How Secure is the Integrity of Your Data?

Manjola Islami
Teaching Assistant at European University of Tirana
manjola.islami@uet.edu.al

Irena Kreci
Albanian-American Development Foundation (AADF)
i.kreci@aaef.com

Abstract

Nowadays, businesses are building bottomless real-time connections with their customers, suppliers, partners, and governments, collecting and selectively sharing huge amounts of data. The value of stored and in-transit information is rising rapidly, driving new markets and generating a need for securely connecting devices and delivering trusted data. Data integrity is a vital component in economy which can pertain to individuals, companies, governments and globally. It is a measure of the validity and reliability of a data. Data integrity can be compromised through human error, transfer errors, compromised hardware, alteration of source devices, or a range of cyber threats that manipulate data. What concerns the business and economy is threat to data integrity, which ensures the validity and soundness of data throughout its life cycle. The challenge of the business is the protection of data integrity and system security which ensures accuracy and efficiency of business processes as well as appropriate decision making. The industry evolves, and the cyber-attacks have become more sophisticated and more complex. Consequently, the businesses in all industries are investing more and more in security of the information. It is obvious that this money could be invested in different things, but the vulnerability of the information has become crucial in a network and internet environment. The actions for data integrity protection relate to systems used and human resources awareness. We need to accept that all risks will never be eliminated, that nothing is permanently safe, and however a strong business reputation depends on a robust data privacy and information security.

Keywords: *Data Integrity, Data Protection, Data Security, Cyber-attacks, Threats*

Introduction

Companies collect, process, report and store large volumes of data in their normal course of business. The ability to examine, analyze and act on data is becoming more and more important to all companies. The Internet allows businesses to use information in a more effective way, by allowing the stakeholders such as customers, suppliers, employees, and partners to get access to the business information they need, how and when they need it. Customers can use the web to place purchase orders which can be fulfilled more quickly and with less effort and less error, suppliers can receive orders as they are placed, reducing or eliminating the need for inventory or stock, and employees/management can obtain timely information about business operations. The Internet also makes possible new, innovative and flexible pricing mechanisms, such as online competitive and comparable bidding for suppliers, and online auctions for customers. These Internet-enabled services translate to reduced costs due to less overhead cost, greater economies of scale, and increased efficiency due to easy and timely access to information. The greatest ability of e-business is being well-timed, more helpful and valuable information accessible to more people, at the same time, at reduced cost of information access. The pace of change requires companies to be able to react quickly to changing demands from customers, offer from suppliers and business environmental conditions. Although prompt action may be required, decisions are more complex as companies compete in local markets, region and in a global marketplace. Managers may need to obtain and understand high volumes of data before they can make the necessary required decisions on running the business. On the work side, the workplace environment has become more dynamic, workforce is highly mobile, and the expectations from the employees rapidly change. Consequently, the concept of a network perimeter is blurred. Employees no longer stay within the confines of a trusted business network, or the restrictions of a specific post or device, making them more productive and efficient, but more difficult on the security point of view. Wearable, accessories, gadgets, sensors, and other things on the internet are creating new connections which expose new vulnerabilities. All information technology products that connect to the internet or internet based networks face the full force of nowadays risks and threats. Privacy of communications is essential to ensure that data cannot be modified or viewed while in transit. Dispersed environments bring with them the possibility that a malicious third party can perform a computer attack by interfering with data and information as it moves between sites. While putting business systems on the internet and

internet based networks offers potentially unlimited opportunities for increasing efficiency by reducing cost and time, it also offers potentially unrestricted risk and threats to the companies. The internet provides great and more important data information, not only to valid and proper users or stakeholders, but also to business spies, hackers, and other potential criminals. The one constant in cyber-security is continuous change. The industry is evolving due to changes in technology, great value of potential targets, the increased demand, capability of attackers, and relevance of resulting influence and impact.

Data integrity

Data integrity refers to the accuracy, consistency (validity) of data over its lifecycle (Cucoranu et al, 2013). Compromised data is of little use to enterprises, not to mention the dangers presented by sensitive data loss. Consequently, data integrity is one of the most critical elements in any system (Subashini & Kavitha, 2010) and it is a core focus of many enterprise security solutions.

