CS HUB MID-YEAR MARKET REPORT 2022

The current challenges facing cyber security practitioners and where they are focusing their investment decisions in 2022 and beyond

INSIDE:

- The state of today's threat landscape
- The security controls CISOs are prioritizing for investment
- Cyber security as a main concern for organizations in 2022

Brought to you in association with:

LastPass

Contents

INTRODUCTION

Cyber security central to operational success

Cyber security practitioners entered 2022 under the shadow of the Log4Shell vulnerability. The vulnerability sent shockwaves throughout the cyber security world and has continued to be used by threat actors.

Just months into 2022, statements from government organizations such as the Cybersecurity and Infrastructure Security Agency (CISA) in the US and the UK's National Cyber Security Centre (NCSC) called on organizations, especially those in the critical infrastructure realm, to enhance their cyber security efforts due to the heightened cyber threat from Russia following its invasion of Ukraine.

These challenges, combined with the continuing evolution of threat actors' tactics, the remote working trends and ongoing skills shortages within the cyber security sector, have placed the role of CISO in the spotlight at organizations around the globe.

In this *CS Hub Mid-Year Market Report 2022*, we asked our network of cyber security practitioners about the current trends in the industry, what their top priorities for investment are today and where they see the biggest threats to their organization.

When asked to consider their organization's approach to cyber security over the past 12 months, the results of the CS Hub mid-year survey 2022 reveal that 30 percent of respondents say their organizations have a high prioritization of cyber security.

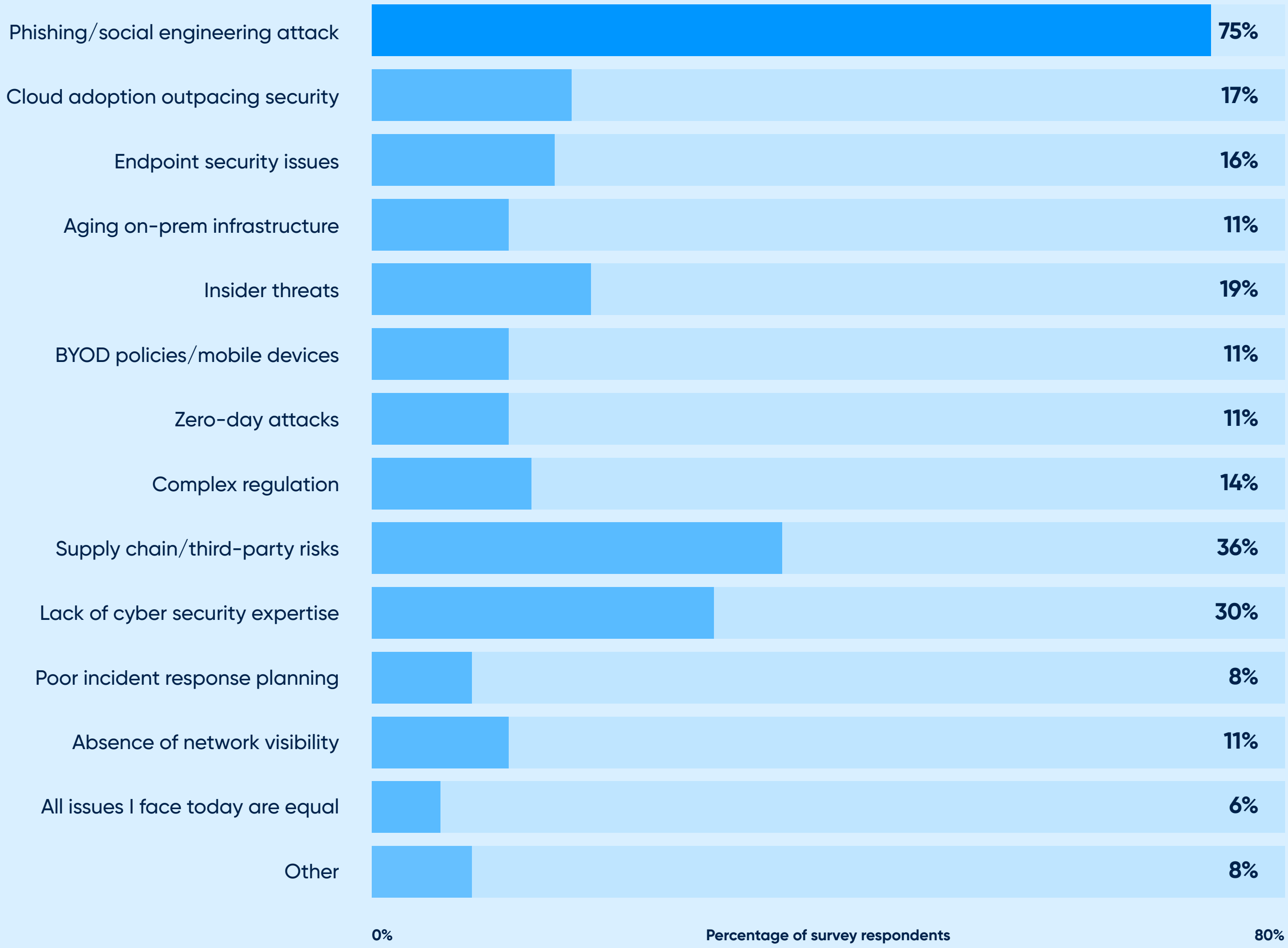
With the aforementioned challenges making the headlines, not just within professional channels but in mainstream media too, it is unsurprising that most organizations consider cyber security a top priority and, as we will see in later chapters, are committing further resources to their cyber efforts.

