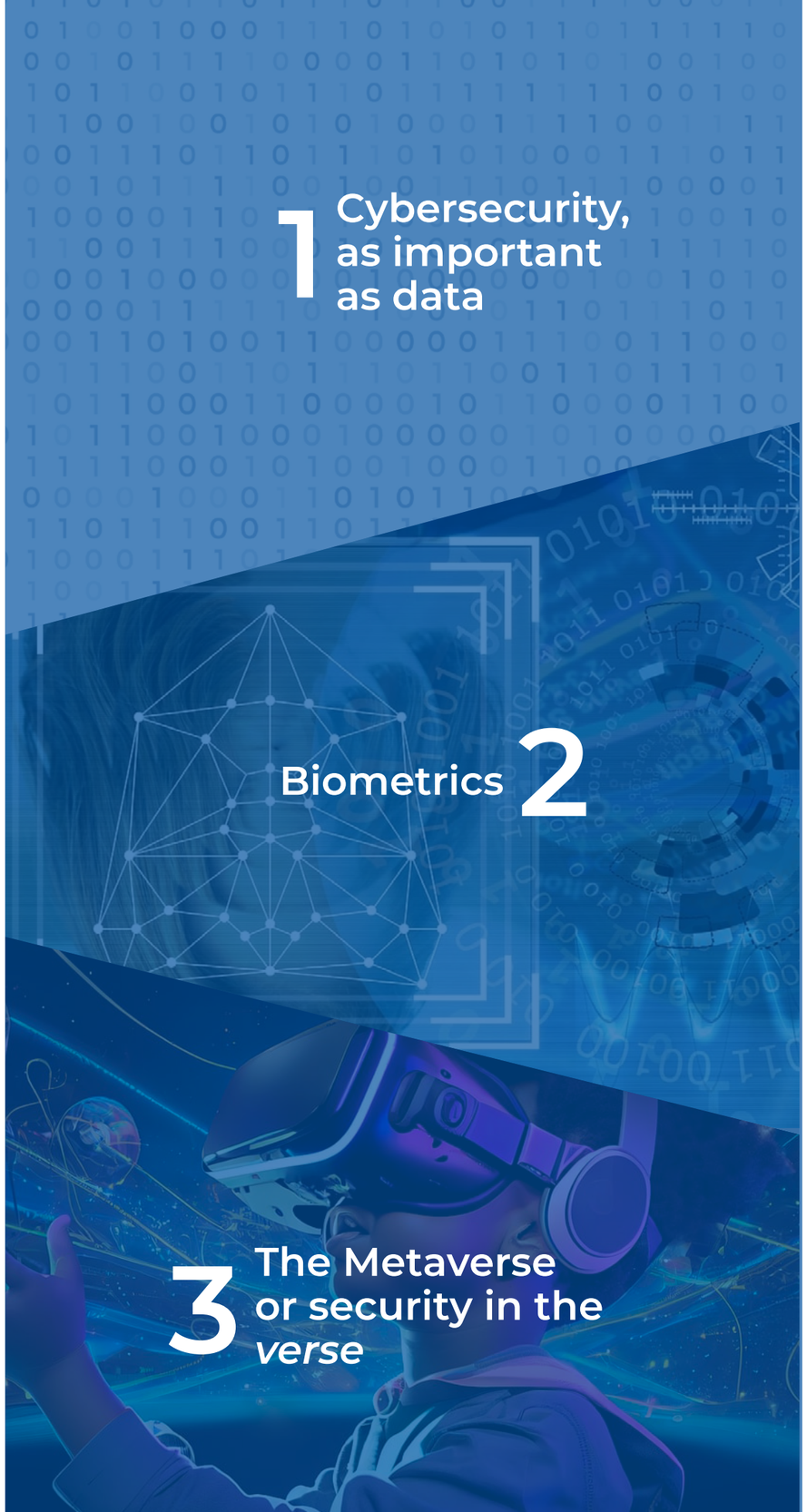
IN
DUS
TRIAL
bites Ebook-3

Cybersecurity

bigD



bigD
Design
that matters

1 Cybersecurity, as important as data.

As industry goes online, digital security goes offline. The more devices in the IoT, the more architectures and technologies come into play, cybersecurity will end up being a state issue or, what is the same, a steering committee.

The data tells us that 90% of organizations barely have cybersecurity experts, 82% do not update the digital records they must protect and 55% have a Cybersecurity Operations Center to detect and counteract cyberattacks, according to the Digital Maturity in Cybersecurity report by Minsait and SIA (2021).

“According to a recent report by Frost & Sullivan and Ricoh, 90% of companies worldwide have been compromised in the last 10 years. A not insignificant fact”.

If cybersecurity is a trend, cybercrime accompanies it and continues to increase. If in Spain there were 133,155 incidents between 2019 and 2020, in 2021 far from being reduced, cyber-attacks in Spain have continued to increase, 26% compared to the previous year according to Deloitte.

Cyber-attacks are our enemy to beat, and the sooner we realize this, a new future will open up before us.

