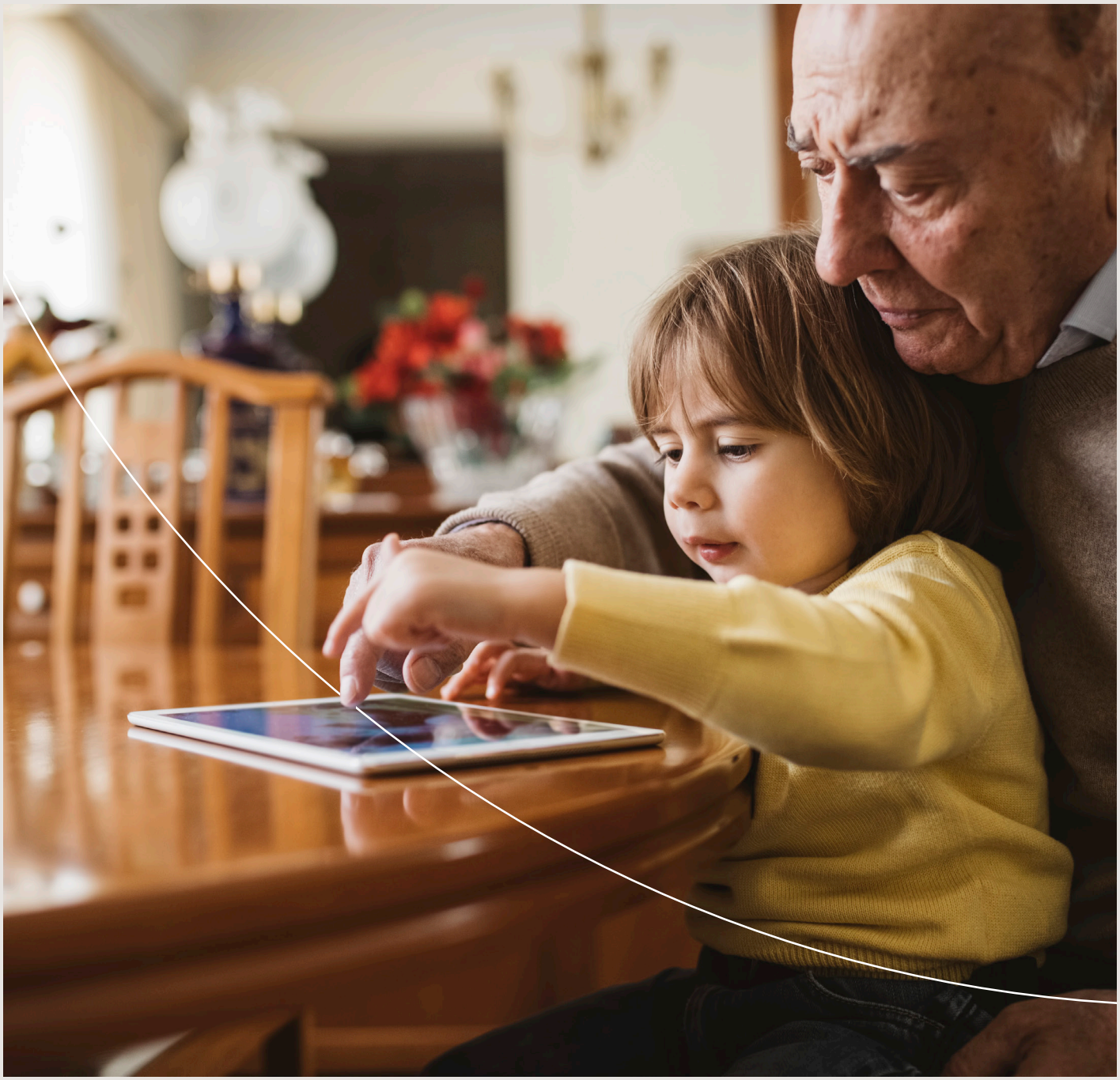


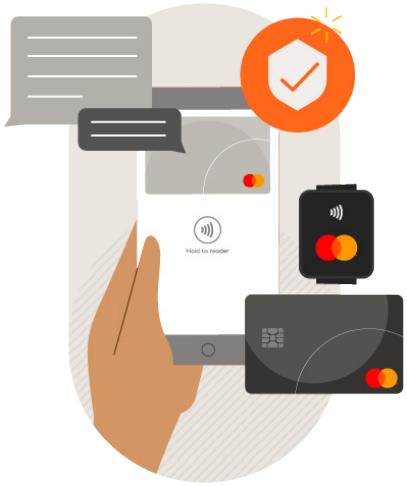
WHITE PAPER

JUNE 2023

Cybersecurity: Building trust in our digital age.

Cybersecurity leaders and their pursuit to manage cyber risk

Foreword



In an increasingly digital world, cybersecurity is climbing the priority list for business leaders. While the excitement around evolving technologies is palpable, the boardroom is becoming increasingly aware of the risks that come with it.

The impact of a cybercrime can be debilitating. Globally, the average data breach costs $4.35 million, rising to $9.44 million in the US.[1] This cannot be left to chance.

In response, cybersecurity has quickly progressed from an IT challenge to a C-Suite priority; it's now the top digital risk businesses face today.

The best way to fight cybercrime is to understand the risk. What does it look like? Why does it happen? How can it be stopped? Both cyber leaders and their vendors must possess this intelligence before they deploy their defenses.

And that's why this piece of research is so important. Data commissioned by Mastercard, collected by Aite-Novarica, and analyzed by the Centre for Economics and Business Research (Cebr) combines to tell the true story of the challenges faced by cyber leaders over the next year.

The data presented in this report provides a unique snapshot into the threats, solutions, and tensions facing cyber leaders in financial institutions and merchants. Cybercrime is an evolving challenge but, by informing cybersecurity strategies with the latest trends – we can anticipate what is coming – and be prepared.

Johan Gerber
Executive vice president, Security and Cyber Innovation, Mastercard

1. IBM (2022), Cost of a data breach 2022

Executive summary

As technology transforms our everyday lives it brings a host of opportunities. Generative AI bots, smart Internet-of-Things powered devices, and the technology behind the virtual workforce have sparked levels of innovation that have never been seen before. At the same time this unparalleled digitization poses new challenges for cyber leaders.

