Global cybersecurity trends to watch in 2020

With the number of cyber-incidents on the rise, there is a pressing need to be on top of IT security more than ever. In this article, we look at the new innovations and emerging technologies in 2020 that are helping organisations strengthen their security practices.

Temps de lecture : minute

24 February 2020

Cybersecurity in business is perpetually evolving as is the legal framework surrounding data and privacy. Take the current UK's 5G agreement with Huawei which shows uncertainties in terms of cybersecurity and engineering. The *Huawei Cyber Security Evaluation Centre 2019 Annual Report* showed serious and systematic defects in Huawei software engineering and cybersecurity competence. According to 5G expert Emily Taylor, 'bugs in software make any system vulnerable to attack'.

In 2018 GDPR was introduced in Europe to better protect citizens from data privacy breaches. As a result, cybersecurity has a role in society as important as in business and the risks can be both personal and financial. A recent report by the search firm Martin Hawk showed that more than 60% of the cyber-security leaders surveyed said talent shortage will get worse over the next five years.

What is a CISO? Since information security goes beyond a simple technical issue and blends risk, people and data management, and technical knowledge, the traditional CTO role had to be revised. This is where the 'CISO' (Chief Information and Security Officer) comes in, following the evolving cybersecurity landscape and changes. The CISO

has more critical responsibilities and has knowledge of potential threats.

Infographic: 5 essential trends in cybersecurity for 2020

CYBERSECURITY TRENDS to Know in 2020

Data Protection Regulation Goes Global

In May 2019, the General Data Protection Regulation (GDPR) celebrated its 1st birthday.

GDPR provides a set of guidelines to help make data security practices more organised, transparent and protected.

Even if you are not affected by GDPR, you should plan to align your organisation's data protection policies with GDPR as it is likely that similar regulation will eventually be implemented in your area.

Several locations around the world have introduced similar regulations including:

Australia: The Notifiable Data Breach (NDB) scheme

Brazil: The General Data Protection Law (LGPD)

California: The Consumer Privacy Act 2018

Canada: The Personal Information Protection and Electronic Documents Act (PIPEDA)

Japan: The EU Commission's "adequacy decision" judged that Japan's data protection regime offers equivalent protection to GDPR

Artificial Intelligence & Machine Learning Security Solutions Go Mainstream

According to Cylance Blackberry, **75.2%** of surveyed security professionals plan to use artificial intelligence for cybersecurity defence, **70.5%** for malware prevention, **68.6%** for advanced threat prevention.

Artificial intelligence and machine learning technologies could potentially be used to identify and respond to threats as they occur.

This tech would gather and analyse enough data to facilitate decision-making, allowing it to act predictively, rather than reactively, to security threats.

Intelligence-driven security "Will allow for the organisation's overall cybersecurity posture to change dynamically in response to the changing threat landscape."

dimension data

Cloud Security Continues to Grow in Importance

As more organisations migrate to the cloud, cloud security will remain a top concern.

Around **28%** of organizations have potential cloud account compromises. (Source: Unit 42)

The biggest risks to cloud security include customer misconfiguration, mismanaged credentials or insider theft.

64% of cybersecurity professionals cite data loss and leakage as their main concern.

62% say data privacy and confidentiality is their top cloud security priority.

Going forward, greater education is needed about cloud protection and hygiene.

"Public cloud is a secure and viable option for many organisations, but keeping it secure is a shared responsibility... Organisations must invest in security skills and governance tools that build the necessary knowledge base to keep up with the rapid pace of cloud development and innovation."

Peter Firstbrook, research vice president at Gartner

The Importance of Security for the "Connected Everything" Age

The number of Internet of Things (IoT) devices is expected to surpass 20.4 billion by 2020. (Source: Gartner)

Potential targets include connected cars, smart cities, smart homes, and virtual assistants.

Increased adoption of IoT will also bring about increased vulnerability for enterprises and consumers alike.

Potential threats include hijacking, privacy leaks, unsecured devices, and even home intrusion.

