UDC 681.321; 322:621.395

# Problems of Developing Information Security Policy

***Shevchuk I.S., Shakleina I.O.***

email: i.s.shevchuk@ukr.net, ioshakleina@gmail.com
Department of Theoretical Physics and Methods of Teaching Physics,
Ivan Franko Drohobych State Pedagogical University,
3 Stryis'ka St., Drohobych,UA–82100, Ukraine

In this article we consider business needs for information security and discuss information security threats, vulnerabilities, explain the concepts of confidentiality, integrity, availability, non-repudiation, authentication, and authorization. The study concerns information security technologies, policies, and technical control which can be applied to solve or reduce the risks of data breach and data theft. We also take into consideration benefits of effective protection measures against data breaches.

*Key words:* authentication, authorization, availability, confidentiality, database, information security, integrity, hardware, non-repudiation, software.

## INTRODUCTION

In today's fast-growing technology all businesses rely solely on operation databases. In this article we attempt to give all-purpose explanation of the business vital needs for information security regardless of business size and give details of latest information security risks, vulnerabilities, explain the concepts of confidentiality, integrity, availability, non-repudiation, authentication, and authorization. General recommendations will concern technologies, processes, and policies which can be useful in solving or reducing the risks of data breach and/or data theft. We will also take into consideration costs and benefits/penalties of effective/ineffective protection measures against data breaches.

Every business possesses technological (software and hardware) assets and non-technological (people, environment and processes) assets where information is created, processed, stored, and transmitted. Regardless of the type, both assets are crucial for a company to operate freely and to acknowledge the importance of information security policy. This policy is multi-purposeful as it protects people and information; sets the rules for expected behavior; authorizes security personnel; defines the consequences of violation; helps minimize risk and tracks compliance with regulations and legislation [1]. Whenever a company has a set of security policies in place it will successfully regulate employee's behavior and methods of using company's electronic communication assets responsibly.

In today's world of online crimes, organization's data faces new security threats more often than ever before. Cybercriminals (hackers, phone phreakers, blue boxers, virus writers, pirates, cypherpunks, anarchists, cyberpunks, etc.) use different kinds of security attacks. Still hackers are the most frequent and the most dangerous of them. They deliberately gain (or attempt to gain) unauthorized access to organization's computer systems. Most feared motives for hacking are data breach, data theft, money or simply system damage. In order for a company to survive and to stay afloat against these current security risks, there should be a continuous and recurring implementation of up-to-date information security measures and vulnerabilities to prevent and fight off those threats. A company must do beyond just setting up technical controls such as firewalls, well configured routers and antivirus programs. Other deeper understanding of securing a network and prevention of the risks discussed previously are confidentiality, integrity, availability, non-repudiation, authentication, and authorization.

Confidentiality comes down to perception of information. It ensures that computer-related assets are limited and disclosed only to the authorized users. Authorization is the function of specifying access rights to resources. Authentication is the process of determining the accuracy of a quality of a separate piece of data or entity. Authentication methods (user-IDs, passwords, etc.) that uniquely identify data system's users and control methods which limit each identified user's access to the data system's resources can ensure confidentiality. In every business computer system, authentication and authorization must work hand in hand to provide effective security against vulnerabilities. Integrity refers to the trustworthiness of information resources. It means that assets can be modified only by authorized users. Availability means that computer-related assets are accessible to authorized users at appropriate times [2, 10]. Non-repudiation is a core property of certified mail systems. It guarantees that involved parties cannot deceive and deny of having participated in a communication [3]. Non-repudiation mechanisms use symmetric and asymmetric cryptography. Non-repudiation of origin, non-repudiation of delivery, non-repudiation of submission, and non-repudiation of transport are the main non-repudiation services.

