



2021 EXECUTIVE SUMMARY

IDG Security Priorities Study

A crisis of confidence **pushes**
new security initiatives

90% OF SECURITY LEADERS believe they're falling short in addressing cyber risk. Some are doubling security budgets, more are investing in new infrastructure, and most are outsourcing more security functions than ever.

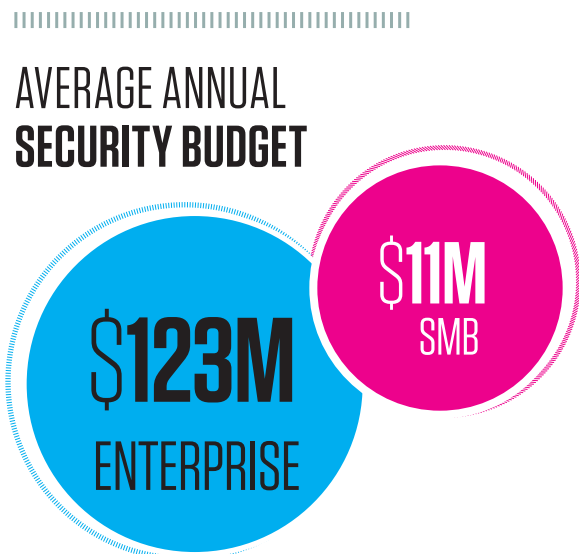
The explosion of ransomware, zero-day attacks, third-party breaches, along with long-term remote work concerns and the integration of operational technology with IT systems have culminated into a crisis of confidence for IT security leaders.

Nine out of 10 IT and security leaders believe their organization is falling short in addressing cyber risks, according to IDG's 2021 Security Priorities Study. In response, they're implementing best practices for proactive security strategies, investing in hardware and software to better protect sensitive data, and increasing security awareness of employees through training. In many cases, they're moving to outsource security. By 2022, one in five organizations (21%) surveyed say they will have fully outsourced security functions.

These initiatives aren't cheap, and organizations are increasing security budgets (on top of last year's security spending increases) to make it happen.

SMBs that plan to increase security budgets this year plan to double their spending on average, from an \$5.5 million last year to \$11 million over the next 12 months. By comparison, enterprises will budget an average \$123 million on security in the coming year.

IDG's 2021 Security Priorities Study surveyed 772 IT security executives, managers, and professionals from around the globe to gain a better understanding of the current security projects that organizations are focused on today and in year ahead. The survey also looked at the issues that will demand the most time and strategic thinking for IT and security teams, with some specific questions about operational technology environments. The



survey defines a security incident as an event that indicates an organization's data or systems have been compromised. This includes a wide variety of security violations, including ransomware attacks, data breaches and third-party or supply chain breaches.

Most security incidents still stem from insiders

Security leaders' perception of falling short in addressing cyber risk appears to be real. For instance, 36% of security incidents in 2020 involved employees falling victim to phishing, or other non-malicious violations of security policy. This year, that number rose to 44% of all security incidents, even after nearly half of those security leaders prioritized security training and awareness for its employees last year.

Employees weren't always to blame. Unpatched software and security lapses by third-party individuals or vendors were tied as the second leading causes of security incidents (27%), followed by misconfiguration of services or systems either on- or off-premises (26%).

Surprisingly, the pandemic and other unexpected business interruptions were blamed for security incidents by just 22% of respondents.

Zero-day and supply chain incidents rise for enterprises

One in five enterprises surveyed has experienced a zero-day vulnerability or a software supply chain breach (21%) in the last 12 months. By comparison, when small to midsize businesses with fewer than 1,000 employees were added to the total, zero-day vulnerabilities decreased to 10% and software supply chain breaches 9%.

A zero-day vulnerability is a software or hardware flaw that has been discovered and for which no patch exists. The discovery part is key to this, but the question of who finds out about these flaws first is crucial to how security incidents play out.




44%

of security incidents in 2021 were caused by employees falling victim to phishing scams, even after nearly half of those security leaders prioritized security awareness training for employees last year.



