tenable

MEASURE TWICE, CUT ONCE:

META-CURIOUS ORGANIZATIONS RELAY CYBERSECURITY CONCERNS EVEN AS THEY PLUNGE INTO VIRTUAL WORLDS

OVERVIEW

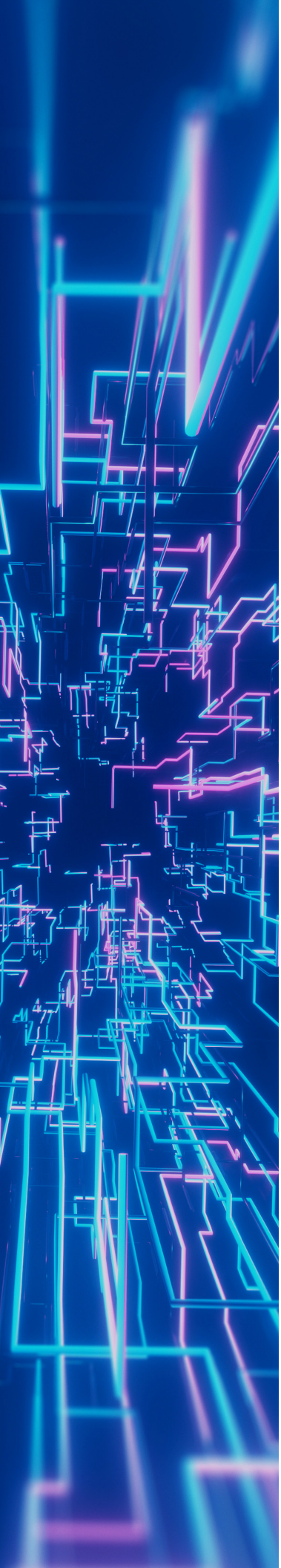
The metaverse has emerged as one of the most exciting new frontiers since the advent of the internet. This massive set of virtual worlds creates endless possibilities and potential for new activities and experiences that have not been available in the cyber world before. Tech giants such as Microsoft, Facebook and Roblox are already investing billions of dollars to become the pioneers of this market, which McKinsey & Company predicts will grow to $5 trillion by 2030. As with all new-frontier ventures, there are very real concerns about the threats and pitfalls that may be awaiting organizations in such a new space.

To fully understand how prepared organizations are to either create their own metaverse initiatives or participate in others', Tenable has conducted an in-depth study across Australia, the United Kingdom and the United States. The study, conducted by Opinion Matters on behalf of Tenable, surveyed 1,500 professionals representing roles in cybersecurity, DevOps and IT engineering. It investigated future business opportunities, potential barriers to adoption and types of cyberthreats emerging in this new realm.

The study offers insights into what organizations perceive as the greatest risks and rewards of investing in the metaverse and the level of development required to take such a major step safely.

KEY TAKEAWAYS

1. Organizations view the metaverse as an opportunity for interaction and collaboration.
2. Security and macroeconomic conditions are top considerations for investing in the metaverse.
3. New cyberthreats will develop in the metaverse and old threats will carry over into the metaverse.
4. Addressing cybersecurity and privacy concerns will give organizations a better chance at succeeding in the metaverse.
5. Re-evaluating the current cybersecurity posture of the underlying infrastructure is a must for organizations that want to scale their business to the metaverse.



A NEW VIRTUAL FRONTIER

While many believe the metaverse to be nothing more than an extension of the Meta (formerly Facebook) platform, in reality there is the potential for unlimited metaverse instances to be built by various platform developers and vendors.

The metaverse, as its name suggests, is said to be the next evolution of the internet in 3D. Emerging technologies — such as virtual reality (VR), augmented reality (AR), artificial intelligence and blockchain will shape each self-sustaining virtual space.

For individuals, this means acquiring a piece of digital real estate, such as artwork, purchasing in-game merchandise or attending social events.

For businesses, the metaverse presents numerous opportunities to build self-owned virtual entities with their own access, monetization rights and technical specifications. These can either support the organization's internal or external operations or ride on existing metaverse platforms built by other companies, such as Roblox or Fortnite Creative.

Building and operating in the metaverse requires sophisticated software development, design and 3D modeling, which typically fall outside the scope of traditional IT.

This exciting new frontier has prompted many organizations to think about how they can uniquely carve out a niche for themselves. These projects could be in the form of cross-office collaboration spaces, employee training modules or external-facing virtual experiences to enhance customer engagement which has a direct impact on an organization's bottom line.

Major brands have begun conceiving how their metaverse investments might take shape. For example, after being approved for a virtual-world simulator patent, Disney has begun developing a theme park which will entertain users in its metaverse through headsetless augmented reality. Visitors to the theme park will be able to project 3D images and virtual effects onto physical spaces. Meanwhile, JP Morgan is the first major bank to launch a lounge in the metaverse using Decentraland, a popular blockchain-based world. Gucci Vault has opened a metaverse world in The Sandbox.

