Threats to Information Security

by David Shakarishvili

ITSS Verona Magazine, Vol. 1, no. 1

Spring/Summer 2022

Threats to Information Security

David Shakarishvili

To cite this article: David Shakarishvili, *Threats to Information Security*, ITSS Verona Magazine, Vol. 1, no. 1, Spring/Summer 2022.

Keywords: Information security, Cyber security, Socio-technical, System threat.

ITSS Verona website: https://www.itssverona.it/itss-magazine

LinkedIn: https://www.linkedin.com/company/itss-verona/

Instagram: https://instagram.com/itss_verona?igshid=YmMyMTA2M2Y=

Twitter: https://twitter.com/itssverona

Published online: June 18th, 2022

Abstract: Information security is an integral part of the modern world. The critical relation between information and national security is growing by the day. This is due to both the advancing of the digital age and the systematic nature of public and private cyber attacks. Countries around the world are trying to develop sophisticated and comprehensive information security policies which will protect critical infrastructure and prevent attacks. As the digital era progresses, this discipline becomes a turning point for both individual development and regional policy. Hence, there is a need for an objective assessment of current issues in information security. More precisely, the specifics of a country, its technological preparedness, and regional positions, should all be taken into account when implementing information security policies.

Scientific Methodology

This essay discusses existing information security practices, international standards, and key challenges through secondary literature and statistical data. The paper also makes use of comparative analysis to present information security policies of developing countries. The aim of this paper is to assess current issues in information security, and to develop recommendations based on best practices. This analysis also seeks to pinpoint under-addressed topics which will likely be the subject of future research in information security.

Introduction

Every day, the importance of information security in the national security system grows. This is due to the progression of the digital age and the regularity of cyber attacks in both the public and private sectors. Countries across the world strive to create sophisticated and comprehensive information security policies, hence the need for a global evaluation of these strategies. In a time of unprecedented globalization, , this discipline becomes a turning point in both international relations and regional policy. Information security management is a discipline

which examines security models associated with the protection of state assets, the classification of sensitive information, and the security of top secrets. In contrast, the majority of social science fields view information security as an independent sphere, rather than the interrelated discipline which it is.

1.The simple understanding of Information Security

The definition of information security is still a matter of scientific debate. For example, the line between cyber security and information security is not clearly defined. However, for many scholars, cyber security is understood as one smaller, technical component of the broader information security system (Hameed, 2020). Cyber security refers to specific network devices, while information security includes all kinds of sources (Gantz & Philpott, 2013).

Theoretical Overview

The main theories used in information security research can be divided into two categories: organizational and state level (Fredonia, 2010). However, be noted that there are organizations that are highly influential actors at state and regional levels. Accordingly, there is a high correlation between organizational and state elements of information security. Confidentiality, which refers to the preservation of organizational assets and sensitive material, authenticity, which refers to data quality assurance in case management processes, and availability, which refers to unrestrained access to classified information, have historically been the three main components of information security. Based on the above-mentioned theories, information security is a systematic set of practices designed to protect data from unauthorized access or alterations, both during storage and in the process of transference from one location to another. The following theories, to be discussed below, help create an assessment framework for key threats.

1.1 Theory of socio-technical systems

The starting point of information security threat detection is the linking of social and technical directive norms (Appelbaum, 1997). Socio-technical theory is based on two main principles. The first principle implies a general set of social and technical factors, the connection of which determines the successful or unsuccessful environment for the process. This relationship is on the one hand linear, which implies the prediction of the technical side, and on the other hand the nonlinear social part, which implies the nature of the individual. The application of this theory is real, and such an interpretation of convergence is not trivial (Walker & Stanton, 2015). Moreover, the determinants of the theory of socio-technical systems are of a beneficial nature to the organization.

1.2 Two dimensions of threat

Placing the above theory in a historical context, it is possible to see that the latter was created based on an effective system of industrial best practices (Trist, 1981). This is evidenced by the basic principles on which the theory was based. The collection of data, these fundamental principles towards alteration in order to optimize social and technical factors. This process highlighted another reliable indicator: the influence of external factors (Doebbeling, 2013). It is in this third determinant that we encounter the hazard identification indications.