One survey respondent, who chose to remain anonymous, comments that "the speed of the evolving threat is outpacing [cyber security practitioners]".

This exclusive *CS Hub* report aims to keep cyber security professionals abreast of today's threats and highlight the areas in which CISOs are allocating security budgets to mitigate the risks facing their organizations.

Today’s threat landscape

FIGURE 1:
What are the three most dangerous cyber security threats your organization faces today?



Source: *Mid-year survey 2022, Cyber Security Hub*

In today’s digital world, organizations’ networks are being spread further than ever before, especially as the number of people working remotely has increased dramatically since the outbreak of Covid-19 in early-2020. Threat actors will exploit just about any vulnerability to disrupt an organizations’ network, compromise data and bring down systems.

We asked our survey respondents what the top three most dangerous threats their company faces today were and the three frontrunners that emerged were: phishing/social engineering attacks with 75 percent of respondents; 36 percent saw supply chain/third party risks as a high risk; and, finally, 31 percent of respondents said the lack of cyber security expertise was a threat to their organization.

Phishing and social engineering remains the top threat vector having featured in 2021’s *CS Hub Mid-Year Cyber Spend & CISO Trends Report* as the most dangerous threat facing CISOs.

Commenting on phishing and social engineering attacks result, Jeff Campbell, technology manager

>>

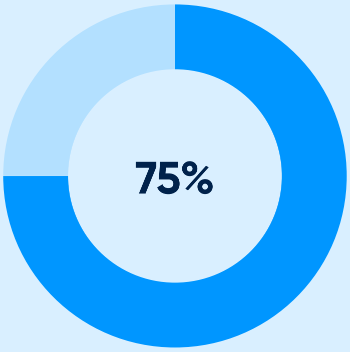
>> and previously CISO at Horizon Power, an Australian power supplier, says: "With the increase in maturity over the years of edge security, the easiest way in is through the weakest link which generally tends to be individuals, so getting an individual to click on a malicious link or giving away information still yields successful results."

Third-party risk and staff shortages

Considering the supply chain is a growing concern for many as ultimately as good as your defenses are, a vendor or supplier could be the weak link in your cyber security efforts.

