**These will be the main cyber security trends in 2020**

In light of the latest cyber security trends, it is clear that firms cannot ignore cyber security without suffering severe financial and reputational consequences. As a result of cyberattacks, we have seen major players fold or suffer severe reputational harm, and other small enterprises have had to shut down.

The industry, corporate world, governments, and the general public have all been significantly influenced by 2019's cybersecurity trends, which have attracted both positive and negative attention from everyone. We'll examine the cybersecurity developments that are most likely to influence the market in 2020 in this post.

**The rise of artificial intelligence (AI)**

In the years and decades to come, artificial intelligence (AI), a genuinely ground-breaking achievement of computer science, will be a fundamental part of all contemporary software. This both poses a threat and a chance. AI will enhance both defense and offense cyberattacks. New cyberattack methods will also be developed to take advantage of some AI technology weaknesses. Finally, the enormous amounts of training data that AI needs will raise their worth and change how we must approach data security. Wise global governance will be required to ensure that this era-defining technology will result in broadly shared safety and wealth.

**AI and Big Data**

In a broad sense, artificial intelligence (AI) refers to computational systems that can do some tasks in place of human intelligence. Similar to the exponential expansion that database technology witnessed in the latter part of the 20th century, this technology is currently developing at a breakneck rate. The foundational technology that powers enterprise-level software is now databases. The majority of the new value that software will provide over the ensuing decades is also anticipated to be driven, at least in part, by AI.

Databases have undergone tremendous change in the last ten years to accommodate the "big data" phenomenon. This is a reference to the unparalleled scope and size of contemporary data sets, which are mostly derived from the computer systems that now serve as the mediators for almost all facets of daily life. For instance, each minute, YouTube receives more than 400 hours of video content (Brouwer 2015).

**The New Value of Data**

As its appetite for data affects what kind of information constitutes a desirable asset, AI technology will revolutionize the cyber security environment in yet another way, turning vast amounts of information that would not have previously been of interest into alluring targets for adversaries.

While some cyberattacks only seek to disrupt, cause harm, or cause mayhem, many are designed to seize key assets like intellectual property. Attackers in cyberspace are increasingly engaging in long-term strategy as they seek to collect data for as-yet-unknown goals. The strategy of "data hoovering" has emerged as a result of AI systems' ability to exploit even harmless data, which entails gathering all available information and storing it for eventual, strategic use, even if that use is not yet clear.

**Implications for Policy and Governance**

The current approaches to cyber security will need to be reevaluated in light of these developing circumstances. Finding the weakest link in a system gets more difficult but also more crucial as it grows more interconnected. There will be an increase in access points for cyberattacks as sensors, machines, and people become intertwined data suppliers for useful AI systems. A piecemeal approach to cyber policy will not work; to minimize weak links in cyber security, a holistic strategy is required. It is obvious that national-level control alone will not be sufficient because the training data that fuels the most significant and groundbreaking AI technology is global in scope and obtained from across many different countries.

Applying AI to established cyber assault tactics like spear phishing will increase their potency while expanding the pool of actors capable of carrying them out by getting over labor restrictions. This increases the urgency of ongoing initiatives like the UN Group of Government Experts' endeavor to develop generally acknowledged standards of behavior for behaviour in cyberspace and worldwide data protection.

**5G development and adoption of IoT devices increase vulnerability**

Manufacturers have already begun creating 5G enterprise solutions or have made public plans to do so, including Nokia, Samsung, and Cisco.

According to analysts, the full implementation of private 5G networks in the industry will take some time because upgrading existing network infrastructures would cost a lot of money. In the meanwhile, there are examples of office equipment that is already using a 5G network.

However, employing IoT devices without a secure 5G network or the necessary technical skills could jeopardize the privacy of businesses and their employees.

**Why 5G networks pose greater security concerns**

The 2019 Brookings research, Why 5G demands new approaches to cybersecurity, lists five ways that 5G networks are more vulnerable to cyberattacks than their forerunners. They are:

* In the network, distributed, software-defined digital routing has replaced centralized, hardware-based switching. The "hardware choke points" of earlier networks allowed for the implementation of cyber hygiene. In contrast, 5G.
* Cyber risk is rising as higher-level network operations that were formerly carried out by physical appliances are now virtualized in software.
* The 5G network is currently run by software, even if network-wide software vulnerabilities are secured. That implies that a hacker who takes over the network management software also has control over the network.
* The 5G network's huge increase in bandwidth opens up new attack vectors.
* increased vulnerability due to the IoT network being connected to tens of billions of hackable smart gadgets.

**A call to action on 5G security**

According to Ericsson, the hardware, software, configuration, and apps used by IoT devices should all be trusted from the standpoint of a 5G network. The effectiveness of network operators' and IoT device managers' governance will also determine it:

* Identity and information
* Privacy and security
* Actor adherence to agreed-upon security standards, from beginning to finish

Businesses may improve security on their end by making sure fixes are applied as software updates, according to Bencenti. Before releasing these products on the market, they should also undergo quality assurance (QA) testing, and they should be sure to shut any open ports that lead to exposed entry points.

According to Bencenti, the absence of standards for 5G security "is why these attacks happen day in and day out" and "2019 was deemed the worst year for cybercrime."

**Synopsis**

Thanks to the dedicated and clever work of numerous experts, artificial intelligence has come a long way. One of the most cutting-edge technological study areas today is on automating tasks that currently require human intervention. The AI is very helpful to humans because it can be used for a variety of tasks, including medical diagnosis, internet translation, and precision tools. As computers are predicted to develop consciousness and attempt to compete with humans, artificial intelligence technology is expected to have a significant impact in the future. Although many predictions about the strength and prowess of artificial intelligence have come and gone, it is a sector of technology that has favorably touched the globe and one that still requires more research to reach its full potential.

Over the following few years, 5G networks and services will be introduced in stages to create a foundation for the growth of new digital services and business models. 5G will usher in a new era in communications by offering super-fast connectivity to billions of devices. It will make it possible for devices to communicate in an IoT setting that can power an almost infinite number of services. The exponential growth of IoT use cases and the number of connected devices is made possible by 5G networks, which will also significantly benefit businesses and consumers. In addition to revolutionizing transportation, 5G networks will stably link patients and physicians worldwide, improving access to medical care.

**Reference:**

<https://www.cigionline.org/articles/cyber-security-battlefield/?utm_source=google_ads&utm_medium=grant>

https://www.techrepublic.com/article/5g-and-iot-security-why-cybersecurity-experts-are-sounding-an-alarm/