Adello
BY LAB51

Edition No. 40

TOP 50 BUSINESS & MARKETING *visionaries*

TRUST NO ONE, SECURE EVERYONE

Alexander Pushkin
Chief Information Security Officer @Security Operations Center - PS Cloud Services

KAVYA PEARLMAN

CEO & Founder of XR Safety Initiative (XRSI), Founding Board Member of Metaverse Reality Check (The MRC)

CYBER GUARDIANS FOR THE EMERGING TECH

EDITOR'S NOTE

Dear reader,

In this issue, we delve into the critical realm of cybersecurity for emerging technologies, a topic that is of utmost importance as our world becomes increasingly interconnected and reliant on digital solutions. We are privileged to present exclusive interviews with two exceptional thought leaders in the field: *Kavya Pearlman,* Founder and CEO of XR Safety Initiative (XRSI), and *Alexander Pushkin,* CIS @Security Operations Center (SOC) - PS Cloud Services.

As new technologies like AI, IoT, and the metaverse continue to evolve and reshape our lives, it is essential that we adopt a secure and ethical approach to their development and implementation. The rapid pace of innovation, while exciting, brings with it a host of security challenges that must be addressed to protect the integrity of our digital infrastructure and safeguard the privacy and well-being of individuals.

As we embrace these emerging technologies, it is crucial that we prioritize the security of our existing networks and systems. A proactive approach to cybersecurity, coupled with a strong commitment to ethical standards, can help us build a safer and more resilient digital future for all.

Join us in this fascinating exploration of cybersecurity for emerging technologies, as we learn about the importance of adopting a secure and ethical mindset, the challenges and opportunities in safeguarding our digital world, and the essential steps needed to create a robust and secure foundation for the technologies of tomorrow.

