Проблеми та перспективи підприємництва
в умовах цифровізації економіки

THE SECURITY CHALLENGES OF HYBRID WORK FORMATS IN A DIGITAL ECONOMY

Viktor Sabadash
Ph.D., Associate Professor,
Viktoriia Sabadash
student
Sumy State University (Ukraine)

The digital transformation of the business environment and communication has become a defining economic trend during the coronavirus pandemic. Entrepreneurs are forced to attract and use new business formats in almost all areas: production, logistics, communications, competition, business support strategies. Companies make a large number of business contacts and communications through various technological channels.

Hybrid (remote, blended) work of staff has become a fairly new and risky format of cooperation in the business environment. The changes require additional costs of the company's resources, both tangible and intangible. The format requires not only organizational, communicative, technological, managerial, legislative changes, but also emotional and psychological modifications of established models of work. Remotely work (outside the office and the team) and hybrid work formats have provoked a wave of psychological disorders and disorders in employees, the syndrome of "emotional burnout", and other mental problems.

Models of behaviour of employees and employers are undergoing the most radical changes. In Microsoft's Annual Report (2021) "Work Trend Index" identifies seven main trends every business leader needs to know in 2021:

1) flexible work is here to stay;

2) leaders are out of touch with employees and need a wake-up call;

3) high productivity is masking an exhausted workforce;

4) Gen Z is at risk and will need to be re-energized;

5) shrinking networks are endangering innovation;

6) authenticity will spur productivity and wellbeing;

7) talent is everywhere in a hybrid work world [1].

While maintaining the relevance of these trends, we identify another important aspect of the hybrid business format – the security challenge. The volume of the key resource of the economy – information – has grown significantly over the past few times. The development and success of digital transformation are closely linked to the quality of information and conditions of use. The problem of business information security is a priority for companies.

Modern business operations are impossible without significant amounts of information and data. The amount of information on the market is growing geometrically. Information differs (quite significantly often) in both quality and usefulness for business.

The widespread use of cloud services by companies has greatly simplified and facilitated business intelligence and decision-making on the one hand, but has also increased the vulnerability of company databases to cyberattacks on the other. Commercial losses for global business from unauthorized access to company databases, cyber-fraud and cyberattacks are (according to cybersecurity experts) from 3 to $12 million every minute!

The complexity of decision-making in business is caused by the circulation in the information space of a significant amount of false (incorrect, distorted) information, incomplete data, inside, fakes, etc.

Procedures for accessing, owning, using, transmitting, and storing large amounts of commercial data and information have very serious gaps, both technological and legal. The “open” business environment is largely vulnerable to commercial threats and risks. We identify the following key aspects of cybersecurity for companies in the context of the “new normality” and digitalization of business.

Multifactor (multilevel) verification of customers, contractors, intermediaries, buyers, other economic entities to which the company provides (transmits) commercial

data, personal information, other important information. Many security programs, applications, applications already exist in the market of such services.

Protection of gadgets and devices used by the company (employees). It is desirable to provide secure access (entrance) from all points.

Development and implementation of principles (standards) of security of work with information and data in the corporate culture of the company. Increasing the level of responsibility for working with important commercial information, introduction of access codes, passwords, etc. in companies.

Use of security mechanisms for remote work of employees: encryption, access restrictions, keys, codes and passwords (change more often), monitoring of security of connection to external resources.

The company has a clear and comprehensive (preferably step-by-step) action plan in cases of cyber-attacks, cyber fraud, violation of a company's "security shell", loss or intentional transmission of data and information to others, virus attacks and more.

Introduction of the principles of "digital hygiene" of employees and permanent programs (seminars, trainings) to increase the "digital literacy" of staff in the corporate culture of the company.

Collaboration with IT companies (developers and suppliers) that specialize and have established themselves as non-existent partners in the market of software and security systems for business.

Neglecting data protection and security can lead to business failure. Companies need to realize that half-measures do not work effectively for the future. Point, non-complex actions are a trigger for more serious security issues for the company.

Stakeholders, business owners, CEOs, top-management should become the drivers of secure business changes.

A responsible, conscious and comprehensive approach to building an effective security system, a kind of "security fortress", is the key to productive and successful work of the company, even in remote or hybrid work of staff.

Reference:

1. The Next Great Disruption Is Hybrid Work – Are We Ready? Work Trend Index: Annual Report. Microsoft Corp., March 22, 2021. URL: https://www.microsoft.com/en-us/worklab/work-trend-index/hybrid-work (date of application: 03.05.2021).