




2020 EXECUTIVE SUMMARY

IDG Security Priorities Study

Pandemic drives security priorities and initiatives through 2021

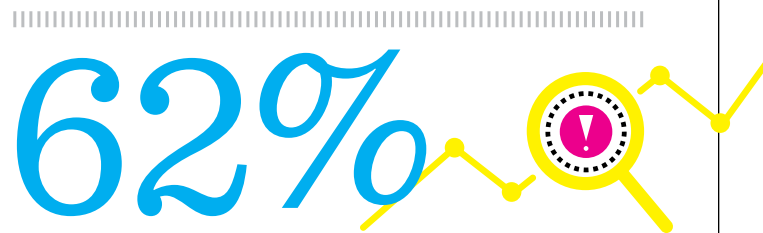


OF ALL THE CURVEBALLS THAT 2020 COULD HAVE THROWN AT ORGANIZATIONS, a global pandemic likely wasn't even among their worst-case scenarios. Still, it has wreaked havoc on the workplace, IT systems and security like no other disaster — with its breathtaking reach and vexing longevity felt at unprecedented measures.

Securing systems, networks and devices, both at home and in the office, has taken on greater urgency and many security leaders have pivoted to shoring up networks and connections rather than executing strategic plans.

More than one-third (36%) of IT security leaders surveyed in our 2020 Security Priorities study say the pandemic and its workforce upheaval, along with unexpected or under-expected business risks, caused them to redirect their time and focus away from more strategic tasks. Almost two-thirds (62%) say they expect the pandemic to impact the way their organization evaluates and responds to risk moving forward.

IDG's annual survey queried 522 IT and security managers and executives who are involved in IT, corporate and physical security decisions to gain a better understanding of the various security projects organizations are focused on now and in the coming year.



62%
expect the pandemic to impact the way their organization evaluates and responds to risks moving forward

This year the research aims to better understand how security has been and is being affected due to the COVID-19 pandemic. IDG fielded the survey from mid-July 2020 through mid-September 2020. The study also explores the security strategies organizations are embracing along with the technologies and initiatives security decision-makers plan to adopt over the next 12 months.

What's Driving Security Initiatives

Almost half of security leaders (49%) say their top security priority today is improving the protection of confidential and sensitive data, followed by improving or increasing security awareness training for end-users (45%). About a third of survey respondents say they've prioritized upgrading IT and data security to boost corporate resiliency (34%) and enhancing identity and access controls (33%). There are a few differences here by company size — enterprise organizations (1,000+ employees) say that improving security in their application development process is a top priority (34%) compared to only 20% for SMB organizations (<1,000 employees). SMBs are more likely to say that upgrading IT and data security to boost corporate resiliency is a top priority (38%) compared to 30% for enterprise organizations.

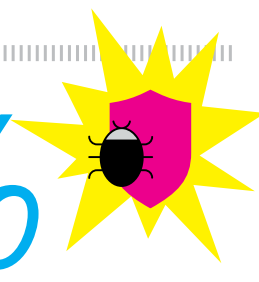
THIS YEAR'S TOP SECURITY PRIORITIES



Security Incidents Stem from User Error

Overall, 87% of security/IT executives say they are aware of what caused their security incidents in the past year. This increases slightly for enterprises (89%) and decreases to 85% for SMBs. It's not surprising that remote work combined with employees using their own internet connections (or worse, public Wi-Fi!) led to an increase in phishing attacks attempting to access corporate data. More than a third of security incidents over the past year (36%) involved employees falling victim to phishing or other non-malicious violations of security policy. Some 29% of security incidents involved unpatched software vulnerabilities. Enterprise organizations reported more security incidents stemming from misconfiguration of services or systems either on- or off-premise (34%) compared to 22% for SMBs.

