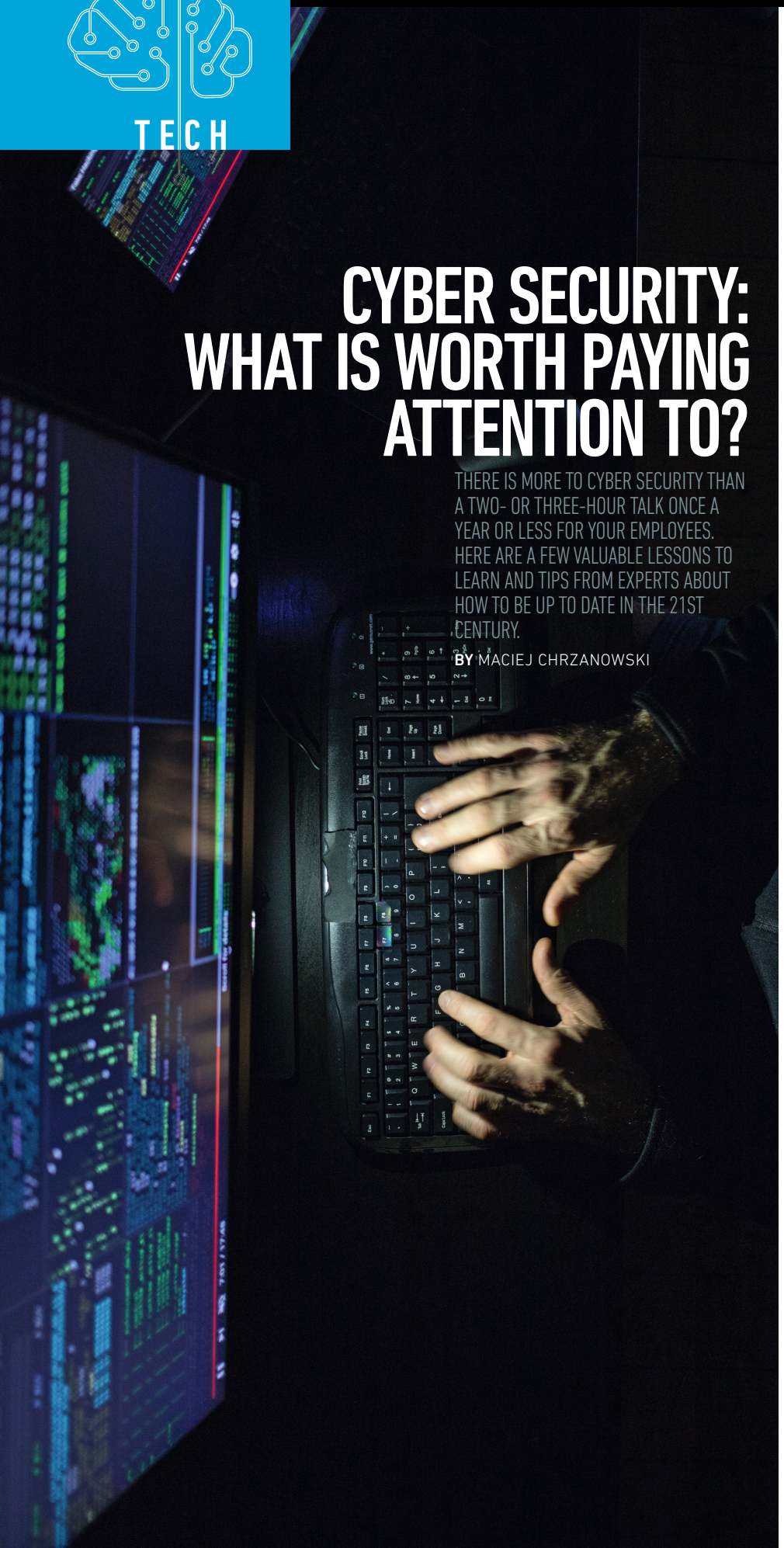

CYBER SECURITY: WHAT IS WORTH PAYING ATTENTION TO?

THERE IS MORE TO CYBER SECURITY THAN A TWO- OR THREE-HOUR TALK ONCE A YEAR OR LESS FOR YOUR EMPLOYEES. HERE ARE A FEW VALUABLE LESSONS TO LEARN AND TIPS FROM EXPERTS ABOUT HOW TO BE UP TO DATE IN THE 21ST CENTURY.

BY MACIEJ CHRZANOWSKI

In the 21st century, work for many of us has become impossible without digital tools. Typically, we begin our day by checking our phones. As with any new technology, the digitization of information and processes has created new risks and challenges. Therefore, in recent years, the issue of cyber security has become increasingly relevant and important. Let's look at this issue from the perspective of companies and their employees.

There are many guidelines and recommendations for cyber security: choosing the right passwords, changing them regularly, locking your computer, using security software, updating systems and software regularly, backing up data, not using public Wi-Fi networks, not opening suspicious links or attachments, not giving out your data... We could go on and on, creating an extensive checklist.

Many of these principles are systematically implemented and enforced in companies, and often dedicated departments responsible for digital security are created and appropriate processes and software are introduced in teams. However, often such guidelines and tools alone are of no use in the face of new threats.

Despite the immense power of machines, it is the human being who is the most sensitive link and it is often our reaction that is most critical in maintaining safety. Therefore, a new skill needs to be developed in everyday functioning — the skill of verification. Adopting vigilance and questioning as your own safety mechanism is an extremely important and useful change in today's world. That's why despite all the "hard" solutions and rigid rules, every company should teach its employees to think critically and stimulate the need to check the information they get. Especially today, when remote

>>>

work has become so popular.

