Top 5 trends Cybersecurity 2022

Big Data Trunk

INTRODUCTION

Covid 19 has taught us to live with constant challenges whether it's about the health of human beings or the health of the internet, IT, and businesses. Along with making our immune system strong, the time has come to make the immune system of your cyber world to protect your businesses.

Remote working has its own pros and cons; one of them is the burning challenge of cyber security. According to the Identity **Theft Resource Center**, the number of data breaches that happened in the year 2021 topped the total for the entire year of 2020. It has become very easy for hackers to expose your personal information or shut down your entire business as almost all the business has come online.

Ignorance in cyber security will not only cost any organization losses of billions of dollars but also their reputation is at stake, due to theft of exposure of personal information of their customers. To counteract these attacks, it's a must for you to know the emerging trends in cyber security. Small businesses are more likely to be targeted by hackers due to insufficient cyber security measures.

In this article, we are going to discuss the top **Cyber Security trends** of the year 2022 and how they are going to reshape internet privacy and IT security.

1. Cyber Threats for the Healthcare Sector

Hospitals and healthcare organizations are more involved in digital security as data breaches are common cyber security threats in health care. When there was no concept of remote working in the year **2015-2019**, that time also almost **157.40 million** healthcare records were exposed.

Due to pandemic and remote work culture healthcare organizations have relaxed their firewall rules to make it easier for staff to work online. Many healthcare organizations also expanded telehealth services and erect temporary medical facilities which have bypassed some of the security diligence of vendors or lacked the common security infrastructure present in established hospitals.

Because of this, cyber-attacks in healthcare are far from being stopped. Data breaches are a continuous threat for health organizations as sensitive information about the business, employees and patients remain the top target of cybercriminals.

Global newswire 2020 has predicted the rise in the healthcare cyber security market to jump to **33.65$ billion** by the year **2027 from 9.78 billion** in the year 2019. Taking into account this clearly means that hospitals and healthcare sectors are going to invest hugely in cybersecurity

2. Machine Learning to decode Cyber Threats

Machine learning can be your biggest savior in terms of cyber security. Decoding cyber threats has become easy with machine learning. ML has made cybersecurity easy, effective, and less expensive.

ML can anticipate and respond to active attacks in real-time by developing and manipulating the patterns from the data set. For this technology to work effectively the data should be rich and effective and it should represent all the possible scenarios so that it can make an effective algorithm.

With this technique, it has become easier for a cyber security system to predict the cyber criminal's behavior and analyze threats. **Click here** to learn more about the Machine Learning Trainings offered by Big Data Trunk.

3. Predictive Cloud Security against Cyber Threats

Today when every business is considering cloud migration, IT professionals should reconsider cloud security and take measures to tighten it.
Some or all the cloud services do not have secure encryption, authentication, and audit logging.

Even some service providers are not able to isolate the data from other tenants sharing space in clouds.

Because of poor configuration in cloud security cybercriminals can bypass internal policies which protect sensitive information in the cloud database. To keep this in mind now many cloud service providers are adapting predictive and innovative security to combat cyber attacks.

Predictive security helps to identify threats before attackers begin their move and pinpoint the attacks that pass through other endpoint security. This leads businesses to implement predictive security cloud with the market gaining a **261% ROI** for over three years now. **Click here** to learn more about the GCP Cloud Security Trainings offered by Big Data Trunk.

4. Phishing Threats

Both Cybercrime and Cybersecurity are products of the human mind, that's why no matter how smartly you secure your digital space, there are always chances that criminals may get over your efforts.

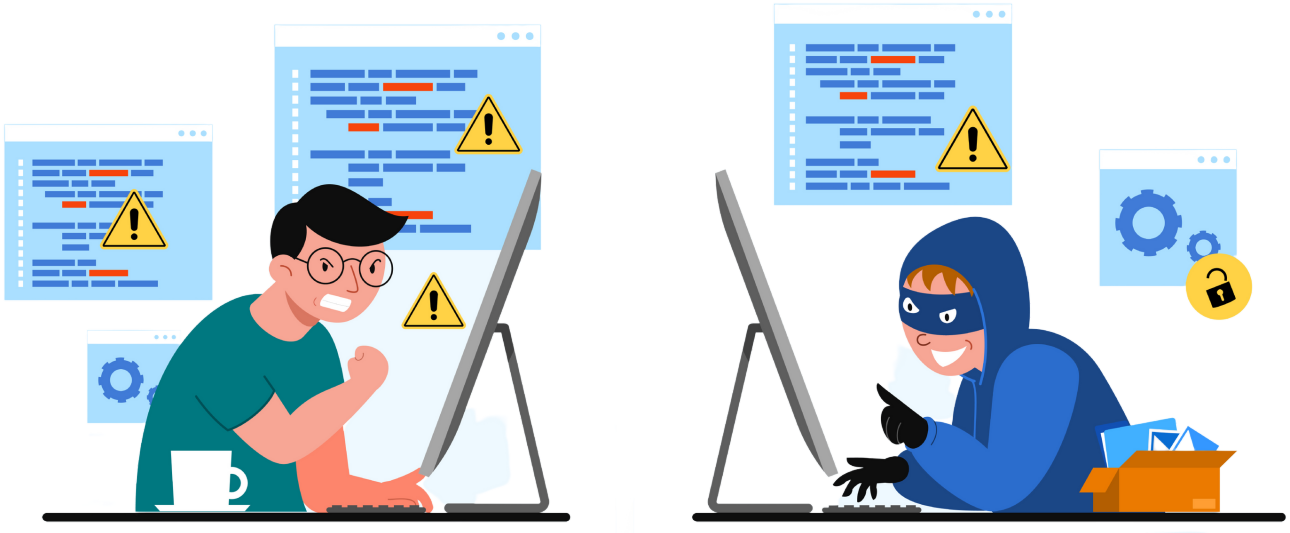
One such example is a phishing attack. The problem with phishing attacks is that you don't even know that you are affected. You may get an email from Netflix with the subject line "Action required. Your Netflix membership has been declined".

And if you owing a Netflix account, then you may be worried that your subscription may get canceled, and then you would log in to an email to rectify the situation. If you don't then you may fear something related to identity threat.

As per the 2019 Data breach investigation report of Verizon, 32% of data breaches involved phishing activities. Thus phishing is more likely to be prevalent in the coming years.

In the year 2020 alone there were 60000 phishing websites and 1 in 8 employees have clicked on that website and showed their information.

This leads businesses to adapt and invest in comprehensive security awareness programs. Organizations are investing in implementing simulators that can explain and recognize emerging patterns of such cyber attacks.



5. Cybersecurity Challenges in Education sector

Cybersecurity has become a top priority in the education sector as well with the growing culture of online education. Cybersecurity in online education involves compromised student data.

In the year 2021, the student data of 3 universities were hacked. This compelled the people in the education sector to tighten the security for the protection of student, faculty, and research data in institutions.

Until now people in the education industry have not focused much on cybersecurity and performing poorly in patching cadence, network security, and application security. But now due to increasing cyberattacks institutions are paying more attention to a new security architecture that includes post-perimeter security on endpoint protection, access to the cloud, and identity information.

Learn more about Big Data Trunk Courses & Training

www.bigdatatrunk.com

training@bigdatatrunk.com

+1-415-484-6702