APU INSIGHTS
Product of APU Commercial Information Services LLC

Mapping the cybersecurity as an underlay for improved customer experience and business growth

RESEARCH SPOTLIGHT

SMART PAPERS

Index

WATCH DIGITAL FUTURES VIDEO

DIGITAL FUTURES

DIGITAL FUTURES is an online content publication platform catering for technology business leaders, decision makers and users, by sourcing and sharing valuable information and best practices in connection to the latest emerging technologies trends and market developments that leverage capabilities and contribute towards enhanced enterprise-wide performance.

WATCH VIDEO

LEARN MORE

Introduction

As the world is becoming more ***interconnected, cybersecurity is*** *expected to grow in* ***prominence*** *globally.*

The cybersecurity market was valued at USD 161.07 billion in 2019, and it is expected to reach USD 363.05 billion by 2025, registering a CAGR of 14.5% during 2020-2025. It is a subsector that affects all aspects of the economy, such as the financial industry, telecommunications, aerospace, healthcare, retail, logistics, manufacturing and other end-user services. Computer networks have become an integral part of our everyday activities in modern life. The internet has changed so many aspects of day-to-day life, not to mention the advancements in the way businesses operate. Connectivity has revolutionized the way we travel, communicate and do business. It is a highly competitive market without dominant players. The five major players are IBM Corporation, Cisco systems Inc., AVG Technologies NV, Dell Technologies Inc. and Check Point Software Technologies Ltd. [1]

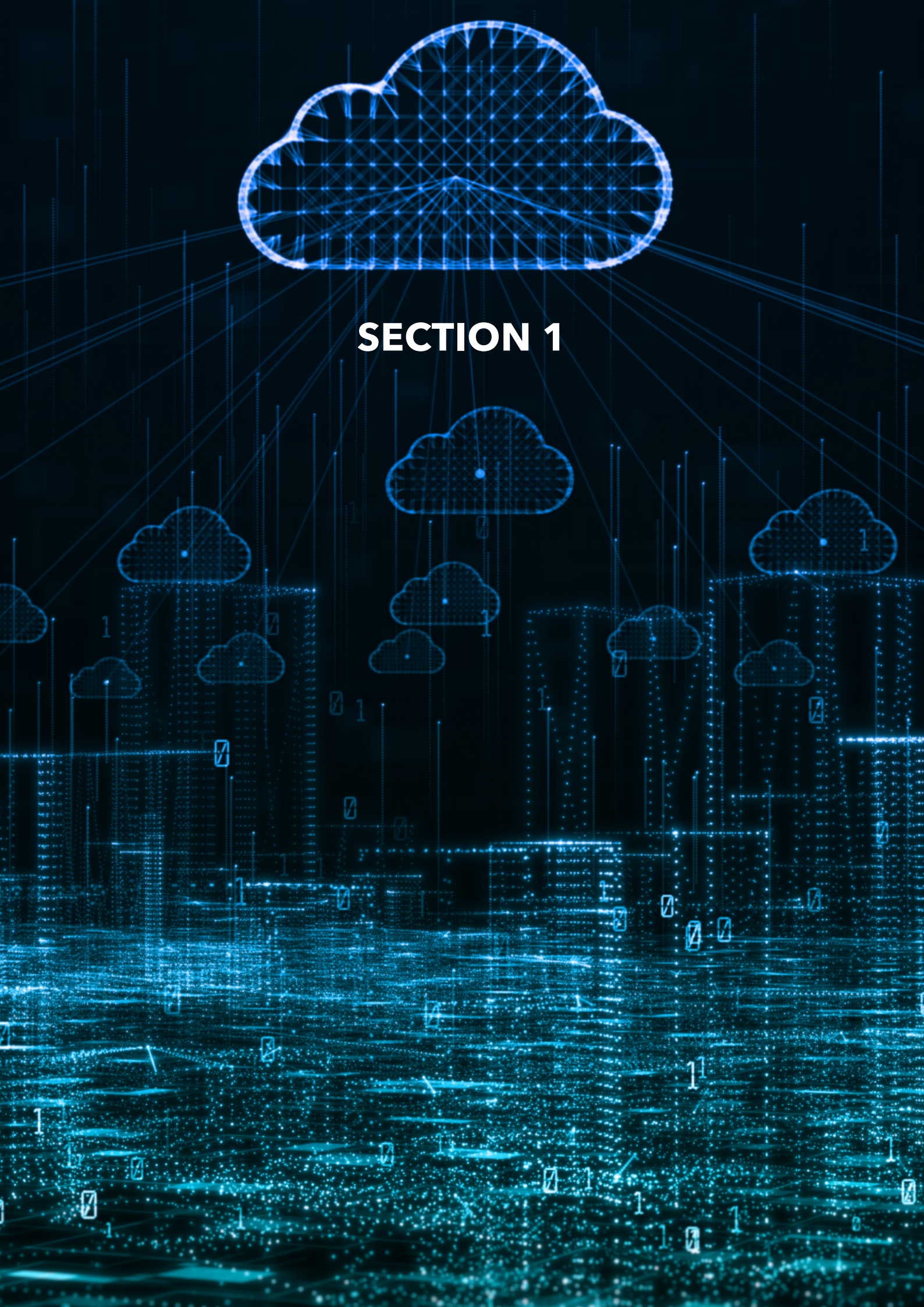
With the advent of digital technologies in many areas of human activity, countless threats have emerged with regards to the security of information. Cybersecurity is the protection of internet-connected devices such as hardware, software and data from cyber-attacks. The practice is used by individuals and organizations to defend against unauthorized access to data centers and other computerized systems. [2] There are various threats associated with their networks, data, and processes in every organization. In an ever-changing cyber threat environment, businesses need to have dynamic and flexible cybersecurity strategies to counter emerging global threats.

