Cybersecurity in 2022: Budgets, Insurance and Vendor Relationships

A look into cybersecurity budget planning, insurance consideration and vendor expectations in the year ahead

kaspersky BRING ON THE FUTURE

Introduction

With the beginning of each new year, business objectives are often established in advance so that organizations are able to work towards their goals from an early start. Key stakeholders will set their sights on strategic initiatives and the tactics that will help them achieve business success to set themselves up for a year of growth.

With the expansion of the cybersecurity industry on the rise, Kaspersky was interested in learning more about how organizations will prioritize their businesses this year in three key areas: cybersecurity budget, cyber insurance and vendor relationship expectations.

As a result, the company commissioned a survey in the months leading up to 2022 to learn more about how IT staff is planning for the year ahead.

This report details the research findings as well as insights from thought leaders in the industry.

Key findings from the study include:

- **Overwhelmingly, 86% of North American respondents said their organization intends to set aside budget for cybersecurity when planning for 2022**
- **But just how much? 85% said their organization's budget would increase up to 50% in the next 12 months, with the majority of respondents (15%) saying their budgets would increase by 11-15%**
- **Cyber insurance continues to be a key area of investment with 28% of respondents saying their company annually invests anywhere from $25K-$50k per year**
- **The top three cybersecurity risk management investments organizations plan to prioritize budgeting for in 2022 are cyber insurance (45%), digital forensics and incident response (43%) and training (42%)**

Research Methodology

This quantitative study was conducted by research firm Opinion Matters via an online survey in October 2021. The survey targeted 600 employees who are key decision makers for the cybersecurity sector within their company. Respondents were based in USA (300) and Canada (300). By conducting this research, Kaspersky is able to shed light on cybersecurity budget planning for 2022 so that vendors have an accurate idea of where cybersecurity business investments will be prioritized.

Throughout the report, businesses are referred to as either SMB (small and medium sized businesses with 0-250 employees), mid-market (251-999 employees) and enterprise (1000+ employees). Not all survey results are included in this report.

86%

Of respondents in both the U.S. and Canada overwhelmingly agreed that their organization intends to set aside budget for cybersecurity when planning for 2022.

Research Findings

Cybersecurity Budgets in 2022

There is no question that budget limitations set the tone for the investments and resources company wide, and that undoubtedly includes cybersecurity.

Respondents in both the U.S. and Canada overwhelmingly agreed (86%) that their organization intends to set aside budget for cybersecurity when planning for 2022. In addition, 85% of respondents reported that their organization's budget would increase up to 50% in 2022, with the majority of respondents (15%) saying their budgets would increase by 11-15%.

Further, of all those surveyed, employees in SMBs had the strongest response with 19% saying their organization will increase 6-10% in the next year as compared to mid-market (12%) and enterprise (11%).

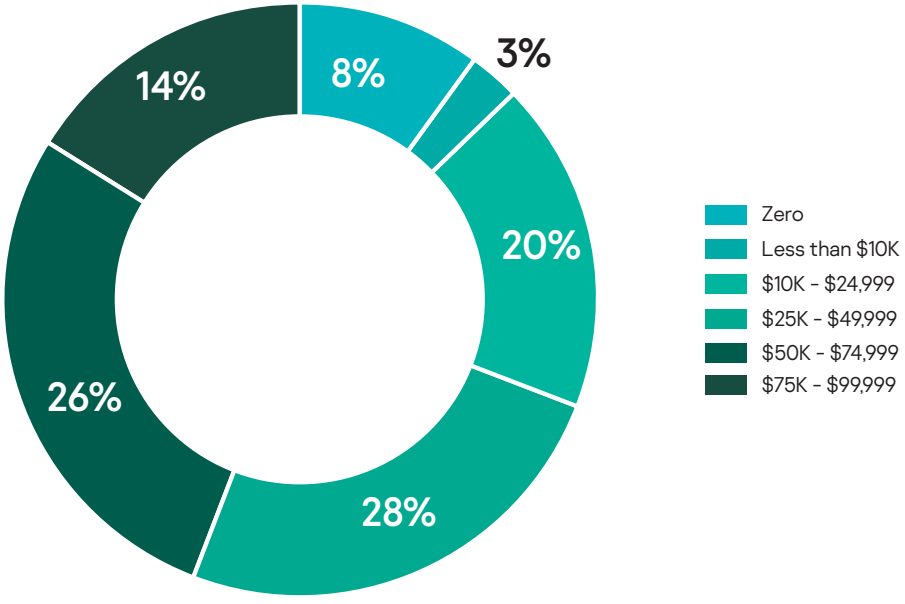
While this upwards trend is not a surprise, many experts agree that the industry at large is facing slowing budget growth when considering the increasing number and sophistication of cyberattacks. While this may be true, the research does highlight that many organizations see the value in investing in cybersecurity and are making a concerted effort to do so, even if their budget to do so is more minimal than they would hope for.