Data integrity defines the quality of information, which guarantees the data exist, is accurate, complete, and has a whole structure. Data integrity is preserved only if and when the data is satisfying all the business requirements and important rules and regulations. These requirements and rules might be how data is processed, linked, validity of details and content, etc. According to data architecture principles, functions such as data transformation and data storage, must guarantee the integrity of data, which means, data integrity should be maintained during input, transfer, storage and retrieval.

The data can be considered consistent and can be given the assurance to be accurate and reconciled if data integrity is well-preserved. In terms of data integrity in databases, should be ensured that the data stored in the database corresponds exactly to the real world details it reflects.

Data integrity can be compromised in a number of ways. Each time data is reproduced or transferred, it should remain unchanged and uncorrupted between updates. Error checking and detecting methods and data validation procedures are typically relied on to ensure the integrity of data that is transferred or reproduced without the intention of alteration.

The term data integrity may lead to confusion because it may refer either to a state or a process. Data integrity as a state defines a data set that is both accurate and valid. Furthermore, data integrity as a process, describes measures used to ensure validity and accuracy of a data set or all data contained in a database or other construct. For instance, error detection and data validation methods may be referred to as data integrity processes.

Maintaining data integrity is important and key to the companies for several reasons as data integrity ensures the accuracy of the information recoverability, searching ability, traceability connectivity and analysis. Protecting the validity and accuracy of data also increases stability, performance and drive decision-making considering the data can be maintained and reused when needed.

Data integrity drives enterprise decision-making, but it may undergo a variety of processes and organizing changes to transform from raw form to usable formats as needed and practical for reporting, analysis and facilitating the users' decisions. Therefore, data integrity is key and a top priority for all enterprises.

There are variety of ways which compromise data integrity making data integrity security practices an essential component of effective enterprise security procedures and actions. Data integrity may be compromised through:

- Transfer errors, including unintended alterations or data compromise during transfer from one device to another;
- Human error, whether unintentional or malicious;
- Viruses or malware, hacking, bugs and other cyber threats;
- Compromised hardware, whether a device or hard-disk crash;
- Physical compromise to computer or data storage equipment.

However, only some of the abovementioned compromises may be adequately prevented through data security. Consequently, data backup, duplication and storage become critical for ensuring data integrity. Other data integrity security best practices include input validation to prevent the entering of invalid data, error detection/data validation to identify and check errors in data transmission, and security measures such as data loss prevention, access control, data encryption, and more.

Most of the business debates and concerns regarding cyber threats have focused on the confidentiality, accessibility and availability of information. In the future, it is expected more cyber operations to change or manipulate electronic information in order to compromise its integrity in terms of accuracy and reliability, instead of deleting it or disrupting access to it. When corporate executives, investors, or other stakeholders cannot trust the information they are receiving, their decision-making will be impaired.

Successful cyber operations targeting the integrity of information would need to overcome any restrictions, data checks and balances designed to prevent the manipulation of the information.

One of the most significant new attack vectors is compromising the integrity of systems, networks and data. Confidentiality and accessibility attacks are loud and obvious. They break restrictions and expose data information causing

embarrassment, inconvenience, and some losses. Data integrity attacks are stealthy, selective, and can be much more disturbing. Instead of doing damage or making off with huge amounts of sensitive data, they instead focus on carefully modifying particular elements within targeted transactions, communications, or data to gain a significant benefit.

Carbanak[1] was significantly different than previous banking malware, which focused on stealing account and login data. Carbanak stealthily compromised about 100 banks and enabled attackers to understand how internal operations were handled (Kam et al., 2015). The malware conducted reconnaissance for attackers who then began modifying selected transactions. When the attack ended, only a small number of accounts were targeted and $1 billion were stolen (Kam et al., 2015). Data integrity attack research is gaining momentum. The risk is data integrity attack in the financial sector in which large amounts of money may be stolen by cyber thieves who will modify selected information in the transaction stream, resulting in a significant redirection of payment to anonym or other designated accounts. The detection of that incident and others actions similar to it is becoming very difficult. Data integrity attacks can appear to be operational problems, accounting errors, audit issues, acts of hackers, or simply human errors. To compound matters, the existing tools, mechanisms, and processes currently available and in use are mostly blind to these types of attack.