Many IoT devices are not secure end-to-end, this is partly due to a lack of any industry-wide security standards.

The Emergence of Next-Gen Authentication Technology

Passwords are problematic for several reasons. Firstly, today's technology makes it easy to hack even the most complex passwords. This is exacerbated by the fact that many users practice poor password habits e.g. rarely/never changed or used across multiple accounts.

Multi-factor authentication will also become more commonplace. This requires the user to provide two or more independent credentials in order to verify their identity.

More than **85%** of cyberattacks are a result of people getting tricked out of their passwords. (Source: CNET)

By 2019, the use of passwords and tokens in medium-risk use cases will drop **55%** due to the introduction of recognition technologies. (Source: Forbes)

Biometric tech offers a safer alternative. This involves identifying people through their unique physical characteristics or behaviours. Examples include facial, voice, and fingerprint recognition.

REFERENCES

unit42.paloaltonetworks.com/unit-42-cloud-security-trends-tips/
cnet.com/news/this-is-how-we-might-finally-replace-passwords/
cylance.com/content/dam/cylance-web/en-us/resources/knowledge-center/resource-library/reports/SANSSurveySecurityGetsSmartWithAI.pdf
dimensiondata.com/en/insights/technology-trends/cybersecurity-trends-2019
forbes.com/sites/forbestechcouncil/2019/02/07/five-cybersecurity-trends-to-watch-for-in-2019/#7d2b9a614c66
gartner.com/en/newsroom/press-releases/2019-09-09-gartner-identifies-the-top-seven-security-and-risk-ma?utm_medium=socialbutm_source=bambubutm_campaign=SM_GB_YOY_GTR_SOC_BU1_SM BA PR
securitymagazine.com/articles/90705-cyber-security-trends-to-watch-for-in-2019
siliconrepublic.com/enterprise/cybersecurity-trends-iot

Paradyn

paradyn.ie

With the rise of potential threats in IoT, companies need to implement strong cybersecurity systems to prepare for and deal with cyberattacks. The above infographic compiled by IT solutions network Paradyn highlights the major changes for companies to take into account this year in anticipating cybersecurity breaches.

Data protection regulation goes global

GDPR provides a set of guidelines to help make data security practices more organised, transparent and protected. As seen in the infographic, several locations around the world have introduced similar regulations to GDPR. Companies should systematically plan to align their organisation's data protection policies with GDPR as it is likely that similar regulation will eventually be implemented in their area.

AI and machine learning security solutions go mainstream

According to Cylance Blackberry, 75.2% of surveyed security professionals plan to use artificial intelligence for cybersecurity defence, 70.5% for malware prevention and 68.6% for advanced threat prevention. Artificial intelligence and machine learning technologies will potentially be used to identify and respond to threats as they occur.

Cloud security continues to grow in importance

As more organisations migrate to the cloud, cloud security will remain a top concern. Around 29% of organizations have cloud account compromises. The biggest risks to cloud security include customer misconfiguration, mismanaged credentials or insider theft: 64% of cybersecurity professionals cite data loss and leakage as their main concern and 62% say data privacy and confidentiality is their top cloud security priority. Moving forward, greater education is needed for cloud protection and safety.

> *“Public cloud is a secure and viable option for many organisations, but keeping it secure is a shared responsibility… Organisations must invest in security skills and governance tools that build the necessary knowledge base to keep up with the rapid pace of cloud development and innovation.” - Peter Firstbrook, Research Vice-President at Gartner*