Yours,

Anna Pak

CMO at Adello and LAB51

Trust no one, Secure everyone

Insights from Alexander Pushkin's Microsoft Channel Connect 2023 Presentation

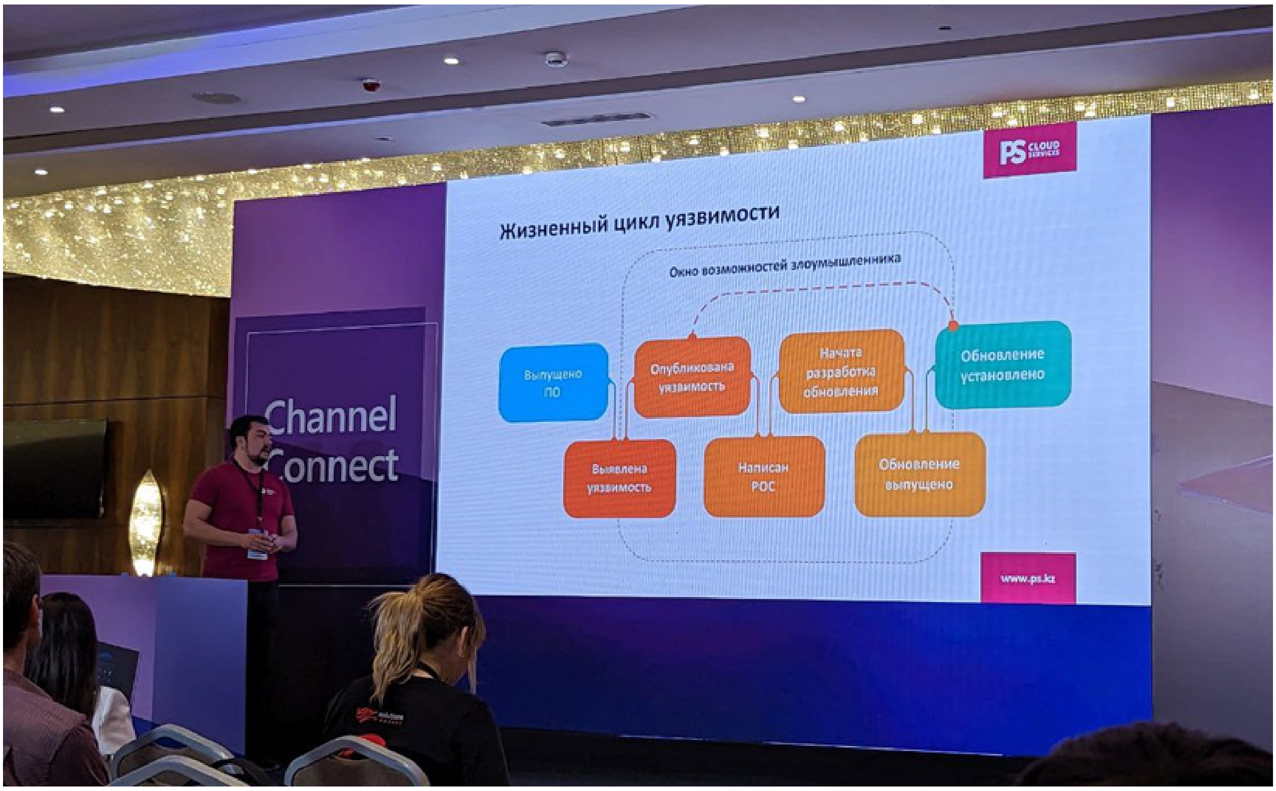
ADELLO'S FOCUS OF THE WEEK

At the recent Microsoft Channel Connect 2023 event, Alexander Pushkin, Chief Information Security Officer at Security Operations Center - PS Cloud Services, delivered a captivating presentation on the importance of cybersecurity for small and medium-sized enterprises (SMEs). Alexander's speech emphasized the need for SMEs to stay vigilant and proactive against constantly evolving cyber threats. This article reviews the key topics covered in Alexander's presentation, offering insights on how businesses can enhance their cybersecurity posture.

Botnets: Distribution and Multiplication

A botnet is a network of interconnected devices, such as computers, smartphones, or IoT devices, that have been infected with malware and are controlled by a cybercriminal, known as a botmaster. Botnets are used to launch a variety of cyberattacks, including distributed denial-of-service (DDoS) attacks, spamming, and data theft.

According to Alexander, botnets are typically distributed and multiplied through various methods, such as phishing emails, malicious websites, and software vulnerabilities. Cybercriminals exploit these methods to trick users into downloading and installing malware, which then adds their device to the botnet. In his presentation, Alexander stressed the importance of raising awareness about these threats and training employees to recognize and avoid common attack vectors.



Жизненный цикл уязвимости

Окно возможностей злоумышленника

Выпущено ПО

Выявлена уязвимость

Опубликована уязвимость

Написан POC

Начата разработка обновления

Обновление выпущено

Обновление установлено

www.ps.kz

The Vulnerability Lifecycle and the Dangers of Unsupported Software

The vulnerability lifecycle is a term used to describe the stages through which a software vulnerability passes, from its discovery to its eventual patching or resolution. The lifecycle generally consists of the following stages: discovery, disclosure, exploitation, and patching. Unsupported software, or software that no longer receives updates and support, presents a significant risk to users, as vulnerabilities in such software often remain unpatched.

Alexander explained that when a software vendor stops providing updates and support, the vulnerability lifecycle is interrupted. This leaves security holes open indefinitely, making the software an easy target for cybercriminals. Businesses that continue to use unsupported software are at an increased risk of falling victim to cyberattacks, as these vulnerabilities can be exploited by threat actors. Thus, it is essential to replace or upgrade outdated software to maintain a secure environment.

One-Day and Zero-Day Vulnerabilities

During his presentation, Alexander touched upon the concepts of one-day and zero-day vulnerabilities.

One-day vulnerabilities refer to known software flaws that have been publicly disclosed but have not yet been patched by the software vendor. Cybercriminals exploit these vulnerabilities while patches are still being developed and deployed.

Zero-day vulnerabilities, on the other hand, are previously unknown software flaws that are discovered and exploited by cybercriminals before the software vendor becomes aware of them. Since zero-day vulnerabilities have not been disclosed or patched, they pose a considerable risk to businesses, as there are no existing defenses against them.

> ”
> **Safety is not 100%, but it should not go to zero**
> “

The Zero Trust Concept and Its Importance

Alexander introduced the concept of Zero Trust, a security model that assumes no user, device, or network can be trusted by default. Instead, each component must be continuously verified to prevent unauthorized access or malicious activity. This approach aligns with Alexander's mantra: "Trust no one, secure everyone."