Perhaps one of the most prevalent vectors for integrity attacks is in the rise of ransomware[2], which modifies only a few files. Ransomware, a permanent form of a denial-of-service attack, leaves the system working with all data present, but due to the integrity compromise certain files are no longer usable (Gazet, 2008). Attackers then demand a ransom to restore the original integrity. This attack path will also grow significantly in 2016 (McAfee Labs Threats Predictions, 2016).

Data integrity vs. data security

Data are the most important asset to any organization. Therefore, it must be made sure that data is valid, accurate and secure all the time.

Data integrity and data security are two different aspects that make sure the usability of data is preserved all the time. Main difference between integrity

[1] **Carbanak** is an APT-style campaign targeting (but not limited to) financial institutions that was claimed to have been discovered in 2015 by the Russian/UK Cyber Crime company Kaspersky Lab who said that it had been used to steal money from banks. The malware was said to have been introduced to its targets via phishing emails. The hacker group was said to have stolen 1BN dollars, not only from the banks but from more than a thousand private customers (Kam et al., 2015).

[2] **Ransomware** is a type of malware that prevents or limits users from accessing their system. This type of malware forces its victims to pay the ransom through certain online payment methods in order to grant access to their systems, or to get their data back (Gazet, 2008).

and security is that integrity deals with the validity of data, while security deals with protection of data. Backing up, designing suitable user interfaces and error detection/correction in data are some of the means to preserve integrity, while authentication/authorization, encryptions and masking are some of the popular means of data security. Suitable control mechanisms can be used for both security and integrity.

Data integrity and data security are two related items and important aspects each playing an important role in the successful achievement of the other of making sure that data is useable by its intended users. Data integrity makes sure that the data is valid. Data security refers to the protection of data against loss, unauthorized access or corruption and is necessary to ensure data integrity.

That said, data integrity is a desired result of data security, but the term data integrity refers only to the validity and accuracy of data rather than the act of protecting data. Data security, in other words, is one of several measures which can be employed to maintain data integrity, as unauthorized access to sensitive data can lead to corruption or modification of records and data loss. Whether it's a case of malicious intent or accidental compromise, data security plays an important role in maintaining data integrity.

For modern enterprises, data integrity is essential for the accuracy and efficiency of business processes as well as decision making. It's also a central focus of many data security programs. Achieved through a variety of data protection methods, including backup and replication, database integrity constraints, validation processes, and other systems and protocols, data integrity is critical yet manageable for organizations today.

Fundamental data security requirements are confidentiality, integrity and accessibility.

A secure system ensures the confidentiality and privacy of data. This means that it allows individuals to see only the data or information categories which they are supposed to see. Confidentiality has several different aspects dealing with privacy of communications, secure storage of sensitive data, authenticated users and access control.

Privacy is a very broad concept. According to Oracle Corporation[3], in the business world, privacy may involve trade secrets, proprietary information about products and processes, competitive analyses, as well as marketing and sales plans.

Once confidential data has been entered, its integrity and privacy must be protected on the databases and servers where it resides, while authentication is a way of implementing decisions about whom to trust. Authentication methods seek to guarantee the identity of system users for data accessibility: that a person is who he says he is, and not a deceiver.

[3] Oracle is a computer technology corporation developing and marketing computer hardware systems and enterprise software products.

