**Cybersecurity report**

**1. What does it do?**

**State of the art of cybersecurity:**

* Hardware authentication: This method is about [baking authentication into a user's hardware](http://www.pcworld.com/article/3024314/security/intels-authenticate-tech-brings-simple-but-powerful-security-to-skylake-chips.html). It can combine a variety of hardware-enhanced factors at the same time to validate a user's identity (John 2017).
* User-behavior analytics: This technology uses big data analytics to identify anomalous behavior by a user (John 2017).
* Data loss prevention: A key to data loss prevention is technologies such as encryption and tokenization. They can protect data down to field and subfield level, which can benefit an enterprise in a number of ways (cyber-attackers cannot monetize data in the event of a successful breach, data can be securely moved and used across the extended enterprise) (John 2017).
* Deep learning: This technology encompasses a number of technologies, such as artificial intelligence and machine learning. Like user behavior analytics, deep learning focuses on anomalous behavior (John 2017).
* The cloud: More organizations use the cloud for what has traditionally been the domain of on-premises IT, more approaches to security that are born in and for the cloud will appear (John 2017).

[John P. Mello Jr](https://techbeacon.com/contributors/john-mello). 2017. “5 emerging security technologies set to level the battlefield.” TechBeacon, accessed December 3, 2019. <https://techbeacon.com/security/5-emerging-security-technologies-set-level-battlefield>.

**What can be done?**

The transformation of the digital techonology has changed our world. While technology is a major driver for achieving economic and social advantages, it also presents new challenges in terms of security. Cybersecurity is behind most organizations' cutting-edge, which means that robust safety is not offered. Increasing assaults and violations are damaging individuals and organizations.

Research and innovation will allow cyber security to catch up with changing cyber risks. This helps in building a digital environment of trust and resilience. A more ambitious and challenge-driven research funding organization should be established to support progress in cybersecurity research and research should be pursued which incorporates perspectives from various disciplines and around the world.

**What is likely to be able to be done soon?**

* Utilization of data across the enterprise – As data is shared across an organization, it must be secured. Industry will recognize how the application of data models can result in better, more effective security (Sean 2019).
* Security assessments – The number of businesses that are required to provide some form of security assessment, audit report, or attestation will increase along with general cybersecurity awareness (Sean 2019).
* Moving to the cloud: Organizations are shifting their workloads into the cloud as their on-premises systems become end-of-life and they look to leverage the latest technology and tools available (Brian 2019).
* **Log monitoring in cloud environments:** With new tools to help sift through large amounts of data, security specialists will be looking to take advantage of automation, enhanced visibility, and alerting (Angelo 2019).
* Blurred lines related to legacy computer networks: As systems are moved to the cloud and as more of today’s workforce shifts to a remote working environment, a blurred line of where enterprise data lives and who is responsible for its integrity will be seen. This presents cybersecurity challenges as data moves out of the enterprise environment and onto shared systems like mobile workstations and virtual machines (Brian 2019).

“Cybersecurity Trends for 2019”. CISecurity, accessed December 5, 2019. https://www.cisecurity.org/blog/cybersecurity-trends-for-2019.

**2. What is the likely impact?**

**Potential impacts of cybersecurity:**

* Vulnerable big data: Most people nowadays generate and store massive amount of data using smartphones and other browsing devices. The rapidly increasing number of these devices has led to data distributed uncontrollably. People post photos and videos in real time to social platforms, not being aware of their exposure to cyber criminals. There have also been certain social networks accused with leaking data for political purpose.
* **Cloud security:** The more developed cloud infrastructure is, the more attractive a target it will become for cyber criminals. Because big companies are trying to protect their data, there is a high demand for expertise in this area. Some of the greatest risks to cloud infrastructure include data breach, system vulnerabilities, hijacked accounts and malware attacks.
* Intrusion detection: This is one of the must-have and in-demand skills in cybersecurity. Intrusion detection involves identifying and minimizing the consequences of malicious cyber activity. Breaches can now be detected from outside or inside a system or organization. Intrusion detection helps developing a prevention or mitigation plan for future risks so that organizations will react quicker.

**What is likely to change?**

* In 2019 and beyond, companies that process large volumes of personal data and companies that provide software/hardware/services used by financial, healthcare and retail sectors will continue to be targeted by hackers…” **(Marzena Fuller 2019).**
* The future of cybersecurity will center around industry adoption of 5G networks. 5G technology will enable billons of new devices to be connected to the Internet – with more speed, density and efficiency than ever seen before**(Ryan Webber 2019).**
* In the future, cybersecurity will focus more on the security controls related to adoption of IaaS and use of SaaS applications and continue to evolve to secure newer technologies like containerization as it becomes mainstream. Cybersecurity will also continue to become more ingrained into the newer devops model of software introduction (Frances Dinha 2019).
* The future of cybersecurity is going to include humans working alongside automated assistants, where AI/ML assist in operations (Joshua Davis 2019).
* The future of cybersecurity will be led by a workforce that intentionally studied cybersecurity, rather than fell into it as a default (Mike Stamas 2019).

Sam Mire. “What’s The Future of Cybersecurity? 38 Experts Share Their Insights”. Disruptor Daily, accessed December 6, 2019.https://www.disruptordaily.com/future-of-cybersecurity.

**3. How will this affect you?**

**In my opinion, cybersecurity can impact on human privacy and freedom of expression. Some policies created to protect the Internet** and other information communication technologies can be overly broad by restricting the free flow of information. For example, US companies such as Google and Facebook face stricter censorship due to the new Vietnam cybersecurity law that took effect in January 1, 2019.