Under the Zero Trust model, organizations implement robust security measures at every level, from user authentication to network segmentation and data protection. By doing so, they create a layered defense that minimizes the risk of a breach, even if one component of the network is compromised.

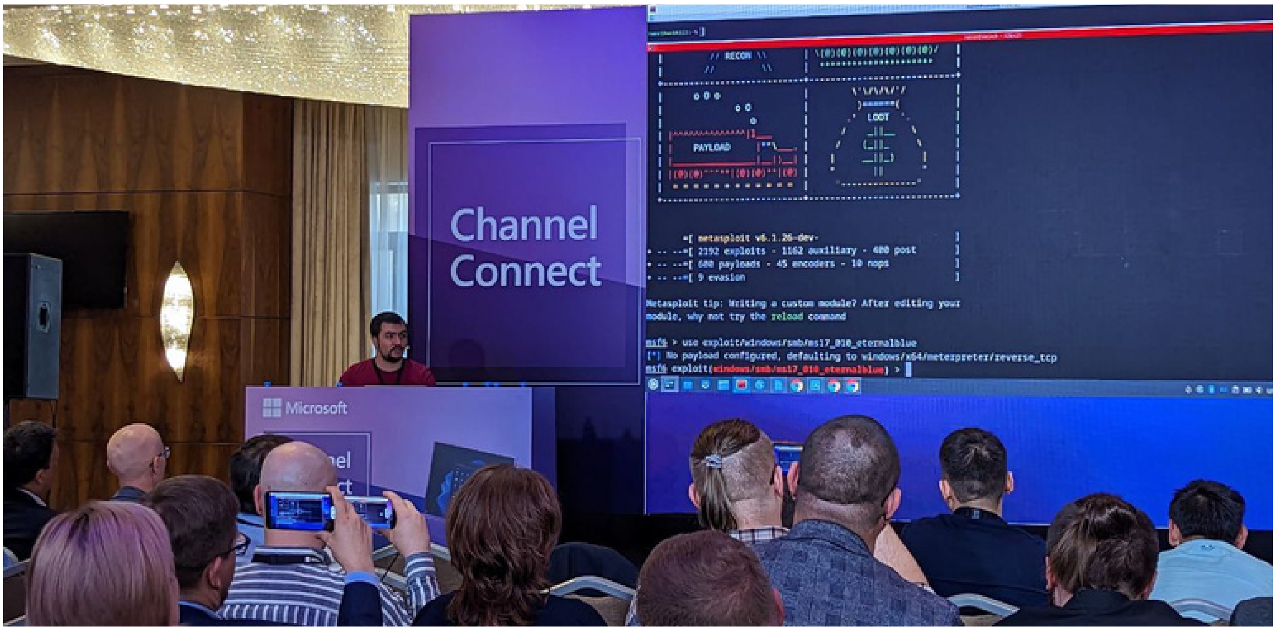
Alexander emphasized the importance of securing every component of the network to protect sensitive data and maintain business continuity. By adopting a "Zero Trust" mindset, SMEs can significantly reduce the likelihood of a successful cyberattack and better safeguard their digital assets.

Software Updates and the Limits of Antivirus Solutions

In his presentation, Alexander highlighted the importance of regularly updating operating systems and software. Updates often include security patches that address known vulnerabilities, helping to protect against potential cyberattacks. Failing to install these updates can leave businesses exposed to significant risks.

Alexander also discussed the limitations of relying solely on antivirus software for cybersecurity. While antivirus programs are an essential layer of protection, they are not sufficient on their own. They primarily focus on detecting and neutralizing known malware, which means that they might not be effective against zero-day threats or advanced persistent threats (APTs).

Instead, Alexander recommended adopting a comprehensive cybersecurity strategy that encompasses a range of measures, such as employee training, intrusion detection systems, network segmentation, data encryption, and incident response planning. By combining these approaches with antivirus solutions, SMEs can create a more robust defense against cyber threats.



```
       =[ metasploit v6.1.26-dev-                         ]
+ -- --=[ 2192 exploits - 1162 auxiliary - 400 post       ]
+ -- --=[ 600 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Writing a custom module? After editing your
module, why not try the reload command

msf6 > use exploit/windows/smb/ms17_010_eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) >
```

Alexander Pushkin's presentation at Microsoft Channel Connect 2023 underscored the urgency of cybersecurity for SMEs. His "three-line code" hacking demo served as a reminder of the critical role that cybersecurity plays in today's digital landscape. By taking a proactive approach to cybersecurity and implementing the concepts and best practices discussed during the presentation, organizations can safeguard their digital assets, protect sensitive data, and maintain business continuity in the face of increasingly sophisticated cyberattacks.

