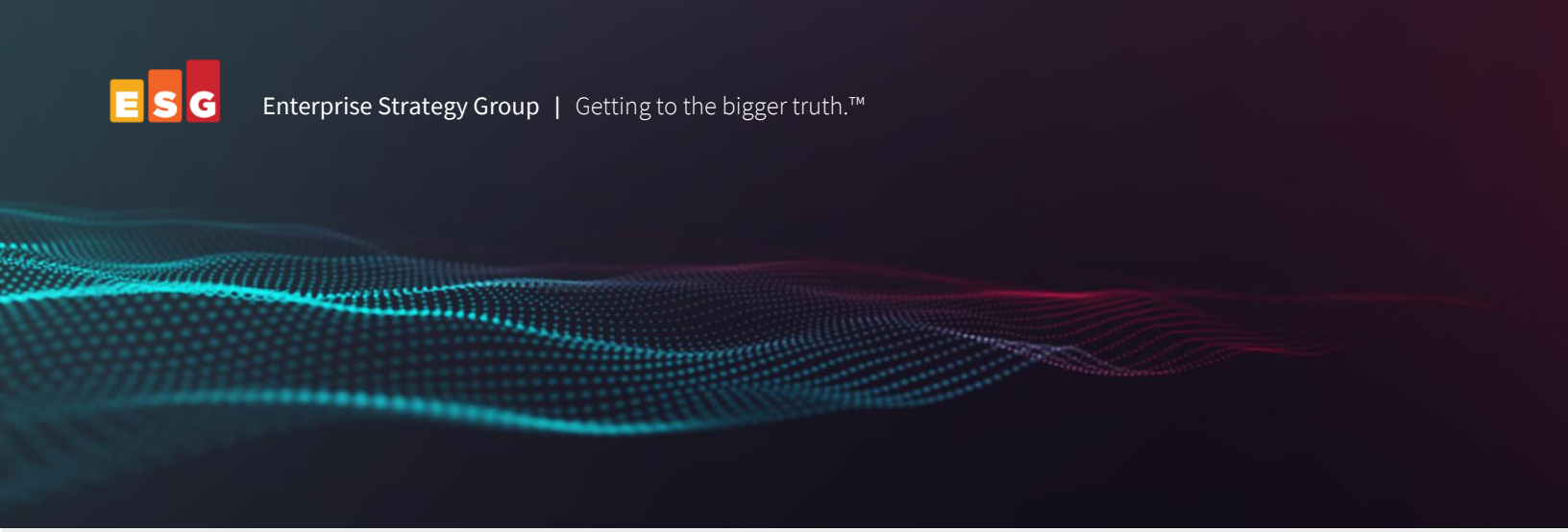


ESG WHITE PAPER

The Impact of COVID-19 on IT and Cybersecurity

Current Effect and Future Trends

By Jon Oltsik, ESG Senior Principal Analyst and Fellow

July 2020

This ESG White Paper was commissioned by IBM and is distributed under license from ESG.

Contents

Executive Summary 3

The Impact of COVID-19 3

Cybersecurity Challenges Posed by COVID-19 5

Cybersecurity Budgets 6

The New Normal? 7

The Bigger Truth 8

Executive Summary

By March 2020, the novel coronavirus upended business (and cybersecurity) as usual for most organizations. CIOs and CISOs were forced to respond and reprioritize everything. With the passage of time, organizations have forged ahead, encountered problems, and learned valuable lessons.

What changes were necessary to address the unexpected global pandemic? What types of cybersecurity challenges did the transition present? How are organizations doing? To answer these questions, ESG conducted several research projects between March and May to gain a perspective on the impact of COVID-19. Based upon the research data presented, this white paper concludes:

- Pandemic response success has some dependencies. Organizations with significant investments and experience in cloud computing (i.e., developing applications, moving workloads to the public cloud, etc.), SaaS, and work-from-home (WFH) initiatives have been much more successful in coping with changes wrought by COVID-19. Success here is defined as minimizing business operations while identifying, monitoring, and mitigating cyber-risks.

- Security responses proceeded through phases. When the lockdown started, security and IT teams scrambled to give employees secure access to networks and applications, secure endpoint devices, and scale their infrastructure to handle the excess load. Since then, the focus shifted to normalizing WFH security. This effort includes actions like fine-tuning access policies, monitoring end-user behavior, and supporting developers and administrators who never worked remotely in the past with privileged accounts.