Cyber-attacks

Cyber threats to economic security are increasing in frequency, scale, sophistication, and severity of impact. The ranges of cyber threat actors, methods of attack, targeted systems, and victims are also expanding. Overall, the unclassified information and communication technology networks that support economic activities remain vulnerable to disruption. Cybercriminals are increasingly targeting midmarket companies and startups in hopes of easy access (PWC, 2015). The cost to a business can be high, ranging from financial loss to reputational damage. With heightened awareness, private companies can fight back. With cyber-attacks on the rise, technology experts worry about the looming threat to data integrity. In a data modification attack, an unauthorized party on the network interrupts data in transit and changes parts of that data before retransmitting it. An example of this is changing the euro amount of a banking transaction from €1,000 to €100,000. In a replay attack, an entire set of valid data is repeatedly interjected onto the network. An example would be to repeat, one thousand times, a valid €1,000 bank account transfer transaction. Data must be stored and transmitted securely, so that information such as credit card numbers cannot be stolen.

These quiet, insidious attacks may come in the form of planted malware or selective hacks that seize, modify or delete data or transactions in ways that benefit the perpetrators. For example, an attack could change a bank account's direct deposit setting to channel deposits to another account. High-profile attacks continue to increase in frequency.

James Clapper, Director of U.S. National Intelligence, last year warned of a growing number of low- to moderate-level cyber-attacks against private sector targets from a variety of sources, including several nations. These attacks resulted in stolen or deleted corporate data, compromised personally identifiable information and sizeable remediation costs to companies and consumers.

Like any business, most cybercriminal operations follow the money, looking for the easiest way to steal something of value. Payment systems used to be simple. To buy something, all we needed was enough cash. Today, however, the number of alternate payment methods is rather dizzying, from credit cards, and debit cards, mobile applications, to online payment services. Significant security focus is placed on vulnerabilities associated with credit and debit card transactions because most digital transactions use these forms of payment. With the growth in alternate payment methods, the number attack surfaces have multiplied, giving cyber thieves many, many targets from which to choose. The 2014 data breach at Home Depot exposed information from 56 million credit/debit cards and 53 million customer email

addresses. Home Depot estimated the cost of the breach to be $62 million (Hawkins, 2015). Most attacks approach payment card theft in the same way they have for the past 10 years, by attacking payment mechanisms or the databases containing card data. Once the card data have been obtained, they sell it as quickly as possible and pocket the profit. Now, however, the things are changing. Given the abundance of payment methods, most of which still require usernames and passwords, credentials have become very valuable. To steal credentials, the cybercriminals are targeting the consumers directly because they are both the source of the credentials and the weakest link in the payment process. The studies (McAfee Labs Threats Predictions, 2016) predict that in 2016, payment system cybercriminals will increasingly focus on attacks that lead to the theft and sale of credentials. The experts think that they will leverage traditional, time-proven mechanisms including phishing attacks and keystroke loggers, but new methods will emerge too. They also predict that the number of payment system thefts will continue its relentless growth.

Protecting data and system integrity

Although threats to data change constantly, companies should adopt proactive strategies to safeguard the integrity of their data and systems. Data integrity security measures struggle to prevent the accidental, unauthorized or deliberate modification, removal, destruction or insertion of data. According to Sarb Sembhi, president of the London chapter of ISACA[4] there are standards, methodologies and audit guidelines for managing risks to data availability and data confidentiality, but there seems to be no such guidance for managing threats to data integrity. We now see more spending on security. To be mentioned is that after the 2012-13 distributed denial of service (DDOS) attacks on the US financial sector, JPMorgan Chase (JPMorgan) announced plans for annual cyber security expenditures of $250 million by the end of 2014 (Shields, 2015). According to JPMorgan's CEO they would probably double JPMorgan's annual computer security budget within the next five years after the company suffered a hacking intrusion in 2014.

Companies spend huge sums of money every year to maintain a security perimeter designed to fend off cyber and insider threats. According to Gartner[5], worldwide spending on information security will reach $71.1 billion in 2014, an increase of 7.9 percent over 2013. Total information security spending will grow a further 8.2 percent in 2015 to reach $76.9 billion. Other Gartner figures show that in 2013, average budget allocations for information security were 5.1% of the overall IT budget, up 8.5% from 2012.

[4] ISACA is a nonprofit, independent association that advocates for professionals involved in information security, assurance, risk management and governance.