ORGANIZATIONS CHARGING HEADLONG INTO METAVERSE INVESTMENTS

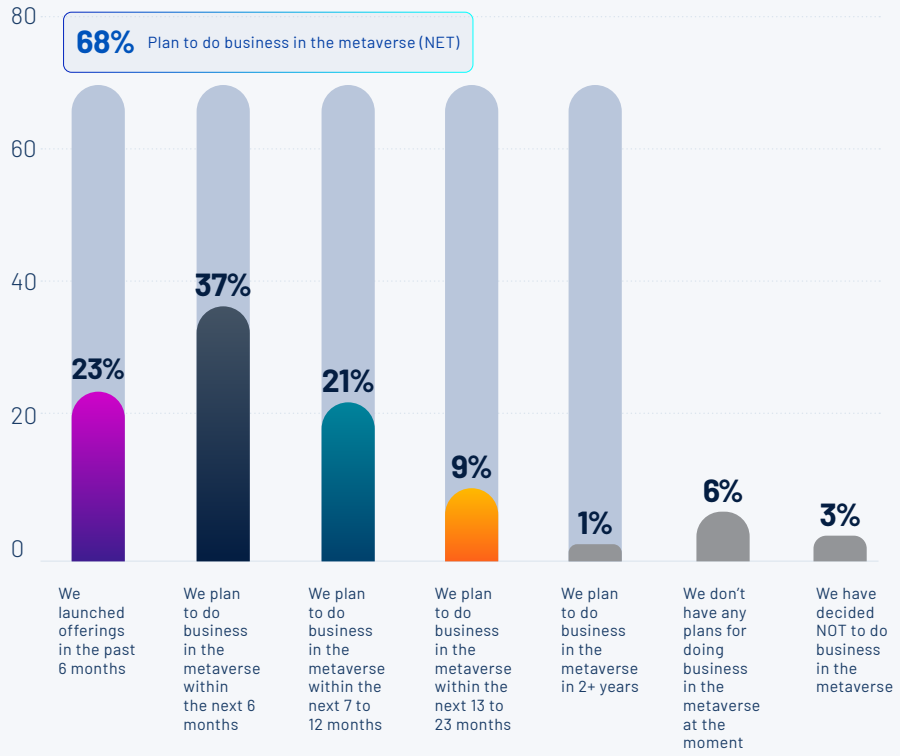
The relative infancy and many unknowns of the metaverse have not dissuaded organizations from participating, as they recognize the vast potential it represents for their business expansion prospects.

This is strongly evident in the responses to Tenable's study, in which almost seven in 10 (68%) respondents stated that their organizations have plans to do business in the metaverse over the course of the next six to 36 months. A further 23% of all respondents have already begun developing initiatives in the metaverse in the past six months. (See Fig. 1.)

> "Almost **seven in 10 (68%) respondents** stated that their organizations have **plans** to do **business** in the **metaverse** over the course of the next **six** to **36** months. A further **23%** of all respondents have already begun **developing initiatives** in the **metaverse** in the past **six** months."

Q3. How is your organisation planning to do business in the metaverse?

FIG. 1
SOURCE: A STUDY CONDUCTED BY OPINION MATTERS ON BEHALF OF TENABLE, OCT. 25 – NOV. 8, 2022



With these notable statistics in mind, it's apparent that many organizations are not willing to miss out on the multitude of opportunities presented by the metaverse. Organizations that dismiss or lack interest in the metaverse could find themselves losing out to their forward-thinking competitors who commit to investing in it.

INTERACTION AND COLLABORATION AS KEY BUSINESS OPPORTUNITIES

Interaction in a professional and business sense is a key focus of businesses wanting to participate in the metaverse, which offers a new space to learn, conduct business and collaborate. The cybersecurity professionals, IT engineers and DevOps managers surveyed expressed interest in the business opportunities that the metaverse offers in areas such as customer engagement (44%), improved learning and training (41%) and better workplace collaboration (41%). This comes as no surprise as tech giants such as Microsoft, Nvidia and Meta, and startups like Varjo, Virbela and Spatial, all reportedly view the metaverse as the next stage of workplace collaboration. (See Fig. 2.)

