WRITTEN BY

**PETRA KRAJČIOVÁ**
Security Specialist
Deutsche Telekom IT Solutions
Slovakia

**BRANISLAV KMEC**
Security Specialist
Deutsche Telekom IT Solutions
Slovakia

DEUTSCHE TELEKOM IT SOLUTIONS

# A FORGOT-TEN FACET

## OF YOUR DIGITAL TRANSFORMATION

Accelerated by the recent crises – pandemic, energy, and war-related – many organizations brushed up their strategies and plans for digital transformation. To achieve positive return on investment, the boards opt for a "minimal" setup with cloud-based infrastructure and applications landscape. In their effort they often overlook that digitization of tools and processes with little or no insights into cybersecurity may seriously backfire and wipe out any benefits.

The COVID pandemic has significantly impacted the way we live and work. The so called "new normal" refers to broad changes individuals but also organizations are experiencing in various aspects of their existence, including work, education, business operations or social interactions. One area that became more prominent during the pandemic and even more so in reaction to the war in Ukraine is cybersecurity. The shift to remote work has brought in new security concerns, triggered new security policies, rules, and impacted processes, systems, hardware and software.

When an IT service provider reviews the cybersecurity topic with their clients, 75% quote the need to attend to data and systems security as one of their top three priorities. Yet, shockingly, only 16% of the same clients feel prepared to tackle the security challenges in their transformation journeys! Companies feel intimidated by the emergence of new security policies and may get quickly lost in this rapidly changing market. When sourcing your IT services partner, the way they react to your cybersecurity probing concerns is a good differentiator between "the good" and "the best"...

### SECURITY INTEGRATES WITH IT ARCHITECTURE

An often-overlooked aspect of digitization related to cybersecurity relates to mobile communication protection. With employees working remotely, we see an increase in the use of mobile devices (smartphones or tablets). These devices do access sensitive organizational data and resources – making them an attractive target for hackers. A simple but often-forgotten protection is your mobile device management (MDM) strategy. MDM policy helps ensure that devices are secure, updated and use strong passwords, because some 60% of users in companies have simple and non-expiring passwords. With mobility comes a risk of phishing attacks. Remote workers rely on intensive use of email, messaging, or collaboration tools. Hackers use these apps to launch phishing attacks, attempting to trick the user and steal sensitive information or gain access to corporate systems. On average, 17 000 euro is lost to a single phishing attack every minute.

The digital business landscape impacts security policy settings too. CIOs and COOs shall ensure that their security policies are up to date and reflect the way their business units operate. For example, take stronger role-based access control over your resources. Regularly audit how the policies are enforced and their consistency is vital. Why? A typical employee has access to 10+ million documents in their organization – 99% of them are not in the scope of his or her attention. Yet, through that person's compromised security credentials, the accessible but "out of radar" documents are a gold mine for a hacker. A breach of this kind costs, and the costs to the organization grow by some 130 000 euro every month.

> **One third of breaches can be attributed to internal actors and their compromised passwords.**

### WHERE TO LOOK FOR QUICK WINS?

Support for new security policies and requirements may bring in new applications or software-defined solutions to your IT architecture. A simple aspect of your revised IT architecture suiting the digital ambitions touches endpoint security. Remote workers or digitally connected business partners may use their personal devices and public networks to carry out business with your organization. That increases the risk of cyberattacks. The number of connected endpoint devices will double between 2022 and 2025. With that number, hacker attacks occur every 40 seconds and unprepared organizations see their impact in their accounting sheets. Failure to address security aspects of digitization may also result in fines from regulatory bodies and reputational damage in the eyes of consumers and/or business partners.

An example of a policy implied by the situation around us as well as regulatory changes is data classification policy. This policy outlines different types of data within the company and accesses to it. It also provides guidelines how specific data is stored, shared, and disposed of. Confidential data may trigger a need of a secure server and more explicit authorization management, while public data may be shared and moved across IT landscape more freely. Password policy is an evergreen, yet it continues to cause the majority of security breaches. In fact one third of breaches can be attributed to internal actors and their compromised passwords. This policy shall not only stipulate strong passwords, but also their internal testing and regular change enforcement. Two-factor authentication is becoming a standard security measure, but only few end users possess the know-how of how to introduce it, maintain and audit it effectively and efficiently.

A third policy that may have a quick and relatively cheap impact is the implementation of a remote access policy. This policy guides the employees in accessing company resources from outside the office, usually by means of virtual private networks (VPN). VPN is a simple starting point in securing information and data flows. To achieve its full protective potential, however, digital transformation leaders shall think of how to monitor and control the flow of individual data elements, not only the connectivity pipe. To address this challenge, robust DLP strategies need to be co-created that are specifically designed for remote work. This may include more detailed and centralized access management or network segmentation to create multiple layers of protection. DLP is an ongoing process, and companies need to continuously monitor and update its evolution to stay ahead of threats.

There is no single silver bullet in creating a secure digital experience. However, the key pillars of your successful (and effective) cybersecurity strategy are found in vigilance, pro-activity of systems architects and leaders, and continuity in bringing the topic to the attention of the board, the employees, and business partners.