That's why we wanted to get an unrivalled perspective on the risks associated with today's technology trends, as well as to understand their views on the types of solution that are helping them adapt to the threats and to become cognizant of the extent to which business is ready to invest in cybersecurity.

Earlier this year Aite-Novarica completed surveys and interviews with cybersecurity leaders from financial services firms and merchants in eight countries.[2]

The findings are revelatory. These technologies are supercharging cybersecurity solutions. AI, in particular, is generating excitement among leaders, although it's accepted that further innovation is required before it fulfils its potential.

The combination of rising cyber risk with more effective tech-powered solutions is encouraging organizations to invest. Cybersecurity budgets are increasing. Of the FI's who we spoke to 54% increased their budget between 5-10% in 2022 vs. 2021, a trend expected to continue in 2023 and 2024.

Cyber investment is only as valuable as the expertise and knowledge behind it. This remains a critical challenge for cyber leaders. In short, they need help.

Also, eighty-four percent of cyber security leaders surveyed said they would benefit from third-party assistance in deploying AI-powered solutions, navigating digital identity, API security, and knowing which cyber threats are coming around the corner.

Now, the needle swings to security vendors. At a time when almost half of cyber leaders told us they're considering switching their solution providers, there is a clear opportunity for technology companies and vendors to provide trusted consultancy, support, and training to truly make the difference to their customers.

2. The countries surveyed were: Australia, Brazil, Germany, India, Saudi Arabia, UAE, UK, and the US.

Cyber challenges

93%

of consumers admitted they're concerned about cybercrime with one in ten already falling victim to a related incident.

We are living in times of rapid innovation. Digitization is moving faster than ever before, but with every leap forward, there is new challenge, and more sophisticated risk. The more technology businesses use, the more data they produce, the greater the risk and the larger the opportunity for cybercriminals to strike.

