BULGARIAN ACADEMY OF SCIENCES
PROBLEMS OF ENGINEERING CYBERNETICS AND ROBOTICS • 2020 • Vol. **72**, pp. 29-40
p-ISSN: 2738-7356; e-ISSN: 2738-7364
https://doi.org/10.7546/PECR.72.20.04

Vulnerability and Protection of Business Management Systems: Threats and Challenges

Ivan Stankov[1], *Georgi Tsochev*[2]

[1] *Technical University of Sofia, Sofia, Bulgaria*
[2] *Laboratory of Telematics - BAS, Sofia, Bulgaria*
Emails: istankov@tu-sofia.bg, gtsochev@cc.bas.bg

Abstract: The implementation of an information system is a complex process. It is even more complex when it comes to business information systems. These information systems have now evolved into what are more commonly known as enterprise information systems. Then the threat of cyberattacks must also be considered. In this paper we make a brief overview of major business information systems. Based on the literature review we identified the most common vulnerabilities associated with them and make some recommendations for stopping different kind of threats against them.

Keywords: vulnerability, busmen management systems, threats, enterprise applications, security

1. Introduction

Human reliance on computers to operate safely and reliably in an environment ranging from air traffic control and telemedicine to e-commerce and telecommunication emphasizes the need to design, develop and maintain secure computer systems, including secure email communication [1]. As new products are continually being introduced to the market, a significant portion of security vulnerabilities and vulnerability classes are regularly detected and exposed during a product's service life. This trend is likely to continue given the time pressure, complexity of the security assessment process, the unlimited number of system configurations, product revisions and upgrades, and different levels of experience of the system administrator.

Today, business operations are carried out through technology. From the meeting room to the post office, companies transact, deliver goods, track their client accounts and inventory the company's assets by implementing information technology (IT) systems. IT enables the storage and transportation of information – often the company's most valuable resource – from one business unit to another. The trading venue is not static; it moves whenever employees travel from office to

office, from city to city, or even from office to home. As businesses become more flexible, “computer security” becomes “information security”, which covers a wider range of issues, from data protection to human resources protection. Information security and cyber protection is no longer the responsibility of a small specialist team of experts within the company and is particularly of high importance [2]. It is now the responsibility of all employees, especially the managers. That is why the network security policies are one of the most important elements in any organization [3].

The purpose of this article is to present the vulnerability of various business management systems, the threats and challenges they face, and some ways to protect them. To achieve this, I have considered the aforementioned points in four types of business management systems, the so-called Enterprise Applications: 1) Enterprise Resource Planning (ERP); 2) Customer Relationship Management (CRM) systems; 3) Supply Chain Management Systems (SCMS); 4) Knowledge Management Systems (KMS).

2. Review of enterprise systems

1.1 Enterprise Resource Planning Systems

Enterprise Resource Planning (ERP) systems integrate information about different business units and processes into one organization, providing a highly centralized and always up-to-date look at key areas such as sales, manufacturing, finance/accounting, human resources management and others ERP systems represent the business critical infrastructure of the world. Large and medium-sized companies, government and defense organizations rely on these platforms to process and store their most valuable information and manage their core business processes. In the large corporate market, SAP is the leading player, followed by Oracle, which has grown through the acquisition of several smaller vendors such as PeopleSoft, Siebel and JD Edwards in recent years [3]. From a technical point of view, the system can be divided into the following layers:

- The layer of the operating system responsible for launching basic ERP software applications.
- The database layer responsible for storing ERP technical and business information.
- The ERP business infrastructure layer, which is responsible for serving as the basic framework that supports user interaction with ERP business modules, as well as for critical technical tasks.
- ERP business logic layer representing ERP business modules and controls.

It is important to note that each component is an essential part of the system and because of the way they are designed, the successful attack on one of them can mean a fatal risk to the entire platform [3].

1.2 Custom Relationship Management Systems

The purpose of customer relationship management (CRM) is to identify, acquire and retain clients. CRM software or systems include sales, customer service and support,

call centers, sales automation systems and order management. In the last ten years, software companies have been trying to consolidate some of these technologies into an integrated system.

Because the CRM system is customer oriented, a multi-channel strategy is used by the underlying CRM software. All types of machines, such as handhelds, fax machines, and cellular phones, can be interface devices for accessing CRM systems, and Internet access becomes a necessary requirement for most CRM systems.