A supply chain attack, or third-party attack, occurs when someone infiltrates your system through an outside partner or provider with access to your systems and data. This has dramatically changed the attack surface of the typical enterprise in the past few years, with more suppliers and service providers touching sensitive data than ever before.

70% of security incidents are **detected within the first week** of occurring



On average, the longest amount of time that passed before a security event was detected – **5.1 weeks**

Detection improves

There is some good news. When bad actors infiltrate corporate systems, they don't stay hidden for long. 70% of security incidents are detected with in the first week of occurring, according to survey respondents. That's slightly lower for enterprises (63%) and higher for SMBs (80%). With quick detection times, it makes sense that 91% of all organizations are aware of what caused their security incidents over the last year. However, on

average, the longest amount of time that passed before a security event was detected was 5.1 weeks – and again, this increases to 5.3 weeks for enterprise and is 4.9 for SMBs.

Top security priorities: Be prepared, be secure, be aware

With their shortfalls in mind, security executives' have carved out three top priorities for the next 12 months. They want to be better prepared to respond to the next unexpected security incident (48%). They also seek to better protect sensitive and confidential data (43%), and to improve security awareness of end-users through training (42%). Following close behind is upgrade IT and data security to boost corporate resiliency.

Security preparedness scored even higher for SMBs, who place this as their top security priority in the coming year (53%), followed by increased security awareness training (46%). While enterprise organizations more highly rank upgrade IT and data security to boost corporate resiliency (45% vs. 38% SMB).



TOP SECURITY PRIORITIES FOR NEXT 12 MONTHS:

<p>Better prepared to respond to unexpected security incidents</p>	<p>Better protect sensitive and confidential data</p>	<p>Improve security awareness of end-users through training</p>

These priorities make sense because they address the top challenges that security leaders faced over the past year that forced them to redirect their time, including unanticipated business risks (like the pandemic), employees’ awareness and training issues and dealing with a fresh crop of outside cyber threats. Security leaders were also redirected by governance and compliance regulations that have changed security requirements in many states. (26%)

Looking to Zero Trust & SOAR for answers

To meet these priorities, security leaders are investigating an arsenal of security tools and solutions that will mitigate security risk. At the top is zero trust, with 52% of respondents currently researching or piloting the technology, and another 21% have zero trust in production, up from 18% a year ago. An additional 25% of security leaders say they plan to adopt zero trust in the next 12 months.

Zero trust technology can protect the widest swath of attack surfaces because it eliminates implicit trust in any one element, node, or service. Instead, it relies on stringent authentication and authorization processes to give users needed access to digital assets but in constrained ways that limit damage when a breach or compromise occurs. It has even gained steam in government agencies, as the Office of Management and Budget and CISA in May issued guidance to move all federal agencies to a shared zero-trust maturity model in FY 2022-2024. Funding will be a major hurdle, similar to some organizations in the private sector.

STRATEGIC TIME REDIRECTED DUE TO SECURITY CHALLENGES



Unanticipated business risks



Employee awareness and training



Preparing for or addressing risks from outside cyber threats

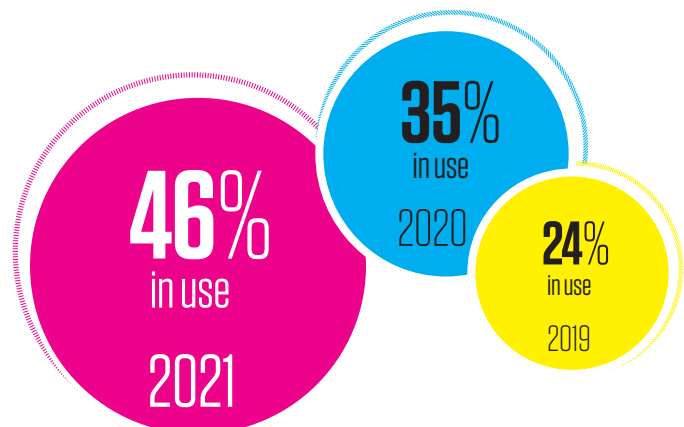


Budgetary constraints / demonstrating ROI



Meeting governance & compliance regulations

GROWTH AROUND ZERO TRUST CONTINUES



Security orchestration, automation and response (SOAR) solutions are also gaining traction, with 49% of respondents researching or piloting this security platform that coordinates information produced by a wide range of security tools and automates much of their analysis and protective responses. Ideally, SOAR platforms are meant to help organizations make better use of the resources—including both technical tools and employees—that they already have. In practice, however, there can be quirks, especially when it comes to getting ready to move to a SOAR paradigm, but overall these offerings hold promise for making sense of all the security-related data modern enterprises need to analyze.