This is not a challenge that will go away and one that – if not addressed appropriately – can irrevocably damage hard earned trust and derail the entire organization.

Fear around breaches is palpable: 93% of consumers admitted they're concerned about cybercrime, with one in ten already falling victim to a related incident.

Today's cyber leaders are under unprecedented pressure to make the right decisions and alleviate anxiety among customers and key stakeholders. However, it's impossible to know which issues to prioritise without first identifying the source of the problem.

Cyber leaders named the following technologies as those that would cause the most complex challenges to their specific team:

Non-human actors (BOTs)

Internet of things (IoT)

Virtual workforce

The reality is that it's the same, new, and exciting technologies – from generative AI bots and connected smart devices to work–from–home platforms – are the ones posing the most significant challenges to the cybersecurity sector.

The digital transformation conversation is often dominated by the need to be the fastest and the most innovative. Yet – as organizations race to be the first to implement new technologies – the message from cyber leaders is clear: slow down, don't cut corners, and put security first.

Source: Horn, John. cybersecurity 2023, InfoSec leaders pursue the future of financial services, Aite-Novarica. May 2023

Cyber solutions

Respondents selected AI as the most exciting cyber solution currently available to them.

56%

of respondents believe the technology still requires further innovation.

As Albert Einstein is purported to have said: "In the middle of every difficulty lies opportunity." Cybersecurity is no exception. It's widely known that businesses suffer a wide range of cyber issues, ranging from malware and phishing attacks to employee knowledge gaps and third-party vulnerabilities. What is lesser known is the technology that can power effective cyber defenses in 2023.

Cyber leaders tend to have a personal passion relating to cyber security solutions. Artificial intelligence (AI), in particular, is igniting the imagination of the cyber industry and has the power to take cybersecurity professionals into realms previously deemed implausible if not impossible to reach

Respondents selected AI as the most exciting cyber solution currently available to them and it's easy to understand why. Imagine a world where an AI-powered shield – or threat protection system - automatically defends organizations against cyber threats without the need for human intervention.

While significant progress in AI has been made towards this reality, over half (56%) of respondents believe the technology still requires further innovation.

There are many aspects to cybersecurity measures. When asked, cyber leaders identified the following as priority interests for their security solutions:.

Defending against the attacks of tomorrow

Identity (Digital workforce and digital transformation)

API security (Open banking)

When deployed in unison, cyber leaders can defend their organizations in the same way that we might defend our homes. They ensure all doors and windows are secure to prevent unauthorized entry, similar to API security; they provide authorized visitors – colleagues – with the right key to enter, the same as identity; and they receive real-time weather intelligence to see if a threats coming and whether more action is needed.

This is the future of cybersecurity. The innovation taking place today will empower tomorrow's cyber leaders to tackle their greatest fears – providing they're granted the resources to do so.

Financing cybersecurity

4.5%

cybersecurity budget growth in 2022 compared to 2021[4].