1.3 Dimension of External Factors

External factors can include all events that threaten information security at the state and organizational levels. Threat classification can be either sectoral or common. Sectoral threats are specific to a certain direction, while common threats are multisectoral in nature. For example, industrial/ economic espionage undermines the information security of the business sector, while cyber-attacks are a multisectoral challenge (Shakarishvili, 2021). In conclusion, the theory of

socio-technical systems is only effective when the specifics of the sector are taken into account.

2.Threat identification in the information security system

Using the theories presented here, this essay analyzes what kind and/or degree of correlation there is between information security and management. This paper has outlined the key components of an organizational information security environment. Measuring the resilience of an information security environment helps to determine whether the latter is ready to withstand damage caused by an external factor as well as what impact it has on security scales.

2.1 Classification of Threats

Information security threats can be divided between those motivated by human factors, and those motivated by technological factors. However, these threats tend to be varied, dynamic and time-dependent.on security. These threats are:

1. Threats motivated by the human factor;
2. Threats motivated by the technological factor (Champion, 2004);

Human-caused threats are often considered to stem from internal organizational issues whether intentional or unintentional (Jouini, Rabai, & Aissa, 2014). Technological threats are mainly due to a lack of information, network and other devices (IT SECURITY CENTER (ISEC), 2009). Both risk factors, however, should be investigated as symbiotic, and not independent phenomena. The latest form of such a symbiotic threat is economic espionage. Espionage has been singled out for intelligence purposes, and as a high-caliber information security threat (Shakarishvili, 2021). In addition to the fact that industrial espionage is the second priority of the Federal Bureau of Investigation, the following statistics are also telling.

2.2 Different Types of Threats

Today, the demand and guarantees of business intelligence are so high that they have a colossal impact on the global economy. According to the latest statistics, spending on

intelligence from 2016 to 2020 will increase from $15.24 to $29.48 billion USD, compounded by an 11 percent annual growth rate (Bulao, 2021). This is a growing trend incloud-based businesses, whose spending in 2013-2018 has grown from $750 million to $2.5 billion USD, with a compound annual growth rate of 31 per cent (Bulao, 2021). Forty-six percent of small businesses use business intelligence tools as key elements of their organization's strategy. It also named four of the largest and most protected mega corporations in business intelligence: 1. Amazon Web Service; 2. Microsoft Azure; Google Cloud; 4. IBM Bluemix (Shakarishvili, 2021).

As of 2020, the picture of espionage targets is diverse. However, the top three victims in the industrial sector are financial, informational, or public profile organizations (Joseph Johnson, 2020).

As seen from the data, information security threats are growing which has also caused an increase in the share of costs corporations will spend fighting them from year to year. Furthermore, in addition to the private actors, international standards on what kind of information security policies should be pursued are also important.

3.International Information Security Standards

3.1 The Main Standards of European Union

In 2020, the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy presented a cyber security strategy with new focuses (Commission, 2020). These included the following:

1. ***NIS directive*** - Network security and information systems that address the information security readiness of States. The directive obliges member states to set up an interagency coordination council and to cooperate with one other. This indicates the growing scale of

the threat. In recent years, information security attacks have not only been a source of harm to some countries, but also a kind of measure by which the information security environment has been assessed. This new strategy,implies that the challenges of information security are of unlimited scale and need to be addressed at the continental level (Commission, 2020);

2. ***Public-Private Partnership (PPP)*** - The strategy also makes recommendations for private-public sector cooperation. Whereas the private sector is more flexible and dynamic in implementing innovations, the public sector ought to create stronger legal framework (Commission, 2020);
3. **Voting s*ecurity*** - The electoral process remains one of the main challenges to information security, especially in developing countries. The strategy created by the EU is also acceptable for non-EU countries, because it is schematic. A key purpose of attacking an information security environment is to influence voters using a tool of instant effect, to put it more simply, to leave a shocking and negative mark on the public (Shakarishvili, საქართველო, 2020). In such a case, the goal is to split public opinion based on contradictory views that are still strongly prevalent in post-Soviet countries; for example, Soviet nostalgia, lack of freedom of choice, disproportion of election results and voter turnout. In short, the information security attack introduces a new narrative and/or promotes the popularity and/or democratic values of the existing narrative, attacking common sense (Shakarishvili, საქართველო, 2020).