- The coronavirus will have a long-lasting impact on IT and security. Organizations have been going through digital transformation, altering and modernizing business processes for revenue generation and cost cutting. WFH initiatives are now driving similar IT transformation, making the infrastructure more dynamic, elastic, flexible, and scalable. ESG research indicates that this is likely to become the new normal even when the pandemic finally wanes. CISOs must prepare accordingly, with new policies and technologies that offer similar attributes.

The Impact of COVID-19

At the end of Q4 2019, CISOs fine-tuned their cybersecurity program and budget plans for 2020 with the goal of mitigating cyber-risk and aligning security with the business. Progressive firms painstakingly thought through every detail and planned for every contingency. Unfortunately, few cybersecurity professionals anticipated how their lives would be turned upside down a few months later. With the spread of COVID-19, businesses around the world were forced to cease operations or adopt work-from-home (WFH) policies, processes, and technologies in rapid fashion.

How did this swift and unanticipated transition go? The results are mixed. According to ESG research, 21% of IT executives claim that the conversion was very smooth while another 46% claim it was smooth with some minor disruptions to daily operations. Still, 27% say that it could be better, with several disruptions to business operations but some improvement. The remaining 6% had far more trouble, admitting that COVID-19 and WFH initiatives have been rough or very rough.[1]

Through further analysis, ESG discovered a few interesting links buried within the data. Successfully adopting to COVID-19 and WFH was closely correlated with:

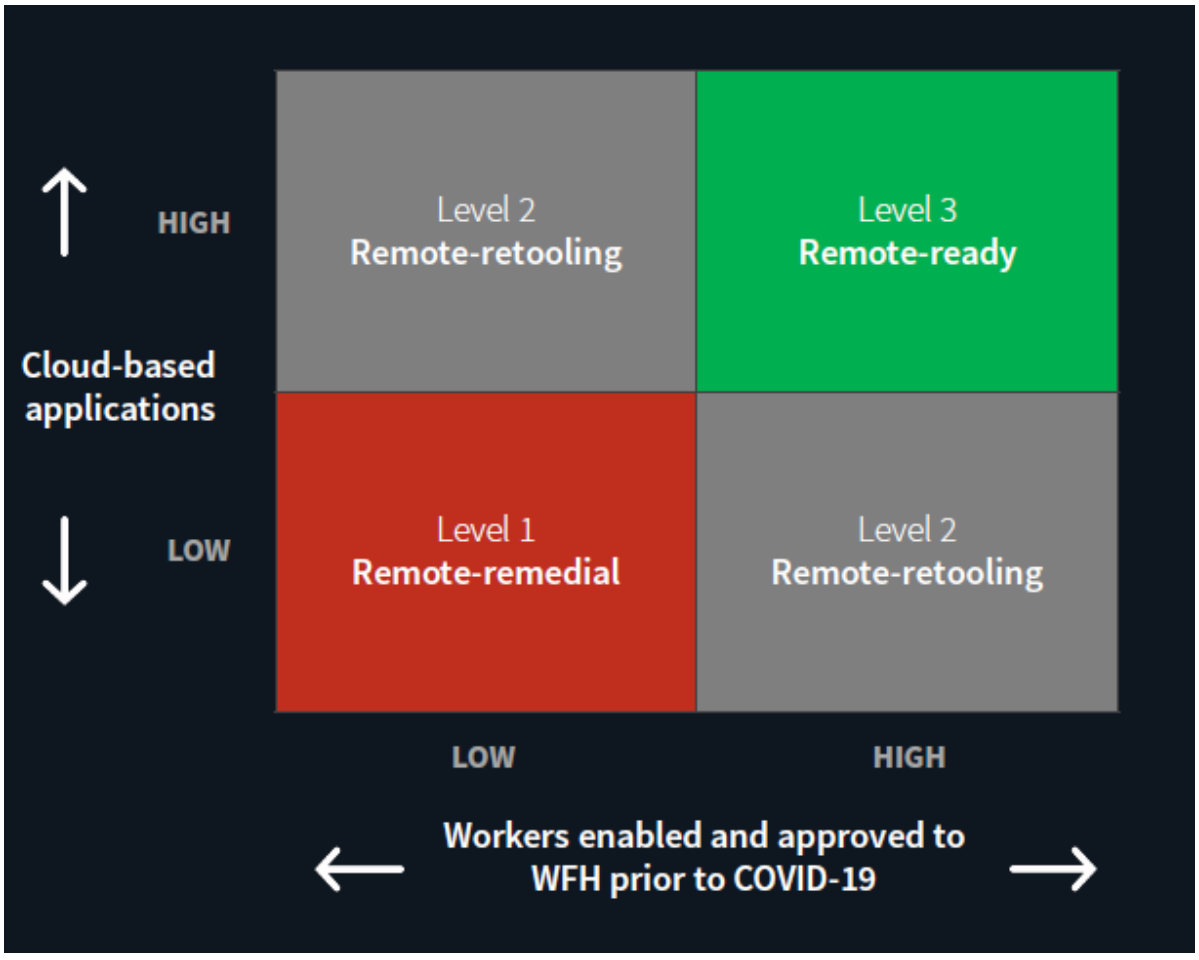
[1] Source: ESG Research Report, *The Impact of the COVID-19 Pandemic on Remote Work, 2020 IT Spending, and Future Tech Strategies*, June 2020. All ESG research references and charts in this white paper have been taken from this research report, unless otherwise noted.

