


Remote work and cybersecurity

by  **Pavol Gabaj**,
Senior Consultant
Risk Advisory
Deloitte in Slovakia



Most, if not all companies, have been moving toward digitization for some time now. Operations across companies are going digital, as companies are seeking to utilize any viable potential for increased efficiency and to increase the quality of the service or product they offer.

The speed at which this change is being implemented varies across industries and companies, with the main drivers being the appetite for change, the size of an entity and the competitive pressure.

Over the last few months, the Covid-19 pandemic has forced many companies to accelerate their remote work initiatives. As office closures and travel restrictions compelled everyone to adopt a remote working environment where feasible, many institutions are now reaping the benefits of such a move.

This sudden shift, however, has also brought to light certain challenges for many information security officers and cybersecurity teams charged with securing the companies. Hackers, scammers and other cyberspace-based adversaries have taken the opportunity to exploit the increased attack surface this shift has brought with it.

The imperative is clear: To adapt to this new organization of work, the companies need to empower their cybersecurity function to keep pace. This shift brings an increased risk of incidents, not only due to changes in operation and access to the assets within the company, which on its own brings challenges and space for human error, but also an increased attack surface for potential external attackers.

For the third consecutive year, Deloitte surveyed FS-ISAC members on how they are confronting cyber challenges. The survey identified a clear trend where cybersecurity function is being given increased priority and an

increased budget year by year. This indicates that companies are recognizing the challenges connected with the future we are headed for. The future is likely to see an increasing amount of remote work, the trend being further accelerated by the current Covid-19 pandemic.

Despite the positive trend of increasing budgets, the main focal areas have not changed significantly over the three years of the survey. The main areas (depicted in shades of green in the budget allocations graphic) still received more than half of the budget.

The pandemic has proven disruptive to many industries. It has forced employers to implement remote work policies, which has brought the use of videoconferencing and remote access applications into the daily repertoire of an unprecedented number of people. This trend is not expected to disappear with the easing of travel and social distancing restrictions, quite on the contrary. This is also in line with the findings of a recent Deloitte survey, where the main takeaway is that companies plan to increase the number of permanent remote roles. The survey found some companies are considering moving a third of their workforce to a remote setup.

This shift means that cybersecurity suppliers and service providers will have to come up with innovations to better assist organizations with adapting to this new environment by exerting greater control over company assets. For the companies, this brings the necessity of increasing security awareness and a focus

on the challenges of work-from-home environments. Therefore, the focus on cybersecurity is expected to be even more pronounced in 2021.

All of this blurs the formerly straightforward classification and separation of employees, customers, contractors, vendors and others. Thus, a good

approach is to consider adopting a "zero trust" principle for access, as the perimeter of an organization is no longer as easy to define as it used to be. This means that for every interaction with an asset, a microperimeter is set up around the asset to enforce a strict least privilege access policy.

Companies should also empower their cybersecurity function, while focusing on agility and automation. This, along with treating cybersecurity as a crucial element of the IT service development process, as well as of the software development lifecycle, will help minimize the potential attack surface.

Cybersecurity spending across sectors

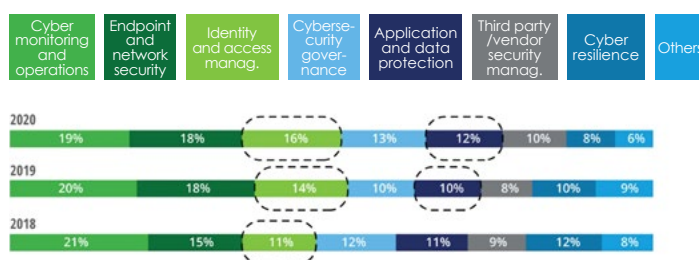
Percentage of revenue
Percentage of IT spending
Per FTE

	2019	2020
Retail/corporate banking	0.3% 10.1% US\$2,074	0.6% 9.4% US\$2,688
Consumer/financial services (nonbanking)	0.3% 9.7% US\$2,817	0.4% 10.5% US\$2,348
Insurance	0.3% 9.3% US\$2,245	0.4% 11.9% US\$1,984
Service provider	0.6% 8.9% US\$1,956	0.6% 7.2% US\$3,226
Financial utility	0.8% 15.2% US\$3,630	0.8% 8.2% US\$4,375
Aggregated total	0.3% 10.1% US\$2,337	0.5% 10.9% US\$2,691

Note: FTE= Full time employee or equivalent.
Source: FS-ISAC/ Deloitte Cyber & Strategic Risk Services CISO survey reports, 2019, and 2020; Deloitte Center for Financial Services analysis.

Budget allocations have remained largely consistent across different cybersecurity domains, with a couple of notable exceptions

Budget allocation across cybersecurity domains by survey respondents



Note: Percentage totals may not equal 100% due to rounding.
Source: FS-ISAC/Deloitte Cyber & Strategic Risk Services CISO survey reports, 2018, 2019, and 2020; Deloitte Center for Financial Services analysis.