Within the past few years we have been witnessing an increasing regularity in data breaches resulting from unauthorized access. Data breaches are a primary source of identity theft. They are considered to be very dangerous because unlike some other privacy problems, they cause "tangible harm to both organizations and individuals" and may "lead to spillover effects for other firms in the same industry" [4, 678]. Because of data breach companies may experience issues ranging from loss of key information, adverse publicity, loss of trust, legal action by customers, and official censure by regulators. "All of which can be avoided with a little forethought and a professional attitude to the use of data encryption" [5, 22]. Full disc encryption should be mandatory to all organizations no matter what size. Technology could be used to encrypt information, but training people is not a technology problem. It's a people problem. Employees are likely to become the weakest link of security if they do not comply with the policies of the organization. Organizations must enforce existing data-handling procedures so employees don't become lax. To prevent an unauthorized access causing data breaches, the organization should provide physical access control (mechanical locks and keys, electronic access control technology, or any combination of these methods) and network access control (a "least privileged" access, use of trusted software and network security devices such as routers, firewalls, and Intrusion Prevention System). It is important to know that "sometimes several controls are needed to cover a single vulnerability, and sometimes one control addresses many problems at once" [2, 32].

Every year, data breaches cost companies millions of dollars. That's why it is important to know how to manage these risks. For sure, developing a secure operating system and installing the corresponding protection measures beforehand would cost the company about 1% of its total losses. It is impossible to regard security as an added cost of doing business. To the contrary, security and privacy should be looked upon as business accelerators and sources of substantial competitive advantage [6, 32].

Every company should commit to protecting its employees, partners, and clients from damaging acts that are intentional or unintentional. The Information Security Program establishes and states the policies governing business's Information Technology (IT) standards and practices. These policies define the objectives for managing operations and controlling activities. The policies represent the program or protocols for achieving and maintaining internal control over information systems as well as compliance with the requirements imposed on the organization.

Effective security is a team effort involving the participation and support of every company's user who interacts with data and information systems. It is the responsibility of every user to know these policies and to conduct their activities accordingly. Protecting company information and the systems that collect, process, and maintain this information is of critical importance. Therefore, the security of information systems must include controls and safeguards to offset possible threats, as well as controls to ensure accountability, availability, integrity, and confidentiality of the data:

- Confidentiality – this security component addresses preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
- Availability – this security component addresses ensuring timely and reliable access to and use of information.
- Integrity – this security component addresses the property that sensitive data has not been modified or deleted in an unauthorized and undetected manner.

Security measures must be taken to guard against unauthorized access to, alteration, disclosure, or destruction of data and information systems. This also includes measures against accidental loss or destruction.

All individuals accessing the company's data are required to comply with state laws, policies, and procedures regarding security of highly sensitive data. Any employee, partner, or client with access to data who engages in unauthorized use, disclosure, alteration, or destruction of data is in violation of this plan and will be subject to appropriate disciplinary action, including possible dismissal and/or legal action.

## 1. SECURITY POLICY AND PLANNING

Responsible party is Chief Information Officer (CIO) or Chief Information Technology Officer (CITO). Policy Statement demands that security policies should be reviewed any time hardware or software is upgraded, as necessary, or at least annually, to ensure that policies continue to meet the needs of the business, protect confidential data, and comply with applicable laws as both technology and the threats against it evolve. When possible, when a change to hardware or software is planned, applicable security policies should be reviewed and updated prior to implementation of the new hardware or software.

Policies not up to date with current technology and threats leave security holes that will be exploited sooner or later. By reviewing policies regularly for applicability to current needs, threats, and laws, updates can be made in a timely manner to avoid potential security incidents.

## 2. PROBLEMS OF MANAGEMENT

### *2.1. Personnel Management*

Responsible party is Human Resource (HR). Policy Statement says that all personnel working for the company, as regular employees, contractors, or third party, are required to have a preliminary background check and receive training covering all company security policies, know repercussions for when security incidents occur, and to sign applicable statements of understanding, to be filed with HR.

Humans are the weakest link in the IT security field. Proper training and awareness will help to offset this. Knowledge of proper security procedures and consistent enforcement will mitigate many issues before they happen.