44%
Enhanced customer engagement

41%
Improved learning and training

41%
Remote working and better collaboration

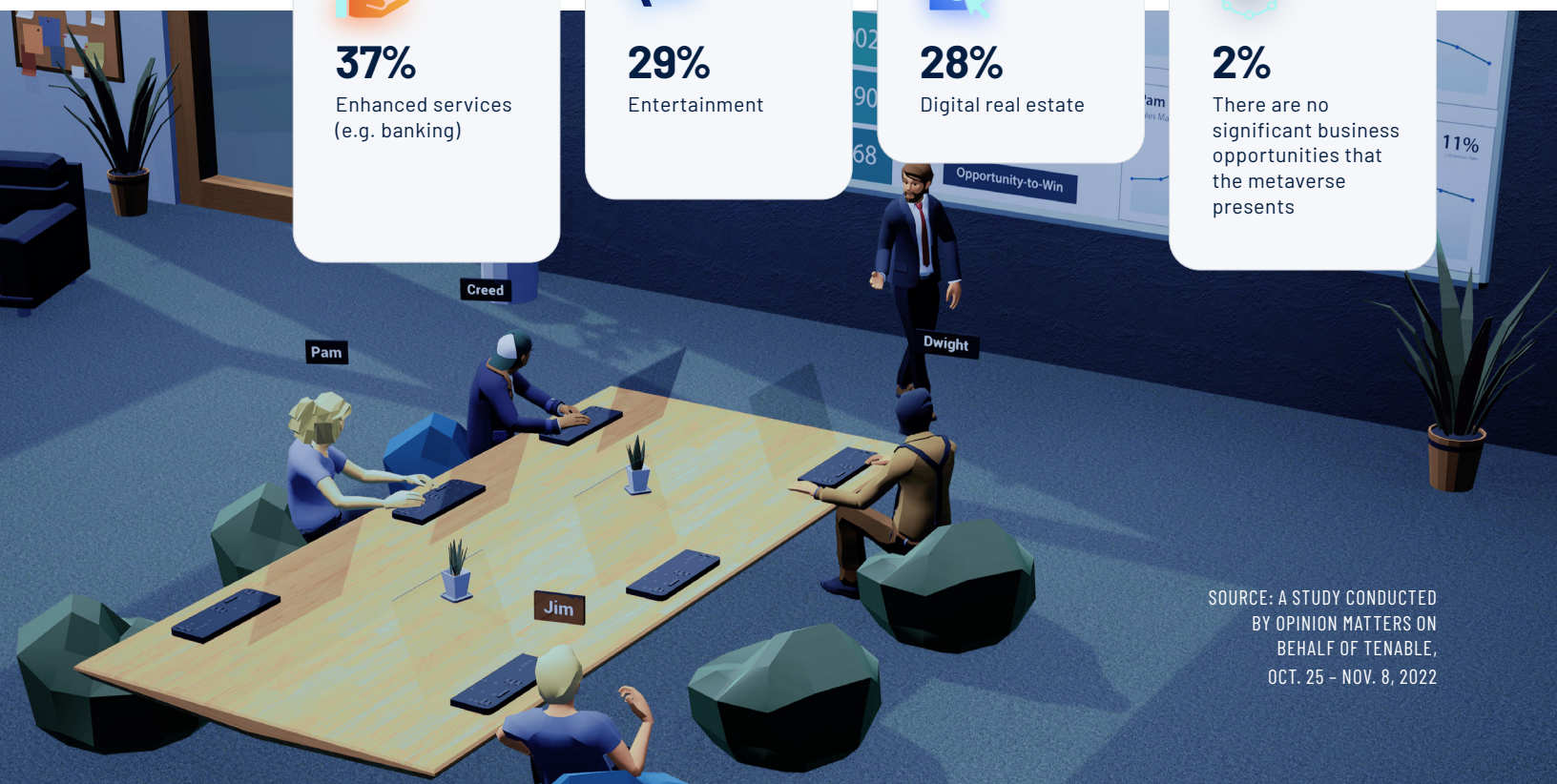
37%
New revenue streams

37%
Enhanced services (e.g. banking)

29%
Entertainment

28%
Digital real estate

2%
There are no significant business opportunities that the metaverse presents



SOURCE: A STUDY CONDUCTED BY OPINION MATTERS ON BEHALF OF TENABLE, OCT. 25 – NOV. 8, 2022

Q4. What are the top considerations affecting your organisation`s decision to invest (or not) in the metaverse over the next 12 months?

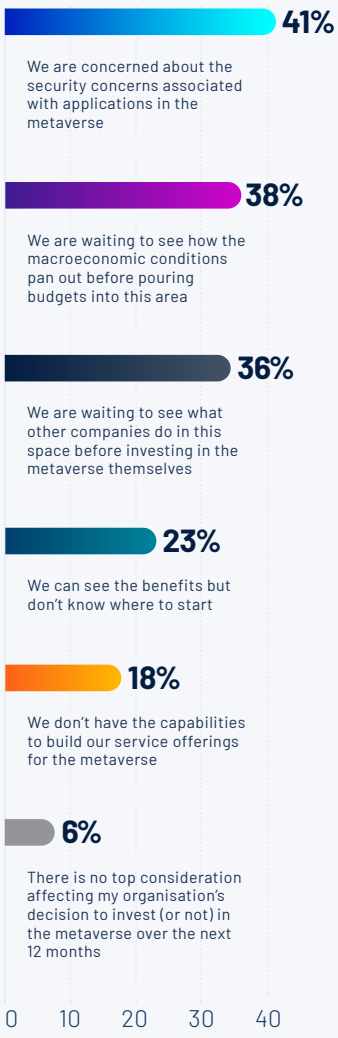


FIG. 3

SOURCE: A STUDY CONDUCTED BY OPINION MATTERS ON BEHALF OF TENABLE, OCT. 25 - NOV. 8, 2022

THE PAUSE FACTOR: CYBERSECURITY AND MACROECONOMIC CONSIDERATIONS

Despite such significant results, not all organizations are jumping headfirst into this new world, just yet. In fact, respondents indicated safety and security to be the top factors affecting the commitment to operate in a virtual environment, even ahead of macroeconomic concerns.

