Guidelines for the Management of Cyber Risks

Gabi Siboni and Hadas Klein

Cyber risk management is crucial to improving the level of organizational defense and preparedness for cyber events. This process is an important component in an organization's operational risk management and in its overall risk management. Organizations in several sectors within Israeli society are obligated to a process of managing cyber risks in accordance with the instructions of the regulator. The aim of this article is to examine the method of risk management, to propose guidelines for the management of cyber risks, and delineate the major stages of this process.

Keywords: Risk management, business continuity, cyber risks, cyberspace

Introduction

In May 2017, the media published reports about the theft of personal information of Kmart customers, marking the second time in three years that the data of Kmart shoppers had been stolen. Several small banks in the United States reported that they received warnings from credit card companies regarding a number of batches of stolen credit cards, which all had one thing in common: They were used to make purchases from the retailing giant Kmart. Given the reports in the media, Sears Holdings, the owner of Kmart, confirmed that some of its payment systems had been damaged by

Dr. Gabi Siboni is the head of the Cyber Security Program at the Institute for National Security Studies. Hadas Klein is a researcher in the Cyber Security Program at the Institute for National Security Studies.

hostile code. According to the company, advance detection failed to identify the code, but after detecting the cyber event, the malware was cleaned from the systems. Sears Holdings, however, did not address the question of how many of Kmart's 735 stores had been compromised by the event.[1]

The response of Sears provides additional evidence that preventing cyber events is critically important, even more so than the ability to identify and recover from them. This was especially significant in the case of Kmart, which was first attacked in October 2014 and has still not recovered; since the first cyber event, its sales have plummeted by more than 72 percent and its stock price has fallen by 88 percent.[2]

Addressing these attacks as a series of individual events as opposed to a systemic failure can be problematic, particularly when it results in insufficient treatment that should be done across the organization. The management of cyber risks and risks to supporting systems is meant to address systemic problems precisely of this kind. Kmart did not provide detailed information about the event, but involved parties have noted that even though the source of the problem may have been a component of the supply chain or employee negligence, it can be assumed that the root of the problem in both instances was the same: poor risk management, lack of inter-organizational transparency, and difficulty identifying the relationships between different systems.[3]

The management of operational and financial risks within organizations is a well-developed approach that is today widely implemented. In recent years, many organizations have also been applying this approach in managing computerized systems risks and cyber risks. This article seeks to provide those engaged in this work with guidelines and a methodology for conducting risk management in the cybersphere. It begins with a theoretical survey of the field of risk management and its benefits for organizations and then continues with a detailed proposal to implement in practice.

[1] Brian Krebs, "Credit Card Breach at Kmart Stores. Again," *KrebsOnSecurity*, May 2017, https://krebsonsecurity.com/2017/05/credit-card-breach-at-kmart-stores-again.

[2] Steven Minsky, "Kmart Cyber Breach: Another Failure in Risk Management," *LogicManager*, July 26, 2017, https://www.logicmanager.com/erm-software/2017/07/26/kmart-cyber-breach.

[3] Minsky, "Kmart Cyber Breach."

The Theory of Risk Management

Risk management is a method that became a subject of study and research following World War II. The knowledge of this field originated with two books published in the mid-1960s that addressed the theory of risk assessment.[4] The process of risk management first began by examining market risk to defend against financial losses that could result from events and accidents. In the 1970s, it began to develop as a tool for managing the financial risks faced by financial institutions, banks, and insurance companies. Analysis of operational risks and liquidity risks appeared in the early 1990s.[5] Since then, risk management has become widely practiced within a variety of organizations, including commercial companies, airlines, state authorities, and so forth.

In the business world, risk management is conducted in many areas, including operational risk management; that is, assurance that the operational infrastructure of the organization will continue to function even if fundamental components should fail; financial risk management, including credit risk, currency risk, and market risk; and the management of risk related to regulation, law, or ethics.

The aim of the risk management process is to reduce the impact of irregular events on the organization. The process involves formulating risk scenarios that could detrimentally harm the organization; assessing the potential for damage should these scenarios occur; estimating the probability of the scenarios in question; prioritizing control measures for addressing scenarios based on their intensity, which is a combination of the impact of the risk and the probability of its being actualized; and finally, devising a plan to reduce risk. The life cycle of the risk management process typically consists of several stages, as discussed below.

