How to cite this article:
Prigoda, L., Cekerevac, Z., Dvorak, Z. & Cekerevac, P. (2015, Apr 19). *One look at the modern information security*. Sustainable Development of Mountain Territories. 4(22). ISSN 1998-4502.

ONE LOOK AT THE MODERN INFORMATION SECURITY

Ludmila Prigoda[1], Zoran Čekerevac[2], Zdenek Dvorak[3], Petar Čekerevac[4]

Modern business is linked to massive use of the Internet and mobile communications. Use of these communications can compromise the integrity and confidentiality of data during their transmission and their storage. Remarkably rapid development of IT allows efficient data protection, but also gives new opportunities for eavesdropping and spying. Even with the latest protection there are ways to access data unnoticed. The topic becomes more significant when one considers the recent events related to an affair with wiretapping of internet posts by the NSA. This paper discusses the current state of the e-business, in particular the protection of data and electronic mails.

Keywords: Information, information technology, information security, data protection, wiretapping, electronic mail, law, e-business, data communication, internet

1. Introduction

Modern business, including all forms of contact between stakeholders, cannot be realized without massive use of electronic communications. In business communication e-mail and cell phones are indispensable components. While companies want their marketing information available to public, they certainly want maximum protection of payments and e-mails. Since such information is for the attackers most interesting battle over the protection of information intensifies.

Electronic fund transfers, especially credit and debit cards as well as payments via the Internet are most commonly used for non-cash payments. Recently, the mobile banking and bitcoin system began to be used for payments, although their application is still relatively limited. According to the annual report of the European Central Bank (ECB) in respect of non-

[1] Prof. Dr. Ludmila Prigoda, Maikop State Technological University, Maikop, Russia
[2] Prof. Dr. Zoran Čekerevac, Faculty of Business and Industrial Management of the „Union“ University Belgrade, Serbia
[3] Prof. Ing. Zdenek Dvorak, PhD, Faculty of Special Engineering of the University of Žilina, Žilina, Slovakia
[4] Petar Čekerevac, MSc, Libek, Belgrade, Serbia

cash payments, the credit card payment covered 41% of all transactions in 2011. (European Central Bank, Payment Statistics for 2011, 2012)

In 2012, the growth of non-cash payments in relation to the previous year was 4.2% and reached 95.5 billion EUR. Card payments reached 42%. (European Central Bank, 2013) In recent years, mobile banking has been rapidly growing. This growth is not evenly distributed, as can be seen on figure 1. The mobile banking is most common in Sub-Saharian Africa and involves mainly micro-payments provided by mobile providers.

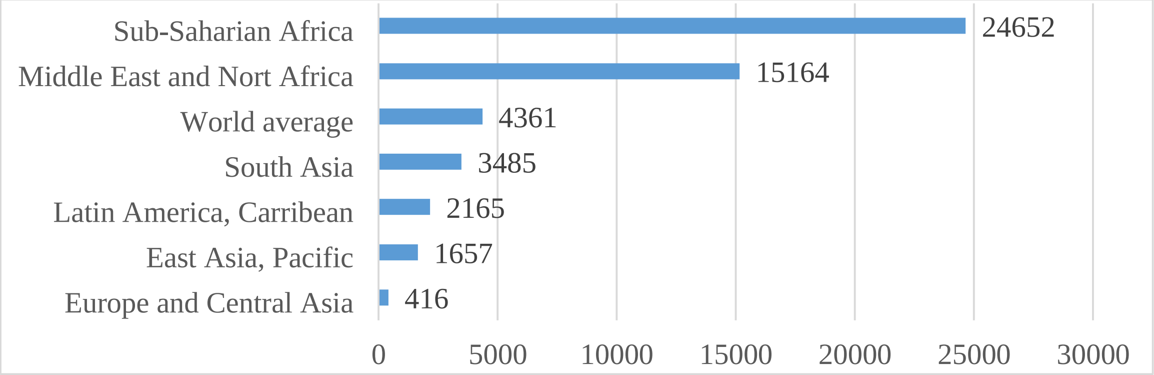

Fig. 1 Mobile financial accounts per 100,000 adults in June 2013 (Source: Groupe Speciale Mobile Association, World Bank (Stevis & McGroarty, 2014)*)*