[5] Gartner, Inc. is an American research and advisory firm providing information technology related insight. Its headquarters are in Stamford, Connecticut, United States.

According to Bruce Snell, Technical Director at McAfee, unfortunately, a lot of this money may not be spent in the most effective manner, but the overall security investment will rise for most businesses. Smart organizations will spend their money not just on technology, but also on more training, awareness, and personnel. Getting into the enterprise via employees outside of the protected network is nothing new. Malware or advanced persistent threats should lead to IT organizations taking a hard look at what it means to be secure. It isn't enough to worry about security only on the company's network. The number of attacks continues to grow, attacks that start with an employee-owned system or a company system that is in an insecure location such as a hotel or coffee shop. Currently, most organizations provide employees with VPN software to allow for a secure connection to the enterprise network. However, most people access the Internet from multiple devices. Although a company laptop may be secure, who knows what protection employees use on their home systems. Most organizations deploy firewalls, web and email gateways, IPS, and other technology to secure their infrastructures, yet most home users barely have antimalware installed and typically have no firewall or gateway. According to Matthew Rosenquist, Cyber-security Strategist at McAfee, these omissions leave employees wide open at home as targets of an attack directed at their employers.

There exist several tactics which every company should employee to reduce their exposure to data integrity attacks, and hence high-value frauds:

Access Control: The so called "virtual keys to the kingdom" are the log-on credentials for privileged users such as systems executives and administrators and which are the main target of hackers. Accordingly, the companies should strictly enforce the implementation and monitor access control policies and procedures to protect data and information system integrity.

Behavior Analyzing: Cyber criminals can use valid credentials to stealthily enter systems when gain access, because they appear to be valid users and this allows them to receive and collect data, install malware and plant attack campaigns to trigger later. Sometimes, the only indicator of attackers' presence is their behavior, which may not appear quite "normal". Security analysts have started to use advanced analytics and huge data to develop behavior-detection capabilities to identify and eliminate abnormal activity.

Tokenization use: The process of replacing sensitive data with unique identification symbols which are non-sensitive and that retain all the critical information about the data without compromising its security or "tokens" has become the way for small and medium enterprises to strengthen the security of their transaction for different methods of payments such as point-of-sale, e-commerce and of credit and debit card transactions. Tokenization enables companies to ensure protection

of customers and their business as well to perform transactions at minimal cost and complexity while complying with industry standards and government regulations. Tokenization of data access makes it more difficult for hackers to enter to cardholder data or the valid user information, as compared with previous older systems in which credit or debit card numbers were registered in databases and exchanged freely over networks. Tokenization technology can, in theory, be used with all kinds of sensitive data including bank transactions.

Data classification: Grouping data into categories enables access control per each category and encryption that are defined by business use and protection needs. Although this may be considered as a redundant process, data risk management software often includes grouping capabilities that make data classification easier to perform.

Data encryption: Is the most effective way to achieve data security by translating data into a secret code. The company/employee must have access to a secret key or password that enables it to decrypt and be able to read an encrypted file.

Protecting sources: Data is transferred, processed and stored in multiple devices such as tablets, Smartphone's, consumer devices, mobile payments and through various channels and corporate systems. Thus, protecting source data at a very detailed level of data transmission can mitigate damage, even if a breach should occur.

IoT security: The establishment of sound IoT security[6] standards is critically important because so many IoT devices collect very personal or vital business data. That data could destroy a business or be personally fatal when in the wrong hands.

Raise employee awareness: While cyber attacks are growing and become significantly more sophisticated, the main reason for security breaches remains quite basic and relates to the lack of security awareness among employees. The problems can be as simple as employees leaving their passwords written and visible to others or failing to turn off their computers when live the office and which are actions that could be addressed with adequate training and notice.

Due diligence on third-party security providers: Every question that a company would put to its own company about security standards should also be put to its third-party providers. The company should establish the standards up front so that it doesn't have to recreate a security questionnaire for each new arrangement.

