Organisations in Digital Age – Information Security Aspects of Digital Workplaces

Csaba Kollár

assistant professor
drkollarcsaba@gmail.com

József Poór

professor of management
poorjf@t-online.hu

Abstract: The digital age – although differently in each sector and area – is present in the life of all the companies. It means not only the IT support of planning, production, manufacturing, warehousing, trading, etc. processes, because they have already been applied for several decades and developed permanently. The digital age strongly affects the entire company, all the divisions, departments, sites, and all the employees and executives working there. The concept of digital workplace, however, goes beyond the traditional physical framework of the company, because teleworkers, suppliers and customers are also connected into the IT processes. The information has become a new type of economic commodity, acquiring, possessing or owning it, and the control above it has become an increasingly serious and complex aspect of the company's success. In spite of the fact, that the success of the business is the well-understood interest of the company's stakeholders (employees, employers, owners, suppliers, etc.), in a lot of cases the (not always) ethical hackers dealing with social engineering are able to find the weak points of the company's information system through the human side of information security, due often to human negligence and irresponsibility. Our own research – involving more than 400 people from the executive staff of Hungarian companies – has led to the conclusion that only a very few of them have appropriate information security awareness. Therefore a chapter of our study introduces some possible forms of human attacks against digital workplaces and the prevention of these attacks.

Keywords: information security, social engineering, digital age, organization, workplace, employee

1 Our present age, the digital age

1.1 Introduction

The digital age first had existed parallel with, but later replaced the information age. The most typical feature of digital age [1] is that the phenomena, reaching us from the outside world and perceived (heard, seen, etc.) or not perceived by our senses, are digitalized at the earliest possible stage of information processing. These products can be shared with much more people and more quickly (contagious spreading) than conventional goods. When a digital date/information is entered in a network environment, it becomes practically undeletable. The digital age started in the first decade of the 21st century. Although its antecedents had been described earlier [2], the fundamental works were published later [3], and [4], as well as [5] and [6]. The digital age has brought some new economic and social models and some processes have begun in the information society with the help of which people (including all the aspects of the concept) have started to use IT devices and applications (hardware and software) on a daily level, and they have become connected with each other regardless of their distance in the physical world (wired world). In addition to money (and sometimes even overtaking it), information (the sacrifice made for obtaining it, the content, the analysis of its content, etc.) has been gaining weight.

1.2 Employees in the digital age

At the moment the groups of veterans, baby-boomers, X, Y, Z and the alpha generations can be distinguished in the society. As employees, the veterans (born between 1925 and 1945) are mostly out of the labour market already, while the members of alpha generation (born after 2010) are not yet on the labour market.

Out of the generations, the baby-boom generation (born between 1946 and 1964) makes up a significant proportion of labour market, but many of them are preparing to retire now. They use the digital devices, but they first met these at the age of 30-40. The members of X generation (born between 1965 and 1979) form the backbone of the labour market (together with the members of baby-boom generation, they are mostly the employees aged above 45 years). They met digital devices as teenagers. The members of Y generation (born between 1980 and 1995) are the careerists, because most of them have several years of work experience or still study somewhere. For them the use of digital devices – since they have been using these from their early childhood – does not mean any problems. The Z generation (born between 1996 and 2009) was dripped into the world of internet, they are still studying or some of them are already employed. Those born in the last third of Z and Y generations (after 2004) are very interesting in regard to

workforce management, because they represent different set of values, and work differently than their predecessors. They are less in numbers, the labour market demand is increasing for them. It is a problem, that there is one pensioner per 2.4-3 members of Z generation in the developed countries which is going to pose serious challenges for the state care systems. Those who were born after 2004 have difficulties to tolerate the corporate regulations, they are harder to integrate into the business organisation. One of the reasons is that, as freeters, they have built personal brands and work towards self-realization. The realization of their own dreams is much more important for them than to achieve the objectives and represent the interests of the company. They long for freedom, and they usually achieve it due to their status on the labour market. They might be ready even for unemployment or atypical employment. Since they know and confidently use the latest digital devices, techniques, applications and services, it is not a problem for them to be engaged in teleworking, to understand teleworking processes and to actively participate in them. They punish, although not deliberately, the older employees (digital immigrants) because they move more comfortably in the (virtual) working environment built up by bits and bytes, and they are impatient and less tolerating with their older colleagues who have only shallower knowledge and make slower use of devices.