It is also a public issue that receives inadequate recognition. Almost everyone has heard about cyber security, however the adopted level of urgency and reaction of organizations does not represent a high degree of knowledge. The Internet is all too often seen as a safe environment for information sharing, transactions and physical world control. Yet cyber wars are underway, and there is an urgent need to be better prepared.[3]

1. Fortune Business Insights. (n.d.). Cybersecurity Market size,share and Covid-19 Impact Analysis.

2. Rouse M., (2020, April). What is cybersecurity? Everything you need to know. TechTarget.

3. de Brujin, H. and Janssen, M. (2017). Building Cybersecurity Awareness: The need for evidence-based framing strategies. Government Information Quarterly.



SECTION 1

Six key megatrends impacting the cybersecurity industry

Internet of Things

It is crucial to focus on cybersecurity for the environment and appliances of the Internet of Things, provided that the number of IoT devices is rising all the time. In today's society, essentially all devices are interconnected across networks. The recent rapid growth of IoT and its potential to deliver various types of applications have made it the fastest-growing technology with a significant effect on social life and the business world. The widespread distribution of connected devices has generated a huge demand for robust security in response to the increasing demand for millions or even billions of connected devices and services worldwide. [4]

Nowadays, customers can buy all sorts of goods with an internet connection. The current internet-based devices are connected to smart cities, transport, logistic warehouses, retail stores, smart power plants and healthcare facilities. As the IoT market continues to grow, so do the number of potential menaces that threaten the performance and safety of devices and the integrity of data. The demand for the technology and the associated threats will only continue to rise in the near future. The amount of IoT devices deployed is expected to grow to almost 31 billion worldwide, ending the 2020. [5]

4. Abomhara, M., (2015). Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks. Journal of Cyber Security and Mobility, 4(1), 65-88.

5. Forcepoint. (2020, March). What is IoT Cybersecurity?

As a result, the security aspect of this technology is becoming more and more imperative. IoT provides innovative directions for companies to generate value, but constant connectivity and data sharing also entails a risk for information to be compromised. The danger is two-faced: more data is exchanged via the IoT devices among multiple users, while more confidential data is being shared. As a consequence, the risks are exponentially higher. At every step in the IoT path, digital security is at stake, awaiting a bunch of hackers to take advantage the potential vulnerability of the system. Unfortunately, the varied data type and processing power among IoT devices doesn't allow a 'one size fits all' solution to secure a safe deployment.