- Cloud adoption. Organizations with broad adoption of public cloud computing and SaaS applications experienced a smoother transition than organizations with fewer cloud-based resources.
- An existing population of WFH employees. Organizations with large populations of employees previously enabled and approved to work remotely fared better than those with more office-bound employees.

Based upon this data, ESG created a taxonomy of three types of organizations (see Figure 1):

1. Remote-ready. These organizations represented 38% of the total survey population and were further along with both cloud computing and WFH adoption. On average, 45% of their applications were cloud-based and 78% of knowledge workers were permitted to work remotely.
2. Remote-retooling. Organizations in this category represented 35% of the survey population and were advanced in either cloud computing or WFH adoption but not both. On average, 34% of their applications were cloud-based and 48% of knowledge workers were permitted to work remotely.
3. Remote-remedial. Organizations in this category represented 27% of the survey population and were further behind in cloud computing and WFH adoption. On average, 19% of their applications were cloud-based and 21% of knowledge workers were permitted to work remotely.

Figure 1. ESG Segmentation Model

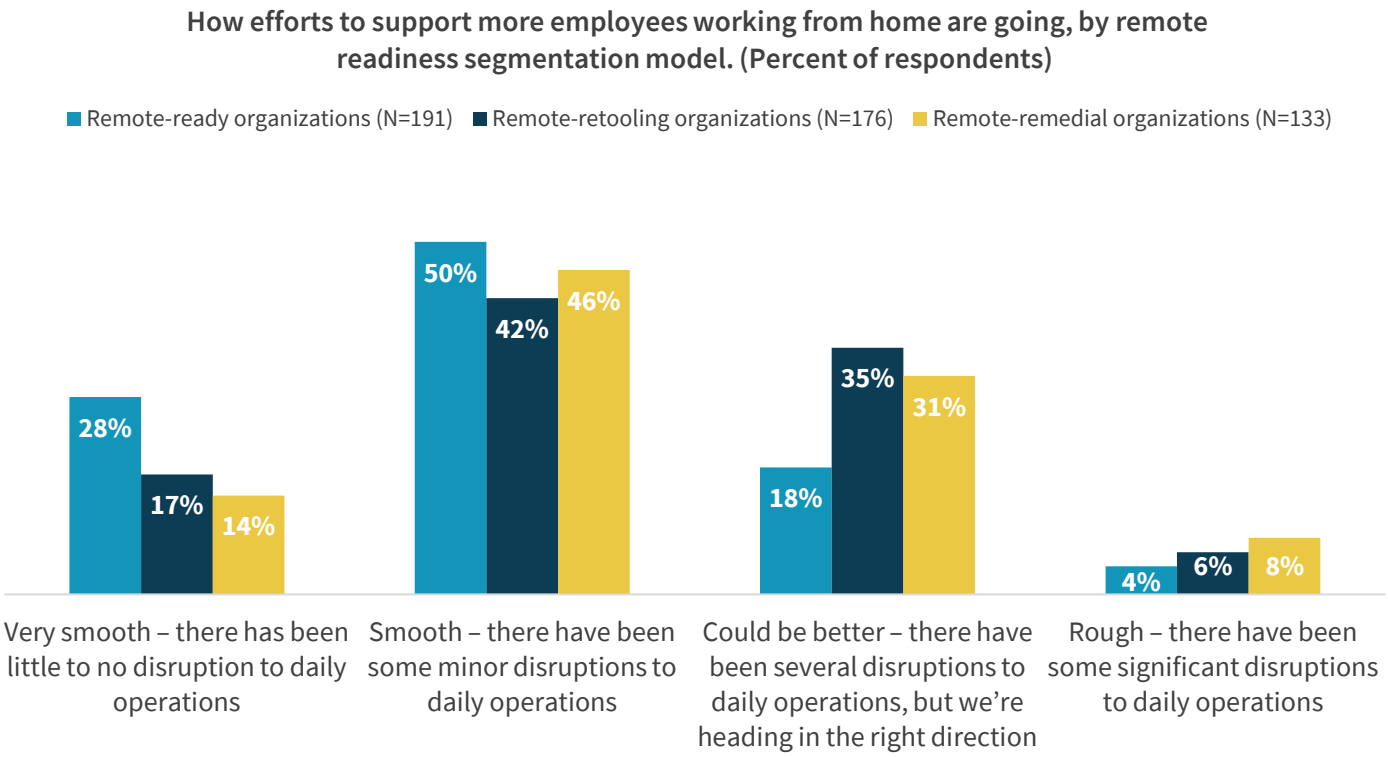


Source: Enterprise Strategy Group

When viewed through this lens, the data paints a different picture. More than one-quarter (28%) of remote-ready organizations claim that the coronavirus-driven transition was "very smooth" as compared to 17% of remote-retooling and 14% of remote-remedial organizations. Alternatively, only 22% of remote-ready organizations said that things could have been better/were rough compared with 41% of remote-retooling and 39% of remote-remedial organizations.

The data offers a strong lesson for business, IT, and security executives for future planning. Regardless of the global pandemic, IT is growing increasingly more remote and distributed. Thus, organizations that proactively build and evolve a distributed IT infrastructure will be better prepared for planned and unexpected business events including digital transformation to business processes or an effective response to a global pandemic.

Figure 2. Effectiveness of Efforts to Support More Employees Working from Home



Source: Enterprise Strategy Group