The members of the above mentioned young generation(s) pose new challenges to the organisations. Due to the increasing generation gaps (the basis of which is the seemingly irresolvable digital gaps), and the lack of understanding of the "special" functioning of younger employees, the knowledge, role plays and case analysis connected with Z generation have been included in the further training of the (senior) executives of companies and in the range of professional services (e.g. coaching) offered for them. Although the traditionally functioning HR of the companies know and, some of them, apply the atypical forms of employment for a smaller group of employees, but they are not prepared to change the employment policy of the company in order to include mostly freeters and teleworkers in it. In theory, there are many good reasons for atypical employment, but at the moment, - besides the members of Z and Y generations and disabled employees - neither the X generation and the baby-boomers, nor the employment side or the business organisation itself are able to provide work organisation, working conditions or to create value based on digital platforms (teleworking). The atypical employment is approved and frequent in case of project companies and startup enterprises, but their current contribution to the GNP is minimal.

1.3 Employers in the digital age

The digital age is not simply a problem to solve for the company with a clear beginning and end, similarly to a project plan. The change-over to the digital age is a long-term decision which requires serious reorganization regarding the whole operation of the company, (internal) training, reconsideration of work processes,

more adequate measuring of performance, (hopefully) seamless connection to suppliers, (corporate) buyers, radical transformation of the content and platforms of internal-external communication – just to mention some of the main areas. The change-over concerning multiple areas is a lot easier for smaller or newly established enterprises, startups (the use of digital platforms from the beginning), while the larger companies, or those operating for a longer time, usually determine in multiple stages/milestones how to realize the transformation according to the requirements of the digital age e.g. in regard to employer and employee relations. Schillerwein [7] in his Infocentric study in 2013 distinguishes four steps of this process, as it is described in Table 1:

	First step	**Second step**	**Third step**	**Fourth step, and then…**
Title	Basic Intranet	Extended Intranet	Basic Digital Workplace	Full Digital Workplace
Business focus	Give information	Enable general interaction	Support actual work	Business transformation
Focus of applied technology	Ensure content	Cooperation	Portal and search	Other, specified by the company
Main features	(Internal) news Information libraries Self-service solutions for employees Simple applications	Basic social media and cooperation General process support Extended employee profiles Updated applications Personalization (customization)	Developed social cooperation Developed integration and applications Strong employee profiles Developed and more determined processes (eg.: project, innovation, frontline management) All kinds of information support and processing	Holistic process support in the whole organisation and beyond Meta-functionality (e.g.: social, cooperation) integration in all the areas Content- and intelligent filtering Almost smooth integration Universal inboxes Permanent transformation of the company Driving force: change, culture, commitment

Table 1
From the Intranets to the Digital Workplace

The employer side – especially the (top) executives in decision-making situations – should change employees, organisations and the tools/processes with the help of (reformed) way of thinking, considering the capabilities and abilities. McConnell [8] identifies nine areas which concern the company in the digital age and in the replies given to the challenges of the digital age:

1 Leadership: pays attention to all the parts and all the levels of the company which have impact on changes. If required, the furthermost parts (e.g. subsidiaries, foreign branches) should be directly involved, monitored and directed.

2 Organisational culture: employee attitudes, expectations and behaviour in an open, receptive working environment. If required, the basic values forming the organisational culture should be changed.

3 Organisational processes: Launching new and updated organisational/business processes which integrate the social collaboration. If required, significantly more independent/freelancer developers, testers, test buyers, business partners should be involved even in the early phase of processes.

4 Organisational structure: virtual operational environment, where groups, communities and networks cooperate. If required (1) the operational environment should be extended to the social media (e.g. the Facebook page of the company where the customer/consumer reactions can be permanently tracked), (2) a new virtual operating environment should be developed which increasingly meets the comfort and communication requirements that have already been usual in the physical world.

5 Access: equal, relevant and interactive access for all the employees in the whole working process, so that they can connect to the (protected) IT resources of the company from anywhere, anytime with any type of communication device. If required, the IT department of the company should be supported with more funds in order to ensure the due implementation of all the developments which ensure the maximum protection of company databases and other resources against unauthorized hacking/break-in .

6 Company: cooperation in all directions, including the entire company. If required (1) the (digitalised) platforms of cooperation with suppliers, subcontractors and customers should be reconsidered and changed; (2) the seamless cooperation of colleagues should be supported with all kinds of (organisational development) tools, methods and possibilities (e.g. training, courses, joint programs, playful competitions).

7 Business: the clients, partners, users and buyers of the company's products and services should be served to the maximum. If required, new digital communication platforms – which meet their needs – should be introduced and regularly used (e.g. WEB 2.0).

8 Personal development: supporting programs which focus on creative, cooperative employees, who are glad to share their knowledge/expertise, permanently develop their knowledge, easily work in teams and easily adapt to the permanently changing environment. These programs aim to develop these types of competencies, skills/abilities. If required, the above qualities should be put in front of the actual professional knowledge (it is easier e.g. to train a

programmer than to find an employee with the above detailed parameters or to develop these abilities in the current ones).