1.3 Supply Chain Management Systems

At the most fundamental level, supply chain management (SCM) is the management of the flow of goods, data and finances related to a product or service, from the purchase of raw materials to the delivery of the product to its final destination. Although many people equate the supply chain with logistics, logistics is actually just one component of the supply chain. Today's digital-based SCM systems include material and software processing for all parties involved in product or service creation, order fulfillment, and information tracking – such as suppliers, manufacturers, wholesalers, transportation and logistics service providers, and retailers.

Supply chain activities include procurement, product life cycle management, supply chain planning (including inventory planning and maintenance of enterprise assets and production lines), logistics (including fleet transport and management), and procurement management. SCM can also cover global trade activities, such as global vendor management and multinational manufacturing processes [14].

1.4 Knowledge Management Systems

A knowledge management system is defined as information systems designed specifically to facilitate the classification, collection, integration and dissemination of organizational knowledge. With KMS, organizations are able to respond more quickly to changing market conditions and improve decision-making and productivity. To maximize the value of knowledge assets in organizations, KMS is used to support the integrated knowledge management process.

Utilizing Web 2.0 technologies, KMS focuses primarily on the pooling of knowledge in a centralized repository and the integration of knowledge within practical communities. According to a study on technologies used in the development of KMS, 90% of organizations use browser tools to display and disseminate knowledge to organizations on the Internet. The other two most common tools are email and search and return tools.

In general, KMS requires a variety of technological tools in the database and its management, communication and messaging, as well as in surfing and retrieval. With the advent of cloud computing, organizations are considering using cloud services to support a variety of applications, including KMS. The availability and immediacy of a cloud-based KM application enables users to expand their IT environment. Cloud service providers control KM content applications, such as

creating, refining, storing, using and sharing knowledge, and make them available to users on demand [18].

3. Vulnerabilities of Enterprise Applications

3.1 ERP Vulnerabilities

ERP systems stores many and different kind confidential information. That is why they are the target of various types of cyber attacks. In recent years, their security has been enshrined in the concept of evening companies using such systems. The Association for Information Systems Auditing and Control (ISACA) recommends that a comprehensive security assessment of the ERP system, verification of ERP servers for software vulnerabilities, configuration errors, segregation of obligations, compliance with relevant standards, and vendor recommendations be performed on a regular basis. In an SAP CRM system, the administrator can set over 1500 parameters that can be configured in any application server. Some of the reasons for the vulnerabilities of ERP systems are complexity and a large number of custom settings including:

- Lack of competent specialists;
- Lack of security audit tools;
- Traffic Capture and Modification – Sending a Password in Explicit Text and Using Unencrypted Links (SAP J2EE Telnet/Oracle Listener Older Versions);
- Protocol vulnerabilities (such as RFC in SAP ERP and Oracle Net in Oracle E-Business Suite);
- OS Software Vulnerabilities – In 2017, there was a major vulnerability in Microsoft SMB MS17-010 that led to a large amount of information leakage;
- Weak OS passwords;
- Insecure OS settings – SAP data becomes available to remote users via NFS and SMB;
- Web application vulnerabilities (XSS, XSRF, SQL injection, split responses, code execution);
- Buffer overflow and string formatting in web servers and application servers (SAP IGS, SAP Netweaver, Oracle BEA Weblogic);
- Uncertain Access Privileges (SAP Netweaver, SAP CRM, Oracle E-Business Suite).

3.2 CRM Vulnerabilities

Implementing CRM systems is a challenge for companies because they cannot effectively and/or adequately utilize customer relationships. Modern CRM systems contain a variety of business information for companies from coordinate information to sales and customer data. One feature of such systems is the business-to-consumer relationship. This is where the main security problem arises. Possible attacks on this type of system are:

- Denial of service – Denial of service (DOS) means making an attacked system inaccessible to customers. Possible attackers include angry customers, scripts, previous employees and competitors.
- Intrusion into sales automation systems and customer database – Sales automation systems typically have a wealth of customer information. Potential attackers can break into systems and steal customer information.
- Identity Theft – Identity theft occurs when "someone uses your personal information without your permission to commit fraud or other crimes."
- Malware attacks – Malware includes viruses and worms; Malware attacks can cause DOS, hardware damage and data loss [8].