#persona

ALEXANDER PUSHKIN

Chief Information Security Officer
@Security Operations Center - PS Cloud Services

Alexander Pushkin is a seasoned cybersecurity expert with a wealth of experience in practical security. Born and raised in Ukraine, Alexander gained over 15 years of experience in penetration testing and red teaming in the international arena. Thus, he has honed his skills in identifying vulnerabilities and testing the security of networks and systems. In 2021, he shifted his focus to blue teaming, bringing a comprehensive approach to securing cloud services as the Chief Information Security Officer at Security Operations Center (SOC) at PS Cloud Services.

Alexander has built a successful commercial SOC with three lines of analysts from the ground up, ensuring that PS Cloud Services stays ahead of potential security threats. In addition to his extensive professional work, Alexander has also shared his knowledge and expertise with others, having conducted educational courses on web application security that have educated over 130 students. One of his courses was even featured in the magazine "Hacker."

Alexander's reputation as a leading cybersecurity expert extends beyond his professional work and courses. He has been a speaker at over 30 practical security conferences across Eastern Europe and Central Asia. Additionally, he holds an Offensive Security Certified Professional (OSCP) certificate, a testament to his deep understanding of offensive security tactics.

Notably, Alexander has also excelled in multiple international hacking competitions, earning several victories and podium finishes. His achievements reflect his ability to work and lead his team under pressure, identify vulnerabilities, and develop effective security solutions.

Weekly Highlight

CyberGuardian for the Emerging Tech

INTERVIEW WITH KAVYA PEARLMAN

In this interview, we hear from the founder of XR Safety Initiative (XRSI), an organization that develops standards for the emerging technology ecosystem. The XRSI focuses on creating a culture of safety and inclusion in extended reality (XR) technologies by identifying potential cyber attacks, cybersecurity privacy ethical risks, and proposing solutions to mitigate them. Many stakeholders consider XRSI an essential element for predicting and tackling cybersecurity challenges that researchers across the world face when defining fundamental guidelines and detecting new cyber threats in emerging technologies.

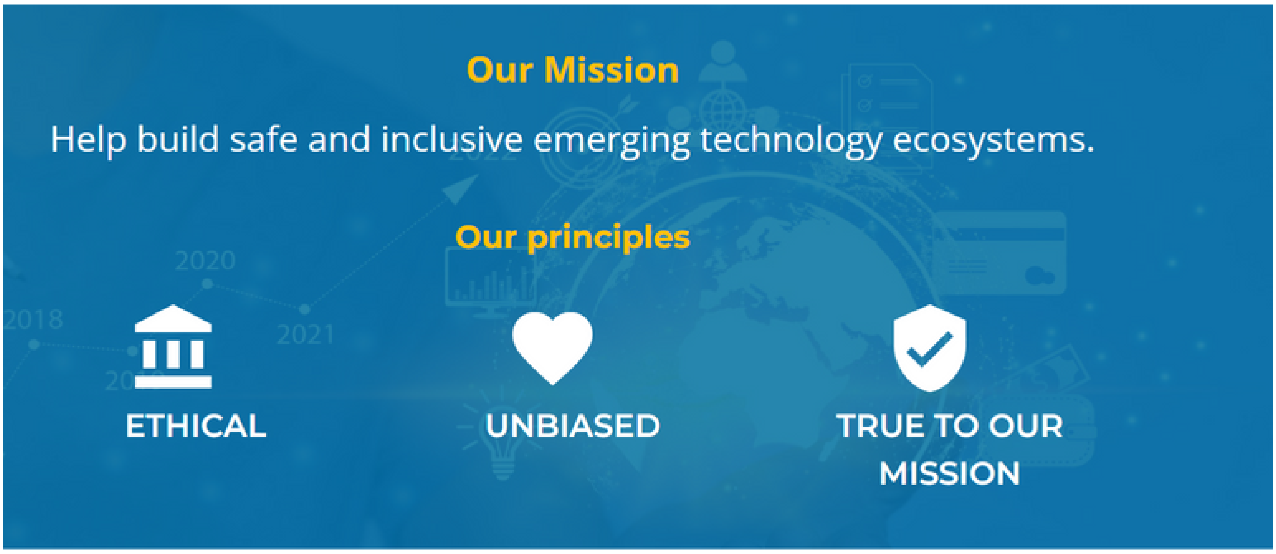
Can you tell us about the XR Safety Initiative's mission and what inspired you to start it?

