KOVRR

Cyber Decisions. Financially Quantified.

www.kovrr.com

Cybersecurity Investments vs. Actual Risk and Cyber Risk Mitigation

JANUARY 2022

Over the last couple of years companies in various sectors have steadily increased their investment in cybersecurity and are forecasted globally to reach $150 billion in 2021. There are many factors that would contribute to the rise in the budget dedicated to cybersecurity, among them is the awareness and experience with the ever-developing cyber threats (both in complexity and frequency) and the IT challenges that come with them.

But this budget growth begs the question - what is this budget spent on? How is it distributed? And is it in line with the real financial business impact due to cyber risk that the companies are facing?

A survey conducted by Deloitte in 2020 shows that there was a notable increase in cybersecurity investment within its clients' companies in the past three years and that many of those companies consider cybersecurity to be a part of the IT function and budget. Generally speaking, this step can be viewed as a positive integration - as many cybersecurity implementations require a close relationship with the IT infrastructure - but also potentially a negative one if the budget distribution within this field can be vetoed in favor of IT over security.

The survey further shows that clients now spend approximately 11% of their IT budget and on average about 0.55% of the company's revenue on cybersecurity.

Security services including consulting, hardware support, implementation and outsourced services represent the largest category of spending in 2021, at almost $72.5 billion worldwide.

Information Security & Risk Management End User Spending by Segment
2020-2021 (Millions of U.S. Dollars)

Market Segment	2020	2021	Growth (%)
Application Security	3,333	3,738	12.2
Cloud Security	595	841	41.2
Data Security	2,981	3,505	17.5
Identity Access Management	12,036	13,917	15.6
Infrastructure Protection	20,462	23,903	16.8
Integrated Risk Management	4,859	5,473	12.6
Network Security Equipment	15,626	17,020	8.9
Other Information Security Software	2,306	2,527	9.6
Security Services	65,070	72,497	11.4
Consumer Security Software	6,507	6,990	7.4
Total	**133,776**	**150,409**	**12.4**

Source: Gartner (May 2021)

The rise in both budgets and awareness of cybersecurity threats costs companies a great deal of money these days, but do they invest in the right fields? Are these expenditures aligned with the actual risk a business is facing? To answer these questions we need to know what the main concern in the eyes of the companies' leaders is when it comes to cybersecurity.

It seems that the top 5 priorities for cybersecurity investment this year are:

1. Cloud security
2. Data security
3. Third-party vendor security
4. Automated processes
5. Mobile security

Looking back at the large scale cyber attacks over the past year it is understandable and justified to invest resources in cloud, data and third party security given that the most prominent attack vectors and threats at the moment are ransomware attacks and data theft (either as part of a double extortion ransomware or on its own).[1]

Business migration to using various cloud services provides additional levels of protection to the companies' data as it is easier to retrieve backups in case of ransomware and an attack directly on a cloud service provider is unlikely and therefore the data is more secure than when it is saved locally.

The most surprising appearance in the top 5 list is mobile security. While there's no doubt that mobile threats are becoming increasingly widespread and varied, the impact of a successful attack on a personal mobile device which is also used for corporate activities (such as emails and calendar) remains relatively low in comparison to attacks on personal computers or corporate services. This is primarily due to the fact that PCs and corporate services typically allow for much more direct and simple access to the corporate network itself, whereas mobile devices usually connect to narrow or limited interfaces of that network.

1. For more information on ransomware trends and double extortion please see Kovrr's blog post: Key Drivers of Rise of Ransomware in 2020

Furthermore, exploitation of mobile devices typically can only be achieved by advanced threat actors. Why? For starters, mobile iOS apps must undergo a review process prior to being registered to be available for download. For Android, apps can be sideloaded, but it's a very cumbersome process. Meanwhile, unregistered PC apps (some infected with malware) are widely available online. Given these hurdles, it's much harder to exploit a smartphone than a PC.

Yes, it's true that mobile remote access Trojans (mRATs) can provide unauthorized stealth device access. An attacker can exploit mRATs to exfiltrate sensitive information from devices such as location, contacts, photos, screen capture, and even microphone eavesdropping. However, attacks such as mRAT are not common or effective attack vectors against organizations and companies. Mobile device attacks are usually very localized to a single user victim. This makes it harder to leverage the attack to expand through the organization. The PC is an easier target and has more damage potential.

While there are a wide range of potential threats out there, it's not feasible, nor financially wise, to invest in security against every possible attack. From a business perspective, one should ask, "For any given cyber threat, what's the potential financial downside?" In the case of mobile, the financial exposure is quite low, so cybersecurity investment should be adjusted appropriately. For instance, basic Mobile Device Management tools should be adequate for most use cases, such as preventing device theft or unauthorized app installation.

Security spending should correlate with actual risk and the risk mitigation actions that correspond to the risks. This even includes potential edge cases regarding mobile security that are identified as high risk. For example, some sectors—such as government, defense contractors, healthcare or other highly regulated industries—might require more advanced mobile defense systems. This is where a quantification model built on threat intelligence and impact data can help guide decision making about security investment, whether it be mobile or otherwise.

> **To see how Kovrr's cyber risk quantification models can help your organization gain a more complete picture of the ever developing cyber threats and improve your company's budget dedicated to cybersecurity, get in touch with our experts today.**

The Author

Yakir Golan

CEO

About Kovrr

Kovrr’s cyber risk modeling platform delivers global (re)insurers and enterprises transparent data-driven insights into their cyber risk exposures. The Kovrr platform is designed to help chief risk officers, chief information security officers, underwriters, exposure managers, risk professionals and catastrophe modelers understand, financially quantify and manage cyber risk by utilizing AI-powered risk models.
To learn more please contact the Kovrr team: contact@kovrr.com