This was demonstrated when Okta, an identity and access management company, was compromised by one of its third-party vendors in January 2022. On 23 March, Okta disclosed that the company's security team had been alerted that a new factor was added to a Sitel, one of Okta's vendors, customer support engineer's Okta account. The compromise saw the Lapsus$ hacker group post on its Telegram channel that it had breached the company.

As a result of the incident, Okta took action to strengthen its security posture and third-party risk management strategy.



The percentage of survey respondents who say that phishing/ social engineering attacks are a top concern for their organization

Tom Kartanowicz, regional CISO Americas at Commerzbank AG, a major German bank, comments that third-party risk reflects larger societal issues having downstream effects on cyber.

"We've experienced two years of Covid-19, lockdowns, rampant inflation and nation-state conflict, and we're fortunate it hasn't been worse," Kartanowicz remarks. "Companies that outsourced or near-sourced functions are very much dependent on the defensive position of those firms. And sometimes the best way to get in is through an indirect source such as a third party who may have weaknesses that enable the end-goal and objective of the attacker."

Encouraging people into cyber

Those plugged into the cyber security community will find it unsurprising that a lack of skilled cyber personnel is an ongoing concern for many organizations, while global workforce shortages continue to hamper organizations' abilities to secure systems and networks.

In 2021, (ISC)^2 Cybersecurity Workforce Study stated that the "global cybersecurity workforce needs to grow 65 percent to effectively defend organizations' critical assets".

Commenting on the skills shortage, Kartanowicz says that "there isn't any magic pill" to be able to overcome this issue.

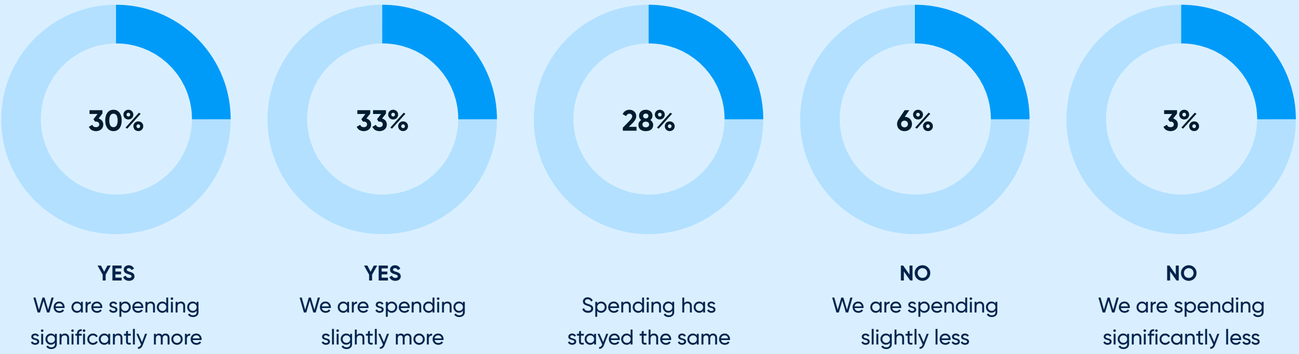
"You need a pipeline of talent and sometimes it takes a while for talent to get experience which leads to expertise," Kartanowicz notes. "I also think that a lot of potential expertise exists in the current IT field which could be leveraged if IT professionals transition over to careers in cyber – especially as defenders or operational staff."

With these three important issues in mind, operational resilience is key for organizations to overcome today's evolving threat landscape, not just in terms of the technology that is being invested in, but also the human element of employees.

Cyber security investment in 2022

FIGURE 2:

Is your organization spending more on cyber security now compared with FY 2021?



Source: *Mid-year survey 2022, Cyber Security Hub*

Considering the context set out in the introduction of this report, as well as the threats organizations are facing as shown in the previous chapter, it is positive to see that investment in cyber security is increasing.