Security outsourcing gains steam

As vulnerabilities and attack vectors grow, more IT leaders are finding it easier and often safer to leave security to the experts.

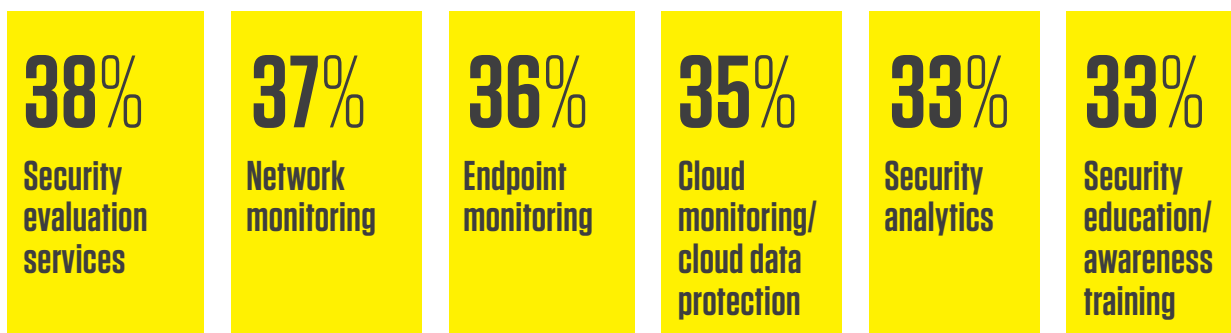
Today, almost half (49%) of organizations say they already or will outsource some of their IT security functions over the next 12 months. An additional 13% say they already or will outsource all of their IT security functions over the next 12 months.



Currently, organizations most often outsource evaluation services, such as pen testing, risk assessments and security audits (38%) followed by monitoring of the network, endpoint and cloud, and security analytics (33%). But in the next 12 months, behavior monitoring/analysis (29%) and security awareness training (27%) are most likely to rise on the list of outsourced functions.



SECURITY SERVICES CURRENTLY BEING OUTSOURCED



Still, 68% of organizations today handle the majority of IT security functions in-house, and that percentage is not expected to change dramatically in 2022. However, this is down from 72% in 2020. More likely, contractors and staff augmentation, which represents 20% of security functions today, will be replaced with outsourced services, leading to the increase in outsourcing numbers.

The budget breakdown

When looking at overall spending of security budgets, respondents say that one-fifth of the pie will be allocated to on-premises infrastructure and equipment, and another fifth on skilled staff. Sixteen will be spent on on-premises software, and 10% on cloud-based security solutions. Security awareness training gets 7% of the budget, on average.

The remaining 27% will go toward services – security consulting, monitoring, evaluation and incident response services.

Goals for IT spending vary by organization size. SMB's most often want to establish security best practices (59%), while enterprise security spending is driven by compliance with new security/privacy regulations and mandates (50%). Both groups want to be ready for unknown risks from sudden workforce changes or business dynamic (40% enterprise, 43% SMB).

Looking at the technologies that security leaders plan to increase their spending towards over the next 12 months, cloud data protection (30%) tops the list, followed by access controls (29%). Additional technologies include cloud-based cybersecurity services (28%), data analytics (28%) and authentication (27%).



SECURITY LEADERS PLAN TO INCREASE SPENDING TOWARDS



Cloud data
protection



Access
controls



Cloud-based
cybersecurity
services



Data
analytics



Authentication

More on the shortfall in addressing cyber risk

A whopping 90% of security leaders say they believe their organization is falling short in addressing cyber risks. That’s up from 87% last year during the pandemic.