3.3 SCM Vulnerabilities

SCM systems, by their very nature, require partnerships for collaboration between people and organizations. This can create a number of problems. These relationships between companies unknowingly reveal the sensitive aspects of their business and open up opportunities for cybercriminals. Threats to SCM systems can be identified as follows:

- Cybersecurity threats in the supply chain
    - Networking or computer hardware that ships with malware installed on it (such as Superfish installed on Lenovo laptops).
    - Malware that is embedded in software or hardware.
    - Vulnerabilities in software applications and supply chain networks detected by malicious hackers [17].
- Improper management of cloud access – these types of systems are increasingly found in the cloud as a different type of service.
- Third party data trust
- IoT compromise – a gateway that cybercriminals can exploit is Internet of Things (IoT) sensors. IoT devices must be checked for security and encryption must be applied to all points of the IoT ecosystem [16].
- Physical device tampering – Purposeful tampering with physical devices is another huge security threat in managing the supply chain [15].

3.4 KM Vulnerabilities

Data transmission confidentiality is very important in the creation, improvement, sharing and use of knowledge. At the same time, the need to be concerned about the confidentiality of the data stored in the database can better assist the knowledge retention process. Access control concerns are a must in all KM processes, since in each process the organization must be able to control who has access and authority to perform specific activities to the organization's knowledge assets.
It seems that preventing data loss or leakage is a problem that should only be addressed in the knowledge retention process where the organization tries to retain knowledge for future use as much as possible.

Next, throughout all KM processes, an organization must take cyber-attacks into account, as many different types of cyber-attacks can occur at any time when

users interact with a knowledge repository or when knowledge resides in the repository.

Other problems in all KM processes are related to accessibility and reliability. The system must be accessible and reliable when users want to use it. For example, if users are often unable to extract, share, or use existing knowledge, this would cause a bad impression and users may hesitate to use the system. In addition, a DoS or DDoS attack can corrupt any server that supports all of these KM processes.

Finally, browser security is also another aspect that should be addressed in almost all KM processes, since browser is a commonly used tool that users use to interact with the system. Because users have to perform all the activities through the browser, an insecure browser can hurt the users' computers and annoy the users. In summary, almost all different types of security issues play an important role in all knowledge management processes.

Therefore, data security and privacy issues, access control, cyber attacks, and accessibility and reliability issues are the most critical security issues for successful cloud-based KMS. The second most critical security issue would be the browser security issue that contributes to KM processes. The problem of data loss or leakage prevention, which relates solely to the process of knowledge storage, cannot yet be ignored because of the importance of the knowledge repository on organizational secrecy [18].

4. Security Measures for Enterprise Applications

4.1 ERP Security

Researchers place a number of solutions to the current and immediate risk of ERP systems and the valuable data they hold. On the system side, they recommend identifying and mitigating ERP application-level vulnerabilities, insecure configurations, and excessive user privileges in a number of ways. Some common solutions for securing the ERP systems are:

- Double and triple check your system configurations;
- Update your ERP software regularly;
- Set up an ERP system administrator – Designate your IT team (if any) or responsible person to monitor system logins, identify suspicious threats, and make timely communications. You can consult with your ERP training provider and come up with an appropriate plan [4], [5];
- Full access rights – It is important that you maintain audit logs to keep track of all changes. It is also worth adding "permissions" to checklists for new hires, promotions, and any documentation for changing roles [6];
- Create strong protection against Ransomware/Malware;
- Reduce internal human errors – The only most effective way to combat this problem is to allow only the most trusted individuals to perform vital processes in the ERP system;
- Failure to comply – Choose an ERP system that is designed to meet the requirements and always pay attention to and comply with industry-specific

requirements. It is also important to change your provider-issued password and always adhere to good security practices. Credit card numbers and social security information must always be heavily encrypted, and other common requirements include firewalls, unbreakable passwords, and other precautions [6, 7];

- Single authentication – The obvious solution is 2FA. The good news is that the 2FA industry has changed in recent years and no longer needs a physical device. Instead, a code can be sent to an email address [6];
- Develop an effective recovery plan – Discuss with your ERP provider (and IT team) who understands your company's requirements for developing a final recovery plan [4];
- Use ERP Security Scanners – ERP Security Scanner is software designed to look for vulnerabilities in ERP systems. Examples of such scanners ERPScan for SAP ERP, Onapsis for SAP ERP, AppSentry for Oracle E-Business Suite, MaxPatrol for SAP ERP [1].