Looking at past surveys conducted by *CS Hub*, in November 2020 60 percent of respondents stated they anticipated a decrease in cyber budgets for the first half of 2021. When asked in the first six months of 2021, 45 percent of respondents said their cyber security budget had increased, which increased in the second half to 51 percent.

Considering today's expenditure, 63 percent of respondents to the 2022 survey say they are spending either slightly or significantly more than in FY 2021 (see Figure 2). Just nine percent claim they are spending slightly or significantly less, and 28 percent say spending remains the same.

Pleasingly, we have reached a point where cyber security has become a recognized business risk and spending is now matching this risk profile, notes Horizon Power's Campbell.

While the increase will be good news to cyber security professionals everywhere, Kartanowicz warns that the macro-economic climate is a cause for concern about FY 2023 budgets.

"It's easy to spend when the economic climate is one of growth but with recession forecasts for 2023 and a deteriorating economic environment," Kartanowicz remarks. "I'd be surprised if this trend carries on into next year. It's a healthy budget state today but I'm worried about tomorrow."

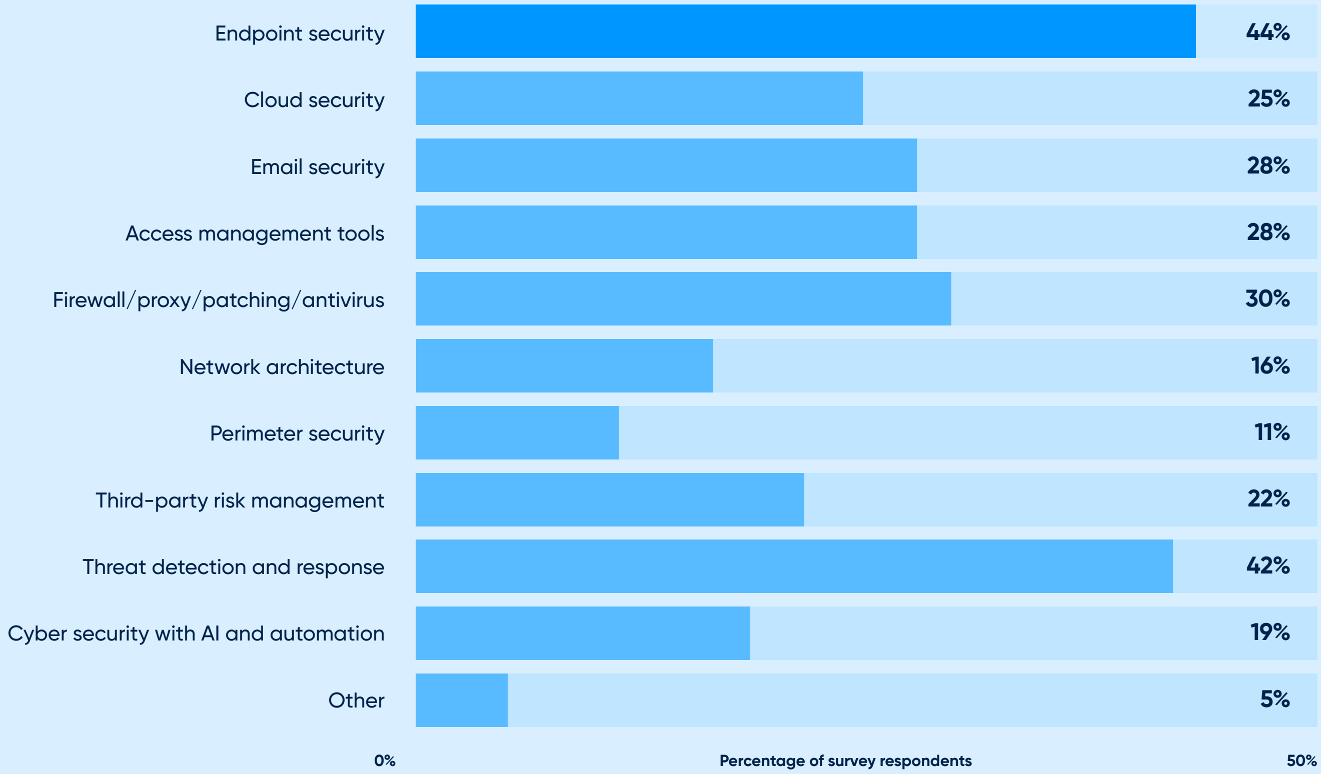
It is difficult to predict how spending will look in the future and whether risk reduction can be demonstrated then we could see cyber security spending continue on a slow growth. However, look to the wider economy, when organizations are forced to tighten their purse strings a plateau or even shrink in spending is possible.