Responsible party is HR or Training Department (TD). Policy Statement declares that all persons requiring access in any capacity to the company network or data will complete applicable training prior to being granted access. This training will cover:

- appropriate use,
- applicable laws,
- what constitutes misuse,
- applicable consequences,
- corporate security measures,
- how to apply personal security.

Upon completion of training and prior to accounts being created or access being granted, users will sign non-disclosure agreements, acceptable use and monitoring memos, and security policy statement of understanding.

Responsible party is HR. Policy Statement claims that no core company functions should be outsourced. Auxiliary functions, such as payroll or advertising, should be outsourced when beneficial to the company as a whole. When this is the case, the outsource company must sign a legal contract to adhere to all current and future security policies of this company. If the outsource company needs access to corporate data, it should be provided in the form of a separate database from the primary company data, but updated from the primary data on a basis consistent with the needs of the function being provided by outsourcing. When possible, this auxiliary database should be on a separate server, and different outsource partners will each have a separate database, even when the data may overlap or be the same. This will reduce any damage that can be done by a security breach through a third party connection.

Outsourcing always has a risk because the people being contracted to do the work do not have the same personal stake in the company as regular employees and so are less likely to take security as seriously.

Responsible party is Security Department Head. Policy Statement consists in the following:

- Paper documents should be scanned and archived in the database, then either shredded or archived in an on-premise vault.
- Access to areas containing computer systems connected to the corporate network or containing sensitive data will be limited to employees. Any visitors must be escorted at all times when in these areas.
- Access to server rooms will be limited to cleared company IT employees only.

There arise vulnerabilities or risks:

- Disposal of hard copies in a readable form compromises data.
- Physical access to computer systems could allow malicious software to be introduced.

Countermeasures or Risk Mitigation Strategy:

- Shredders will be used.
- Building should be locked with a high-security physical key outside of business hours.
- Security guards should be utilized to verify people entering during the day and to secure the facility outside of business hours.
- Access badges should be used to allow passage past a lobby or waiting area.

Area cipher locks can be used to control personnel accessing sensitive areas.

### *2.3. Data security management*

Responsible Party is CIO or CITO, all users of systems. Policy Statement says that all data will be encrypted so that unauthorized personnel will not have easy access to the information that need to be kept confident. Data encryption can be done through approved software and/or hardware. Backups will be made everyday so that if there is a situation where data is lost and unrecoverable, the backup data can easily replace the data that is gone.

If a threat were to get into the network and access the information, data could be manipulated or deleted which would then show the lack of integrity with the data. Data could even be entered into the system incorrectly, whether something was misspelled or numbers were inserted incorrectly. Backing up databases can be a problem if the data is not backed up frequently or if an attack happens where data is deleted and the last time the data was backed up was several days ago, then it does not help because a lot of the data could have changed in that period.

Therefore, the data and all relevant information will be protected through *encryption* by having the data converted into unreadable code that unauthorized personnel will not be able to decode. Data can be *backed up* so that if any data is lost, the backup data will be available. *Data masking* involves taking the data which are in a database table or cell and masking the data so that unauthorized personnel cannot see the data. An example of this is with numbers and only having the last couple of digits visible. One more technique is *data erasure*. This is the process in which software would overwrite the data on the hard drive or other media so that any data is not accessed when a hard drive is used in the future for other needs.

### *2.4. Software Security Management*

Responsible Party is CIO or CITO, all system users. Policy Statement reads that software security must ensure that the processes, procedures, and products used to produce and sustain the software conform to all requirements to govern the processes, procedures, and products. All software developed for the company usage must adhere to the software development life cycle.