> "The metaverse, calculated by Bloomberg to be an **$800 billion market** as early as 2024, has organizations seriously concerned about the security associated with virtually hosted applications. Four in 10 respondents (41%) indicated that **security is the top consideration** affecting their organization's metaverse investment decisions."

Most security solutions today were not built for applications like the ones found in the metaverse. Security needs to be ubiquitous throughout the development process in order to sufficiently protect each transaction across the platform, weaving security into the core application layer.

Another major factor that is causing trepidation in many organizations' future plans for the metaverse is an economic one. As central banks raise interest rates to curb inflation in an effort to stave off an economic recession, 38% of respondents stated that their organizations would wait to see how the macroeconomic conditions unfold before committing resources to an unknown venture. There are also businesses that are more inclined to follow in the footsteps of others and want to gauge how other businesses fare in the metaverse first (36%). (See Fig. 3.)

A cautious approach is completely reasonable in the face of shifting cyberthreats as organizations continue to expand their on-premises and cloud infrastructure and incorporate new endpoint devices, further expanding the attack surface. When embracing the metaverse, new threats are bound to emerge, not all of which can be mitigated with current solutions.

RISE OF NEW THREATS AND THE PERSISTENCE OF OLD ONES

Managing the digital attack surface is already challenging enough for organizations. Adding a new virtual dimension to the simultaneous use of different technologies, accompanied by the collection of data, is likely to serve as a whole new breeding ground for cyberattacks. This level of complexity breeds a new set of risks.

The majority of respondents surveyed (86%), stated that they would be comfortable sharing personal identifiable information (PII) of users between different services in the metaverse. While this trust is encouraging, it could be misplaced, making users vulnerable to cyberattacks if the security framework to protect them is not in place prior to launch. In readily sharing such information without safeguards, organizations could be putting both themselves and consumers at risk.

> "The majority of respondents surveyed (**86%**), stated that they would be comfortable **sharing personal identifiable information** (PII) of users between different services in the metaverse."

Survey respondents highlighted both **new and old threats** that are likely to take place in the metaverse.

1

Cloning of voice and facial features and hijacking video recordings using avatars

Having avatars with synthetic voices and facial features that mimic those of users or employees can make the metaverse experience more personal. These avatars also generate various data, such as voice, video and messages, as they navigate their metaverse for business meetings and access personal information for services. Cybersecurity professionals and DevOps managers are concerned that there is no way of identifying who is really behind the avatars. Personal information and content stored in a virtual environment, metaverse platform or service system can be forged and leaked.

It is for this reason that 79% of respondents say it is very likely or somewhat likely that the cloning of voice and facial features and the hijacking of video recordings using avatars will occur in the metaverse. This creates serious concerns about the true identity behind the digital mask.

> **79%**
> of respondents say it is very likely or somewhat likely that the **cloning of voice** and **facial features** and the **hijacking of video recordings** using avatars will occur in the metaverse.

2

Invisible-avatar eavesdropping or 'man in the room' attacks

Research undertaken by Vondrek et al. demonstrated the possibility of executing the first man-in-the-room attack by exploiting the security vulnerabilities of a widely used VR social application called Bigscreen. The vulnerabilities allowed attackers to invisibly eavesdrop in VR rooms. Attackers could also exploit the flaws to gain complete control over Bigscreen users' computers, to secretly deliver malware, and even to start a worm infection spreading through VR.

With the use of VR headsets being a key technology in the metaverse, these "peeping Tom" scenarios could proliferate, with (78%) of respondents saying such attacks are very likely or somewhat likely. What's more interesting is that 84% of the 118 respondents in the financial services and/or insurance industries say these attacks have a high possibility of taking place.

Imagine a financial consultant offering advice to a consumer in what they think is a private room in the metaverse, not knowing that a third party is also present in the room eavesdropping with impunity. These scenarios are things that organizations need to safeguard against.

3

Conventional phishing, malware and ransomware attacks

The same cyberthreats that organizations currently contend with will also carry into various metaverses. The vast majority of respondents (81%) say it is likely or somewhat likely that conventional phishing, malware and ransomware attacks might occur in the metaverse. Cybercriminals who have had much success exploiting existing unpatched software vulnerabilities and cloud misconfigurations can just as easily look for the same in the metaverse. Nascent metaverse providers may not have mature security programs nor be able to provide reasonable assurances regarding their security. This is when third- and fourth-party security (an organization's vendors' vendors) becomes paramount.