Among the shortfalls, enterprise IT leaders say security is not always addressed during application development, they are not investing enough security budget for people and technologies and that the security team is not involved prior to implementing new technologies (27% each). SMBs attribute their shortfalls to not investing enough in security budgets, people and technologies (32%) and not being proactive enough in security strategy (31%).

90% of security leaders believe their organization is **falling short in addressing cyber risks**

Up from 87% in 2020

Operational technology is a growing concern

The convergence of operational technology (OT) and information technology and the loss of the historical “air gap” between the two has increased the risks of ransomware and other security vulnerabilities in formerly isolated OT systems.

While critical infrastructure entities are often targeted, such as solar energy panel networks, water control systems and building automation systems (BAS) have been targeted, the same techniques are being used against academic and private residency internet-of-things (IoT) devices, too.

45% of organizations that have an **OT environment** report that their OT environment is **connected to their IT environment**

Today, 42% of all industry IT security leaders surveyed say their organization has an OT environment. Yet 45% are “not sure” if they do, suggesting a growing/widening security gap as these operational systems connect to IT environments. (61% of manufacturing industry respondents have OT environments.)



38% of security leaders with OT environments **rate their vulnerability concerns** as grave or significant

OT environments are now connected to IT systems in 45% of organizations surveyed, and 35% acknowledge that security risks are increasing, citing technology that’s outdated and with operating system no longer supported by the manufacturer (25%), and difficulty retaining the knowledge base for supporting the OT technology (23%). One third of security leaders with OT environments report “grave” or “significant” vulnerability concerns.

Conclusion

The IT threat landscape continues to grow broader and more complex, and it's weighing on security leadership, who overwhelmingly believe that their organization is falling short addressing cyber risks as ransomware and other attacks increase, employees continue to fall for phishing scams and leadership isn't convinced of the severity of the situation.

In response, they're launching new offensives to be better prepared to respond to the next unexpected security incident, to better protect sensitive and confidential data, and to improve security awareness of employees through training.

They're looking at an arsenal of new solutions, including zero trust and SOAR solutions, as well as increased security and awareness training for employees, and outsourcing of more security functions.

Almost half of organizations (44%) are increasing security budgets to fund these initiatives, and SMBs are doubling their budgets on average to cover security best practices and the tools to be more proactive with security strategy.

ABOUT THE SURVEY

The 2021 Security Priorities Study analyzed data from an IDG online questionnaire given to 772 security professionals between August and September 2021. All respondents are involved in IT and/or corporate IT and physical security decision-making, with 77% having an executive IT or security title. Respondents represent companies primarily in the U.S (57%), with some in the Asia-Pacific region (35%) and in Europe (17%). These companies come from a variety of industries, including technology, manufacturing, financial services, professional services, healthcare, government, education, and retail. The average company has 11,535 employees.

Examining the Marketplace

Research is a valuable tool in understanding and connecting with customers and prospects. Our research portfolio explores our audiences' perspectives and challenges around specific technologies — from analytics and cloud, to IoT and security — examines the changing roles within the IT purchase process, and arms tech marketers with the information they need to identify opportunities. **To see what research is available, visit [idg.com/tools-for-marketers](https://www.idg.com/tools-for-marketers). For a presentation of full results from any of these studies and to understand how we can help you engage this audience, contact your IDG sales executive or go to [idg.com/contact-us](https://www.idg.com/contact-us).**

Want to know more about what content drives IT decision-makers and fuels their engagement during the IT purchase process? IDG's Customer Journey poster, and vertical white papers serve as your content marketing guide to strategically reach your target customers. **Find it all on www.idg.com.**



Additional ways to stay on top of information from IDG

- » **Sign up** for IDG's newsletters and receive media and marketing trends as well as our proprietary research, product and event information direct to your inbox. Go to <https://resources.idg.com/marketingfit-subscribe-rl>
- » To get results from IDG research when it happens, or any other news, follow us on Twitter: [@IDGWORLD](https://twitter.com/IDGWORLD)
- » Visit us on LinkedIn for research, services and events announcements: <https://www.linkedin.com/company/international-data-group--idg/>