The first step for any company is to perform a thorough security risk assessment that can predicts vulnerabilities in the equipment and the network infrastructure, as well as in consumer and client back-end systems. [6]

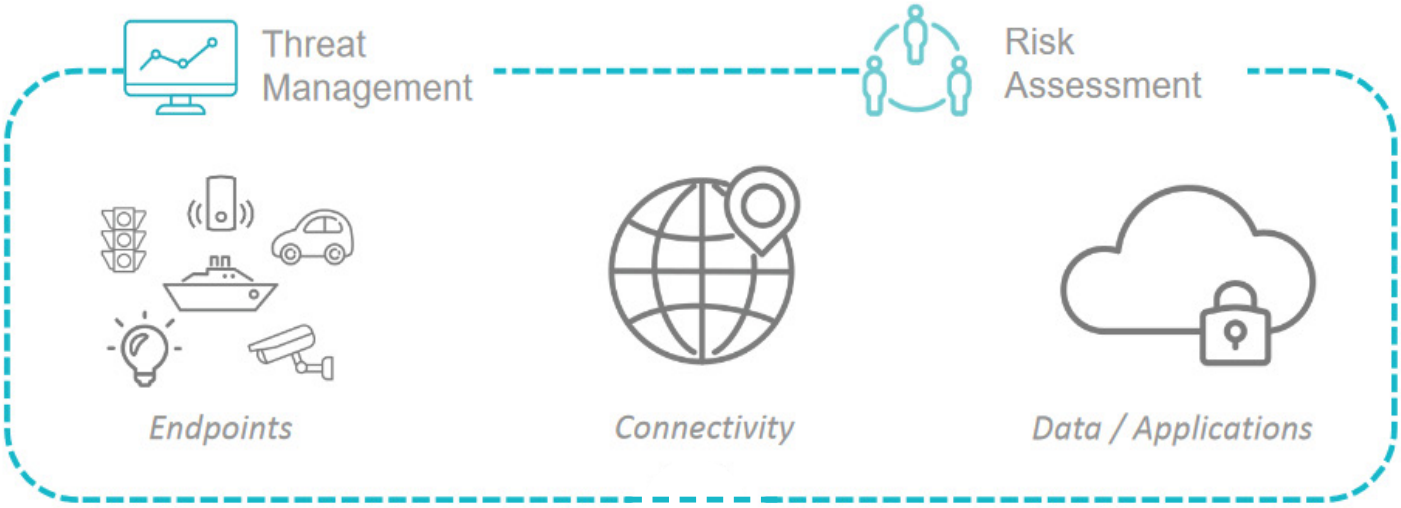


Figure 1. IoT Cybersecurity Framework. IoT Cybersecurity Alliance. (2017, July).

6. Thales. (2020). Building trust in IoT devices with powerful IoT security solutions.

In most large organizations, the approach to cyber risk may vary depending on the area, product or business unit. Safeguarding the IoT path can be really complicated, given the size and the data complexity, not to mention the fact that most of the technology is currently managed or accessed by third parties. As a consequence, several leaders are adopting a global cyber risk approach, raising expectations for cyber risk at all levels of the enterprise, from pre-threatening to post-event.[7]