For those spending less on cyber security compared to FY 2021 it is concerning and they will likely be the most vulnerable to cyber-crime if they do not have sufficient security controls in place.

Cyber security investment in 2022

FIGURE 3:

In which security controls are you currently investing?*



*Respondents were asked to select a maximum of three options

Source: *Mid-year survey 2022, Cyber Security Hub*

Solution investment

Endpoint security (44 percent) and threat detection and response (42 percent) are the top two security controls that cyber security practitioners say their organizations are investing in (see Figure 3). Cloud security (25 percent), email security (28 percent), access management tools (28 percent) and firewalls/proxy/patching/antivirus technology (30 percent) are also considered top investment priorities in 2022.

This aligns with trends identified in *CS Hub*'s 2021 industry report which saw endpoint security as a top investment option.

Considering the survey results, Kartanowicz says, endpoint and threat detection and response fully align with the never-ending barrage of phishing and social engineering attempts.

"It doesn't address the talent topic and lack of expertise at all, however, and there are not any platform or shiny box that blinks that can help that one," Kartanowicz notes. "But from a tech spend perspective I 100 percent agree with the findings of the survey."

Early detection is a sound investment

Endpoints themselves are not a new phenomenon and today's organizations must consider that the number of devices has risen exponentially, with most employees having access to multiple devises in order to carry out their work. This, coupled with the emergence of a remote-working culture and the

>>

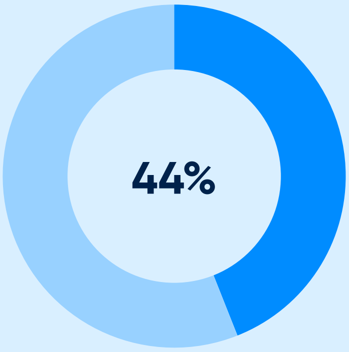
move away from a secured-on premises network, means organizations need the be ever-more vigilant about endpoint security.

Campbell notes, “Any investment that provides early detection and response is a good investment as it increases your capability to minimize the risk of a breach. Layering controls and then making sure you have your SIEM configured to provide data into a SOC is where I would start.”

In terms of solutions, we have recently witnessed the emergence of extended detection and response (XDR) technology in the general endpoint detection and response (EDR) market which many CISOs implement to bolster their endpoint security.

The next 12 months

When asking our survey respondents what the biggest priorities for investment over the next 12 months is, the results vary wildly with no single investment priority coming out on top. Secure access and network visibility is, however, the least likely to be a priority, which Campbell says may be related to investments priorities having already been made in previous years.



The number of survey respondents who say endpoint security is currently being invested in

Campbell says: “Most organizations have implemented VPNs and multi-factor authentication (MFA), are utilizing next-gen firewall capability to provide network visibility, and they have done so for many years.”

Priorities for the next 12 months, however, do include basic security fundamentals (30 percent), secure data management (39 percent) and threat detection and incident response (36 percent).

We can clearly see that threat detection and incident response continues to be a top priority.