6.2%

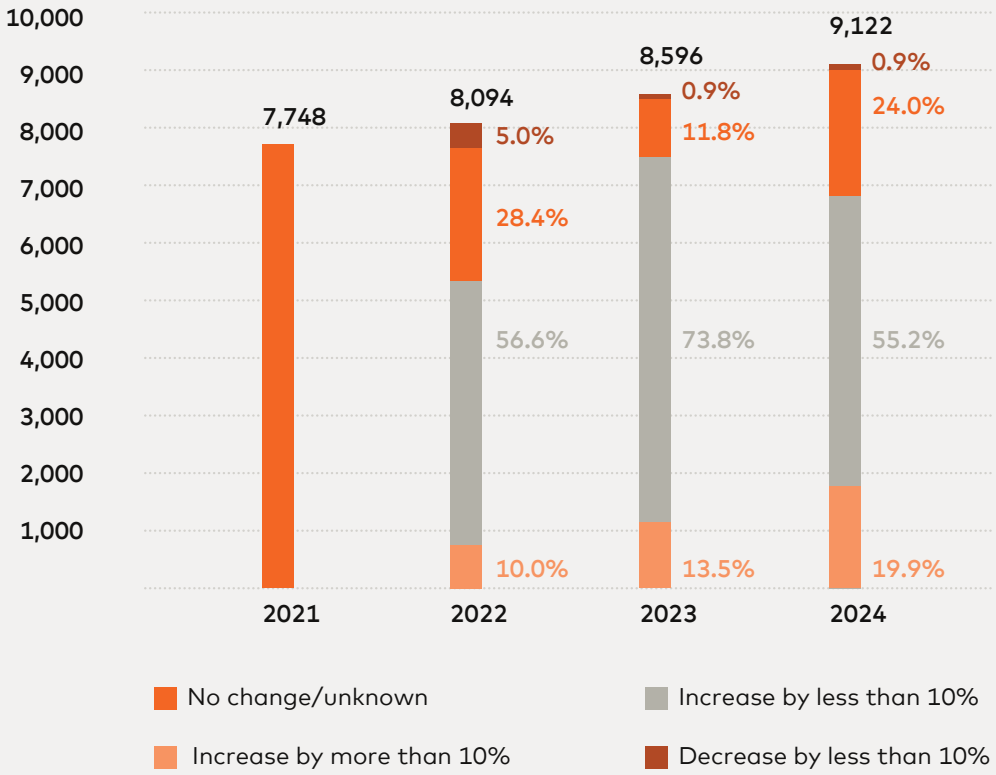
cybersecurity budget growth in 2023 compared to 2022[5].

Fortunately, organizations are now recognizing that more resources are required to effectively defend against cybercrime. The combination of rising threats, a better understanding of capital and reputational risk, and more effective solutions entering the market is encouraging C–Suite leaders to allocate more budget to cybersecurity.

In 2022 – despite challenging business conditions[3] – the cybersecurity budgets at financial institutions rose on average, by 4.5% year–on–year. This upwards trend is expected to accelerate further in 2023 and 2024, as organizations demonstrate an increased understanding of its value to their growth journey. The data (Figure 2) underlines this yet further, showing that of all those surveyed the number set to increase their budgets by more than 10 percent has doubled from 2022-24.

3 OECD (2023). 'Business Confidence Index (BCI)'
4 Source: Horn, John. cybersecurity 2023, InfoSec leaders pursue the future of financial services, Aite-Novarica. May 2023
5 Source: Horn, John. cybersecurity 2023, InfoSec leaders pursue the future of financial services, Aite-Novarica. May 2023

Figure 1: Year-over-year cybersecurity budget trends across all 221 surveyed institutions ($, million)



Source: Horn, John. cybersecurity 2023, InfoSec leaders pursue the future of financial services, Aite-novarica. May 2023

"We are concerned about our infrastructure security and cloud security. This consists of identifying our futuristic cybersecurity needs, budgets & investments in software and hardware."

– Respondent[6]

Cyber leaders are looking to equip their people with the right solutions to tackle threats coming their way. With increased budgets – and a catalogue of products on their desk – they must now decide which areas of their security infrastructure require the most urgent upgrades.

In 2023, Cybersecurity professionals stated the following as their top investment priorities:

Malware defences

Infrastructure security

Cloud security

API security

6. Source: Horn, John. cybersecurity 2023, InfoSec leaders pursue the future of financial services, Aite-novarica. May 2023

Cyber leaders need support

$4.35m

the average global cost of a data breach in 2022

84%

claimed they would be interested in receiving assistance from a third party around AI–powered cyber solutions.

46%

of cyber leaders stated they are likely to change vendors in the next three years.

Organizations have access to an abundance of cyber solutions, and resource. Despite this, there is still a recognized need for more innovative solutions, to address more sophisticated threats and tackle the wave of cyber threats heading in their direction.

What support do they require? The large majority of cyber leaders surveyed require third–party assistance in the form of knowledge, design, and solution training. A significant knowledge gap still exists within financial institutions and merchants which – if not addressed – is detrimental to the business.

The average global cost of a data breach in 2022 was $4.35 million[7]. While not only financially crippling to a business, this could also prove disastrous reputationally when coupled with the loss of consumer confidence and customer trust.