It's impossible to be up to date on all security technologies or every cyber weapon available. The best thing we can do to enhance the digital security of our company and our employees is to grow awareness of these threats. Established rules can always be circumvented, and this kind of universal internal cyber-verification can provide an effective response even to risks that are not yet known. With all the other threats that business is experiencing in these difficult times, being aware of the possible dangers will help our companies to tackle them.

These kinds of skills distinguish between digitally produced reality and actual reality, and sometimes just knowing that these two are not the same. The reality that surrounds us is not necessarily real. Questioning and checking digital reality should be part of our cyber hygiene on a daily basis, put on par with the reflex to lock the computer when we leave our desks.

Translating this into a practical example: your eyes see an email from a contractor with action guidelines, but it may not be an email from the contractor. Be vigilant when checking the email address, platform or sender. Questioning such correspondence does not negate the existence of trust and belief in goodness and honesty, but let that trust guide our actions through the internal verification channel. Nurturing such a culture and practice in our team will help to prevent confidential data, company trade secrets or other sensitive information from leaking out.

Not only that phishing emails are the scourge and the terror of the Internet. These days, also known as the Fake News Era, are dominated by the Internet and social media, which have become the main reliable source of knowledge. Unfortunately, it is an extremely insidious space and very susceptible to falsification and misrepresentation (whether intentional or not). Fake news spreads at breakneck speed, and while sometimes it is innocent false gossip, in some cases the news reported can threaten people's lives and health, the security of a company or even entire societies and countries. The news can be disseminated as statements, which are recordings of famous people with their voices and facial expressions artificially manipulated to match the image — known as deepfake video. The technological possibilities in this area are enormous, so we should also always review our decisions and beliefs based on cyber news. From a business perspective, it is also important to be able to quickly discover and react to such situations in order to protect the organization's image and the safety of its employees, partners and customers.

The war in Ukraine, the cyber warfare and sanctions have shown another layer that is emerging. It turns out that who provides software, who maintains it or even who are the programmers who work for a given company are starting to be important. Until now we didn't look at these phenomena in terms of a threat, but this element will become more and more practical in our everyday life. We will be checking (auditing) our suppliers, verifying who works for them and whether in that scope we do not expose our business to the risk of e.g. continuation of operations, data theft or technological sabotage. The geopolitical struggle behind the development of the 5G network in Central Europe might be only the first sign of things to come. ●

> AS WITH ANY NEW TECHNOLOGY, THE DIGITIZATION OF INFORMATION AND PROCESSES HAS CREATED NEW RISKS AND CHALLENGES

EXPERTS' OPINIONS

The Polish CERT unit, responsible for recording cyber security incidents, provides the following data about economic sectors. The largest number of incidents, 38.28%, took place in the media sector, 17.38% concerned commerce (wholesale and retail), 14.71% were postal and courier services and 13.38% took place in the energy sector, while only 8.36% of incidents concerned individuals.

CERT recorded a total of 29,483 unique cyber security incidents. The value of incidents handled increased by 182% compared to 2020.
As many as 86.49% of incidents were computer fraud, while 9.66% involved malware. The remaining incidents were related to offensive and illegal content, information gathering, hacking attempts, resource availability, information security and vulnerable services. Importantly, CERT reports only officially accepted incidents. There is a grey area of companies that fell victim to attacks but did not report them. Hence, in my opinion, the annual report may be clearly understated.

The Cyber Security Trends 2021 report shows that most companies use rather very basic forms of security. 94.5% – antivirus software, 89.6% — backup and disaster recovery (DR), but e.g. training is provided in only 49.1% of companies. On the other extreme, we have only 6.2% of companies using solutions based on AI or other forms of security.

Damian Rokicki
CTO, DNR Group

If I were to answer what is the single most important challenge for Polish companies in terms of cyber security, my answer would be the company's approach to the topic of security. Most companies in Poland focus on procedures (which are not bad but are just a "roadmap") and not on the day-to-day application of security. Often companies are well organized in IT departments and have access to major servers but huge deficiencies exist at the individual employee level. An employee today is one of the links that should protect the company. The question is how can they do it if their digital security education is a two- or three-hour talk once a year or less?

Security is a process. This process is continuous, not spotty. If we neglect employee education then the number of mistakes increases as well. Remember, however, that imposing too strict a framework will have the opposite effect and, in effect, lower the level of safety. If we introduce new guidelines in the company, it is crucial to involve not only the IT department but also the end-users. If we paralyze their work, who will earn for the IT department?

I hope that in Poland a new subject called digital security is included in the curriculum as early as elementary school to complement IT lessons.

Krzysztof Ogorzałek
co-founder, VP, JMK Computerate

Most common cyber security issues in Polish companies:

- lack of qualified IT specialists dealing with security in the company — poor competence
- lack of documentation and regular audits
- board disregard for the business impact of IT security
- low operating budget for risk, audit or incident handling activities
- lack of security monitoring of IT infrastructure and lack of incident analysis and lessons learned

Examples of good solutions:

- training IT staff in event handling
- implementation of procedures such as ITIL to eliminate configuration errors and maintain transparency of changes in the infrastructure
- regular IT infrastructure audits and security audits
- implementing security policies, backups, and disaster recovery (DR)
- employee training
- implementing solutions that enable IT to centrally manage and report
- monitoring IT infrastructure
- centralizing system log collection and analysis
- implementing automated systems to notify security officers of emerging incidents — most executives learn about problems as they arise, most are unaware of security breach attempts, etc.
- implementing a password manager, along with dual authentication integration