With regards to secure data management, it is well known that ‘data is the new oil’ and access to data continues to be the top target for threat actors. Therefore, being able to have a secure data management plan is a must for all organizations today. Data management is also heavily regulated, for example with GDPR and CCPA, so there is an increased need to invest.

Most organizations are aware that a serious and significant data breach can compromise the company’s public perception. One negative headline in connection with a data breach can lead to distrust among an organization’s customers and clients.

Secure data management may have edged to the forefront of investments for the next 12 months, but it is important that many organizations (30 percent) are also considering basic cyber security fundamentals as an area for investment.

We can clearly see that there is a good reason to discuss advanced technologies and the latest trends, however, there is a case to bring it back to basics. Organizations must get to grips with things like firewalls, penetration testing, MFA, incident response planning and web application scanning if cyber security foundations are to be implemented as the first line of defense against threat actors.

Toward a passwordless future

The idea of going passwordless has been ongoing since the early 2000s when Microsoft founder and chairman Bill Gates predicted the death of traditional passwords unable to keep pace with evolving security needs.

While those security savvy folks continue to enter 10+-character passwords with special characters, numbers, lower- and upper-case letters, some have still failed to get the message that '1234', 'qwerty' and 'asdf' remain the most popular passwords among the English-speaking world.

CS Hub chats to LastPass chief secure technology officer Christofer Hoff about the company's recent move toward passwordless technology following its June 2022 announcement launching passwordless login to the LastPass vault through the LastPass Authenticator.

CS HUB: Why is it necessary to look toward a passwordless future?

CHRISTOFER HOFF: Balancing security requirements and user experience for employees is the number one identity challenge facing businesses today, closely followed by employees having to manage "too many passwords". For too long, businesses have put the onus on the individual to create complex passwords, without providing the right education, best practices, and tools to manage and protect these secrets.

The reality is that while many businesses and employees thrive in a digital work environment, security gaps widen as usability becomes complex. This is reflected in the high volume of data breaches, in fact, in the 2022 Verizon Data Breach Investigations Report (DBIR), more than 80 percent of the breaches in web application attacks can be attributed to stolen credentials.

IT leaders must bridge the gap between seamless and secure for their end users, and this can be achieved by using a password manager and by going passwordless.

CS HUB: What are the challenges CISOs and security teams face today that 'going passwordless' seeks to resolve?

CH: It is 2022 and breaches are still caused by poor password hygiene. In the latest LastPass Psychology of Passwords report, 50 percent of respondents stated they have 50 percent more accounts in 2021 than in 2020, that is only expected to grow in 2022 as digital lives expand. What is most concerning is that users do not protect these accounts or credentials, with 45 percent of survey respondents noting they did not change their passwords even after a breach had occurred.

CISO's need to reduce the human error by simplifying their employee's security experience. Employees must be able to access, use and manage important account credentials with internal and external colleagues, from anywhere at any time. Deploying point solutions like single sign on [SSO] is not enough to protect your business as this leaves security gaps for those applications that don't integrate with SSO, think of corporate credit card accounts, Facebook, Twitter, and more – all sites and credentials that are commonly used in business.

Using a password manager and enabling passwordless logins reduces password-related login friction for employees, while maintaining the highest levels of security for IT.

Toward a passwordless future

CS HUB: How do passwordless logins provide better cyber security than traditional log-in credentials?

CH: At its simplest, reducing the frequency in which a password is used or entered, in turn reduces the overall risk and attack surface. Replacing passwords with a form of secure authentication, such replacing them public/private cryptographic keys (the FIDO2 standard), is more secure than what you are doing today for several reasons.

CS HUB: LastPass Authenticator for the LastPass vault – Please discuss how this works, the benefits and how you see it evolving in the future.

CH: Any LastPass end user can download the LastPass Authenticator app for free and use this authenticator to passwordless login to their LastPass vault. To enable passwordless users will login to their account with their master password, follow the guided prompt located in their account settings, and sync the LastPass Authenticator.