9 Resource-evaluation: the digital work environment/workplace is regarded as strategically important and inevitable resource which is a key to the future of the company. If required, the corporate values and resources should be reconsidered and even the basic charters (philosophy, mission, vision) re-defined.

2 Information security of digital workplaces

2.1 Introduction

In our opinion, the ideas about digital changeover [7] and [8] as well as the digital challenges concerning the organisations ignore a very important area, namely the information security. The data, information and the knowledge created from this, has become an asset, and it has resulted increasingly stronger cybercrimes [9], the victims of which – especially the victims of criminal groups – are not only individuals, but the company itself, including the staff, leaders and top executives. The attacks are not simply pranks, but crimes causing serious damages to the company. While at international, and thus at European level, the companies in almost all the countries address the protection and security of data from IT aspects [10], the human factor, as well as the social engineering focusing on it, is still a critical area in information security

2.2 The social engineer

Social engineers – although they use some IT solutions – are rather special because they possess some practical psychological and communication knowledge, and - adapted to the given situation - apply it efficiently. The social-engineer-type attackers can be the staff, leaders, interns of the company, professionals dealing with the activities of the company, employees and leaders of suppliers, customers, as well as staff and leaders of corporate customers, clients, partners, visitors, staff of sub-contractors, practically anybody. According to a former survey done by Deloitte Touche Tohmatsu [11], 91% of company representatives think that their employees directly or indirectly can pose a threat in IT sense. More than three-fourth of them, however, do not enable their staff to collect knowledge or to update their current knowledge concerning information security. Although in the last eight years, information security awareness has moved in the right direction in Hungary (too) and part of the managers (especially

the members of Y and Z generations) are committed (or said to be committeed) to information security, the daily practice proves that even a not-too-creatively elaborated social-engineering-type attack can succeed.

Empirical research

The present study regards all the places as digital workplace where work is made with the help or with the use of info-communication devices, data are created, processed, stored, modified, handled, analysed, conclusions are drawn, then, after some time, these data are destroyed. Thus, besides the sites used for official working activities by the company and/or its partners, the concept is extended to the sites of meetings and talks (e.g. restaurant, tea rooms), the home offices of teleworkers and partners, as well as other places suitable for working. Due to the expanded interpretation of the concept, the employee who has appropriate info-communication devices (laptop, tablet, smart phone), applications, and usually permanent internet connection can work anywhere.

Our hypothesis are as follows:

- Hypohesis one: The majority of corporate executives and managers are very uninforemed of new challeges of information securiry.
- Hypthesis two: While the company – in theory – can have stronger control of the information protection of fixed devices (e.g. desktop computer) of offices, workshops, etc. in its own or rented buildings, in case of portable devices, these regulations – which are usually available in written form as well - can be easily breached, either deliberately or by negligence and carelessness.

The opinion of Hungarian executives regarding digital age was surveyed with the help of an online questionnaire of multiple questions between December 2015 and January 2016. The title of the survey was: Organizations in the digital age. All those staff members were regarded as leaders who line-managed at least one employee and had decision-making competency in certain questions.

Altogether 406 people gave assessable responses to the questionnaire. Due to the limits of the study, it should be mentioned that regarding the acronyms which describe the digital age, the survey asked the concepts belonging to the acronym CAMSSA (cloud, analytics, mobile, social media, security and augmented reality) in open question.

It turned out from the analysis of more frequent and more interesting responses that some of the interviewed executives did not even know the information security risks of the mentioned areas. Regarding the security notion of digital age, we did not want to narrow down the response opportunities by asking the leaders to focus only on data, IT and information security. In spite of this, their replies

concerned, almost without exception, the data security, network security, IT system, access codes and antivirus protection. They did not mention the human aspects of information security or social engineering at all, although the digital workplaces can suffer from social engineering type attacks. The most frequent are as follows:

- Collecting information from the staff in places adjacent to the company (e.g. freely accessible places – courtyard, designated places for smoking, restaurants nearby). The most frequent methods of protection are:
  - preparing the staff for situations like these,
  - excluding those from the conversation who are strangers to the group,
  - the topics of the conversation are about e.g. the hobbies of the colleagues, and not about the company,
  - when it is not being used for entering or identification, the access cards of the staff (ID cards with names and photo) should be held in a way that the data on the card cannot be seen by others. If the card is lost, it should be reported immediately.
  - business lunches should not be held in places where the intimacy of the talks cannot be ensured (although technically a conversation can be easily tapped in any of the public places),
- Unauthorized intrusion in the protected/guarded areas of the company (sites, headquarters, warehouses, office buildings, including offices). The aim can be manifold: to steal info-communication devices, obtain access codes to devices, then, in the possession of these, to steal valuable data and/or uploading harmful applications on the devices. The most frequent methods of protection are:
  - strict admission control (e.g. recording personal identification documents),
  - short-spoken information to the visitor (the history of the company and the actual gossips should not be shared) ,
  - a phone call to the colleague who hosts the visitor in order to check if they expect visitors indeed,
  - providing the name of the expected visitors to the security guards prior to the visit,
  - locking the doors of offices when staff is not in,
  - shutting down the computers or switching to sleep mode with password protection when staff is not nearby or in the office ,
  - destroying all the office waste created in the office (e.g. contracts, drafts, reports) in a professional way.