87%



of IT/security executives are aware of what caused their security incidents in the past year — 36% say they were caused by non-malicious user error

Pandemic Alters Risk Evaluation and Response Strategies

Knowing what they know now, security leaders plan to take new steps when evaluating risk and response — including adding more people and resources. Close to two-thirds (62%) expect the pandemic to impact the way their organization evaluates and responds to risks moving forward. Again, there are some differences here by company size — 64% enterprise vs. 60% SMB. Overall, 43% will invest more in people to enable their

PANDEMIC ALTERING RISK EVALUATION & RESPONSE

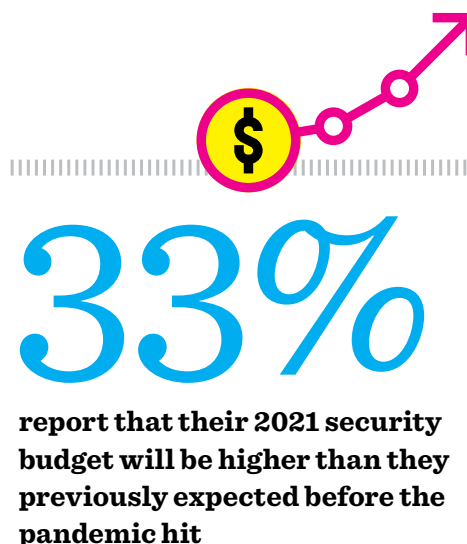


response to risks and 38% say their business will invest more resources in response planning to address risks. Nearly one-third (30%) plan to update and modernize their business continuity plans and close to a quarter say the likelihood of a risk occurring will be more carefully evaluated. Just 19% say they will invest in more technology to enable risk response. The largest difference by company size is that 42% of enterprise security leaders say they will invest more resources in response planning to address risks (42%) compared to 34% for SMBs.

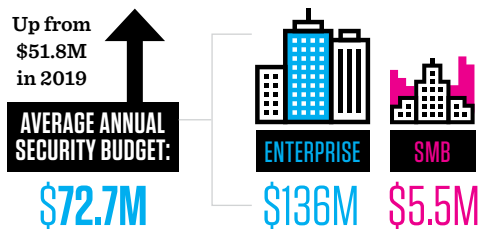
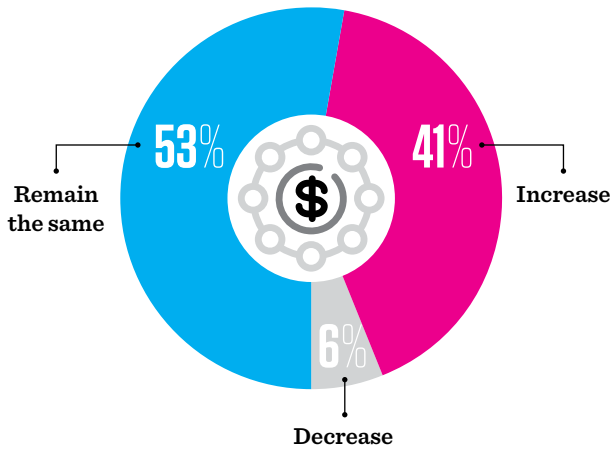
Still, the vast majority of security leaders (87%) feel their organization falls short in addressing cyber risk. Most notably, 31% say they’re not investing enough budget, people and technologies to address risks, 30% say security is not always addressed during application development, and 28% say they are not proactive enough when it comes to security strategy. Close behind, more than a quarter of security leaders say there’s inadequate security training for users and insufficient communication between security teams and lines of business. Other contributing factors include struggling to find, acquire and/or retain technical and professional expertise, and also addressing risks that have arisen from the new work environment brought on by the pandemic.

Looking Ahead to 2021

The good news is – despite the pandemic, or perhaps because of it – some security budgets are growing. About 41% of survey respondents say their budgets are expected to increase over the next 12 months while just 6% expect a budget decrease. The rest expect budgets to remain unchanged. We also see the average annual security budget increasing from \$51.8 million last year to \$72.7 million this year – rising to \$136 million for enterprises and only \$5.5 million for SMBs. To get a better understanding of how the pandemic impacted this, a new question this year asked respondents to think about how their information security budget expectations for 2021 altered due to the pandemic.



EXPECTED CHANGE IN BUDGETS:



One-third say their 2021 budget will be higher than they expected it to be before the pandemic hit, 24% said it will be lower than expected, and the majority (43%) say there will be no change in their security budget expectations.

How will security leaders allocate these funds? Keeping in mind their plans to increase employees and resources to better combat risk, 23% of budgets will go toward skilled staff and 8% to consulting services, 19% will go to on-premise infrastructure and equipment (hardware), 17% towards on-premise tools and software, and 12% will go toward cloud-based security solutions.