We are a non-profit organization based in the San Francisco Bay Area that develops standards. After leaving Linden Lab, the creator of the oldest existing virtual world, where I headed the security department, I founded the XR Safety Initiative (XRSI) in 2019.

I had sensor intuition about how the world might change in the future, with virtual being a primary factor. COVID happened in 2020, and it really pushed people online. Our mission evolved into helping to create a culture of safety and inclusion in this emerging technology ecosystem. That is why, after discovering novel cyber attacks or cybersecurity privacy ethical risks, we make informed and pragmatic decisions and then propose potential solutions to mitigate them.

XRSI was one of the first such global initiatives. As a result, we are in a unique position to provide practical, factual, and research-based knowledge to individuals, corporations, universities, government agencies, and organizations around the globe.

As of today, we are advising over 60 different governments. We are proud to launch one of the first novel privacy and security frameworks that addresses very specific data type considerations for the XR and immersive domains.



Our Mission

Help build safe and inclusive emerging technology ecosystems.

Our principles

ETHICAL

UNBIASED

TRUE TO OUR MISSION

XRSI Mission, https://xrsi.org/who-we-are

What, in your opinion, are the most significant risks associated with extended reality technologies, and how can they be mitigated?

To begin, it is critical to investigate the unique aspects of the risks at hand. Historically, when discussing risk, companies have primarily focused on mitigating it. However, in this scenario, because technology and society have a human loop, the consequences of their convergence affect us. Anticipating these risks is critical. These risks are typically hidden because they occur in the digital realm, but they can have a tangible impact on individuals and the physical world. As a result, understanding what happens in the virtual world is critical.

We began segmenting some of the risks in various ways in order to better understand their origin. A combination of the various factors must exist for the risk to appear. It all begins when two or more people interact in virtual space (metaverse, for instance). Another factor is that when you create virtual objects, there may be cybersecurity risks (for example, somebody could add malicious code to a virtual object). Furthermore, when you connect all of the social media risks, such as bullying, harassment, phobia, behavior, and inappropriate content, all of these obstacles come into play. Furthermore, there is a commercial component that contributes to the emergence of theft-related crimes.

Traditionally, the big companies that own the platform make these and other risk-prevention decisions. However, if they are influencing billions of people's lives and even democracies around the world, as we have seen with Facebook and Google, we must involve other stakeholders in making those decisions, and they must abide by regulations that do not currently exist. And this is another area in which XRSI plays a significant role. We occasionally receive early drafts of various laws. We assist in aligning that from a technological standpoint, as well as talking about and providing research to support those laws in the future.

How do you see XR technologists interacting in the coming years, and what new risks and challenges do you anticipate they will present?

Convergence is one of the most difficult issues for many people to comprehend. It is important to take a holistic look at the risk, not perceive it in a vacuum. We examine all risk intersections, such as decentralized ledger technologies, artificial intelligence, and improved network capabilities, such as 5G and 6G network capabilities, among others. And when they converge, the risk is absolutely magnified. That is the primary differentiator. This section examines how technological convergence will affect humans, societies, and even our ecosystems, planet Earth, societal ecosystems, and economics.

There are also dangers associated with diversity and inclusion. We already know that the Internet has left many users behind, causing a major split between different groups of people. The new convergence of these technologies widens the gap. In 2021, we conducted some research and discovered that one of the major risks was identity issues. Who has control of your identity if you lose it in these convergent systems? A particular government or adversarial element could lead to the destruction of an entire community or demographic.

For example, we've seen the consequences in Myanmar. Indeed, technology was unquestionably to blame for the genocide.

