5 Security Trends to Watch in 2020

From people to products, the cybersecurity industry is advancing at a rapid pace.

December 15, 2019 5 min read

Opinions expressed by *Entrepreneur* contributors are their own.

Presented by
Personal and corporate privacy continue eroding away as cyberattacks and data breaches become more common. In the first half of 2019 alone, more than 4.1 billion data records were exposed in known data breaches. The average cost of data breaches for affected companies is now nearly $4 million per business.

Standing guard while our society becomes ever more dependent on technology is the $120 billion cybersecurity industry, which is expected to grow to $300-plus billion by 2024. With the coming ages of AI and IoT, we stand to benefit from having an internet-connected home, vehicle or daily schedule in order to further automate and organize our lives. But we have to ask ourselves: What are the potential hidden costs of becoming more connected? With a hacking attack occurring every 39 seconds, it’s imperative that companies have the necessary security measures in order to survive as a formidable business. With the end of 2019 quickly approaching, here are five of the top security trends to look out for in 2020.

Related: 3 Cybersecurity Tips for Entrepreneurs

Expansion of Cloud-Based Security

As the world moves a lot of technology infrastructure into the cloud, we're seeing cloud-based security platforms and services follow. Cloud computing has evolved greatly over the last two decades, and now is frequently used to support critical operations of everyday businesses. From cloud-based data-storage services like Dropbox to all-in-one CRM clouds such as Salesforce, consumers and businesses have grown dependent on storing sensitive data in cloud environments.

And the numbers speak for themselves. By the end of this year, cloud-security platform sales, a small sliver of cybersecurity, is expected to become a $460 million industry. Cloud-based security provides several advantages to traditional security approaches, including economies of scale, reduced costs, improved protection performance, greater threat intelligence and quicker compliance with government and industry standards. According to Kaspersky Lab, around 75 percent of companies are expected to move applications to the cloud in the next few years. We can expect cloud-based cyber security to continue thriving well into 2020.

Advancements in Data Encryption

Since cyber attacks have gotten more sophisticated over recent years, a growing number of data-encryption advancements have followed suit. A recent study carried out by the Ponemon Institute revealed that 45 percent of surveyed companies have an encryption strategy that is applied consistently across their enterprise. But when a particular encryption technology or strategy becomes outdated and vulnerable to cyber attacks, all data can be compromised.

We're seeing many encryption advancements to help stay ahead of security threats. These include leading privacy technologies, ring signature and zero-knowledge proof and

distributed ledger technologies. When these technologies are used in combination with one another, not only is full or partial data anonymization achievable, but data and identity verification is also automated.

Shigeki Kakutani, CEO of QURAS, a next-generation privacy protocol, says that “as data is being democratized, the premise for privacy protection is naturally important. Globally, we need to provide secure solutions that can be used in both business and consumer situations, while always taking into account the level of privacy and security needed across any industry or transaction.”

Cyber Insurance

With all of the cyber threats that our world faces, cyber insurance has quickly become a growing need for both small-to-medium enterprises and large corporations. The aggregate global loss associated with cyber hacks and extortion is estimated at $11.5 million for 2019, so it’s no surprise that companies are taking preventive measures like buying insurance.

Currently, the size of the cyber-insurance market is estimated to stand at $2.4 billion in premiums, according to Stanford University’s Cyber Policy Center. This market is expected to double, or even triple, by the end of 2020, but the high cost of coverage and restrictive conditions on insurance policies may restrict some growth.

When estimates have pegged the digital economy at around $11 trillion as early at 2016, it’s clear that the “new” digital economy is severely under-insured. Insurance providers have had a difficult time keeping up with the changing landscape of cyber risk, including the onset of more connected devices and the expanding role that IoT is to play in coming years. As data breaches continue to make headlines, you can be certain that cyber insurance will be growing for years to come.

The Growth of “Passwordless” Authentication

Password privacy and protection is a major security issue plaguing us since the dawn of AOL. But just recently, a new authentication method has sought to take the place of passwords. Passwordless authentication tools can include hardware tokens or one-time password generators, biometric authentication and knowledge-based authentication.

By 2022, Gartner research predicts that 90 percent of mid-size companies will implement a passwordless authentication approach in more than half of use cases. Companies like GetID are helping other businesses process KYC & AML checks for their customers using a secure and compliant biometric product. Since passwords are one of the biggest attack points for hacking, it is easy to see why identification through any other means is top of mind for many businesses.

Related: 5 Cybersecurity Tools Your Company Should Have

Need for Cybersecurity Talent

The World Economic Forum reported a shortage of people trained in cybersecurity in 2017, and that shortage has only increased since. It’s been projected by Cybersecurity Ventures that there will be 3.5 million unfilled cybersecurity jobs globally by 2021, up 350 percent from 2014. In the U.S. alone, the total cybersecurity workforce consists of nearly 1 million people, and there are currently around 500,000 unfilled positions. With the list of security-training companies and security certifications only growing, employment in this space is almost certain if you are qualified. The time to secure your spot has arrived.

https://www.entrepreneur.com/article/343766