There are also a series of factors that security leaders say are helping to determine their security spending. Overall, best practices (61%) and compliance/regulations or mandates (59%) are the top determining factors, followed by the changing workforce or business dynamics (i.e. increased work from home). Best practices influence security spending for most SMBs (70%), while compliance regulations and mandates are top drivers for enterprise security spending (62%). Ongoing changes in workforce or business dynamics caused by the pandemic has a larger influence on security spending for enterprises (47%) compared to 42% for SMBs.

FACTORS DETERMINING SECURITY SPENDING:

- 1

Best Practices
- 2

Compliance/ regulations or mandates
- 3

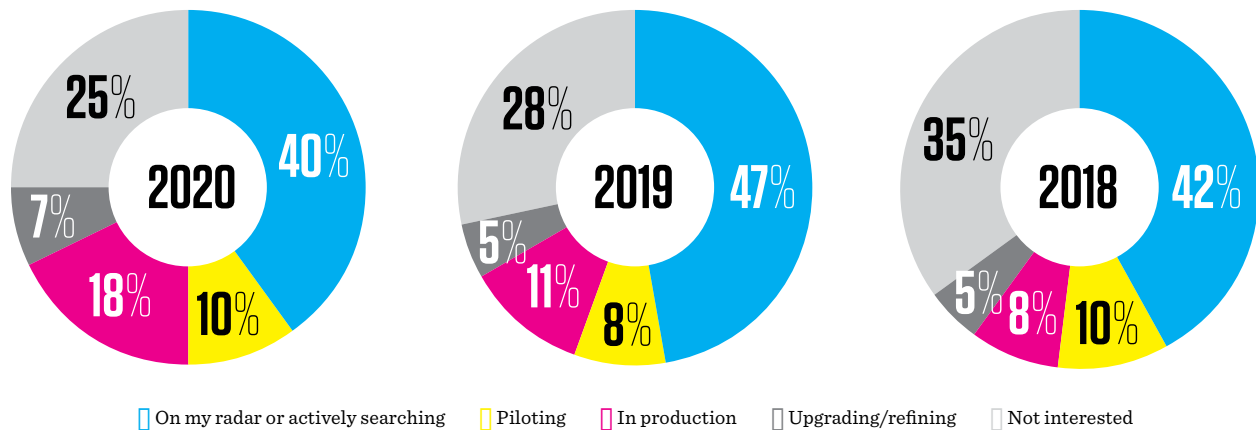
Changing workforce or business dynamics

Putting Faith in Zero Trust

Some 40% of survey respondents say they are actively researching zero trust technologies and 18% of organizations already have zero trust solutions deployed, up from 11% in 2019 and 8% in 2018. We also see that zero trust continues to gain traction as only 25% say they are not interested in the technology, which was 35% in 2018 and 28% in 2019. Another 23% of respondents plan to deploy zero trust in the next 12 months.

Interest in zero trust technologies, which trust no device, individual or location until it is verified, has been bolstered by remote work and increases in public cloud use. As applications, data, and services began migrating to public clouds, security administrators quickly realized that network flows were no longer passing directly through corporate networks, making edge security tools far less effective.

ZERO TRUST CONTINUES TO GAIN TRACTION



Proponents say zero trust provides uniform security across all devices, users and locations with enforced security mechanisms across the entire corporate infrastructure. It also centralizes security logging for better visibility and secures users and devices that connect from or into privately owned and operated networks. One of the drawbacks: legacy systems and applications cannot always be retrofitted to support zero trust.

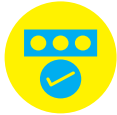
The Art of Deception Technology

Roughly one-third of survey respondents (32%) are actively researching deception technologies — a modern take on the classic, manually deployed honeypot where intruders are led to decoy passwords lists, false databases or fake access. Deception technologies automate the process. Decoys can be generated based on scans of true network areas and data. They are often deployed as mock networks running on the same infrastructure as the real networks. When an intruder attempts to enter the real network, they are directed to the false network and security is immediately notified. Proponents say deception technologies can detect and stop cyber threats of all types, including Advanced Persistent Threats (APTs), malware, ransomware, credential dumping, lateral movement and malicious insiders. Some of the drawbacks: in-network deceptions have to continuously outsmart increasingly sophisticated attackers and companies must be able to deploy, support, refresh and respond to deception alerts without hiring an army.

Most Security Tools Aren't Fully Utilized

These new security tools will be added to about a dozen others that most organizations have already deployed. In keeping with work-from-home security needs, respondents plan to increase spending over the next year on authentication technologies, including multi-factor and role-based authentication (32%), cloud data protection (28%), cloud-based cybersecurity services (27%) and network and data access controls (27%), to name a few.