Banks have realized that mobile providers attract a large number of their clients and they are also beginning to get involved in this type of business. (Stevis & McGroarty, 2014)

According to the results of Osterman Research (Symantec, 2013), 74% of intellectual property of organizations resides in emails as a text or as an attachment. Based on the report of The Radicati Group, Inc. shown in Table 1 it can be seen that it is estimated that in 2013 little less than four billion e-mail accounts (addresses) were in use and that number will increase by over a billion new account over the next four years. About one quarter of all accounts are accounts that are used exclusively for business purposes. It is certain that a large number of private accounts is also used for business purposes.

Table 1 Private and business e-mail accounts 2013-2017 (an estimation)

	2013	**2014**	**2015**	**2016**	**2017**
Worldwide Email Accounts (in M)	**3,899**	**4,116**	**4,353**	**4,626**	**4,920**
Business Email Accounts (in M)	**0,929**	**0,974**	**1,022**	**1,078**	**1,138**
% Business Email Accounts	24%	24%	23%	23%	23%
Consumer Email Accounts (in M)	**2,970**	**3,142**	**3,331**	**3,548**	**3,782**
% Consumer Email Accounts	76%	76%	77%	77%	77%

Source: Radicati & Levenstein (2013)

Mobile communications are extremely popular, if not the most massive form of communication. It was expected that in early 2014 number of cell phone will surpass world’s population (Betakit, 2013) (Pramis, 2013) Based on the statistical data of the World Bank (The World Bank, 2013) by number of mobile phones per 100 inhabitants, list leaders are Macao with 284, and Hong Kong (SAR, China), with 228. At the bottom of the list are Eritrea with 5.4, and Somalia with 6.7. Appropriate number of mobile phones in the United States is 98.1, in the UK 130.75, in Serbia 92.8, and in Germany 131.3.

In view of these data it is easy to perceive the wealth of information that is transmitted daily through communication channels. It is certain that many are interested in collecting data from the communication channel in order of their use or after use.

2. Facts

Every user of the Internet, credit card or mobile phone could easily assume that in addition to being the service user, being at the same time an object of observation, but there are very few who were aware of the size and scope of resources of espionage of communications. A storm around email security and data circulated by e-mails was sharply raised in mid-2013. (Čekerevac, Čekerevac, & Vasiljević, 2013) Although it is believed that the application of a desktop computer, gateway encryption and transmission of electronic mail is safe even in the cloud, Edward Snowden (Snowden, 2013) showed that this was not the case, and that the electronic mails, and not only them, are actively monitored and intercepted. Based on The Guardian series "Glenn Greenwald on security and liberty" (Greenwald & MacAskill, 2013) National Security Agency (NSA) has direct access to the systems of Google, Facebook, Apple and other American Internet giants. In the top-secret document whose content was published by authors, NSA access was part of the previously undisclosed program called "Prism", which allows agencies to collect metadata, including browsing history, e-mail contents, file transfers, and live chats. For example: ”for a telephone conversation, metadata would include the called number and the calling number as well as the duration of call“. (NSA, 2009) Greewald and MacAskill (2013), they argue that the data were collected directly from major American internet service providers.

A favorable circumstance for attackers is rapid growth of smartphones. According to M. Rosenbach , L. Poitras, and H. Stark (2013), smartphones are possessed by more than 50% users in Germany, and two-thirds in UK. In USA, about 130 million users use smartphones. There are a variety of applications prepared for smartphones. According to Rosenbach (2013) there were more than 400,000 applications for iPhone, but it can also mean that there is the same number of possible vulnerabilities. Smartphones as the data storage units, at the same time, are a goldmine, “for an agency like the NSA,…, combining in a single device almost all the information that would interest an intelligence agency: social contacts, details about the user's behavior and location, interests (through search terms, for example), photos and sometimes credit card numbers and passwords.“ (Rosenbach, Poitras, & Stark, 2013).

