Global Cybersecurity Trends in 2020

The internet has brought with it the single biggest revolution to commerce and lifestyle since the industrial revolution. And, while the industrial revolution was mainly a singular event, the world of cyberspace has experienced, and is still experiencing, further revolutions within itself.

Cybersecurity, the realm of practice that deals with protecting individuals and businesses from the new breed of crime that emerged with widespread use of the internet (cybercrime), is also constantly under change.

Here are the top cybersecurity trends for the year of 2020.

Increased Automation

While to many, the world of computing and networking is already synonymous with automation, the truth is that there are degrees of automation. In cybersecurity, a firewall detects and blocks outsider attacks automatically, may even update itself automatically, but must still be installed manually and maintained, to some degree, by a human person. Can these manual processes be automated? Some such processes can be further automated, but somewhere in the workflow, human initiation and intervention will always be required. Yet, particularly in complex business environments, a lot of IT automation is possible. For example, the accounts and access to applications that new joinees of a business would need to be fully functional on day 1, can be automatically provisioned using preset configurations when the employee is entered into the HR system. Such automation reduces the time it typically takes to onboard the new employee (often up to 7 days) and gets them productive much faster.

As far as trends go, a recent Ponemon Institute survey of more than 1,400 IT and IT security specialists found that 79% of respondents either right now use (29%) automation tools and platforms inside their company or plan to utilize them (50%) within the next couple of years.

Increased Spending on Cybersecurity

According to a research commissioned by IBM in 2018, a company **should** ideally **spend** approximately 14% of their IT **budget** on cybersecurity. In that year, however, only 14% of organizations were found to spend more than 10% of their allocated IT budget on security. But today, the trend is showing change. While statistics are currently unavailable for a direct comparison with 2019's IT security spending as a percentage of total IT budget, according to research by industry analysts Gartner, the total spending on cybersecurity by businesses is expected to grow more than 9% from the year 2018. It might be possible that IT budgets as a whole are expanding, nevertheless, business spending on cybersecurity is growing rapidly every year, and this trend is expected to continue into the year 2020.

AI based malicious attacks are rising

AI is a blessing for many, but like every 'weapon in the wrong hands' action movie, it can also be turned into a curse. Hackers (also called 'bad actors') are now using the power of artificial intelligence and machine learning to hack into businesses for their own benefit.

AI based cybersecurity is also becoming more common

While it may seem scary and almost apocalyptic that AI exists which has been created for the sole purpose of crime, the truth is not all that dark. The cybercriminals might have the power of AI and machine learning to aid in their attacks, but cybersecurity specialists have the same tools to work with. The playing field is simply at a more complex level, but is still more or less even.

In a Nutshell

Cybersecurity is a modern essential for businesses and is only growing both in scope and necessity. Increased automation is allowing organizations to maintain more secure environments with less human involvement, and it is such features that are contributing to increased global cybersecurity spending. In particular, AI and machine learning are rapidly developing technologies in the domain and are something to watch.