V. Domarosova, M. Marenich,
1st year students of School of Business of BSU
Scientific supervisor:
senior lecturer
T. Larina

CYBER SECURITY IS BROKEN. LONG LIVE THE CYBER SECURITY

In the second decade of the 21st century there are some issues people had never faced before. One of these problems caused by pressures of modern world is protection of internet-connected systems. Moreover, in today's connected world, it is unfortunately becoming a question of 'when' rather than 'if' some sort of data breach will occur."

Think cybercrime is something only found in fiction? Think again, with 1,5 million annual cyberattacks, online crime is an evident threat to anyone in our Internet-connected society. That number means there are over 5,000 cyberattacks every day, 175 attacks every hour, or nearly 3 attacks every minute. When you have a look at the number of attacks specifically targeting businesses, they're also worrying: IBM estimates businesses are attacked an average of 16,842 times a year. That's 47 attacks every business has to deal with every day – or nearly two attacks an hour.

Should we get worried about these attacks when many hackers target businesses and governments instead of individuals? The answer is a definitely yes: because big organizations hold caches of individual information, they make tempting targets for cyber criminals. **Wherever we go and whatever we do in business, we're most likely to go through it because the importance of business today is pretty big. The Internet is providing great benefits for business communication, moreover, it's the easiest way to connect with customer and clients. That's why where there is business and the Internet, the risk of cyberattacks is rising rapidly.** Moreover, everyone online is potentially at risk of cybercrime. In fact, you're probably more likely to have your email account hacked than your home broken into. So, it's common knowledge that It's no longer a phenomenon that only impacts large companies or governments rather, it's increasingly personal and therefore tangible.

While 10 years ago this might not have been much to worry about, now we're building our societies – our cities, our health services, transport and energy – on top of this digital infrastructure. Health, well-being, and sometimes people's lives depend on this systems' reliability. Unfortunately, many controls systems, despite the fact that we live modern life still run on old or bespoke operating systems making them vulnerable to interference. We need to be aware the foundations we are building on are in far worse shape than we realize.

But who is to blame for our insecurity? I'm sure that the answers you have on your mind are, firstly, the crooks and scammers and secondly, companies, police and governments that spent not enough sum of money to protect data and networks. But there is one other group that needs to acknowledge its share of the blame, too – us. We really need to value our own personal data more. We need to have a better understanding of what we are handing over, what will be doing with our data, and how it will be protected.

What about state of things in Belarus?

It is a common knowledge that when it comes to cybersecurity, not all countries are equal. Unfortunately, Belarusians cannot be sure their data is secure. Do you know that Belarus is among the least cyber-secure countries, according to the research by Comparitech, a UK-based website that specializes in assessing cyber security levels around the world. Several metrics were analyzed: mobiles and computers infected with malware, financial malware attacks, attacks by crypto miners, preparedness for cyberattacks and legislation. Among 60 countries studied, Belarus ranks No 8 (in this case, the higher position in the ranking means the worse cyber security) between Pakistan and India. Belarus has a high percentage of malware on smartphones (9,33 %) and computers (31,1 %) of users. The worst situation with cyber security in the world is in Algeria, Indonesia, Vietnam, Tanzania and Uzbekistan. And the most secure nations are Japan, France, Canada, Denmark and the United States. Our neighbors rank better than Belarus, Poland, for example, ranks the 40th place, Russia – the 38th, Latvia – the 31st, Ukraine the – 10th. Thus, it's a blue sky, open field for us as professionals in the area of information resources management to work on this issue.

So, we have carried out a survey among our peers in the social network "Vkontakte" showing the number of people subject to hacking accounts in social media. 206 people took part in the survey and according to it: 5,88 % of voters said that they have never come across this issue. 41,18 % said that they only have friends or relatives subject to this problem. The same amount of people (41,18 %) have gone through (or survived) cyberattacks 1–2 times in their life. 11,76 % of electors have hit upon hacking accounts in social networks more than 2 times.

After that, we conducted one more poll among the students of the School of Business to identify how knowledgeable they are about the necessary cyber security measures. As it turned out, 10,34 % of voters actually do nothing to protect themselves. They often set easy-to-remember passwords and don't really think about it. Really, a peasant needs thunder to cross himself and wonder.

65,52 % of our respondents said that they are trying not to set simple and obvious passwords. 24,14 % regularly clear outdated information and messages. 34,48 % of respondents always make sure that no one sees the entry of their personal data. Most often it happens simply by carefully looking around. 62,07 % said that they have never visited "questionable" or "suspicious" **websites.**

Analyzing the acquired information we can say that nowadays, ironically, cyberattacks are becoming commonplace, and nevertheless, we've come across not only with a lack of awareness but also with ignorance and even a devil-may-care people's attitude. It turns out that the information they have is not enough to be safe.

Well, how to take the first steps to protect our data?

We have some practical advice out of your research how to build your self-awareness on this issue and to take first steps in order to fight state-backed hackers, crooks and scammers.

Concerning the first one, the thing you really should do is to keep informed. Many modern cyber security threats originate from user error. A huge number of incidents are caused by people ignoring general advice around avoiding clicking on suspicious links and maintaining secure passwords. Hackers love "low hanging fruit," so don't allow you or your teams to be that fruit!

Secondly, you should value your own personal data more. You need to evaluate the situation (understand what will happen to your data after entering them, where it can cause, what exactly will be doing with your personal data and how it will be protected). You should pay more attention on apps, services and online stores you use.

Also, you totally should move beyond antivirus. Antivirus software is still a crucial part of the IT security, but it's not enough by itself to protect from modern threats. When it comes to professional matters technical teams accordingly need many more tools, resources and solutions, but some of them are expensive. However, they're not likely to be as expensive as repercussion after a cyberattack.

Concerning the state level, one more thing likely to be good for you to do is get insured. Cyber security awareness isn't only about protecting against financial risk. If your company is hit by a data breach, it can cause much damage to contain with, and you may need help with that from the specialists.

And what about backup and recovery? A company is hit by ransomware every 40 seconds, but the irony is that none of firm should pay a redemption if they have backups. Yes, any cyberattack causes annoyance and destruction, but if a backup is there, there's no need to pay hackers any money.

One more step to protect businesses' data network connected with the previous one is to adopt standard security measures and manage how the systems are configured and used. Malware protection is an important security consideration. Businesses should install antivirus software and regularly scan for malware. We are talking about updates, fixes and patches which can help prevent successful attacks against networks, because networks are often a weak point in cyber defenses.

Also, the use of media for the import and export of information should be controlled. It's a vital thing. There are so many incidents when scammers exploit removable media vulnerabilities in order to damage or steal information stored on computers. Not only should removable media be scanned for malware, but the type of media and the sort of information that can be transferred should be limited.

And last but not least recommendation is monitoring. Companies are needed to scan inbound and outbound traffic constantly to detect suspicious activity. They should also monitor all ICT systems using specialized intrusion detection and prevention systems.

Thus, as was mentioned above, it's a blue sky, open field for us as professionals in the area of information resources management to work on this issue.

We are building our futures on these digital networks; let's make it very clear that we want, and expect, them to be secure. Because, for those who won't be able to take information we gave into consideration, it's unfortunately likely to be only a matter of time before they find they've been the victim of a cyberattack or a data breach.

So, prevention is much cheaper than cure.