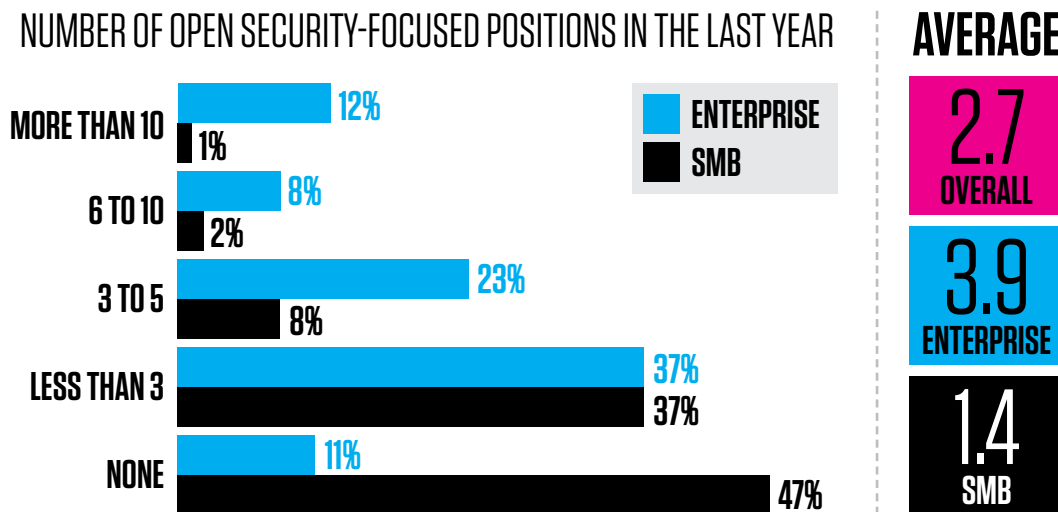
- Cyber threats from outside of the organization
- Budgetary constraints/demonstrating ROI
- Meeting governance and compliance regulations
- Employee awareness and cooperation issues

Those statistics are clearly driving interest in employee awareness training, which is listed as a top challenge among both companies with standalone IT security groups (24%) and those with combined IT and security groups (28%). Overall, 27% of organizations report that employee awareness and cooperation issues are taking time away from security strategy plans.

It also suggests why access controls are the top listed security technology being upgraded (21%) or actively researched (also 21%). That sounds surprising, given that authentication and identity

management technologies have been around for decades. But it likely reflects the reassessment of those legacy tools in the face of an epidemic of phishing and account takeover attacks. In the meanwhile, a new generation of multi factor authentication technologies are rapidly gaining adoption. But there are also notable differences based on the size of the firm. Our survey showed 47% of enterprises had deployed such authentication tools versus just 33% for SMBs.

SECURITY POSITIONS ARE DIFFICULT TO FULL IN ENTERPRISE ORGS



Is There Anybody Out There?

The differences in security practice between security and IT professionals at larger firms and those who work at SMBs are manifold and evident. But our research also reinforces the notion that there are many concerns and experiences held in common by security and IT executives regardless of the size or sophistication of their employer.

For better or worse, large and small firms are stuck competing for scarce talent in the same, challenging market for IT security professionals. Overall, 29% of organizations reported to have had at least three open security positions over the past year , and this rises to 43% for enterprise organizations. At companies with a CSO/CISO, just 1 in 10 said they had no open security positions in the previous year. On the flip side, 37% overall said they had fewer than three positions to fill, while 7% reported needing to fill more than 10 positions for IT security pros in the previous year.

Faces Turned Cloud-ward

If there is consensus that qualified staff is hard to find, there is also consensus on the technologies companies want to invest in and explore to compensate

for both the change in threats and attacks and the difficulty of finding security professionals to mitigate organizational risk.

From previous IDG Enterprise studies, we know that more organizations are adopting, and moving more of their operations into a cloud-model business. Cloud-based security services are just the latest iteration of that trend, with companies offering everything from online reputation monitoring to two-factor authentication to incident response via the cloud.

It's no surprise, then, that security and technology professionals are looking hard at cloud-based security services and better data analysis to keep up with threats and attacks in 2017. Thirteen percent of security and IT professionals said that cloud-based security services and cloud access security brokers

(CASBs) are new areas of investment – the highest percentage of any technology we inquired about.

Those two areas also ranked at or near the top of technologies identified as potential new investment areas.

POTENTIAL AREAS FOR SECURITY INVESTMENT

Cloud access security brokers	32%
Behavior monitoring & analysis	30%
Cloud-based cybersecurity services	29%
Big data analytics	28%
Biometrics	28%

Data analysis tools are also the subject of keen interest from survey respondents, regardless of the size of their employer. Thirty percent of respondents said they expect spending on so-called “Big Data” analytics to increase in the next year. Another 12% said it was an area of new investment and 16% said it was a potential area of new investment .

On the flip side, there are warning signs for legacy tools, as well. While most companies appear to ascribe to a “kitchen sink” approach to security: main-

taining or modestly expanding existing investments in security tools, it is also clear that technologies like antivirus software are showing their age.

Twenty percent of respondents said their spending on antivirus is expected to increase within the next 12 months, but 6% said their spending in this technol-

ogy will decrease, the highest percentage planned decrease of any technology we asked about. In other areas, such as spam filtering and firewalls, modest prospects for increased spending and a substantial (5% or higher) number of respondents who expect their investment to decrease, are trends to watch. Although, this trend may be because organizations have already invested in and installed these technologies.

Conclusion

The 2017 IDG Enterprise Security Priorities survey found that there are more factors linking the experiences and fates of enterprises and SMBs than dividing them. Among them are the potency of online attacks and phishing scams, the increasing sophistication and determination of criminal and nation-backed hackers, the drive to align information technology and information security programs and the difficulty associated with finding and keeping qualified professionals.

It also showed us that in matters of security, size and resources matter now more than ever. As enterprises with greater flexibility in hiring and staffing hone their information security practices to encompass user education, sophisticated network monitoring and incident response, SMBs firms are struggling. Their employees are more likely to juggle both information security tasks and traditional information technology physical security concerns about employee onboarding, doors, badges and the like.

Those challenges represent an opportunity for vendors, who can offer small firms services and tools – from staffing to data analysis and insider threat detection - that put them on par with larger organizations and help them to maintain the integrity of their network and data. In fact, data classification, insider threats and risk management all ranked among the top pain points where respondents said they did not have specific vendors or technologies to serve their needs. Let's hope that is a message that isn't lost!