4.2 CRM Security

4.2.1 Counteracting DoS attacks

Appropriate technical controls must be in place to identify malicious traffic sent to the CRM system. Intrusion Detection Prevention Systems and firewalls often have DoS protection either built into the unit or available for purchase. All technologies used to protect your CRM resources and infrastructure must be equipped to handle this type of attack. In addition to perimeter security, it is important to address internal attacks. Determinants can use the company's technological assets against its CRM system. Make sure that antivirus solutions are installed and updated, computers and software applications also, and that the vulnerability of the infrastructure is overcome to prevent attackers from using your own technology against your CRM system.

4.2.2 Protect your data

Some basic steps that can help you protect your customer data are [11]:

- By having sensitive information and customer records, companies can install sound alarm systems that can detect data breaches and take immediate countermeasures, including those that can help stop the breach immediately;
- Companies can use effective encryption systems as well as identity and access management systems that provide access rights only when needed. Employees who no longer need access rights can be thrown out of the system on a regular basis;
- Additional layers of consumer identification can be used for data protection;
- Cloud CRM systems with IP address restrictions can be used;
- Enable the audit log function of your CRM. The lack of automated audit logs makes monitoring impossible, and forensic investigation is time consuming

and expensive. The lack of audit logs also leaves a gap in all security, certification and regulatory requirements related to audit control;
- Continuous alarm monitoring and filtering: User activity monitoring and alerts provide some peace of mind as well as visibility into suspicious user behavior;
- Emphasizing the importance of data protection can be done regularly in internal company forums and can be an important part of the company's internal training.

4.2.3 Choose a reliable CRM provider

When choosing the CRM provider must fallow some simple steps: 1) research different CRM companies carefully before making a purchase decision; 2) check for ISO 27001; 3) check the vendor website/blog and other IT news sites for past history of data breaches and how the company addressed them.

4.2.4 Educate your employees

With the advancements and proliferation of these dangers, information security solutions used today will be obsolete when looking to tomorrow. The security landscape is continually changing – but if as most analysts report it is the human component of any information security framework that is the weakest link, then only a significant change in user perception or organizational culture can really reduce the number of information security breaches.When home users in many countries are still not aware of, for example, the fact that their personal computers can be controlled without their knowledge by hackers with the intent of electronic identity fraud or as part of a network to launch a Denial of Service attack, then there is clearly a significant shortcoming in information security awareness.

For an effective campaign to positively influence the behaviour of the Target Group, the audience has to first be properly evaluated. The interests, needs and knowledge of the Target Group should be identified so as to allow the message that is delivered as part of any initiative to be perceived as one of personal value or interest. The communication channels need to be investigated so as to optimise the delivery of the campaign message. By identifying the preferred communication channels for Target Groups, the campaign has more chance of success. Establishing the most effective channels to use can be done through utilising focus groups or surveys for example. Awareness in general relies on reaching broad audiences with attractive and/or appropriate packaging techniques. It is worthwhile therefore to investigate good practices for raising awareness in areas outside of information security.

4.3 SCM Security

Cybersecurity is focused on information technology, software and networks. Typical cybersecurity activities in this type of risk minimization system include purchasing only from trusted vendors, shutting down critical machines from external networks, and educating consumers about the threats and safeguards they can take [17].

4.3.1 Cyber security compliance requirements in the supply chain

The various compliance provisions clearly state in their requirements how to manage risks in the supply chain, whether this involves an internal process or the involvement of third-party service providers, traders, etc. For example, PCI DSS 3.0 includes requirements such as intrusion testing, lifecycle security for application development and threat modeling – all related to the fact that supply chain risks are a growing problem.

It is very important for organizations to understand that in order to cover cyber risks in the supply chain, they must not only evaluate everything in their internal environment, but also for all actors in the supply chain. For example, credit card companies that meet the PCI DSS need to assess the risks with merchants, distributors, credit card manufacturers, banks, service providers – all actors in the complete supply chain [17].

4.3.2 Supply Chains and Cloud

The cloud paradigm has a huge impact on supply chains. In this model, computing resources, such as databases, applications, and storage, are consumed as utilities accessible through public or private network connections. Cloud supply chain management software is on the rise and the supply chain without any cloud solution is already an anomaly, not the norm. Cloud offers many benefits, including access to low cost and scalable IT resources at any time. But the cloud model can bring additional complexity and security risks to the IT infrastructure of the supply chain, if not properly managed [14].