We must know that the security of the device is the most important thing because it is the weakest link in the chain and, therefore, the most accessible. And it is that we have and must change our perception of reality. The vast majority of IoT users integrate emerging technologies and it is a big bet, but also, a bet to be vulnerable if we are not aware that we need to protect ourselves.

For example, 5G by design provides security and privacy, which will help us to be protected, although it will not be enough, we will have to put all the means available to avoid attacks from all points of the chain.

According to Microsoft in its "IoT Signals": survey: Approximately 50% of companies that have adopted IoT are concerned about data privacy, 40% about network security, and less than 40% are concerned about computer security device.

Cognitive security promises to revolutionize cybersecurity because it combines neural network technologies, Artificial Intelligence and Big Data (AI and Machine Learning article link) and integrates them with conventional security solutions.

Cybersecurity will be everyone's job, of teams and of transversal effort between companies.

"Communicating and understanding each other are operations that go beyond the intellectual".

2 Biometrics

From self-imposed cybersecurity to facial recognition, although we no longer recognize ourselves in the mirror. Lately, the arrival or application of technologies in areas never imagined far exceed Nostradamus's predictions.

But let's not deviate from what is important, biometrics and their perception. There are many ideas about biometrics, but what cannot be denied are its uses and benefits to prevent cyber attacks.

According to a new report from the World Economic Forum (WEF), stolen data increased by 151% in 2021. But this is where biometrics comes into play, as it is the most reliable solution to verify identity

unlike traditional tokens. The purpose is to create efficient cybersecurity mechanisms that do not allow digital criminals to carry out identity theft or fraud.

In fact, European companies will increase their spending on biometric systems at the end of 2022 by 20%, to 3,300 million euros. And although biometrics has to face some challenges, such as privacy, security and the possibility of bias, 59% of companies will already use it in 2023 according to the IDC consultancy.

From Veridas they share this vision of security and tell us that:

“when we use our biometrics voluntarily, when people want to do so, we are protecting ourselves and we also have a better experience and easier access to procedures or procedures that we could never do”.

In addition, they point out that "facial and voice biometric technologies are already disruptive in sectors such as finance, telecommunications, education or health."

The advantages offered by biometrics are many. Organizations and individuals alike rely on this type of validation for its security, as the data is much more difficult to falsify or steal compared to common token or password-based methods.

In storage, they do not take up much space and can be stored in any storage system. Although perhaps the cost is somewhat higher, its maintenance is not so high and it is worth investing in this type of security rather than investing in recovering stolen data. That is, it is a system, easy to use and non-transferable.

Obviously, biometrics can also be susceptible to attack by cybercriminals and break security systems, but as an authentication method that continues to innovate, the chances of cybercrime are greatly reduced.

The immense reality of 'the virtual' is integrating with the unreality of 'the natural', perhaps one day artificial intelligence will have defeated human intelligence and the Internet with its Web 3 or the Metaverse will be the center but meanwhile, it is clear that we must protect the data and any device that is susceptible to being attacked.

"Distrust is the mother of security".

Aristophanes

3 The Metaverse or security in the *verse*

The next stage is the Metaverse, the digital space with infinite possibilities in the universe (verse). The Metaverse or the multiverse of Marvel, we do not know how far the possibilities will go and even those of Web3 but it is clear that cybersecurity is one of the key pillars.

Security in the Metaverse or any other new trend or technology will be part of the success. They promise us interaction and that means access and data. Both Web3 and the Metaverse use technologies that are based on the Blockchain and thanks to this, cryptocurrencies or NFTs can be generated or used as a secure method for user login or identification.

From an industrial point of view, what began with simple digital designs has evolved into increasingly immersive environments in which process simulations that allow us to interact between robots and digital human avatars are the most common. Now let's imagine that we are working in the connected industry. We have our avatar together with the "new digital twins" or what is the same, our machinery in the Metaverse at our fingertips, like never before. But suddenly, surprise, our avatar has become independent and is managing the machinery. Can you imagine that they supplant your identity in the Metaverse? If we no longer had enough with reality, on top of that they "steal" our avatar.

Well, it can happen, but here is where the industry and technology companies are focusing. Both with new technologies such as 5G, which are already born pre-designed to be secure, as well as the use of biometrics, which is at the forefront of the safest identification systems, come together to almost be an "invincible system".

Having said that, working in digital environments, for example from the Metaverse, is going to give us a very wide vision and room for manoeuvre. Who doesn't want to get ahead of supply chain bottlenecks and develop "digital twins" if I fix the problem? Having a digital platform to map supply lines virtually will help us simulate product runs in advance and spot any issues that may arise. And if we talk about a very advanced level, it will allow us to have an overview of all assets (products, employees, distribution chain, etc.) and collect information to be able to analyze and apply it.

And if we also use computer vision technologies to measure different ratios of supply and demand in real time or analyze which tasks are priorities for future development, the execution will be almost perfect.

Creating synthetic worlds and subsets to check what effect multiple variables have is an advantage. As Doctor Strange said in one of the Marvel movies

"I never saw your future, only its possibilities."

As in Marvel, we may have several universes, the 838 or the 616? Virtual simulation has the answer, at least in the reality of the universe...

Contact bigD

info@bigd.es
www.bigd.es

+34 948 15 63 64