Use the latest security protection to its fullest: Web sense-type anti-spam systems can screen for vulnerable or malicious URLs, or better yet create a white list of websites that company's employees may safely access. But these measures work best when they are kept up to date. Companies are often inclined to wait to push out new security patches during a slow week or over the weekend, but it's best to push them out as soon as soon they become available.

[6] IoT security is the area of endeavor concerned with safeguarding connected devices and networks in the Internet of things.

Have a crisis response ready: Every company should devise a plan for how to take immediate action if a security breach were to happen. Once a plan has been created, the company should run an incident response exercise with key members of it security team, as well as with its employees overall. What actions should employees take to pinpoint and then mitigate the damage? Who should speak to the media, and what should they divulge? Companies that don't build scenario plan for eventualities like these may end up looking like deer in the headlights, making a bad situation worse. Crisis-readiness can help ensure that won't happen.

Have policies and procedures in place: Companies should create policies and procedures for data quality and data integrity and identify the extent of the problem and record incidences of data integrity compromises and suspected incidents of fraud. It is essential to ensure information assets are correctly valued and to undertake threat assessment of valued data. A risk management approach should be taken to protecting data integrity and ensure adequate protection of all data that is relied upon for investigatory purposes. Additionally, data integrity protection should be included as part of security awareness program.

Boosting security efficiency and effectiveness is key factor on running the business. Personal information including credit cards, social security numbers, and addresses for millions of individuals has been stolen and the trend is expected to continue. At the same time the number and required skill level of security professionals is increasing while the availability of those people and skills is way below market demand. Out of necessity, this will lead to deeper and richer automation of security functions. Businesses will also demand predictable levels of security investment and risk management, prompting the continued development of security as a service, security insurance products, and hedging plans against catastrophic security events.

The experts say that looking ahead; the main forces will be the continuing expansion of the attack surface, increased attacker sophistication, the rising cost of breaches, the lack of integrated security technologies, and a shortage of skilled security talent to fight back (McAfee Labs Threats Predictions, 2016).

Most businesses use free or low-cost cloud collaboration services, but security details are often not shared and the risk of hacking and data exposure is unknown. Whether using project management tools, video conferencing and voice mail, cloud-hosted applications, or data storage sites, employees can put companies at risk by accessing, processing and storing company data on third-party sites that do not offer proper oversight on data security management. The opportunity for attacks to listen to private conversations, including conference meetings or targeting the back-end infrastructure to steal information, can be exploited. A cloud service provider must adapt its security controls to address hackers' evolving

techniques and be always alert to the emerging threat landscape. Protecting cloud services requires addressing the potential opportunities for social-engineering capabilities used to gain access to data and taking a comprehensive approach to security controls. Protection also requires access to data only by authorized users and ensuring that a strong level of encryption is implemented.

With network security in place, any company will experience many business benefits. It ensures protection against business disruption, which helps keep employees productive. Network security helps the business meet mandatory regulatory compliance. Network security helps protect all business data, because it reduces the risk of legal action from data theft.

Ultimately, network security helps preventing the reputation risk for a business, as the reputation is one of the most important assets.

Conclusion

We need to accept that the risks will never be completely eliminated and nothing is permanently safe. As long as there are digital swags there will be criminals, so cybercrime will continue to thrive the data integrity.

To keep up with the sophistication and complexity of attacks is a challenge of the new data and systems security products in the market. Building security into the hardware and software layers is essential for new information security products to succeed at convincing users to trust them. On the positive side, new security tools are coming to market and business awareness and acceptance about the importance of good cyber-security has become more familiar in companies of all sizes. However, there we also have to admit that there is no 'one-size-fits-all' solution which meets the security needs of different organizations.

Leading private companies in local markets and globally, recognize that investing in information security is about more than just protecting the business. Strong cyber security can also better position an organization with its business partners, suppliers and customers, not to mention that the company takes safe advantage of newer technologies to help grow the business activities and that is admittedly the most important objective. As with any enterprise-wide initiative, it is important to set the tone at the top, making sure it resonates throughout all organization. Easier said than done, but once being aware on the importance, it is the right time for efforts to be well spent if the company wants to reduce the risk of being the next cyber-attack casualty. A secure system ensures the confidentiality of data, which makes crucial for the business to have a cyber-security strategy.