AI, in particular, was an area in which leaders feel their knowledge is lacking. More than 8 in 10 respondents (84%) claimed they would be interested in receiving assistance from a third party around AI–powered cyber solutions.

As the sector evolves, we must ensure everyone is brought along on the journey. Cybersecurity threats are not the only issue facing organisations at present. Dissatisfaction with external vendors is also escalating.

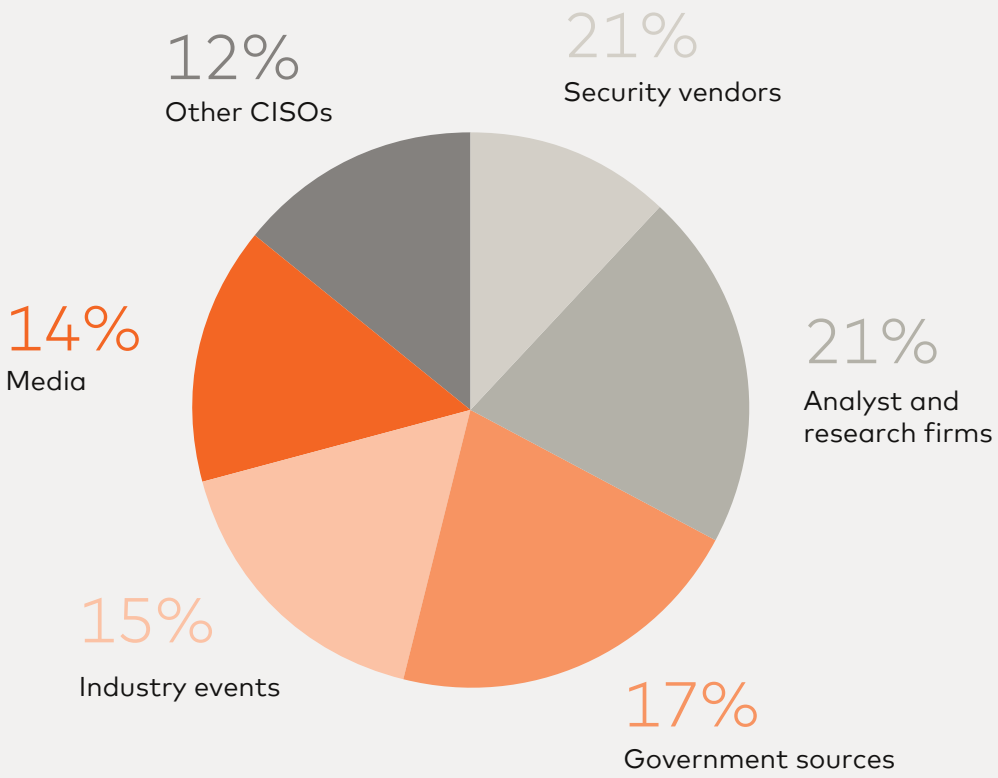
Almost half of security leaders believe they are likely to change vendors in the next three years.

Despite the fact that many vendors face challenges, cyber leaders listed their security vendors as their most helpful sources of cyber threat intelligence, alongside analyst firms and ahead of government sources.

7. Source IBM Security- Cost of a Data Breach Report 2022

Mastercard has worked to build a single cyber service that enables its customers to measure their vulnerability to cybercrime, assess supply chain risk and ensure they can mitigate attacks when they happen

Figure 2: Most helpful sources of cyber threat intelligence to cyber leaders



Source: Horn, John. cybersecurity 2023, InfoSec leaders pursue the future of financial services, Aite-novarica. May 2023

As the threat evolves and grows, so does the opportunity. For vendors, in particular, the need for more cyber consultation presents a significant opening to provide the expertise as well as the tools to augment their offering to businesses.

$4.35m

USD average cost of a data breach in 2022
up 12% from 2020

3x

Globally, ransomware cases have tripled in the last three years.

98%

of consumers reported being concerned about the current level of cybercrime.

Source: IBM 'Cost of data breach' report 2022.

