УДК 811.111.304.21

Kiruscheva A., Hodkova M., Turcheniuk M.

Cybersecurity

Belarusian National Technical University
Minsk, Belarus

Cybersecurity is the collective name for practice of protecting systems, networks, and programs from digital attacks. The history of the cybersecurity has to been considered from the begging of the computer science, because of its definition. The main propose of the cybersecurity is information protection. The period from 1940s to 1970s was only pretendent the cybersecurity emergence. The biggest deal was when the Compatible Time-Sharing System (CTSS), an operating system introduced at MIT in 1961, was the first computer system to implement password login. CTSS had a LOGIN command that requested a user password.

The 1970s could be called a period when the cybersecurity was born. Correctly Cybersecurity proper began in 1972 with a research project on ARPANET (The Advanced Research Projects Agency Network), a predecessor to the internet. And from 1970s began developing of the antiviruses programs. Early antivirus software consisted of simple scanners that performed context searches to detect unique virus code sequences. Many of these scanners also included ‘immunizers’ that modified programs to make viruses think the computer was already infected and not attack them. As the number of viruses increased into the hundreds, immunizers quickly became incompetent. Nowadays the software is moved into the cloud from computer. In 2007, Panda Security combined cloud technology with threat intelligence in their antivirus product – an industry-first. The following year, the

Anti-Malware Testing Standards Organization (AMTSO) was created and started working shortly after on a method of testing cloud products. There are the widespread using of the cloud technology in the cybersecurity which we could see in Multi-factor authentication (MFA), Network Behavioural Analysis (NBA), also in cybersecurity using: Threat intelligence and update automation, Real-time protection, Sandboxing, Forensics, Back-up and mirroring, Web application firewalls (WAF).

Advantages of Data security:

Protection from viruses. Data security guarantees defense from all kinds of virus attacks, malware attacks, worms, spyware and other undesirable programs, which may provoke the appearance of serious threats to your system or network.

Protection from data theft. You can protect your data from theft by using certain measures like creating password protection, encrypting data, keeping your operating system and software up-to-date, proper disposal of sensitive data.

Reduces computers crashes. Keeping data security measures is helpful to reduce computer freezing and slow down.

Cost. It is always less expensive to prevent than to cover up after. The huge advantage that data security provides to its users is cost effectiveness. Data security tools and risk management do not cost a bomb. However, the resultant financial loss, legal hassles and reputational hock will be hard to overcome and will end up costing more.

Enhancement of technology. Data security is not a technology that works in isolation. It is an integral approach and engages all the departments and stakeholders of an organization.

Disadvantages of Data security:

Always changing. Data security is an evolving concept, so users must always purchase upgraded security.

Adaptation. It takes time for the human mind to understand the threat that is being thrust upon them. Tech adoption across the board is a time-consuming affair and expecting things to change overnight is fraught with danger.

Hardware and Software Anomalies. This aspect is often overlooked but in the zeal of upgrading systems, many a times, cyber security teams end up having systems which are incompatible to each other. Firewall rules differ for disparate systems and authorized personnel cannot access the network in such cases. To overcome such challenges a lot of deft planning is required.

Importance of Data Security. Data Security is important to every organization no matter how big or how small they are.

The reasons are:

1. Cybercrime is on the rise. There are roughly 4,000 cyber attacks every day.

2. Damage is significant. Cybercrime can cost organizations millions of dollars in damages.

3. Every organization has vulnerabilities. As organizations merge, evolve and grow during the time, their systems and networks naturally get more complicated, and things may slip through the cracks. Additionally, end users can often be the weakest link in an organization's security.

Data security should be seamless and thorough for everyone — whether you are a business or an individual. According to estimations by the Center for Strategic and International Studies, cybercrimes cost the global economy over 400 billion USD per year. Needless to say, cyber-attacks and data breaches will grow in due time as computer networks expand — cyber-attacks are getting bigger and better every day.