A strong business reputation depends on a strong data privacy, confidentiality and information systems security.

References

Cisco: 'What is Network Security?'. Available at:
http://www.cisco.com/cisco/web/solutions/small_business/resource_center/articles/secure_my_business/what_is_network_security/index.html?referring_site=smartnavRD

Clapper James R.(2016). 'Statement for the Record, Worldwide Threat Assessment of the US Intelligence Community, Senate Armed Services Committee'. Available at:
https://www.dni.gov/files/documents/SASC_Unclassified_2016_ATA_SFR_FINAL.pdf

Cucoranu I.C., Parwani A.V., West A.J., Romero-Lauro G., Nauman K., Carter A.B., Balis U.J., Tuthill M.J. & Pantanowitz L. (2013). 'Privacy and security of patient data in the pathology laboratory'. J Pathol Inform, 4:4.

Dhillon, G. & Backhouse, J. (2000). 'Information system security management in the new millennium'. Communications of the ACM 43(7), 125–128.

Dhillon, G. & Torkzadeh, G. (2006). 'Value-focused assessment of information system security in organizations'. Information Systems Journal 16(3), 293–314.

Gartner: 'Gartner Says Worldwide Information Security Spending Will Grow Almost 8 Percent in 2014 as Organizations Become More Threat-Aware'. Accessed through:
http://www.gartner.com/newsroom/id/2828722

Gazet, A. (2008). 'Comparative analysis of various ransomware virii', J Comput Virol (2010), 77–90.

Gelbstein, E. (2011). 'Data Integrity—Information Security's Poor Relation'. ISACA JOURNAL 6, 20-25.

Gordon, L.A. & Loeb M.P. (2002). 'The economics of information security investment'. ACM Transactions on Information and System Security 5(4), 438–457.

Hawkins, B. (2015). 'Case Study: The Home Depot Data Breach'. Global Information Assurance Certification Paper, SANS Institute.

ISACA: http://www.isaca.org/

Kam, H-J. Goel, S. Katertannakul, P. and Hong, S. (2015). 'Organizational Security Norms in the Banking Industry: The United States vs. South Korea'.WISP 2015 Proceedings, Paper 5.

Kandukuri B.R., Paturi V.R. & Rakshit A. (2009). 'Cloud security issues". IEEE international conference on services computing, 517–520.

McAfee. McAfee Labs 2016 Threats Predictions. Available at:
http://www.mcafee.com/tw/resources/reports/rp-threats-predictions-2016.pdf

Oracle Corporation: Oracle9i Security Overview. Available at:
https://docs.oracle.com/cd/B10501_01/network.920/a96582/overview.htm

PricewaterhouseCoopers: Cyber- attacks on the rise: Are private companies doing enough to protect themselves? Available at: https://www.pwc.com/us/en/private-company-services/publications/assets/pwc-gyb-cybersecurity.pdf

Riahi A., Challal Y., Natalizio E., Chtourou Z. & Bouabdallah A. (2013). 'A Systemic Approach for IoT Security'. IEEE DCOSS, 351-355.

Roman R., Najera, P. & Lopez J. (2011). 'Securing the Internet of Things'. IEEE Computer, vol. 44, no. 9, 51–58.

Shields K. (2015). 'Cyber security: Recognizing the Risk and Protecting against Attacks'. N.C. Banking Inst., Vol. 19. Available at: https://www.law.unc.edu/journals/ncbank/volumes/

volume19/citation-19-nc-banking-inst-2015/cybersecurity-recognizing-the-risk-and-protecting-against-attacks/

Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). "Analysis of End User Security Behaviors". Computers and Security (24:2), 124-133.

Subashini, S. & Kavitha, V. (2010). 'A survey on security issues in service delivery models of cloud computing'. Journal of Network and Computer Applications 34, 1–11.

Straub, D.W. (1990). 'Effective IS Security: An Empirical Study'. Information Systems Research (1:3), 255-276.