[4] R. I. Mehr and B. A. Hedges, *Risk Management in the Business Enterprise* (Homewood, Il: R. D. Irwin, 1963); A. Williams and M. H. Heins, *Risk Management and Insurance* (New York: McGraw Hill, 1964).

[5] Georges Dionne, "Risk Management: History, Definition and Critique," *Risk Management and Insurance Review* 16, no. 2 (Fall 2013): 147–166.

Stage 1: Defining an Organization's Risk Appetite

The term "risk appetite" refers to the amount of general risk that an organization is willing to take in order to achieve its goals.[6] It expresses an organization's willingness to sustain high/low levels of exposure to risk and uncertainty in order to achieve its strategic goals. An organization's board of directors and management typically determine the risk appetite. It is a subjective process that is supposed to strike a balance between the potential returns that accompany the risk taking and the potential loss from it. Risk appetite frameworks provide the management with a clear picture of the desired risk and a perspective to balance between risk and return. An organization's risk appetite is not static; the management may request to change the level of risk it is willing to take according to conditions over the course of time.

Stage 2: Identifying Risk Scenarios

This stage involves identifying the risks by conducting research, which includes formulating risk scenarios based on the history of risks that were internal and external to the organization. This is done by surveying the organization's critical business processes, to understand which are most meaningful for the organization's functioning. These include examining processes of production, operations, and sales; surveying organizational assets that support these processes (such as manpower, computer infrastructure, machines, and so forth); analyzing the organization's exposure to risks that could have implications on its management, such as economic risks (for example, a slowing economy) and how these risks can affect the company's sales; analyzing sectoral risks, such as the impact of Israel's security situation on the foreign tourism sector; and finally, examining the legal and regulatory requirements, such as the impact of safety laws, building laws, and the like.

Stage 3: Analyzing Risk Scenarios

Risk is defined as the probability of a harmful event occurring, combined with the outcome of the event itself. Risk therefore is the product of two parameters: the probability that a specific scenario will occur and the anticipated impact of the damage if the scenario is realized. The result of multiplying these two measures is known as inherent risk i.e., the level

[6] "Principles for an Effective Risk Appetite Framework," *Financial Stability Board*, November 18, 2013.

of the untreated risk. Identifying and analyzing risk scenarios is based on research, which includes examining similar scenarios in the history of the company and elsewhere, providing expert opinions, assessing previous risk management/survey reports, financial reports, legal proceedings, information regarding insurance claims, and so forth.

The intensity of the damage is assessed according to parameters of direct and indirect damage resulting from a scenario of harm to the organization. Direct damage can result, for example, from disrupting an organization's operational continuity as a result of disabling the systems or being unable to engage in production as planned. Examples of indirect damage might include injuring the organization's reputation as a result of being unable to meet its obligations, legal claims, and so forth.

Stage 4: Formulating a Plan to Reduce Risk

Control measures are tools and processes that organizations use to reduce risk. An organization's control system consists of all the tools that are part of an organization's work processes in relation to the objects of risk. An organization cannot run effectively without a systematic and proper system of controls.

The types of control measures that operate within an organization can be divided into several categories:

- *Preventative controls*—designed to prevent causing a failure, including changes to the organization's mode of operation. For example, a production process may be found to be excessively dangerous, and as a result, the management may decide to refrain from employing it.
- *Diversion tactics*—intended to shift the impact of the failure to an external party, such as a subcontractor or an insurance company.
- *Detective controls*—designed to detect undesired actions that have already taken place, which then enables the organization to rectify them after their occurrence. An example is producing a report of irregularities in order to analyze and monitor irregular actions.
- *Corrective controls*—intended to rectify undesired actions after their occurrence. One example is the automatic reconstitution of data after a computer system crashes.
- *Compensative controls*—aimed to provide a response where the existing controls are not sufficiently strong enough.

Stage 5: The Analysis of Residual Risk

Residual risk is risk that remains after applying the risk reduction plan. After implementing the controls, the level of residual risk should be lower than the level of the inherent risk of the event analyzed. In addition, the level of residual risk must be within the limits of the designated risk appetite. If the residual risk is unacceptable (too high), additional control measures must be implemented to lower the residual risk to an acceptable level, as determined by the management in its definition of risk appetite.