INCREASING SPEND TOWARDS THESE SECURITY SOLUTIONS:



32% Authentication



28% Cloud data protection



27% Cloud-based cybersecurity services



27% Access controls



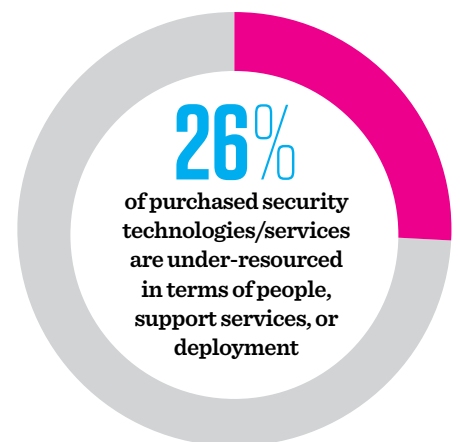
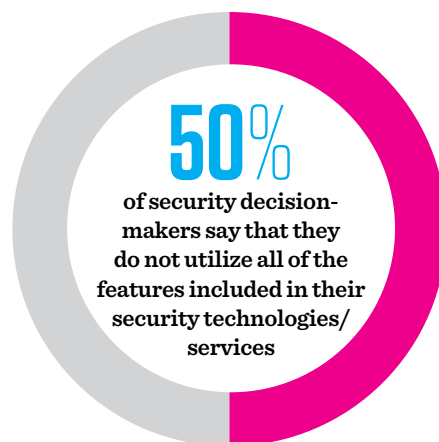
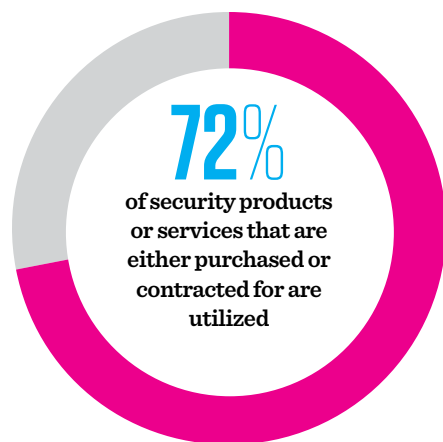
25% Application monitoring

However, many security leaders say that existing security tools aren't being used to their full potential. Although the majority of security technologies purchased are used in some capacity (72%), half of security decision-makers say they do not utilize all of the features included in their security technologies and services. A quarter of purchased security technologies and services are under-resourced in terms of people, support services or deployment.

Outsourcing Cloud and Evaluation Services

Though the majority of IT security functions (72%) are handled in-house, some organizations are planning to outsource important security functions and services that can be more efficiently and cost-effectively handled by outside experts. Nearly a quarter of security leaders surveyed (22%) currently outsource or plan to outsource cloud monitoring and cloud data protection, along with security evaluation services, such as penetration testing, risk assessments and audits. Big data analytics, a skillset still hard to find, is outsourced or will be outsourced in the coming year by 19% of survey respondents.

ARE SECURITY PRODUCTS OR SERVICES BEING USED TO THEIR FULL POTENTIAL?



Conclusion

It could take more than a year for organizations to return to the pre-pandemic security strategies they had imagined for 2020. Security leaders' reaction to risk will never be the same, but the rapid pivot to new security priorities in the wake of COVID-19 have organizations improving the protection of confidential and sensitive data and increasing security awareness for employees and partners.

Many organizations are boosting security budgets to upgrade IT and data security for greater corporate resiliency. They're also continuing to research zero trust and deception technologies, with hopes to implement more of these solutions in the future. Security vendors can also expect to see increased spending towards authentication and cloud data protection technologies in the upcoming year.

About the Survey

The 2020 Security Priorities study analyzed data from an IDG online questionnaire given to 522 security professionals between mid-July and mid-September 2020. All respondents are involved in IT and/or corporate IT and physical security decision-making, with 78% having an executive IT or security title. Respondents represent companies primarily in the U.S (73%), with some in the Asia-Pacific region (21%) and in Europe (6%). These companies come from a variety of industries, including technology, manufacturing, financial services, professional services, healthcare, government, education and retail. The average company has 12,661 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**
- Visit us on LinkedIn for research, services and events announcements: **<https://www.linkedin.com/company/international-data-group--idg/>**