> "**81%** say it is likely or somewhat likely that conventional **phishing**, **malware** and **ransomware attacks** might occur in the metaverse. Cybercriminals who have had much success exploiting existing **unpatched software vulnerabilities** and **cloud misconfigurations** can just as easily look for the same in the metaverse."

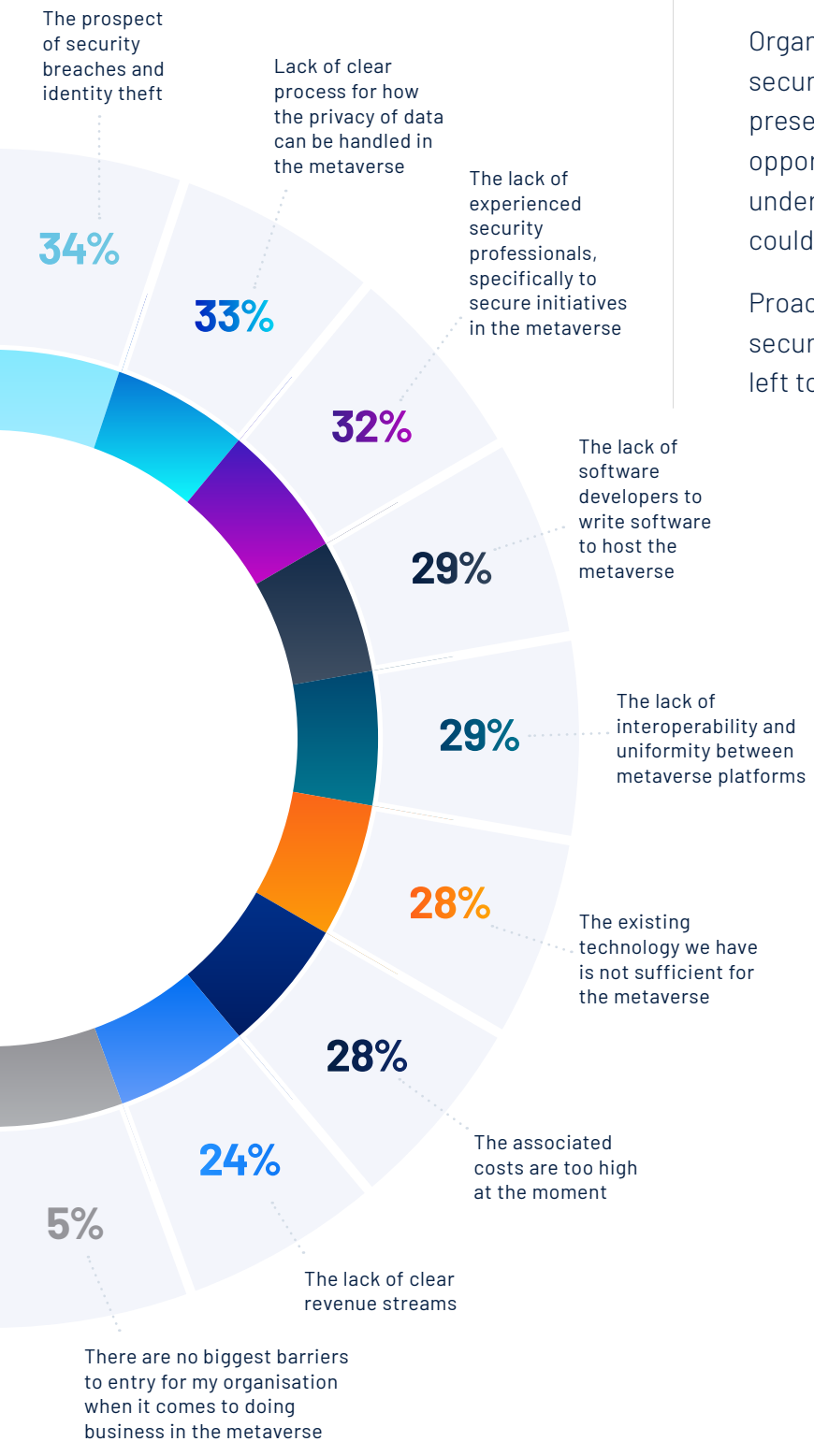
4

Compromised machine identities and application programming interface (API) transactions

Billions of machine-to-machine communications across internet of things (IoT) and industrial-control devices, sensors communicating with control systems, edge-computing devices, cloud-computing systems and traditional IT systems take place with zero human interaction daily. Almost four in five respondents (78%) think it is very likely or somewhat likely that compromised machine identities and API transactions might occur across metaverses.

Top three barriers to entry into the metaverse

FIG. 4



Taking these likely threats into consideration, it comes as no surprise that the prospects of security breaches and identity theft, the lack of clear processes for data privacy and the lack of experienced security professionals to secure the metaverse, were listed as the top three barriers to entry by professionals surveyed. (See Fig. 4.)

Organizations that focus on fostering a safe and secure platform are more likely to see traction in their presence in the metaverse. Those who simply chase opportunities without addressing these two essential underlying areas could experience a false start, which could impact their business in the long run.