The Importance of Cyber Risk Management

The rapid pace of technological change, the increasing number and availability of digital services—interfacing with the old system—and the growing need for lines of communication with suppliers has created a breeding ground for developing cyber threats, thus exposing many organizations to critical cyber risks. The past decade has also witnessed a steady increase in the number of threat factors, in terms of ability, availability, attack tools, and attack groups. As a result, it has been only natural to manage cyber risks with methods of risk management; nonetheless, we still have a long way to go until these methods are routinely implemented.[7]

Cyber risks are part of both the operational and the overall risk management in an organization. According to a survey conducted by Deloitte Israel in 2017, the number of organizations managing cyber risks has increased significantly.[8] Some 60 percent of the major companies in Israel collect and analyze information in order to obtain an updated picture of cyber threats. The survey also indicates that more than 50 percent of the large companies in the Israeli economy maintain a risk management framework and implement a corporate cyber defense policy, while a comparable number conducted a cyber risk survey in the year that preceded the report. Although these figures are higher than average within the Israeli economy as a whole, there is still room for improvement.

Adopting a risk management approach in the field of cybersecurity has a number of advantages:

[7] "The Israeli Market and Cyber Threats: A Situation Assessment, 2017," *Deloitte Israel*, 2017, https://www2.deloitte.com/content/dam/Deloitte/il/Documents/risk/Deloitte_Cyber_Infographic1.2.pdf.

[8] "The Israeli Market and Cyber Threats: A Situation Assessment, 2017."

- *Financial* —Optimizing a cyber defense system and developing an information security policy can prevent not only direct losses, such as monetary theft, but also indirect losses, such as damage to reputation. It can also prevent fines for non-compliance with legal and regulatory requirements. For example, violation of the European Union's international regulations for the protection of data (the General Data Protection Regulation) results in administrative fines of up to €20 million, or up to 4 percent of an organization's annual turnover, whichever is greater.[9] A cyberattack can also impact a company's stock price by dealing a severe blow to customer trust and/or damaging its reputation and brand name.
- *Strategic* —Appropriately addressing the cyber challenge with an optimal cyber defense system enables the organization to clearly understand its exposure to cyber risks. This affects the level of trust among the interested parties and investors in the organization as well as the organization's ability to achieve its goals.
- *Legal* —In many countries, an organization's protection of its information and its digital assets are defined by law as being the responsibility of the organization's managers and board of directors.
- *Operational* —A cyber event may affect a variety of operational elements, including the supply chain, production pricing, manpower, and so forth. For example, a cyber event that damages the lines of communication with company suppliers can result in substantial disruptions to the production process.
- *Business Continuity*—An improved capacity to handle cyber events has a direct result on an organization's ability to maintain business continuity or at least to minimize the time it takes to resume work.

The challenge of cybersecurity is often seen as being within the purview of information system personnel, who also hold the key to the solutions. Today, however, it is clear that cybersecurity is not a problem that can be resolved by using technological tools alone; rather, it is a comprehensive challenge that encompasses people, organizational processes, technology, and organizational policy. These and other elements are extremely important to the organization's overall security, stability, and strength.

[9] Section 83 of Regulation (EU) 2016/679 of the European Parliament and of the European Council, April 27, 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN.

Cyber Risk Management

Cyber risk events can disrupt an organization's proper and secure activity, can cause failure to provide service, expose business or customer information, delete and disrupt data, and so forth. Damage potential is a standard aspect of risk management. In the cybersphere, the potential for damage is manifested not only in damaging the information within the context of the triad of confidentiality, integrity, and availability but also in other aspects, such as reputation, law and regulation, and business continuity.

In recent years, several regulatory directives relating to cyber risk management have been issued. One example is the Bank of Israel's Proper Conduct of Banking Business Directive No. 361 regarding cyber defense management.[10] This directive requires the banks in Israel to manage their cyber risks in order to reduce the probability of their being realized. Defining the methodology of cyber risk management requires organizations to prepare risk scenarios and analyze their systems of protection.

The instructions of Israel's Ministry of Finance stipulate that institutional bodies in Israel must assess their cyber risks using the following measures: identifying processes, systems, and information assets; mapping the risks posed to processes, systems, and information assets; framing the inherent risks; mapping and assessing the control measures for minimizing these risks, including the impact of the control measures on the risks themselves; and finally, assessing the residual risk according to the effect of the control measures that were implemented.