Cybersecurity Challenges Posed by COVID-19

While some organizations had the right cloud and/or remote access infrastructure in place to accommodate new WFH requirements, there were still numerous challenges to address. The top challenges identified in a separate ESG research study completed in cooperation with the Information System Security Association (ISSA) align with the two phases most organizations encountered:[2]

- The scramble phase. The first phase occurred at the start of the lockdown. Once employees were told to work at home, security and IT operations were forced to scramble to get them online and productive, and to provide basic security controls. This phase is reflected by the first two challenges identified: 27% of respondents found it

[2] Source: ESG/ISSA Research Report, *The Impact of the COVID-19 Pandemic on Cybersecurity*, July 2020.

challenging to make sure that employee devices were securely configured while 26% found it challenging to give remote employees secure access to the network.

- The normalization phase. Once users had access to networks and applications, security and IT teams worked together to find security issues like misconfigured systems, inappropriate access privileges, or suspicious user behavior. This phase presented its own challenges: 24% of respondents found it challenging to monitor traffic and user behavior of remote employees, 23% of respondents found it challenging to coordinate moves, adds, and changes with IT operations teams, and 21% found it challenging to secure privileged users who never worked from home before.

Those organizations with minimal investments in the public cloud, SaaS, and WFH infrastructure find the normalization phase especially challenging. These firms may not have the processes or scale needed to collect, process, and analyze highly distributed security assets and security telemetry. Supporting WFH also demands strong and dynamic policy management with the ability to alter policies based on changing risk. This is especially difficult for organizations used to office-based employees and applications anchored in corporate data centers.

While many organizations have found workarounds for these challenges, CISOs should seek more strategic solutions that offer the scale and flexibility needed to support a dynamic IT infrastructure featuring remote users on one end and cloud-based applications and data on the other.