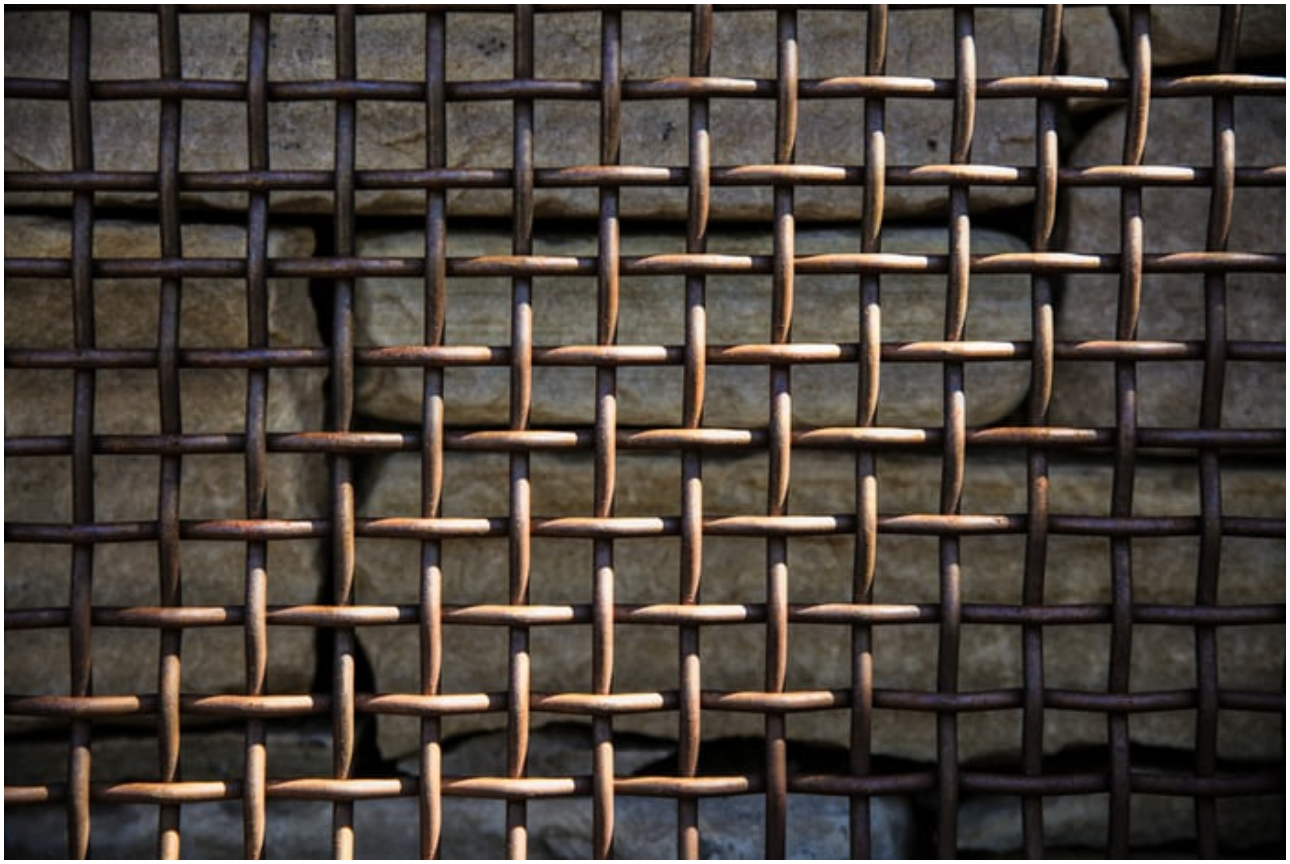
The importance of security in the “Connected Everything” age

By the end of 2020, the number of Internet of Things (IoT) devices is expected to surpass 20.4B. The increased adoption of IoT will also bring increased vulnerability for enterprises and consumers alike. Many IoT devices are not secure end-to-end, and this is partly due to a lack of security standards.

The emergence of Next-Gen authentication tech

More than 80% of cyberattacks are a result of people getting tricked out of their passwords. Today’s technology makes it easy to hack even the most complex passwords. This is even worse when many users continue to use poor passwords across multiple accounts.

Biometric tech offers a safer alternative where users are identified by their unique physical characteristics or behaviours: facial, voice, and fingerprint recognition. Multi-factor authentication will also increase and become more commonplace: this requires the user to provide two or more independent credentials in order to verify their identity.



Read also
11 startups tackling cybersecurity in the UK

Article by Maddyness