Known vulnerabilities or risks are as follows:

- Buffer Overruns – an application error that occurs when more data is sent to a program buffer than it is designed to handle.
- Command Injection – when user input is passed directly to a compiler or interpreter. The developer failed to ensure that command input is validated before it is used in the program.
- Cross-site Scripting (XSS) – when an application running on a Web server gathers data from a user in order to steal it.
- Structured query language (SQL) Injection – when developers fail to properly validate user input before using it to query a relational database.
- Trojan horses – software programs that hide their true intentions and reveal their true intentions when activated. They are disguised as helpful, interesting, or necessary pieces of software.
- Back Door or Trap Door – A virus or worm that has a payload that installs these components in a system, which allows the attacker to access the system at will with special privileges.
- Polymorphism – a threat that over time changes the way it appears to anti-virus software programs.

Countermeasures to be taken involve Software Development Life Cycle (SLDC):

- planning,
- implementation,
- testing,
- documenting,
- deployment,
- maintenance.

### *2.5. Hardware security management*

Responsible Party is CIO or CITO, all system users. Policy Statement demands that all hardware that will be used should be subjected to certification and accredited by a senior agency official. All hardware that enter the space will be approved by the CIO. Any hardware that must be used in conjunction with any preapproved hardware must be approved. All hardware must go through a checklist set up by a senior level employee. Any hardware that is not approved can bring external threats to the designated hardware that would in turn cause a risk to the system connected to that hardware. New hardware introduced to an environment can bring in external threats that could be transferred from hardware to hardware and eventually reaching a network and its servers.

Risk Mitigation Strategy involves Certification & Accreditation (C&A). Certification is a comprehensive evaluation of the hardware to make sure that the design and any components meet the security requirements set forth by the CIO or another senior level figure. Accreditation is the formal declaration of a Designated Accrediting Authority (DAA) or a Principal Accrediting Authority (PAA), that the hardware is approved to be operational at the level of risk that was set.

### *2.6. Network security management*

Responsible Party is CIO or CITO, all system users. Policy Statement: the network security states how assets stored on the network should be protected. Storing and transmitting protected information assets must ensure confidentiality, integrity, and availability. Network attacks launched from the Internet or from organization networks can cause significant damage and harm to information resources including the unauthorized disclosure of confidential information.

In order to provide defensive measures network attacks, firewall and network filtering technology must be used in a structured and consistent manner. The company maintains appropriate configuration standards and network security controls to safeguard information resources from internal and external network mediated threats. Firewalls and Intrusion Detection Systems (IDS) are deployed at the organization border. They are appropriate to limit access to systems that host restricted or essential information. The company audits and manages its network with Network Inventory Advisor. It maintains Virtual Private Networks (VPNs) access, which establishes a normal network connection between distant systems and allows remote users to connect to the office network without compromising network security. A network security audit is part of an overall information systems audit framework that includes application software audit, operation system audit, and business audit.

## 3. BUSINESS CONTINUITY

### *3.1 Business impact analysis*

Responsible Party is CIO/CITO, all system users. The company should provide a safe, secure IT environment to serve its customers' requirements, ensure stability and continuity of the business, and promote confidence in its ability to not only continuously provide services, but also to recover quickly from disaster and minimize disruption. It has to meet stringent industry regulations and client requirements for business continuity. It ensures business continuity and provides non-stop user accessibility even during planned maintenance. The threats that confront business are constantly changing and increasing in complexity.

Countermeasures consist in developing a Business Continuity Plan (BCP). The BCP acts as an over-arching plan that encompasses all activities that ensure business continues in the event of a significant impact or disaster.

The Business Impact Analysis (BIA) is a critical step in IT contingency planning. It results in the differentiation between critical and non-critical organization activities. BIA correlates specific system components with the critical services that they provide, and based on that information, to characterize the consequences of a disruption to the system components. BIA results in the recovery requirements for each critical activity.

The company must develop recovery priorities for the system resources. A scale of high, medium, low should be used to prioritize the resources. High priorities are based on the need to restore critical resources within their allowable outage times; medium and low priorities reflect the requirement to restore full operational capabilities over a longer recovery period. By prioritizing the recovery strategies, the company's business may make more informed decisions regarding contingency resource allocations and expenditures, saving time and effort.