To implement these principles, it is recommended to act according to the risk scenario—based on the organization's processes and the information assets that are to be protected—and to continue defining the cyber risk scenarios to which the organization is vulnerable. It is also recommended to assess the inherent risk should the scenario be realized, as well as to analyze the maturity of the cyber control system by evaluating the extent of its assimilation, and then to consider the effectiveness of the organization's available cyber controls. Finally, it is recommended to evaluate the residual risk and the breaches in defense and to prioritize formulating a work plan designed to meet these gaps.

[10] Bank of Israel, Circular 2457-06-H, Cyber Defense Management, March 16, 2015, http://www.boi.org.il/en/BankingSupervision/LettersAndCircularsSupervisorOfBanks/Curculars/h2457_en.pdf.

Defining Risk Scenarios

The method of defining risk scenarios begins with analyzing the organization's critical business processes, in addition to their supporting digital systems and assets. It then continues with formulating possible cyberattack scenarios. This stage is based on intelligence gathering and analyzing attack trends and potential cyberattackers. In addition, unintentional technological fault scenarios should also be analyzed. The attack scenarios should be mapped onto the critical processes and their supporting systems.

The critical processes and their supporting digital systems and assets are analyzed by applying the Business Impact Analysis (BIA). BIA is part of a broad toolbox meant to contribute to business continuity and help the organization recover as quickly as possible after an event. BIA is part of the recovery plan as it can help estimate the damages caused and the relative importance of the different parts of the organization. Organizational BIA documents sometimes fail to relate to the various aspects of the cybersphere, such as confidentiality and informational integrity. Documents that do not address specific cyber elements should be updated accordingly. The BIA and the organizational cyber defense strategy document should provide a prioritized list of the digital assets that are designated for protection. In this framework, it is important to define the principles and the aims of defense, as determined by the organization's board of directors, the regulators, and other parties of interest.

Contending with possible cyberattack scenarios requires an assessment of the organizational cyber risks as they relate to a number of points: Who are the parties that could have an interest in attacking the organization? What are their capabilities and the tools at their disposal? Who have they attacked in the past and in what manner? This assessment should rely on a preliminary process of intelligence gathering, including analysis of attack trends, potential attackers, and their capabilities.

Intelligence gathering focused on the needs of the organization should define the relevant components of information to be gathered. This action is usually referred to as EEI (essential elements of information). EEI defines the range of relevant sources of information and the focus areas for information gathering. For example, a banking organization in Israel should concentrate its intelligence gathering on threats to the banking industry by criminal organizations, enemies, and activist groups that could take action against a specific economic policy or against "global capitalism."

The information gathered serves two primary goals. The first is to continuously update the threats, which serves the organization in assessing the situation and in providing rapid and focused responses to new threats. The second is to formulate risk scenarios with which the organization could be forced to contend, while also noting relevant parameters for quantifying the threat, including the probability of the event, the extent of damage, and so forth. The sources of information for intelligence gathering include commercial information services (in accordance with EEI), available free sources, cooperative endeavors, and information sharing with relevant parties (such as sectoral cooperation centers), CERT (Computer Emergency Response Team) and other parties, and finally, parties that provide the organization with guidance.

The Assessment of Inherent Risk

The process of assessing inherent risk is conducted in two stages: weighing the damage potential in the event that a risk scenario is realized, and evaluating the probability that the scenario will take place. Assessment of the damage potential of each scenario should be done in consultation with commercial parties. They can estimate the extent of economic loss for each scenario while analyzing the risks to strategic business assets as defined by the organization and important to protect. In addition to the direct damages, indirect damages—such as exposure to legal claims, sanctions, damage to reputation and functional continuity—should also be considered.

A number of measures are used to determine the probability of a scenario being realized. The first is the realization of a similar scenario in a comparable organization in the past. However, due to the difference among cyberattacks and the existence of an extremely wide variety of attack scenarios and events, we cannot rely solely on this measure. It is therefore possible to use two additional measures. The first one reflects the cyber intelligence team's subjective assessment of the probability of a risk being realized, using a ranking of 1–5 (with 5 indicating the highest likelihood of occurrence). The second measure is the level of structural exposure, or how easy it is to attack the assets as described in the scenario. Structural exposure is determined by the different attributes of the organization's internal technological environment, which include the number of interfaces, the number of users, internet access, communications equipment, connectivity between stations, and so forth. Each attribute is given a value, which ranks the technological environment's level of exposure to cyberattack. These values are also based on a scale of 1–5, with 5 indicating the most easily attacked. For example, the more internet access points an organization has, the easier it is to attack it. An organization with one point of access to the internet, therefore, will receive a ranking of 1, whereas an organization with dozens or hundreds of internet access points will receive a ranking of 5. Each attribute is similarly assessed. To calculate the level of structural exposure, an adjusted calculation of the average scores of the various parameters is conducted.