Proactive strategies to strengthen the safety and security of operations in the metaverse should not be left to organizations alone to be determined.

> "IN FACT, **87%** of respondents say they think the **metaverse should be regulated.**"

SOURCE: A STUDY CONDUCTED BY OPINION MATTERS ON BEHALF OF TENABLE, OCT. 25 – NOV. 8, 2022

ESTABLISHING FOUNDATIONAL CYBERSECURITY PRACTICES IN EXISTING INFRASTRUCTURE IS CRITICAL

Although many of the emerging technologies being used to access the metaverse (such as AR, VR and AI) are familiar to security professionals today, the ability to secure them while operating in a shared virtual environment is not assured. Only 48% of respondents are very confident that their organizations' existing cybersecurity measures are sufficient to curb cyberthreats in the metaverse.

> "**Nine** in **10** respondents agree that organizations need to adequately develop a **cybersecurity framework** prior to offering services in such a **virtual environment**."

Organizations need to re-evaluate the current cybersecurity posture of their infrastructure if they want to scale their business to the metaverse and not let the allure of the growth opportunity sway them from applying sound cybersecurity fundamentals.

With certain metaverses being built on blockchain technologies, such as Ethereum, which utilize smart contracts, it's imperative that organizations planning on entering into such metaverses require the production of smart contract audit reports. These reports are developed to provide confidence that no vulnerabilities or misconfigurations have been introduced into the smart contracts that underpin these metaverses.

SPECIALIZED TALENT IN DEMAND

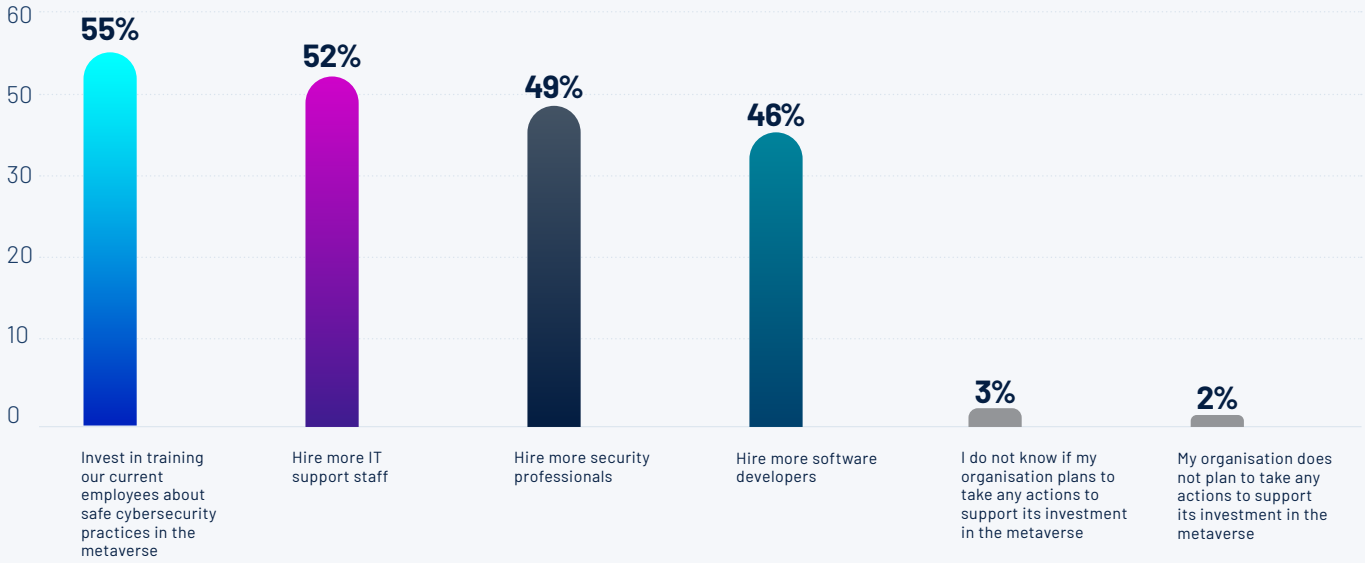
While it's clear that security experts are concerned about the new frontier of the metaverse and how these virtual worlds will be navigated, this hasn't discouraged their desire to embrace the opportunities. The respondents' answers suggest that a proactive strategy to train, educate and encourage talent will be a necessity to allow organizations to operate safely inside the metaverse.

More than half (55%) of respondents said their organization will need to invest in training their current employees about safe cybersecurity practices to support their investment in the metaverse. Organizations that are currently investing or have plans to invest in their own metaverse say hiring talent will be crucial in specialized areas, such as IT (52%), cybersecurity for the metaverse (49%) and software development (46%). (See Fig. 5.)