4.3.3 Monitoring for threats and new technologies

Security is imperative in the supply chain and there are a variety of risks that modern supply chain management faces. As technology evolves, attack vectors will evolve with it and become more sophisticated. Clearly, a prudent security approach must be multifaceted, encompassing protection against a vast array of physical and virtual threats. Examine your vulnerability to these threats to find out well where your weaknesses are, and then prioritize them. There are new technologies, such as control towers, blockchain, authentication and serialization, as well as custody chain solutions and others that can help protect your supply chain [16].

4.4 KM Security

First, the details of how cloud providers will handle security and legal issues, asset control, data transfer and deletion, business continuity, archiving and security policies must be clearly stated in the level agreements. Service level agreements (SLAs). Businesses, every time they use the services of cloud providers, must implement the ISO/IEC 27002 framework, which consists of three broad categories: organizational infrastructure, technical infrastructure and information security, which must be specified in the SLA.

Organizational infrastructure refers to information system management procedures, enterprise assets and security policies. Businesses must ensure that suppliers provide an adequate level of security to protect their assets and propose

appropriate procedures for managing the information system and security policies, including standards and guidelines.

The technical infrastructure includes access control, for which the provider must implement policies, to protect networks from unauthorized activities and to provide secure remote access to data. Systems development and maintenance, communications and operations management, physical and environmental security and incident management are also part of the technical infrastructure, and suppliers must have appropriate security controls and procedures recorded in the SLA. In addition, information security concerns human resources security, business continuity management, compliance and risk management. Sellers must follow recruitment policies and procedures, provide consumer training and carry out risk analysis and assessment. Businesses must have business continuity plans and independent plans for backup or migration to other cloud providers in the event of a disaster.

The technical measures used to improve data security are data protection at rest of the server, encryption of data during transfer and encryption of data by the client. Customer encryption will not be discussed as it is not attractive to most businesses and is not recommended for several reasons. For example, sharing encrypted data would mean handing over a private symmetric key, which could lead to other security issues. In addition, if users lose their personal key or forget their password, access cannot be restored by the administrator, which can result in complete loss of data [18].

For server-side encryption, businesses can use third-party software or features provided by the operating system, such as BitLocker or the built-in NTFS file system encryption mechanism. Both techniques offer protection when attackers have access to the hardware directly or unauthorized users log on to the OS level. For application-level server-side encryption, the optional ownCloud extension must be used. Enabling this feature has no functional limitations, but only the file content is encrypted while the filenames remain legible. However, businesses should be aware that some information, such as a search index, may not be encrypted because it still contains plain text. Another solution is to apply said techniques, which use data masking and data encryption. However, masking and encryption operations are performed on the organization's server, not on the client machine or the cloud server. KM data is stored in a cloud-based database in masked or encrypted form, ensuring data confidentiality and confidentiality while allowing data to be verified.

Data protection during transfer is also essential as the cloud storage service is also accessible through public networks such as the Internet, which can be interrupted during the transfer. Businesses must use Hypertext Transfer Protocol Secure (HTTPS), which uses Secure Socket Layer (SSL) or Transport Layer Security (TLS) for authentication and encryption of communication. For security reasons, it is recommended to use TLS in version 1.1 or 1.2 in combination with modern browsers, whereas TLS 1.0 and SSL 3.0 should only be implemented for compatibility reasons. HTTPS can ensure that the partner is actually the country that he or she is and that no one can read sensitive data easily.

The Federated Identity Management (FIM) system should be used to manage identities, allowing the identity entity to establish links between his/her identities

and for various services across organizational boundaries. The Federation of Identity is about establishing a logical link between identities and is a group of organizations that build trust in each other for secure business cooperation. One example of federal identity is the process of repeating user authentication or simply called single sign-on. Single sign-on causes damage to information leaks if user identity is compromised. Another problem is that FIM systems today do not yet have a dynamic federation and flexible mechanism. Therefore, FIM systems need to be properly implemented, monitored and further enhanced to mitigate these security risks.

One of the other common solutions is to use a firewall to reduce the attack surface of virtualized servers in cloud computing environments. The bidirectional firewall must be deployed on separate virtual machines to provide centralized management of the server firewall policy, and must include predefined templates for common enterprise server types. The firewall should allow features such as virtual machine isolation, fine-grained filtering, coverage of all IP-based protocols, coverage of all types of frames, prevention of denial-of-service attacks, ability to design network interface policies, etc.