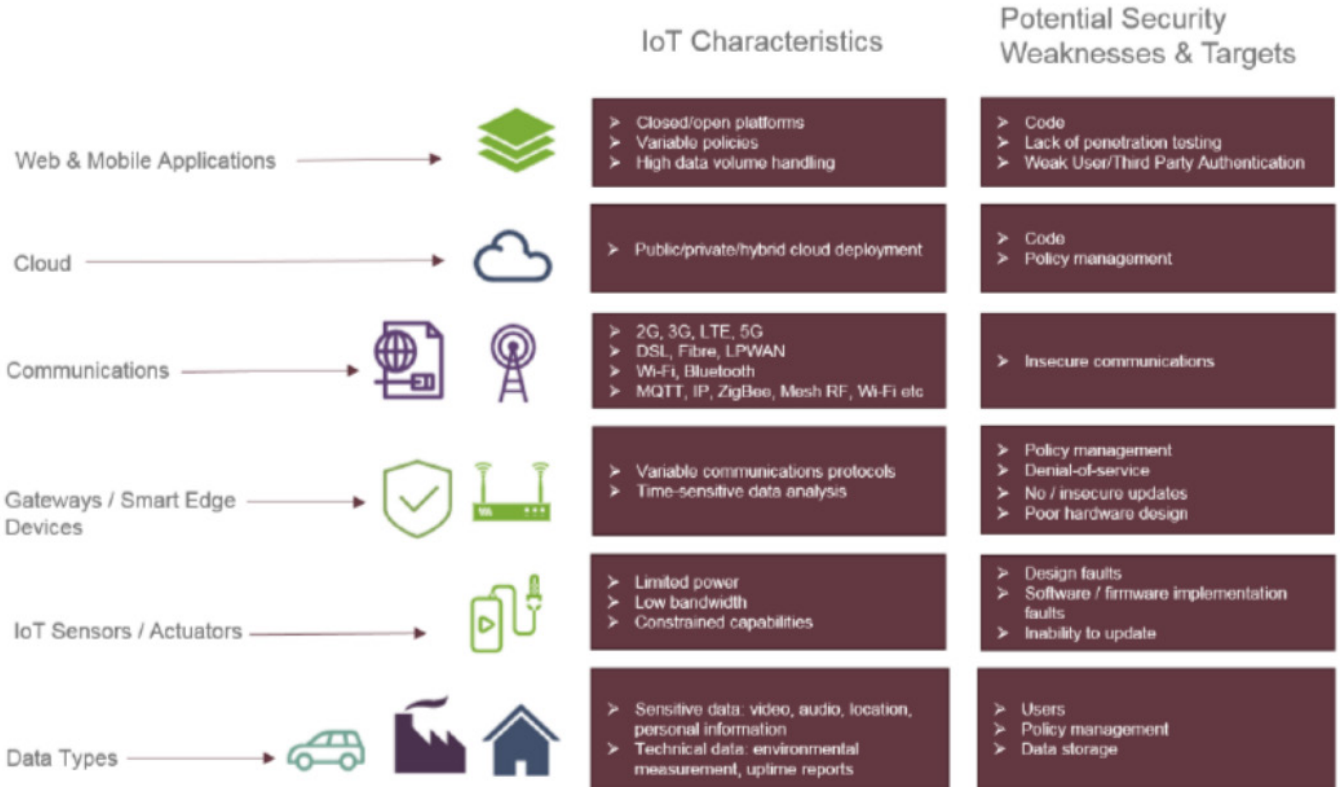


Figure 2. Deployment of the IoT (Juniper Research). Thales. (2020). Building trust in IoT devices with powerful IoT security solutions.

7. Deloitte & Touche LLP. (2020, April). Cyber risk in an Internet of Things world.

Security specifications in the IoT setting are not different from any other ICT system. If devices are not regularly patched or upgraded, it may be compromised by an attacker leveraging software's vulnerability, which in turn it could be used to interrupt the network of the election office. Sometimes these devices are mass-produced and identical, which enables an adversary to learn how to infiltrate them. [8] A survey conducted in Japan, Canada, the United Kingdom, Australia, the United States and France found that 63 percent of IoT customers assume that these devices are "creepy" due to inappropriate protection. Research results have underscored that 90 percent of customers are not sure about cyber security in IoT. [9]