The metaverse presents an exciting opportunity for those looking to learn new skills. When asked about the skills required for the metaverse, respondents cited user interface/user experience (UI/UX) designing, 3D modeling, blockchain and gaming development, cybersecurity and software development as important development areas. Honing technical know-how in these areas will be a differentiating factor for talent as organizations start putting in the building blocks to realize fully-functioning metaverses.

Q19. Which actions, if any, will your organisation need to take to support your investment in the metaverse:

FIG. 5
SOURCE: A STUDY CONDUCTED BY OPINION MATTERS ON BEHALF OF TENABLE, OCT. 25 – NOV. 8, 2022



RECOMMENDATIONS

Respondents to the Tenable study indicated that organizations planning to launch projects in the metaverse should strengthen the cybersecurity posture of their underlying infrastructure today in the following ways:

1 Shift left in the metaverse

With the default vision for metaverse experiences involving the use of AR and VR headsets, there's no question there will be a massive volume of software needed to design and host metaverses — both the expanding infrastructure and the applications on it.

This shines a spotlight on how metaverses will be built and secured at the deeper level of their underlying programming.

Nine in 10 respondents agree that building cybersecurity into software code will be important in securing metaverses.

> "The term **"shift left"** will become more prominent as developers think about security the moment they write the first line of code. The vast majority (**93%**) of respondents believe that **identifying vulnerabilities** before **code** reaches runtime will be important."

2 Identify all cloud misconfigurations and vulnerabilities

It's important for organizations to not just focus on the new threats that may unfold in the metaverse but also reduce the risk of old threats that exist on current assets before they transcend the metaverse. Conducting a comprehensive asset inventory provides an organization with full visibility into all assets, whether on premises or in the cloud, regardless of the data source (vulnerability management, web app security, cloud security, IoT and identity security, etc.). This centralized view streamlines analysis, simplifies reporting and helps organizations take action faster.

3 Gain visibility into all internet-facing assets

As more assets, services and applications reside on the internet, security teams need to be aware of their full virtual footprint. Continuously mapping the entire internet and discovering connections to internet-facing assets can help assess the security posture of an organization's entire external attack surface, including any presence in the metaverse.

About Tenable

Tenable® is the Exposure Management company. Approximately 40,000 organizations around the globe rely on Tenable to understand and reduce cyber risk. As the creator of Nessus®, Tenable extended its expertise in vulnerabilities to deliver the world's first platform to see and secure any digital asset on any computing platform. Tenable customers include approximately 60 percent of the Fortune 500, approximately 40 percent of the Global 2000, and large government agencies. Learn more at www.tenable.com.

CONCLUSION

While there are many differing opinions about when metaverses will achieve widespread adoption, the Tenable study shows that organizations have either already started investing in their own metaverses or plan to do so within the next three years. Opportunities are not without consequences if security and privacy are not taken seriously when building offerings and services. Organizations will have to upskill or hire new talent to help navigate an expanded attack surface rife with both old and new cyberthreats. Progressive organizations that start by re-evaluating their existing infrastructure today will be better equipped to navigate and build out their metaverse worlds.

Methodology

Opinion Matters conducted an online survey on behalf of Tenable from Oct. 25 - Nov. 8, 2022, with 1,500 professionals representing roles in cybersecurity, DevOps and IT engineering. Respondents came from organizations with 26 or more employees in Australia, the United Kingdom and the United States. The margin of error is +/- 4.38% with 95% confidence.

APPENDIX: ADDITIONAL DATA

COUNTRY	
Australia	500
United Kingdom	500
United States of America	500

JOB TITLE	
Director in IT or cybersecurity	27%
Manager in IT or cybersecurity	25%
Senior-most IT or cybersecurity decision-maker in the firm	20%
VP in IT or cybersecurity	10%
DevOps manager	7%
Head of DevOps	3%
IT Engineer	3%
Security analyst	5%

INDUSTRY SECTORS	
Financial services and/or insurance	8%
Financial services and/or insurance	4%
Retail	9%
Gaming	2%
Technology and/or technology services	49%
Telecommunications services	4%
Energy, utilities, and/or waste management	1%
Healthcare	3%
Consumer product goods and/or manufacturing	1%
Construction	3%
Food and/or beverage	1%
Transportation and logistics	2%
Business or professional services	3%
Media and/or leisure	1%
Electronics	2%
Consumer services	1%
Biotechnology and/or pharmaceuticals	1%
Education and/or nonprofits	1%
Chemicals and/or metals	0%
Government (federal, local and state)	2%
Legal services	0%
Advertising and/or marketing	0%
Agriculture	0%
Travel and hospitality	1%
Other	1%

APPENDIX: ADDITIONAL DATA

COUNTRY SPECIFIC DATA

"When is your organization planning to do business in the metaverse?"