Once enabled, the next time a user initiates a login they will instead receive a push notification through the LastPass Authenticator rather than entering their master password, verify the access request through a push notification, and then entering their vault. The LastPass Authenticator becomes the primary method of authentication into the LastPass vault.

In the future, a smartphone that end users have in their possession can be converted to a roaming authenticator, so users can authenticate, and ensure future logins do not require registration at new device login. LastPass is actively driving toward this FIDO2 standard.

CS HUB: What do you see as the biggest challenges facing organizations today who want to embark on making their company's passwordless? How can they overcome these challenges?

CH: At the end of the day, passwords are going to be around for many, many years – despite device, operating system and web browser vendors (often the same company) making enormous strides. The biggest challenge will be the long tail of adoption of passwordless, because applications must be rewritten to take advantage of WebAuthn capabilities. That will just take time and unification efforts across many vendors.

While that adoption occurs, it is critical that organizations have a cybersecurity strategy that includes IAM technology, such as SSO, MFA, and password management, together. While some IT leaders – 57 percent, have passwordless technology on the roadmap for their businesses, all IT leaders should be driving the conversation on how they can simplify the usability of these security measures.

Cyber security remains an operations priority

Organizations in 2022 have accepted that cyber security is a high priority and the threat landscape we live in today means they have to continue to evolve their security posture to ensure operational resilience.

We can clearly see that the threat of phishing and social engineering attacks has not gone away and continues to be a top concern for cyber security practitioners. Meanwhile, an emerging issue is that of third-party vendors. Organizations are now not just concerned with what is happening within their own remit but now must consider the security posture of their partners and vendors to avoid an attacker using a third, fourth or even fifth party to gain access to an otherwise secured network.

All this while at the same time security leaders must deal with a shortage of skills in the cyber space which will require long-term investment to encourage people to join and remain within the cyber security field.

Investment in cyber security should continue

Correlating with the issues that we saw in terms of the threats organizations face today, endpoint security and detection and response capabilities were the top two security controls organizations are looking to invest in today.

Ultimately this investment aligns with the ongoing phishing and social engineering threats from ransomware gangs and cyber criminals.

It may not be possible to stop 100 percent of attacks and breaches against an organization making detection and response capabilities crucial in the fight against today's threat actors. The faster a breach can be identified the more chance an organization has of containing it before it becomes headline news.

What we can consider to be established technology, based on a lack of investment prioritization, is secure access and network visibility. Over the next 12 months these two factors are set to see the least amount of investment based on our survey results, in part because most organizations have already implemented next generation firewall capabilities in order to provide network visibility.

Overall investment in cyber security is increasing compared with FY 2021, however whether that trajectory continues could be dependent on factors outside of most organizations' controls. The economic fallout from the COVID-19 pandemic combined the Ukraine-Russia conflict has seen the global economy take a turn, with some considering that 2022 will be a year of at least mild-recession for many.

The trickle on impact of this is organizations may be forced to tighten the purse strings in order to ride out this period, ultimately this could have an impact on cyber security budgets. As Kartanowicz commented, today's budget state is healthy but tomorrow is a concern.

Keep up cyber hygiene

"Trends will come and go but the fundamentals of cyber hygiene are fairly constant—do it right (no easy task) and your organization will be moving in the right direction," Kartanowicz says.

It is clear that new technologies like XDR and passwordless innovations are ripe for investment in the face of today's threat landscape, at the same time, budgets may fluctuate depending on global economics. As Kartanowicz rightly points out, this will allow your organization to move in the right direction when it comes to its cyber security posture.

In the introduction of this report, we found that organizations have a high prioritization of cyber security and with this cyber security basics must be implemented at all organizations whatever their size, status or location.

Basic security fundamentals are a top priority for 30 percent of our survey respondents, clearly getting the basics right is a high priority and is the most important step to take to enhance security postures and build a more advanced cyber security programs to meet the evolving threat landscape.