Electronic mail as an important collection of data is particularly interesting. In accordance with the 18 U. S. Code § 2703 a distinction is made between the various e-mail messages depending on their age. 180 days rule is applied. This is explained in detail in A User's Guide to the Stored Communications Act - And a Legislator's Guide to Amending It (Kerr, 2004), but it is important to note that “If an unopened email has been in storage for 180 days or less, the government must obtain a search warrant.” and “If a communication has been in storage for more than 180 days or is held ‘solely for the purpose of providing storage or computer processing services’ the government can use a search warrant, or, alternatively, a subpoena or a ‘specific and articulable facts’ court order (called a 2703(d) order) combined with prior notice to compel disclosure. Prior notice can be delayed for up to 90 days if it would jeopardize an investigation. Historically, opened or downloaded email held for 180 days or less has fallen in this category, on the grounds that it is held ‘solely for the purpose of storage.’” (Kerr, 2004)

The legal basis for the collection of data lies in USA Patriot Act (2001), Protect America Act of 2007 (2007), Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008 (2008), 18 U.S. Code § 2701 - Unlawful access to stored communications (2701, 2012), 18 U.S. Code § 2703 - Required disclosure of customer communications or records (18 U.S.C. 2703, 2012), and others.

3. Company Information security and modern challenges

The use of Internet provides a lot of advantages and cost-savings to every company, but at the same time it brings significant care about data security. When the information is within company’s LAN, data are safe, but almost every LAN is connected to the Internet, and employees hardly resist not to use company’s computers to connect to different social media. Allowing interactive access to their partners or even customers, companies make their document to be Internet friendly, but this also facilitates the task of potential attackers. Modern way of doing business implies growing outsourcing and its influence. There are also numerous laws which need to be incorporated in everyday’s functioning of a company. They help company to protect itself, but also to avoid to be penalized through litigations in the courts of law. Some of them are listed in the article of A. Oloko (2011). In the modern age it is hard to determine all possible attacks to the company information system, from Trojan horses, viruses, warms, adware, spyware, rootkits, and backdoors, up to user errors.

To minimize risks a company should create (and use) information security policies. They are essential to secure business, and the company should create a "security culture", which means that policies needs to be distributed to employees and fully explained to them. W. Deutsch (2014) suggests six security policies:

1. Internet usage
2. Email/social networking
3. Key control
4. PDA/mobile device security
5. Visitor management
6. Non-disclosure agreement

He gives quick guide to procedure creation, and also suggests that "key to creating effective policies is to make sure that they are clear, and as easy to comply with as possible. Policies that are overly complicated only encourage people to bypass the system." S. M. Heathfield (2014) highlights that: "Voice mail, email, and Internet usage assigned to an employee's computer or telephone extensions are solely for the purpose of conducting Company business." In this light one should consider a software access procedures, Internet, email and social media usage. Each employee should pay a special attention to the fact that all his communications sent via company email or stored on company devices are company propriety.

In order to protect its resources, the company must use all available means. There is no sufficient level of protection, as the situation changes daily. According to MAAWG research (Ipsos, 2010), 33% German email users describes itself as "an expert" or "very experienced", in the U.K. (22%), the U.S. (21%), Spain (19%), and 8% in France. As it can be seen, there are significant differences between countries, but also between young and elderly persons. The same analysis was conducted about content of emails and user behavior when faced to spam messages. More than four of ten said that they opened email although the mail looks like spam, and not opened only. Around 20% opened spam emails or/and clicked on link in spam message. This risky approach is more common for young population of users. On the other side, according to the same source, around 60% (in average) of users believe that their computers were affected by viruses, but less than half were informed about meaning of the word "bot", although 84% were aware about bot concept. Two-thirds think that for their protection ISPs should be responsible. More than one half believes to anti-virus software companies, but a bit less than one half is aware of their own responsibility.

What a company or single user can do to protect data and privacy? First of all, hardware and/or software firewall should be installed to prevent hackers, viruses, or worms attacks. It is to recommend that anti-virus software has its firewall. Each computer should be clean, without unnecessary programs and applications, and each installed software should be kept up to date. Each computer should have its own anti-malware software, with at least daily scanning. Special attention should be paid to Wi-Fi and smartphones. Wi-Fi connections must be secured at least using WPA2. It is recommended that for financial transactions one separate computer is used. It should be wired connected to the network, and powered up only while it is used for making transactions. For e-mails use of encryption is recommended, including S/MIME (Secure/Multipurpose Internet Mail Extensions) or OpenPGP as it is explained in (Čekerevac, Dvorak, & Čekerevac, 2014).