Cybersecurity Budgets

The global pandemic caused severe business disruption, especially in industries like healthcare, hospitality, retail, and transportation. How has this affected security budgets for 2020? The ESG/ISSA research indicates that 20% of organizations believe their 2020 security budget will increase, 41% of organizations say that their 2020 security budget will remain unchanged, 25% anticipate a security budget decrease, and 13% responded that they don't know/it's too early to tell.[3]

Those organizations planning on increasing security budgets were then asked to identify areas of investment. The top responses from the ESG/ISSA research included (see Figure 3):[4]

- Identity and access management (IAM). Today's disjointed IAM infrastructure is difficult to use and cumbersome to operate, and doesn't scale. Organizations need a more modern IAM infrastructure that accommodates changing business and security policies to provide the right access, to the right applications and data, to the right users, at the right time.

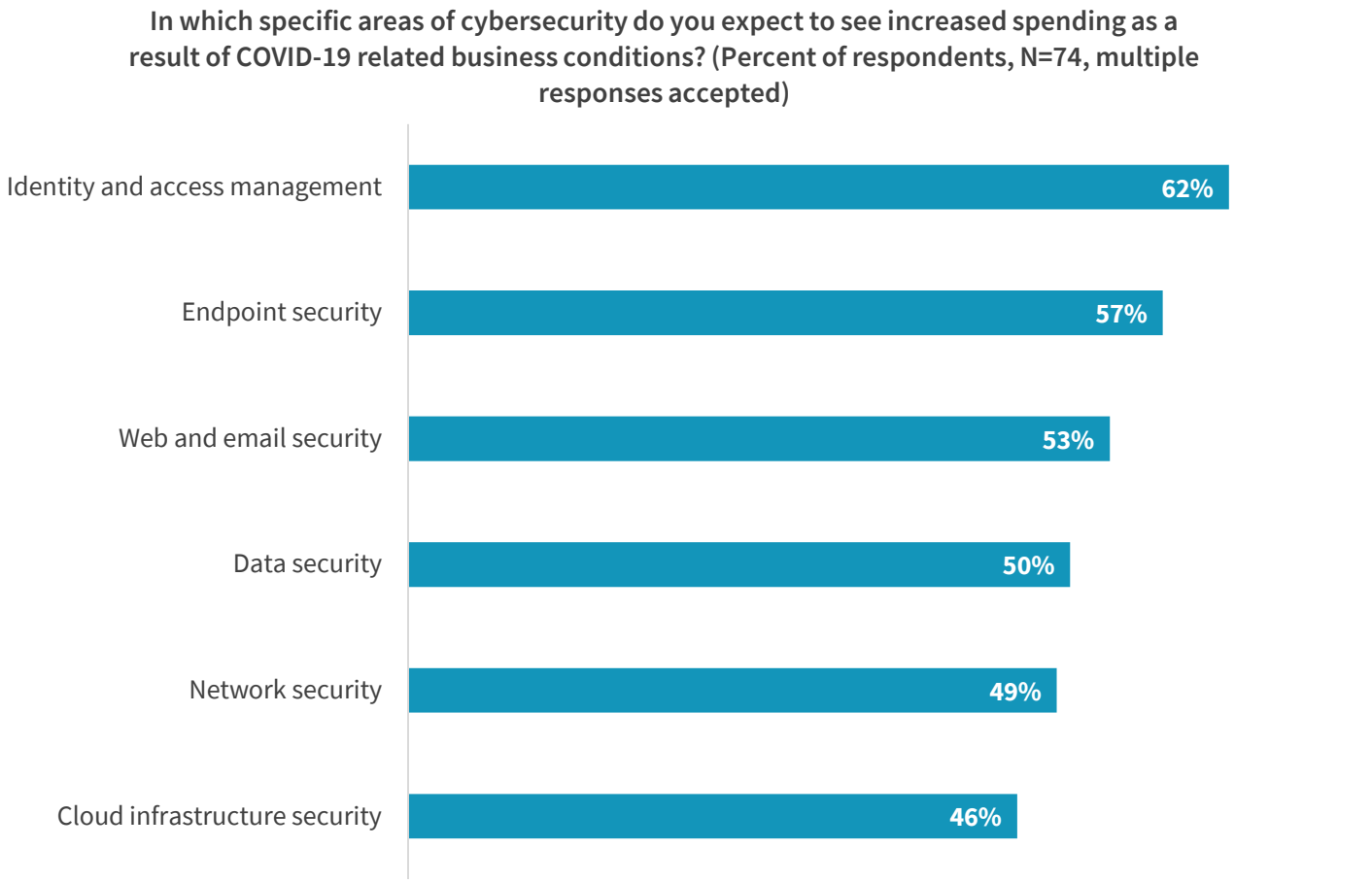
- Endpoint security. It's likely that organizations want tightly integrated endpoint security suites that include capabilities for threat prevention, detection, and response. Some organizations also want tools that can help them merge endpoint security and operations.