Data owners and custodians are responsible for maintaining the BIA documents. A periodic review of the BIA should be performed by the data owner to ensure accuracy and completeness.

### *3.2 Disaster recovery*

Responsible Party is CIO or CITO, all system users. Disaster recovery planning is a subset of business continuity planning and should include planning for resumption of applications, data, hardware, communications (such as networking) and other IT infrastructure.

Disasters can be classified in two categories: natural disasters (floods, hurricanes, tornadoes or earthquakes) and manmade disasters (hazardous material spills, infrastructure failure, or bio-terrorism).

The company must develop the Disaster Recovery Plan, which is a part of BCP and contains detailed information on how to continue business operations and perform all tasks required to do so while the computer hardware, network and data are being recovered. While preventing a natural disaster is very difficult, measures such as good planning, which includes mitigation measures, can help reduce or avoid losses. In the instances of manmade disasters, surveillance and mitigation planning are invaluable towards avoiding or lessening losses from these events.

The company should provide the following preventive steps:

- Backups made to disk on-site, or directly to off-site disk;
- Replication of data to an off-site location;
- High availability systems keeping both the data and system replicated off-site;
- Surge protectors, uninterruptible power supply and/or backup generator;
- Fire preventions — alarms, fire extinguishers;
- Anti-virus software and other security measures.

## 4. INCIDENT REPORTING

Responsible Party is CIO or CITO, all system users. A Security Incident is a violation or imminent threat of violation of computer security policies.

An IT security incident could result in misuse of confidential information (social security number, grades, financial transactions, etc.) of individuals, jeopardize the functionality of the business's IT infrastructure, provide unauthorized access to resources or information, provide illegal copies of software to others through peer-to-peer file sharing services.

When such an incident occurs, the company has a plan for dealing with (i.e., reporting, investigating, and resolving) the incident. This plan helps ensure the safety, confidentiality, availability, and integrity of information.

If a company user suspects that its assets are being misused or are under attack, the user has an obligation to report that incident. In case of an IT security incident, immediate action should be taken to isolate the problem from the organization network. You should:

1. Contact your system administrator or designated IT support person.

2. Send an email regarding the incident. The email should contain as much of the following information as possible:

- a description of the incident;
- any steps that have been taken to correct or isolate the incident;
- any other IT professionals that have been contacted regarding this incident.

## CONCLUSIONS

As outlined in this paper, all companies regardless of size must protect their assets against all potential threats and vulnerabilities by applying information security measures and at the same time deploy policies and technical controls to ensure a proper use of its assets. Preventing data breaches is the highest priority for today's organization. Consumers cannot completely protect themselves from a data breach that is why the organizations, which collect sensitive consumers' information (especially Social Security and credit card numbers), ought to take the steps to ensure the privacy and security of the data they collect and maintain, by developing an appropriate secure operating system.

## REFERENCES

[1] Canavan S. Information Security Policy – A Development Guide for Large and Small Companies / S. Canavan, S. Diver – SANS Institute, 2007. – 43 p.

[2] Pfleeger Ch. P. Security in Computing, 4th Edition / Ch. P. Pfleeger, Sh. L. Pfleeger – New Jersey: Prentice Hall, 2007. – 880 p.

[3] Tauber A. A survey of certified mail systems provided on the Internet / A. Tauber // Computers & Security – 2011. –V. 30, № 6/7. – P. 464-485.

[4] Culnan M. J. How Ethnics Can Enhance Organizational Privacy: Lessons from the ChoicePoint and TJX Data Breaches / M. J. Culnan, C. C. Williams // MIS Quarterly. – 2009. – V. 33, № 4. – P. 673-687.

[5] Allen M. Coping with a major security breach? / M. Allen // Management Services. – 2006. – V. 50, № 2. – P. 22-23.

[6] Lemecha D. ChoicePoint: Back From The Breach? / D. Lemecha // Optimize. – 2007. – V. 6, № 5. – P. 28-32.