All explained measures can reduce the risk from hacking by common hackers, but if the company or even the single user is of great interest to someone (or to the government), there is little chance that one can resist such attacks. How deep eavesdropping can go is explained in B. Gellman article (2013)

What is to expect? In the near future new EU General Data Protection Regulation is to be expected. Its draft was published in January 2012, and till now it got around one hundred amendments. Though the regulation should be implemented in 2015, it is known that it will affect EU business including cloud computing providers. The new regulation “requires data controllers (enterprises that own the data) and data processors (such as cloud providers and datacentre hosting companies) to share the liability for data breaches and violations of the law.” (Venkatraman, 2014) Problem is that only a few cloud service providers are prepared for the upcoming regulation.

4. Conclusions

Based on the presented analysis it can be concluded that the issue of data security of business enterprises and individuals is becoming more and more important. It is (and will be) very difficult to determine all threats, and thus all the harder to know which measures to undertake to secure data. Many of non US companies and single users will try to avoid use of Internet servers located in the US because of controversial rules in domain of Internet privacy. Also, use of the European servers will not guaranty privacy, because all governments have the same needs in data collecting. As users move away from VPNs, they will be exposed to more security risks. Operating systems will be changed aiming to provide more security, but generally it could be noticed that none of them give more security then old Unix. The main security treats are caused by software bugs. Security tools, including anti-malware, anti-virus, …, firewalls, they become more intelligent and useful, but they are still not reliable enough to satisfy users. They help in a lot of cases, but certain amount of actions are in wrong direction and make the use of computer uncomfortable. The main hope for ensuring data protection is cryptography. Today's encrypted messages are generally safe and practically it is uneconomic to decipher them because it takes too much CPU time. Over time, the hardware will become faster and it is likely that it will be necessary to increase the key length. But, sending and receiving encrypted messages is not so comfortable. Users need to exchange their private keys before transaction, and there is also a possibility of "the man in the middle" attacks. It seems that it is still best to take a thick book and create own encryption code, or very important information deliver in person. Any other information that travel through the Internet should be regarded as if it was withheld on the bulletin board that can never be erased.

Works Cited

18 U.S.C. 2703. (2012, 01 03). *18 U.S. Code § 2703 - Required disclosure of customer communications or records.* Retrieved from GPO: http://www.gpo.gov/fdsys/granule/USCODE-2011-title18/USCODE-2011-title18-partI-chap121-sec2703

2701, 1. U. (2012, 01 03). *18 U.S. Code § 2701 - Unlawful access to stored communications.* Retrieved from Cornell University Law School: http://www.gpo.gov/fdsys/granule/USCODE-2011-title18/USCODE-2011-title18-partI-chap121-sec2701

Betakit. (2013, 10 29). *Number of cell phone plans expected to surpass world's population in early 2014.* Retrieved from Betakit: http://www.betakit.com/number-of-cell-phone-plans-expected-to-surpass-worlds-population-in-early-2014/

Čekerevac, Z., Čekerevac, P., & Vasiljević, J. (2013, 09 07). *Internet safety of SMEs regarding the security of electronic mail.* Retrieved 09 19, 2013, from FBIM Transactions: http://www.meste.org/fbim/fbim_srpski/FBIM_najava/III_Cekerevac.pdf

Čekerevac, Z., Dvorak, Z., & Čekerevac, P. (2014). Internet safety of SMEs and e-mail protection in the light of recent revelations about espionage of internet communication system. *10*.