This strategy is not only of a recommendatory nature, but also provides solid leverage to address fundamental issues. For example, given the scale of information security threats, a cyber unit and a blueprint have been developed for risk assessment and prevention. However, the effectiveness

of the strategy cannot be assessed, as future risks and information security challenges determine how effective, efficient, and prevention-oriented the strategy is in dealing with such crises.

Conclusion

The threat to information security can be shaped by both external actors (neighboring state - society) and as internal actors (government - society). To state that a threat provoked by an outside state is more dangerous than a campaign initiated by a local is false. Both are aimed at the destruction of society, and attempt to influence public opinion through undemocratic manipulation. In some cases, propaganda produced by a local government to serve private interests can also act in the interests of a foreign nation. Thus, the following factors should be considered when implementing regional and organizational information security policies:

1. ***Innovation -*** The development of artificial intelligence and its proper formation in a multi-sectoral environment to contribute to the strengthening of information security. With proper algorithms and programming, an autonomous system will be able to identify threats motivated by human, technological and external factors.
2. ***Openness of experience*** - Even the most effective information security structure requires consideration of multiple actors. Accordingly, the creation of legal bases and circular systems should be based on the principle of cooperation. The advantage of this is that the threat will be identified from different perspectives.
3. ***Raising of awareness*** - Different sectors in developing countries need to focus on knowledge specialization. Personnel with high visibility and low probability of risk are directly proportional.

As the challenges facing information security have grown so dramatically in recent years, each aspect of the discipline must be considered in order to respond quickly and effectively.

Reference list

Appelbaum, S. H. (1997). Socio‐technical systems theory: an intervention strategy for organizational development. *Management Decision*, *35*(6), 452–463. https://doi.org/10.1108/00251749710173823

Bulao, J. (2022). 45 Amazing Business Intelligence Statistics for 2022. *Techjury*. https://techjury.net/blog/business-intelligence-statistics/#gref

Champion, A. (n.d.). *Threats and Attacks*. CSE 4471: Information Security. http://web.cse.ohio-state.edu/~champion.17/4471/4471_lecture_2.pdf

Flanagan, M. E., Saleem, J. J., Millitello, L. G., Russ, A. L., & Doebbeling, B. N. (2013). Paper- and computer-based workarounds to electronic health record use at three benchmark institutions. *Journal of the American Medical Informatics Association*, *20*(e1), e59–e66. https://doi.org/10.1136/amiajnl-2012-000982

Fredonia, S. (2010). *Information Management and Cyber Security Policy*. https://www.fredonia.edu/sites/default/files/section/about/offices/information-technology-services/_files/isec.pdf

European Commission. (n.d.). *Cybersecurity Policies | Shaping Europe's digital future*. Digital-Strategy.ec.europa.eu. https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies

Johnson, J. (11 C.E., November). *Industries most targeted by cyber espionage 2019*. Statista. https://www.statista.com/statistics/221293/cyber-crime-target-industries/

Jouini, M., Rabai, L. B., & Aissa, A. B. (2014). Classification of security threats in information systems. Ambient Systems, Networks and Technologies. Tunisia: ScienceDirect. (ANT-2014). 489 – 496.

Kim-Kwang Raymond Choo, & Dehghantanha, A. (2017). *Contemporary digital forensic investigations of cloud and mobile applications*. Elsevier.

Sarker, I. H., Furhad, M. H., & Nowrozy, R. (2021). AI-Driven Cybersecurity: An Overview, Security Intelligence Modeling and Research Directions. SN Computer Science, 2(3). https://doi.org/10.1007/s42979-021-00557-0

Shakarishvili, D. (2020, October 28). საქართველო.Shakarishvili, D. (2021, May). STUDIES IN A CHANGING BUSINESS ENVIRONMENT. Economic Espionage Review, 158-121.

Trist, E. L., & Ontario Quality Of Working Life Centre. (1981). *The evolution of socio-technical systems*. Ontario Quality Of Working Life Centre.