	AUSTRALIA (N = 500)	UNITED KINGDOM (N = 500)	UNITED STATES (N = 500)
We launched offerings in the past six months	17%	18%	34%
We plan to do business in the metaverse within the next six months	38%	32%	40%
We plan to do business in the metaverse within the next seven to 12 months	26%	23%	16%
We plan to do business in the metaverse within the next 13 to 23 months	10%	12%	5%
We plan to do business in the metaverse in 2+ years	1%	1%	1%
We don't have any plans for doing business in the metaverse at the moment	4%	11%	3%
We have decided NOT to do business in the metaverse	3%	4%	2%

Note: Percentages may not total 100% due to rounding.
Base: Professionals representing roles in cybersecurity, DevOps and IT engineering.
Source: Opinion Matters conducted an online survey on behalf of Tenable from Oct. 25 - Nov. 8, 2022

"What are the top considerations affecting your organization`s decision to invest (or not) in the metaverse over the next 12 months?"

	AUSTRALIA (N = 500)	UNITED KINGDOM (N = 500)	UNITED STATES (N = 500)
We are concerned about the security concerns associated with applications in the metaverse.	43%	34%	45%
We are waiting to see how the macroeconomic conditions pan out before pouring budgets into this area	35%	36%	42%
We are waiting to see what other companies do in this space before investing in the metaverse themselves	36%	36%	35%
We can see the benefits but don't know where to start	29%	21%	21%
We don't have the capabilities to build our service offerings for the metaverse.	26%	15%	13%
There is no top consideration affecting my organization's decision to invest (or not) in the metaverse over the next 12	4%	7%	8%
Others: Please specify	0%	0%	0%

Note: Percentages may not total 100% due to rounding.
Base: Professionals representing roles in cybersecurity, DevOps and IT engineering.
Source: Opinion Matters conducted an online survey on behalf of Tenable from Oct. 25 - Nov. 8, 2022

APPENDIX: ADDITIONAL DATA

"What are the most significant business opportunities the metaverse presents, if any?"

	AUSTRALIA (N = 500)	UNITED KINGDOM (N = 500)	UNITED STATES (N = 500)
Enhanced customer engagement	42%	43%	48%
Improved learning and training	37%	38%	49%
Remote working and better collaboration	37%	40%	46%
New revenue streams	35%	38%	38%
Enhanced services (e.g. banking)	36%	29%	35%
Entertainment	31%	28%	28%
Digital real estate	31%	25%	27%
There are no significant business opportunities that the metaverse presents	1%	3%	1%

Note: Percentages may not total 100% due to rounding.
Base: Professionals representing roles in cybersecurity, DevOps and IT engineering.
Source: Opinion Matters conducted an online survey on behalf of Tenable from Oct. 25 - Nov. 8, 2022

"What are the biggest barriers to entry, if any, for your organization when it comes to doing business in the metaverse?"

	AUSTRALIA (N = 500)	UNITED KINGDOM (N = 500)	UNITED STATES (N = 500)
The prospect of security breaches and identity theft	35%	33%	35%
Lack of clear process for how the privacy of data can be handled in the metaverse	35%	33%	35%
The lack of experienced security professionals, specifically to secure initiatives in the metaverse	31%	33%	33%
The lack of software developers to write software to host the metaverse	31%	26%	30%
The lack of interoperability and uniformity between metaverse platforms	33%	26%	28%
The existing technology we have is not sufficient for the metaverse	31%	29%	25%
The associated costs are too high at the moment	30%	27%	26%
The lack of clear revenue streams	22%	24%	25%
There are no biggest barriers to entry for my organisation when it comes to doing business in the metaverse	2%	5%	7%

Note: Percentages may not total 100% due to rounding.
Base: Professionals representing roles in cybersecurity, DevOps and IT engineering.
Source: Opinion Matters conducted an online survey on behalf of Tenable from Oct. 25 - Nov. 8, 2022

APPENDIX: ADDITIONAL DATA

"How comfortable will your organization be in collecting and sharing personal identifable information (PII) with third-party services in the metaverse, if at all?

	AUSTRALIA (N = 500)	UNITED KINGDOM (N = 500)	UNITED STATES (N = 500)
Very comfortable	42%	33%	58%
Somewhat comfortable	44%	47%	32%
Not particularly comfortable	8%	14%	7%
Not at all comfortable	3%	4%	3%
Don't know	2%	1%	1%

Note: Percentages may not total 100% due to rounding.
Base: Professionals representing roles in cybersecurity, DevOps and IT engineering.
Source: Opinion Matters conducted an online survey on behalf of Tenable from Oct. 25 - Nov. 8, 2022

"How important, if at all, would it be for your organization to weave cybersecurity into your service offerings in the metaverse from the start?"

	AUSTRALIA (N = 500)	UNITED KINGDOM (N = 500)	UNITED STATES (N = 500)
Very important	47%	49%	71%
Somewhat important	43%	41%	26%
Not very important	8%	7%	2%
Not at all important	1%	2%	0%
Don't know	1%	1%	0%

Note: Percentages may not total 100% due to rounding.
Base: Professionals representing roles in cybersecurity, DevOps and IT engineering.
Source: Opinion Matters conducted an online survey on behalf of Tenable from Oct. 25 - Nov. 8, 2022