- Unauthorized intrusion in the home or home office of teleworkers. Since they are the furthermost from the focus of information security of the company, the implementation of protection is the most difficult in these cases. The company can do the following:
  - can make the employee aware of the possible attack,
  - can provide increased protection for the info-communication devices used by the employee for work (e.g. password entry, tracking in case of being stolen, remotely controlled switch of camera and/or microphone),
  - can ensure the protection of the working environment at home and provide financial support for the purchase of a shredder for the employee if necessary,
  - can regulate what platforms and which places are to be used for work by the teleworking employee.
- Attack from a partner (e.g. supplier, corporate buyer). These attacks can be ranked in two groups: (1) deliberate attack on behalf of the partner, (2) attack using the good faith or inattention of the partner. In these cases the intruder attacks not only the company, but the partners as well. The harmonization of this area is one of the most difficult corporate tasks because the companies should share their regulations concerning information security with each other, in order to develop an efficient and joint safety awareness.

Conclusions

The first part of our study discusses digital age and the employees of digital age. By segmenting the employees according to generations we underlined that the members of the younger generation(s) pose new challenges to the organisations. There is not only a generation gap in regard to info-communication tools and applications used by the generations, but new types of management procedures and the increasing share of atypical employment forms should also be considered. The transition into the digital age is not a one-time job, the companies and the employees should permanently implement the solutions, services and developments offered by digital age, in order to maintain their market positions and competitiveness. The highest stage in this process is the Full Digital Workplace where business transformation is put in the focus of business. It has been concluded that although digital age concerns the companies in several fields (according to our references: in nine fields), the information security - especially the human information security – is not really discussed by the referred authors. Our theoretical statement has been examined empirically, too, by analysing the responses given to our survey by more than 400 employees working in executive status. Both of our hypotheses can be regarded confirmed because (1) the majority

of corporate executives and managers appeared to be uninformed concerning the new challenges of information security; (2) the majority of the surveyed companies know IT regulations only regarding the physical locations and equipment belonging to their own supervision, and beyond this, they handle the issues with a certain negligence. That is why, in the last chapter of our study, we consider it important to introduce the main social engineering type attacks on companies, as well as the frequent ways of protection against these attacks.

Finally it should be noted that there are more and more hacker attacks against companies which indicates that information security should be given much higher priority than before. The analysis and evaluation of attacks, as well as the honest and objective internal communication about attacks can be the basis of moving the security attitude of employees in positive direction.

References

[1] Kollár, Cs. (2014). *Communication in the digital age.* Budapest, HU: PREMA Consulting.

[2] Dyson, E. (1998). *Release 2.0*. London, UK: Broadway.

[3] Saphiro, C. & Varian, H. R. (1999). Information Rules: A Strategic Guide to the Network Economy. Boston, MA: Harward Business School Press.

[4] Levine, R., Locke, Ch., Searls, D., Weinberger, D., McKee, J., Rangaswami, J. P. & Gillmor, D. (2001). *The Cluetrain Manifesto: The End of Business as Usual.* New York, NY: Basic Books.

[5] Kehal, H. S. & Singh, V. P. (2004). *Digital Economy: Impact, Influences and Challenges.* London, UK: Idea Group Publishing.

[6] Lessig, L. (2004). *Free culture. How Big Media Uses Technology and the Law to Lock Down Culture and Control Creativity*. New York, NY: Penguin Group.

[7] Schillerwein, S. (2013). *Digital Workplace Framework.* (electronic presentation): http://www.slideshare.net/IntranetMatters/digital-workplace-framework?related=1

[8] McConnell, J. (2015). T*he Workplace in the Digital Age.* (electrinic presentation): http://www.slideshare.net/NetJMC/e2-summit2015-netjmc

[9] Mitnick, K. D. & Simon, W. L. (2005). *The Art of Intrusion: The Real Stories Behind the Exploits of Hackers, Intruders and Deceivers.* Indianapolis, IN: Wiley Publishing.

[10] Schneier, B. (2008). *Schneier on security*. Indianapolis, IN: Wiley Publishing.

[11] Oroszi, E. D. (2008*). Social engineering*. Budapest, HU: BCE