The likelihood of a risk (RL) being realized is calculated by the following formula:[11]

$$RL\ (Risk\ Likelihood) = \frac{RE\ (Risk\ Exposure)\ \times AS\ (Analyst\ Score)}{5}$$

when RE is the score for structural exposure, and AS is the score given by the intelligence investigator to the probability of the risk being realized. The purpose of dividing by 5 is to standardize the probability for values between 1 and 5.

Inherent risk (IR) is calculated as follows:

$$IR\ (Inherent\ Risk) = \frac{RL\ (Risk\ Likelihood)\ \times RI\ (Risk\ Impact)}{5}$$

when RL is risk likelihood, and RI is risk impact.[12] The purpose of dividing by 5 is to standardize the probability for values between 1 and 5.

The analysis of systems that support critical processes in an organization, the gathering of intelligence and its analysis for threats, and the completion of risk analysis enable the assessment of the organization's critical cyber risks. Below is an example:

[11] All values are ranked from 1–5.

[12] The approach to calculating inherent risk presented in this article is one of a number of existing approaches. It is presented here for the purpose of example.

Title of the Threat	**The Title of the Threat for the Sake of Establishing a Common Language**
Cause of the Threat	The cause of the threat based on the intelligence gathered.
Route of Attack	The route of the threat being realized based on the organization's intelligence and technological information.
Critical System Affected	From the list of systems that support critical processes.
Probability	Assessment of the probability of the scenario's realization.
Damage	Assessment of the potential damage stemming from realizing the scenario.
Inherent Risk	Measure of the inherent risk as calculated using the inherent risk equation.

Assessment of the Maturity of Cyber Defenses

Controls in the cyber realm can be classified into three primary categories:

1. *Preventative control measures,* which are meant to assist in monitoring and supervising data and activities and in preventing errors, oversights, and intentional damage. Examples of control measures in this category include the separation of positions and permissions, entry controls, and the gathering and analysis of cyber intelligence.
2. *Detective control measures,* which assist in identifying irregularities. Examples of control measures in this category include systems for the detection of anomalies in the users' behavior, such as a user working at unreasonable hours and performing actions that are not part of the usual work of his or her position.
3. *Corrective control measures*, which assist primarily in restoring the previous situation and routine (for example, back-up and reconstitution processes) and in improving defenses.

The overall control system should be adapted to meet the needs of the organization. Today, there are a number of standards and directives that define a general control system structure. Examples can be found in the recommendations of the National Institute of Standards and Technology (NIST), which provides guidance for US federal bodies,[13] and the Federal Financial Institutions Examination Council (FFIEC), which sets standards for the banking sector in the United States.[14] Organizations can also make use of the cyber defense doctrine that was written by Israel's National Cyber

[13] "NIST Cybersecurity Framework," *NIST*, https://www.nist.gov/cyberframework.

[14] "Cybersecurity Assessment Tool," *Federal Financial Institutions Examination Council (FFIEC)*, https://www.ffiec.gov/cyberassessmenttool.htm.

Directorate.[15] Assessing the control measure maturity is done individually by analyzing two parameters: first, the extent of the control's implementation and second, its effectiveness.

Assessing the control maturity requires conducting interviews with technological personnel within the organization and with other parties, such as a risk management unit (if such a unit exists within the organization). A table should be prepared for each control measure, reflecting its own unique scoring. A scale assessing the implementation of the control measure within the organization needs to be defined. This analysis is done according to the unique parameters of each control measure, using a scale of 1–5, with 5 indicating maximum implementation. The following table provides an illustrative example analyzing the control measure of employee awareness of cyber risks:

Assessment of Assimilation of Control Measure	**Score**
There is no process of building employee awareness.	1
There is a basic process of awareness building, including instructional sessions, fliers, organizational portal.	2
An advanced process of awareness building has been implemented, including general exercises.	3
An advanced organizational process has been implemented, including performance control and measurement.	4
An advanced organizational process has been implemented, in addition to an external process aimed at building business partners' awareness of cyber risks.	5