The intrusion detection/prevention system must also be deployed on virtual machines to protect vulnerabilities in operating system and enterprise applications from known and unknown attacks. Integrity monitoring software must be implemented at the virtual machine level to detect malicious and unexpected changes to operating system files and applications that potentially compromise cloud resources. Finally, log checking software must be implemented at the virtual machine level to collect and analyze operating system logs and applications related to security events. These events can be sent to a stand-alone security system or to a centralized registration server for correlation, reporting and archiving for maximum benefit [18].

5. Conclusion

The full protection of enterprise applications is a comprehensive process with a lot of steps that the corporations must think of. And every step is an important one because building a secure environment is like building a wall – if there is a missing piece it could crumble under the smallest shake.

Acknowledgment

This work is supported by National Science Program “Information and Communication technologies for unified Digital Market in Science, Education and Security”.

References

1. Dokev, N., Blagoev, I.: Probable risks concerning security in email communication and a protection approach. Problems of Engineering Cybernetics and Robotics 64, 38-51 (2011).

2. Tsochev, G., Yoshinov, R., Iliev, O.: Key problems of the critical information infrastructure through SCADA systems research. In: SPIIRAS Proceedings, vol.18, no.6, (2019), https://doi.org/10.15622/sp.2019.18.6.1333-1356.
3. Kostadinov, G., Atanasova, T.: Security policies for wireless and network infrastructure. Problems of Engineering Cybernetics and Robotics 71, 14-19 (2019).
4. ERP security. https://en.wikipedia.org/wiki/ERP_security.
5. Customer relationship management. https://en.wikipedia.org/wiki/Customer_relationship_management
6. Nunez, M.: Cyber-attacks on ERP systems. Datenschutz Datensich, 36, 653-656 (2012).
7. Synergix Technologies.: 6 Ways to Avoid Security Threats in an ERP System. 2018, https://www.synergixtech.com/news-event/business-blog/6-ways-avoid-security-threats-erp-system/.
8. Montalbano, E. Report: Cybercriminals target difficult-to-secure ERP systems with new attacks, 2018, https://securityledger.com/2018/07/report-cybercriminals-target-difficult-to-secure-erp-systems-with-new-attacks/
9. Dimitrov, K.: 7 Common ERP system security problems and safety steps. https://www.comparethecloud.net/articles/7-common-erp-system-security-problems-safety-steps/
10. Hale, Z.: 5 ERP security threats you can stop right now. (2018), https://www.softwareadvice.com/resources/erp-security/
11. Lee, H., Chen, K. L., Shing, Ch.-Ch., Shing, M.-L.: Security issues in customer relationship management systems (CRM). In: 37th Annual Conference, Bricktown – Oklahoma City, pp. 271-274 (2006).
12. DoS attacks against CRM systems – what you should know. (2014), https://it.toolbox.com/blogs/johndoe/dos-attacks-against-crm-systems-what-you-should-know-062614.
13. Why CRM solutions are targeted for attacks, (2014), https://it.toolbox.com/blogs/johndoe/why-crm-solutions-are-targeted-for-attacks-060414
14. Desai, A.: Data breach in your CRM system. Do you know the risks? (2016), https://www.schellman.com/blog/data-breach-in-crm
15. Yonatan, R.: The practical guide to CRM data security in 2018. (2018), https://getcrm.com/blog/crm-security/.
16. Sreenivasan, S.: How to protect your customer relationship management (CRM) data from hackers, (2017), https://staysafeonline.org/blog/protect-customer-relationship-management-crm-data-hackers/
17. Oracle. What is supply chain management? https://www.oracle.com/applications/supply-chain-management/what-is-supply-chain-management-system.html.
18. Scott, O.: How cybercriminals can initiate attack through a supply-chain partner. (2019), https://www.supplychainbrain.com/blogs/1-think-tank/post/30282-cybersecurity-risks-in-supply-chain-management.
19. Wainstein, L. 7 Supply chain security concerns to address in 2019. https://supplychainbeyond.com/7-supply-chain-security-concerns-to-address-in-2019/.
20. Cyber Security Risk in Supply Chain Management: Part 1. https://resources.infosecinstitute.com/cyber-security-in-supply-chain-management-part-1/.
21. Gunadham, T., Kuacharoen, P.: Security concerns in cloud computing for knowledge management systems. In: Proc. of International Conference on Information Technology and Statistics, pp. 53-61 (2016).