Another risk is undoubtedly ethical consideration. Most people accept ethics, but this does not prevent them from engaging in illegal behavior. So we make every effort to route everything through the legal system or potential technical considerations at the engineering and code levels.

Another important drawback of the Internet era is determining what is true and what is not.

There are a plethora of alternative data sources. As a result, determining what is real in the virtual world or metaverse may become increasingly difficult. We are transitioning from a post-truth to a post-reality era of constant reality capture, in which we can no longer tell what is real. There is a convergence of brain-computer interfaces, so data is being transferred directly from our brains. What does this mean for us as humans? There are some philosophical concerns.

Because of the constant data collection, there are concerns about surveillance. What does this mean for humans who are constantly monitored by corporations, governments, and so on?

All of this is very concerning. We can help with search awareness as a starting point. People must pay close attention to how these technologies are shaping and impacting the world.

What steps have been taken to ensure that XR devices are safe for users?

With such initiatives, we can prepare for the future. I was once asked if the metaverse existed. I said I was not sure if it was real or not, but we should prepare for this convergence. All of these technologies will evolve quickly, and they will have a significant impact on our society.

And this is where an increasing number of governments are concerned. We've been speaking with the entire Arab League, which includes 22 Middle Eastern governments.

Last year, I visited NATO headquarters and spoke with some of the European Union's defense secretaries, as well as the former NATO General Secretary. These are the important issues. Virtual reality headsets are being used to shoot down drones over Ukraine.

These technologies are being used to conduct cyber wars on disinformation, misinformation, and similar campaigns.

This year, in a few months, we will announce another effort in which we will provide advice as well as engage in more legislative activities. Similarly, at the World Economic Forum, we were approached by the governor of Australia, who used one of our standards to create their positioning statement, indicating that they intend to protect their elderly and children as well as create awareness activities.

My goal is to bridge the gap between various governments, technological systems, and businesses so that they can communicate with one another and create better laws and technology as a result of those laws.

What are the potential implications of XR technologies for the labor market? How can we ensure that they are used in an ethical and responsible manner?

The key is to set standards and regulations and hope that they are followed ethically.

It is simply not permissible to standardize and limit the potential applications of these technologies. If someone crosses that kind of line, there will be consequences.

What are some of the most important ethical considerations for developers and designers when creating XR experiences?

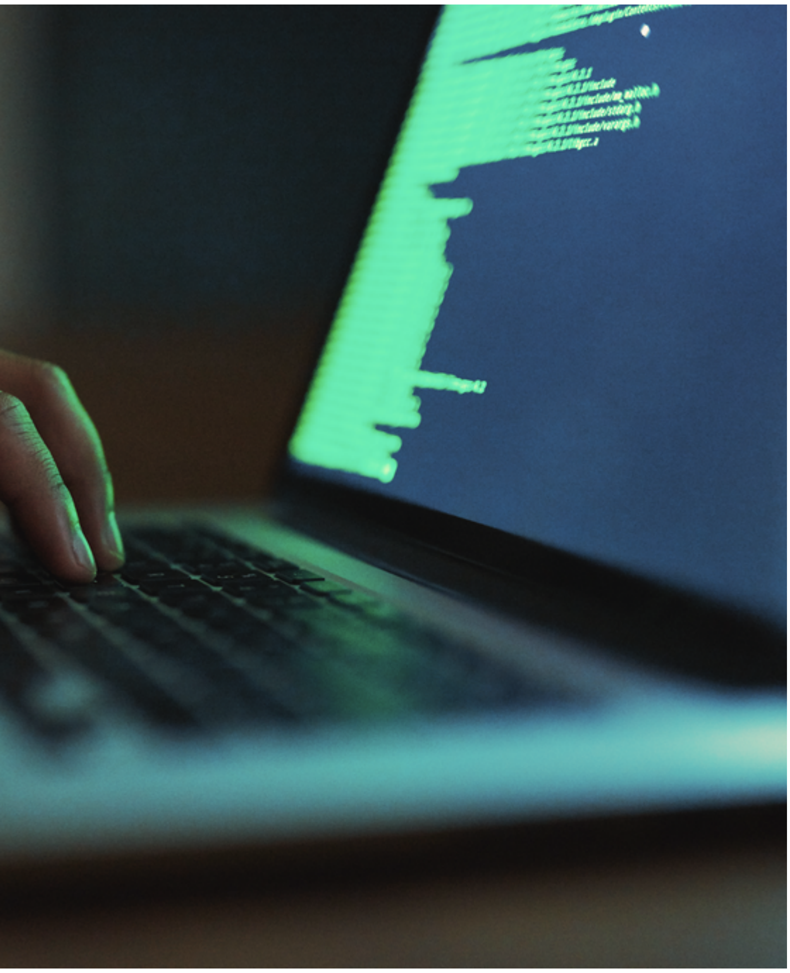
The type of ethical considerations that should be made is determined by the context. In the medical context, for example, when attempting to use these technologies to make a diagnosis, much more data is required. In that case, securely sharing data and sharing more of it is actually a good thing. However, sharing that data within the United States with the insurance provider may result in coverage being denied. As a result, these ethical considerations may differ from one context to the next.