The IoT Security Whitepaper, commissioned and released by Canonical, closely examines the behavior and perceptions of 2,000 UK customers towards IoT security, examines some of the leading IoT security concerns in the industry and explores how they could be resolved. There are worrying statistics, because 48 percent are not aware that their IoT devices may be hijacked by hackers and 79 percent of customers said they never got exposed to a news article dealing with these hazards. Furthermore, more than a third (37 percent) have admitted that they are not "sufficiently aware of the dangers that can be caused by connected devices and 78 percent have not seen their lack of confidence in IoT security rise over the past year. This is despite the UK Government spending GBP 12 million (USD 15 million) on a cyber awareness campaign. [10] In addition, this research reveals lack of sufficient action to combat security risks, as only 31 percent of consumers upgrade firmware on their connected devices, as soon as updates become available, while 40 percent of consumers claim that either app developers or computer manufacturers are responsible for making firmware updates on their connected devices. Shockingly, 40 percent of users have never made firmware updates on their connected device.[11]

8. Center for Internet Security. (2020, April). Cybersecurity Spotlight – Internet of Things (IoT).

9. Building trust in IoT devices with powerful IoT security solutions, (2020). THALES.

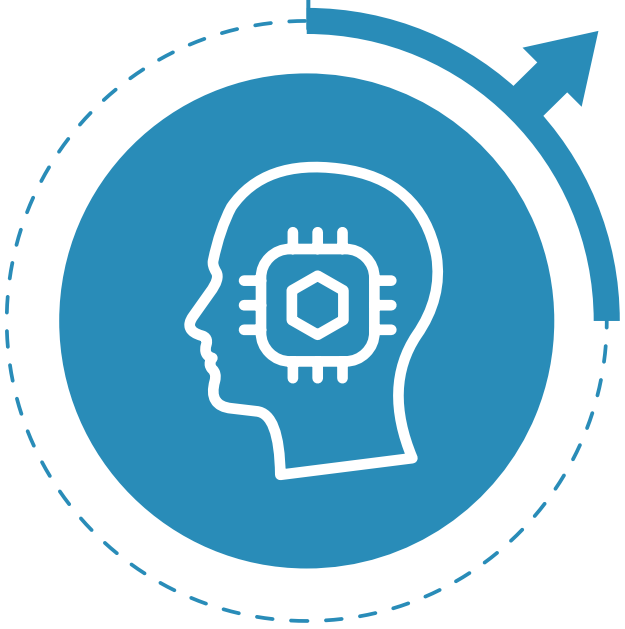
10. Fearn, N., (2017, February). Consumers unaware of the security risks posed by IoT devices, says report. Internet of business.

11. Peasley, S., Mantha, K. and Rao, V. (2017, June). Cyber risk in consumer business Consumer businesses discuss the six main cyber risk challenges they face today.

Artificial Intelligence

The majority of security systems are not designed to respond to a growing range of new threats. The enterprise attack surface is massive and continues to expand and develop rapidly. Companies lose a significant amount of time and money when security attacks take place.[12] A report by Norton found that the global cost of the average data breach recovery is USD 3.86 million. The study also reveals that businesses require an average of 196 days to recover from any data breach. [13]

In response to this enormous threat, cyber security tools focused on Artificial Intelligence (AI) techniques have arisen to help information security departments reduce the risk of vulnerabilities and enhance their security posture quickly and effectively. AI refers to technologies that can understand, learn and function on the basis of acquired and derived information. *Today, AI is operating in three ways:*



