TOP CYBERSECURITY TRENDS THAT EVERY BUSINESS SHOULD WATCH OUT FOR IN 2021!

Cloud Breaches

Businesses increasing confidence into public, private and hybrid data moving into cloud have paved the way for new challenges. Cloud-based security threats give way for stricter security measures, protocols and security testing features. The rise in cloud adoption means an increase trust in infrastructure security.

Insider Attacks

Telecom reports indicate that 34% of cyberattacks in 2019 were misdeeds or internal employees. Employees are increasingly getting involved in data leaks, intentionally or unintentionally.

IoT Threat

Data from sensors placed within the Internet of Things (IoT) increase the attack surface for cyber bad actors. Multiple research reports say that cyberattack traffic has seen a three-time increase to rise to nearly 3 billion events.

BYOB and Mobile Security

The concept of Bring-Your-Own-Device (BYOB) allows employees to use their devices for work. It is encouraged to minimize costs and increase operational productivity by elevating employee flexibility through remote work and leveraging the gig economy.

Transparent Settlements

When working in the field of global financial settlements, businesses need to pay close attention to the latest happenings in cybersecurity. This would be the case for Transparent Systems for online payment through cryptographic systems.

Remote Working

COVID-19 pandemic changed how many organizations operate and turned remote working from a nice to have to a core requirement for many workforces. According to a recent study, a remote workforce sustainably increases the average total cost of a data breach. Three-quarters of organizations that deployed remote work said it would increase the time to identify and contain a potential data breach.

Moving into 2021, remote working referred to as working from home (WFH) will continue long after the COVID-19 crisis. As a result, organizations will endure a lot of decentralization, new network structures that reach out to private, unsecured, or unknown networks. And changing in a network and endpoint environment complicates incident response and security.

Artificial Intelligence (AI)

AI is maturing rapidly as a powerful technology with unlimited applications. AI raises many concerns including a lack of privacy, potential biases in decision, and creating a lack of control over automated systems and robots. Incorporating security and integrated processes will allow organizations to innovate while effectively managing risk and maintaining the quality of development.

Cyber Insurance

To protect against cyberattacks, a cyber insurance policy is imperative to help businesses mitigate financial risks from cyberattacks.

Investments for Security

With increasing awareness among businesses, 2021 will see an increase in spending on cybersecurity. There will also be a rising demand for more security experts across geographies.

Cybersecurity Skills Gap

The demand for cybersecurity professionals far exceeds the supply of qualified experts. Also, as many as two in three organizations worldwide have reported a shortage in their IT security staff. Consequently, automated security tools such as online vulnerability management solutions will become essential to maintain a good security case.

Contact Us

PCS Technology Consultants can perform a cybersecurity assessment to uncover security gaps within your network and applications enabling you to take appropriate steps to mitigate potential cyber-attacks.

For a brief conversation about the most effective cybersecurity tools to further protect your data assets contact us at 678-799-7861 or email at Van@PCSTechConsultants.com.

PCS TECHNOLOGY
CONSULTANTS