- Web/email security. Cyber-threat activity has increased dramatically, with hacktivists, criminals, and nation states taking advantage of the fog of a global pandemic. In response, organizations want to reinforce the most common threat vectors: web and email security.

[3] Ibid.
[4] Ibid.

- Data security. CISOs realize that the combination of remote users and cloud-based applications makes data security especially challenging. Some organizations seek to address this with new technologies for sensitive data discovery classification and monitoring, as well as data security controls.

Figure 3. Areas of Security Spending Increasing Due to COVID-19



Source: Enterprise Strategy Group

Since budgeting is often done late in the year, 2020 cybersecurity budgets were likely crafted in November/December 2019, so it is understandable that the largest percentage of organizations don't foresee any changes in 2020. When ESG asked several CISOs about 2021, budget forecasts were more uncertain. The common refrain was, "it depends." No one can predict future COVID-19 infection rates, hotspots, or government responses. Nor can they envisage progress on medical therapeutics or vaccines. Therefore, 2021 security budgets will be guided by the state of the pandemic in early- to mid-Q4.

The New Normal?

Eventually, COVID-19 will run its course and become a historical footnote. The question remains however: Will organizations return to pre-coronavirus IT infrastructure or will the pandemic initiate permanent changes? Based upon the ESG/ISSA research data, it appears like the current situation has become a tipping point, as 68% of survey respondents say that they expect their organizations to have more flexibility for WFH after the pandemic.[5] WFH initiatives will stretch through the summer and into the fall of 2020, so this strategy will continue to gain momentum.

[5] Ibid.

As WFH and cloud computing become the new normal, cybersecurity processes and technologies will need to become more flexible, scalable, and dynamic. ESG expects changes like:

- An increased focus on policy management. CISOs will need to work with business managers to determine who can do what from where and really (and I mean really) tighten up their security policies with granular and dynamic rule sets. They will also need to build an infrastructure for policy enforcement and monitoring.
- Tighter security and IT operations cooperation. Security policy enforcement and monitoring will need to be coordinated, implemented, and operated across the entire distributed IT architecture. This will require a greater degree of IT/security cooperation, forcing organizations to make organizational, process, and compensation changes.
- A modern IAM infrastructure. Distributed security controls and policy management must be anchored by a modern identity management infrastructure rather than a patchwork of loosely coupled tools. To ease this migration, identity will also migrate to the cloud in a hurry.
- Cyber-threat intelligence at scale. Organizations need to be able to analyze and operationalize threat intelligence at scale, but few have the skills or resources to do so. ESG expects more managed services, process automation, and advanced analytics to help CISOs bridge this gap.
- More help from artificial intelligence and machine learning. Security teams will need to make sense of more assets, more connections, more movement, and more threats—all at once. Human beings can't keep up with this level of scale and change, so advanced analytics will have to lend more of a helping hand.

The Bigger Truth

COVID-19 seems to carry an unexpected result: the new normal for IT and cybersecurity. In analyzing the data presented in this white paper, a few conclusions stand out:

- COVID-19 accelerated rather than initiated IT transformation. Before the pandemic, some organizations were already heading down the IT transformation path, embracing cloud computing, SaaS, and remote access for a majority of their employees. These firms weren't anticipating the coronavirus, but rather building a 21st century IT architecture that could better respond to the business. It's clear now that this type of architecture is well suited to expected and unanticipated business needs.
- Cybersecurity programs must be built for scale and flexibility. CISOs must anticipate a volumetric expansion of attack surface and all the security baggage that comes with this change. This will require improvements in data collection, processing, and analysis, followed by rapid data-driven decision making. To enable and protect the business at scale, organizations must also have strong security policies and granular policy enforcement.
- CISOs will need creativity and help. Existing security processes and technologies can't address dynamic and constant changes across a growing attack surface. Moving forward, CISOs need an open mind about the skills, processes, and technologies needed to mitigate risk and protect critical business assets. With so many challenges in front of them, smart CISOs will take stock of what they do well and seek out professional and managed services help to augment internal staff and skills.

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.


www.esg-global.com


contact@esg-global.com


508.482.0188