Deutsch, W. (2014). *6 Security Policies You Need.* Retrieved 08 18, 2014, from About.com: http://bizsecurity.about.com/od/creatingpolicies/a/6_policies.htm

European Central Bank. (2012, 09 10). *Payment Statistics for 2011.* Retrieved 12 02, 2013, from European Central Bank: http://www.ecb.europa.eu/press/pr/date/2012/html/pr120910.en.html

European Central Bank. (2013, 09 19). *Payment statistics for 2012.* Retrieved from European Central Bank: http://www.ecb.europa.eu/press/pr/date/2013/html/pr130910.en.html

FISA. (2008, 07 09). *H.R. 6304(110th): FISA Amendments Act of 2008.* Retrieved from govtrack.us: https://www.govtrack.us/congress/bills/110/hr6304/text

Gellman, B. (2013, 10 30). *NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say.* Retrieved from The Washington Post: http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html

Greenwald, G., & MacAskill, E. (2013, 06 07). NSA Prism program taps in to user data of Apple, Google and others. *The Guardian*. Retrieved 08 04, 2013, from http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

Heathfield, S. M. (2014). *Internet and Email Policy.* Retrieved from about money: http://humanresources.about.com/od/policiesandsamples1/a/email_policy.htm

Ipsos. (2010, 03). *Key Findings of the 2010 MAAWG Email Security Awareness and Usage Survey.* Retrieved from M3AAWG: http://www.maawg.org/system/files/2010_MAAWG-Consumer_Survey_Key_Findings.pdf

Kerr, O. S. (2004, 10 20). A User's Guide to the Stored Communications Act - And a Legislator's Guide to Amending It. *George Washington Law Review, 72*(6), 1-41. Retrieved from http://ssrn.com/abstract=421860

NSA. (2009, 03 24). *NSA inspector general report on email and internet data collection under Stellar Wind – full document.* Retrieved from theguardian: http://www.theguardian.com/world/interactive/2013/jun/27/nsa-inspector-general-report-document-data-collection

Oloko, A. (2011, 12 15). *Information Security in the Enterprise and Modern Challenges .* Retrieved from dataversity.net: http://www.dataversity.net/information-security-in-the-enterprise-and-modern-challenges/

PAA. (2007, 08 05). *Protect America Act of 2007.* Retrieved from U.S. Government Printing Office: http://www.gpo.gov/fdsys/pkg/PLAW-110publ55/html/PLAW-110publ55.htm

Pramis, J. (2013, 02 28). *Number of mobile phones to exceed world population by 2014.* Retrieved from Digital trends: http://www.digitaltrends.com/mobile/mobile-phone-world-population-2014/

Radicati, S., & Levenstein, J. (2013, 04). *Email Statistics Report, 2013-2017.* Retrieved from The Radicati Group, Inc.: http://www.radicati.com/wp/wp-content/uploads/2013/04/Email-Statistics-Report-2013-2017-Executive-Summary.pdf

Rosenbach, M., Poitras, L., & Stark, H. (2013, 09 09). *iSpy: How the NSA Accesses Smartphone Data.* Retrieved from SpiegelOnline: http://www.spiegel.de/international/world/how-the-nsa-spies-on-smartphones-including-the-blackberry-a-921161.html

Snowden, E. (2013, 06 23). *Edward Snowden News*. Retrieved from Edward Snowden News: http://edward-snowden.net/category/edward-snowden/

Stevis, M., & McGroarty, P. (2014, 08 15). Banks Vie for a Piece of Africa's Mobile Banking Market. *The Wall Street Journal*. Retrieved from http://online.wsj.com/articles/banks-vie-for-a-piece-of-africas-mobile-banking-market-1408122166

Symantec. (2013, 03 13). *Symantec Encryption Solutions for Email, Powered by PGP Technology.* Retrieved 08 01, 2013, from Symantec: http://www.symantec.com/content/en/us/enterprise/fact_sheets/b-encryption-solutions-for-email.pdf

The World Bank. (2013). *Mobile cellular subscriptions (per 100 people).* Retrieved from The World Bank: http://data.worldbank.org/indicator/IT.CEL.SETS.P2

USA Patriot Act. (2001, 10 24). *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001.* Retrieved 08 03, 2013, from epic.org: http://epic.org/privacy/terrorism/hr3162.html

Venkatraman, A. (2014, 08 12). *Only one in 100 cloud providers meet latest EU data protection requirements.* Retrieved from ComputerWeekly.com: http://www.computerweekly.com/news/2240226620/Only-one-in-100-cloud-providers-meet-new-EU-data-protection-requirements?asrc=EM_MDN_32854004&utm_medium=EM&utm_source=MDN&utm_campaign=20140818_Only%20one%20in%20100%20cloud%20providers%20meet%20latest%20EU%2