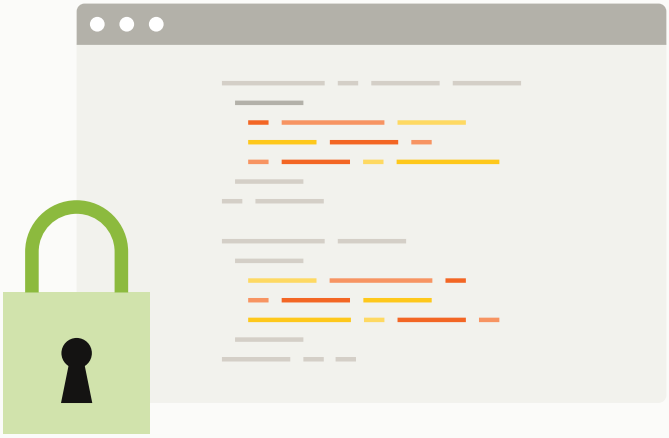
Protecting against tomorrow's attacks is a top priority

89%

of cyber leaders stated innovation is needed to improve solutions available to market.[8]

70%+

of cybersecurity professionals recognise the need to outsource cybersecurity solutions to combat the threat.[9]



Top cybersecurity areas identified by cyber leaders in 2023 are:

AI

AI

Digital identity

API security

8. Source: Horn, John. cybersecurity 2023, InfoSec leaders pursue the future of financial services, Aite-novarica. May 2023
9. Source: Horn, John. cybersecurity 2023, InfoSec leaders pursue the future of financial services, Aite-novarica. May 2023

Cyber leaders biggest perceived cybersecurity threats in 2023/24 are:

- BOTs and non-human actors
- Cloud computing
- Internet of Things (IoT)
- Third party risk
- Virtual digital workforce
- ... and staff using personal devices

Cybersecurity professionals are transforming from technical experts to the gate keepers of cybersecurity...

... they're adapting their business areas and increasing their budgets to keep up with increasing cyber risk.

88%

of cybersecurity budgets have increased year on-year in 2023/24

43%

saw an increase of between 5-10% year on year from 2022/23 to 2023/24.

Top priority budget spend for cyber leaders in 2023/24 is:

- Infrastructure and cloud security
- Malware and ransomware security

Source: Horn, John. cybersecurity 2023, InfoSec leaders pursue the future of financial services, Aite-novarica. May 2023

Concluding remarks

Today's digital transformation is akin to the industrial revolution. The latest technologies are opening doors to realities that, just a decade ago, would have been science fiction and will define how we live and work for the next 100 years and beyond.

The message from cyber leaders is clear: the buzz around evolving technologies cannot cloud the need to put security first. The insights in this report shine a light on the caution that accompanies opportunity inside businesses, merchants and financial institutions around the world.

For now, amid accelerated transformation, cyber leaders require a helping hand. Throughout this report, respondents are honest and transparent about the fact that they cannot navigate this next chapter alone. There is a clear call to action for security vendors to rise to the ever-evolving challenge cybercrimals pose by increasing innovation and providing tailored cyber solutions which meet the current and future needs of businesses and organizations

As the cybersecurity sector moves forwards, it continues to develop in strength, scale and diversity. Cyber leaders are recognizing the need to equip themselves and their organizations with the knowledge and solutions required to fight against cybercrime. Consumers are aware of the risk, and with their awareness they are looking for businesses and organizations they use to take the necessary measures to keep their data and finances secure. This presents an opportunity for security vendors to keep stepping up with new, innovative solutions growing business understanding of cyber risk, and ensuring, collectively, we are well-placed to secure our digital future.

About the research

This paper is a summary of the research commissioned by Mastercard with Aite-Novarica, with supporting analysis provided by Cebr.

The research[10] consisted of 221 interviews with cybersecurity professionals of financial services firms and merchants (banks focused on commercial loans and investments). It was conducted across 8 countries (Australia, Brazil, Germany, India, UAE, Saudi Arabia, the UK and the US) between December 2022 and January 2023.

10. Horn, John. cybersecurity 2023, InfoSec leaders pursue the future of financial services, Aite-novarica. May 2023

Designed by Mastercard Creative Studio