Let me give you another example. When working with artificial intelligence algorithms, it is critical to ensure that the data is free of biases. Because we are discussing the interconnection of various converging technologies, artificial intelligence is important. Data debiasing imposes a physical constraint on the algorithm, ensuring an unbiased outcome.

Let's move on to discuss avatar systems. Traditionally, device developers overlook important details when creating avatars, such as creating a hijabi avatar or considering skin texture. In this case, the ethical thing to do is to be inclusive. What does it mean to be inclusive in the virtual world? It translates to issues of identity. Then we must standardize them so that they are widely used in the industry. You can't make that law, but it's an ethical consideration that any engineer or UI/UX designer should make.

Developers must broaden their horizons and learn about other people with diverse identities who are also interacting with this technology. They must embrace diversity, create equity rather than just inclusion, and go the extra mile to learn about what is going on in other parts of the world.

What do you see as the most important future trend, and what are the major challenges in the cybersecurity industry? How do you believe they will shape the future of this industry?



The shift from servers, networks, and nodes to our brains and living spaces is the most significant trend in cybersecurity. As a result, we must consider how to address these new types of cyber-attacks, which may manifest as actual risks. As previously stated, humans and society are now in the loop, and cyber attackers can manipulate society on a massive scale, even engineering political change. These massive cybersecurity challenges will have far-reaching consequences for our future.

In addition, as immersive technologies become more prevalent, more tools and weapons will be available to distort reality and undermine trust in what is genuine. It will become increasingly difficult to distinguish between fact and fiction.

Furthermore, the convergence of brain-computer interfaces, artificial intelligence, and extended reality poses significant challenges that must be addressed.

#persona

KAVYA PEARLMAN

CEO & Founder of XR Safety Initiative (XRSI)

Well known as the "**Cyber Guardian**," Kavya Pearlman is an award-winning cybersecurity professional and the founder & CEO of the XR Safety Initiative (XRSI), a Standard Developing Organization with the mission to help build safety and inclusion in emerging tech ecosystems. Kavya is the pioneer of the novel XRSI Privacy and Safety Framework for the Immersive Technologies Domain, Metaverse Safety Week Annual Awareness Campaign, and various baseline security, privacy and ethics standards for Emerging Technologies. She won several awards for her work. In 2019, the San Francisco Business Times referred to Kavya as the "CyberGuardian" and awarded her with the Top 40 under 40 business executives award.

Kavya is one of the Top 50 speakers in the cybersecurity industry and constantly shares knowledge via webinars, conference talks, and blog posts around Application Security, Cloud-native technologies, Machine Learning, and the global challenges that come along with the next iteration of the internet, the Metaverse and Web3.

> ***"the biggest danger from the Metaverse is that we may not just lose our privacy, but our agency, our cognitive autonomy and even our free will"***

Adello Group AG.

Forchstrasse 32, 8008
Zürich Switzerland

Adello Malaysia Sdn. Bhd.

Mid Valley City 59200
Kuala Lumpur, Malaysia

LAB51 Inc.

548 Market St, Suite 33114
San Francisco CA 94104, USA

For collaboration:

Marketing: *marketing@adello.com* (+1) 625 225 2446
Sales: *sales@adello.com* (+41) 44 50031 50