Cyber Insurance

Cyber insurance is a newer concept in the industry that allows businesses to hold a policy with an insurance carrier to mitigate risk exposure by offsetting costs involved with damages and recovery after a cyber-related attack, breach, etc. While not all forms of cyber risk are covered by insurance and no two policies are alike, cyber insurance continues to be a key area of investment for businesses.

In fact, the survey research concludes that 28% of respondents said their company annually invests anywhere from $25K-$50k per year in cyber insurance. In addition, the top three criteria organizations said they would be willing to meet in order to obtain cyber insurance include security controls (70%), compliance (52%) and education (44%).

How much, if at all, does your company invest annually in cyber insurance?



Vendor Relationships

The relationship between vendors and their clients is one that develops over time and requires an evolving strategic approach, especially in the case of cyberattacks.

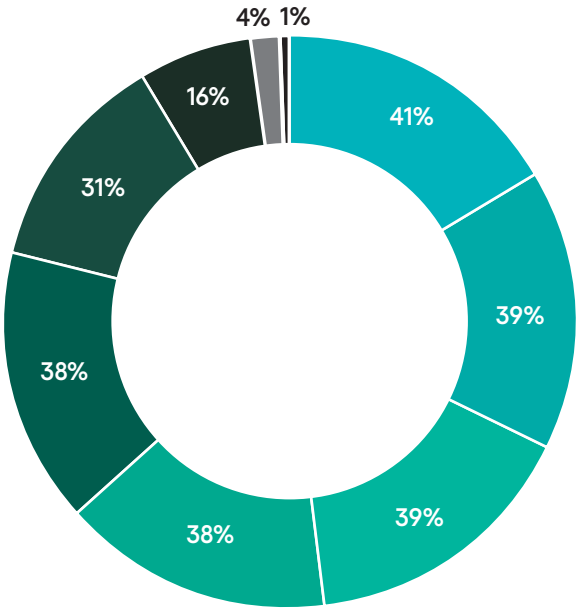
When asking organizations who they would hold most responsible for letting a cyberattack in, vendors were the top choice (25%) with the internal IT team as a close second (23%). Alternatively, 41% of respondents said they would ask their cybersecurity vendor for more recommendations on what their organization could/should do to avoid potential cyberattacks if they were affected by one.

Respondents also agreed that detection (51%) and prevention (50%) are the top two areas where vendors can improve to better protect organizations from cyberattacks. When it comes to risk management investments, the top three areas organizations plan to prioritize budgeting for in 2022 are cyber insurance (45%), digital forensics and incident response (43%) and training (42%).

"Until that unimaginable day when the volume and impact of attacks begins to subside, it's only logical that organizations would increasingly rely on cyber insurance to augment their risk management programs. This being the trend, it will be interesting to see how underwriters tighten up on claims coverage criteria and expand their requirements for security controls. As requirements expand and budgets increase, especially in the mid-market, security vendors should be prepared to meet these organizations at their point of need by improving prevention, detection and response functions while simultaneously improving simplicity in operation."

Rob Cataldo,
Managing Director of
Kaspersky North America

How would a cyberattack affect your organization's relationship with its cybersecurity vendor?



- Ask our cybersecurity vendor for more recommendations on what our organization could/should do to avoid potential cyberattacks
- Put our cybersecurity vendor on immediate notice
- Listen to our cybersecurity vendor's recommendations more willingly
- Change our cybersecurity vendor
- More willing to invest in additional controls with current cybersecurity vendor
- Negotiate additional services with immediate effect
- Negotiate added value for a future/extension to our contract
- We don't have a cybersecurity vendor
- A cyberattack wouldn't affect my organization's relationship with its cybersecurity vendor

Conclusion

With 2022 off to an optimistic and aggressive start, it is important for cybersecurity vendors and internal teams to have a cohesive understanding of their expectations for the year. Whether it is from the perspective of budget limitations, how much they are willing to invest in cyber insurance or how to best work with one another, having a deeper understanding of where opportunities for growth are will continue to be a key element of success in the year ahead.

About Kaspersky

Kaspersky is a global cybersecurity and digital privacy company founded in 1997. Kaspersky's deep threat intelligence and security expertise is constantly transforming into innovative security solutions and services to protect businesses, critical infrastructure, governments and consumers around the globe. The company's comprehensive security portfolio includes leading endpoint protection and a number of specialized security solutions and services to fight sophisticated and evolving digital threats. Over 400 million users are protected by Kaspersky technologies and we help 240,000 corporate clients protect what matters most to them. Learn more at usa.kaspersky.com.

usa.kaspersky.com

kaspersky BRING ON THE FUTURE