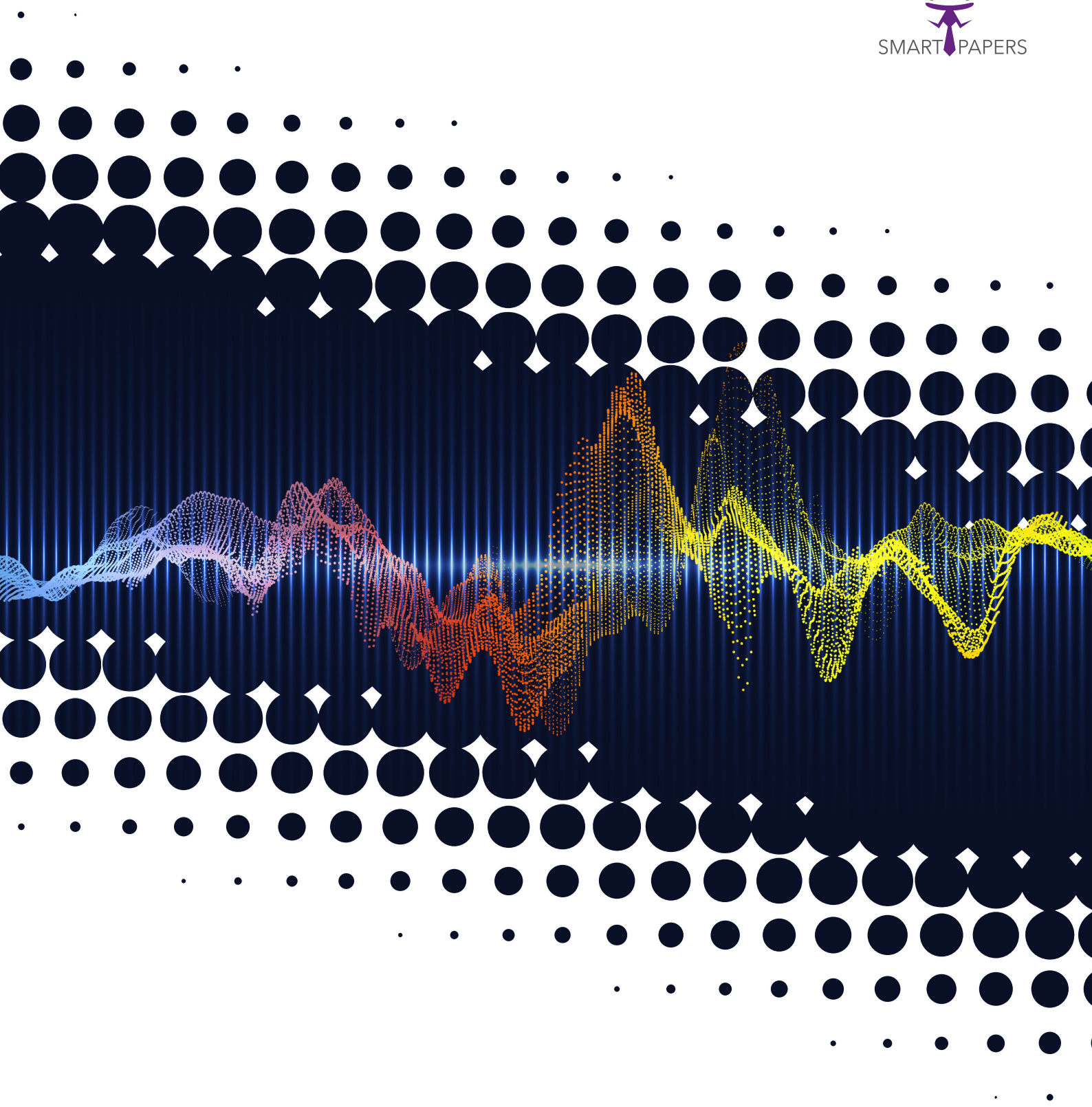
- ***Assisted intelligence, commonly accessible today, enhances what individuals and organizations already do.***
- ***Augmented intelligence, emerging today, uses data set machine learning and predictive analytics to improve human intelligence.***
- ***Autonomous intelligence, being designed for the future, features robots operating on their own. An example of this would be self-driving cars when they are commonly used.*** [14]

12. Balbix Inc. (2020, August). Using Artificial Intelligence in Cybersecurity.

13. NortonLifeLock Inc. (n.d.). 10 cyber security facts and statistics for 2018.

14. Balbix Inc. (2020, August). Using Artificial Intelligence in Cybersecurity.

SMART PAPERS



APU INSIGHTS
Product of APU Commercial Information Services LLC

RESEARCH SPOTLIGHT

FOLLOW OUR THINKING :

Designed and produced by APU Insights Creative Studio