It is also necessary to assign a value to each control measure indicating its importance in the organization's overall defense system. The values range from 1–5: The greater the control measure's importance to the defense system, the higher value it is assigned. At the end of the control assessment process, the maturity score can be determined using the following matrix:

[15] "Cyber Security Methodology for Organizations," *National Cyber Directorate, Prime Minister's Office* [Hebrew], https://www.gov.il/he/Departments/policies/cyber_security_methodology_for_organizations.

$$CM = \begin{array}{cc|c|c|c|c|c|}
 & & \multicolumn{5}{c}{CI\ \text{Control Importance}} \\
 & & 1 & 2 & 3 & 4 & 5 \\
\hline
 & 1 & 5 & 3 & 2 & 1 & 1 \\
\hline
 & 2 & 5 & 3 & 2 & 2 & 2 \\
\hline
CA\ \text{Assimilation of Control} & 3 & 5 & 4 & 3 & 3 & 3 \\
\hline
 & 4 & 5 & 4 & 4 & 4 & 4 \\
\hline
 & 5 & 5 & 5 & 5 & 5 & 5 \\
\hline
\end{array}$$

Control maturity (CM) is a function of control importance (CI) and the extent of the control's assimilation within the organization (CA). It is determined in accordance with the values of the matrix.

Control maturity scores are determined according to the values that appear in the matrix. In this way, a preferred plan can be set up for handling the control measures. The lower the control maturity score is, the higher priority it should be given. This means that the control measures at the top of the list will be optimal to improving the overall system of defenses.

The matrix values deal with extreme situations in the following manner: It is not necessary to invest resources to address a control measure that has a score of 1 (low) in importance; therefore, the control maturity value for all controls with an importance of 1 is 5. In addition, investing in a control measure with an implementation score of 5 (maximum) is unnecessary, and therefore the control maturity value for all control measures with an implementation level of 5 is 5. It is also important to consider the costs of addressing control measure. For example, a control measure with installation and maintenance that is expensive and eats up a significant portion of the budget of the defense system is not necessarily effective, even if defense tops the list of priorities. In such a case, normalization can be conducted, reflecting the relative cost of the control.

Analysis of Residual Risk

Residual risk indicates the potential of damage that could be caused to an organization as a result of a cyber event that occurs after implementing the existing control measures. For the organization to contend with cyber risks, it must assess the residual risk for each individual scenario, as identified at earlier stages of the process. Residual risk (RR) is calculated using the following formula:

$$\textit{RR (Residual Risk)} = \textit{IR (Inherent Risk)} - w \times \textit{CS (Control Score)}$$

when IR is inherent risk, CS is controls score (the quality of available controls), and *w* is a control score coefficient. It is often acceptable to assign a coefficient when calculating the residual risk so that the quality of the available controls is reduced by a certain percent, in order to benefit from a higher level of confidence in the residual risk. For example, it could be decided to make use of a controls score that is 30 percent lower than that calculated, which would require using w=0.7 in the formula.

Calculating residual risk requires determining the overall score of the cyber defense system for the scenario in question. This is done using the following formula:

$$\textit{OCM (Overall Control Maturity)} = \frac{\sum_{i=1} CM_i \textit{ (Control Maturity)}}{n}$$

when the Overall Control Maturity is the average of *n* Control Maturity scores for the scenario in question. The residual risk for each scenario is calculated using the following formula:

$$\textit{RR (Residual Risk)} = \textit{IR (Inherent Risk)} - w \times \textit{OCM (Overall Control Maturity)}$$

when IR is inherent risk, CS is controls score, and w is the CS coefficient.

Now, the organization can assess whether the residual risk is compatible with the risk appetite as defined by the organization's management. In the event of disparities, it will be necessary to return to the stage of control prioritization and to formulate a work plan aimed at improving the system of defenses or alternatively, to reduce dangerous activity in the cybersphere.

Conclusion

The aim of this article was to provide guidelines for the management of cyber risks, based on the basic theory of the discipline of risk management that has been evolving since the 1960s. The article presents one approach to the proposed process. Although other approaches exist, almost all rely on the theoretical basis of risk management.

Managing cyber risks is a critical component in managing an organization's cybersecurity systems in addition to other elements, such as penetration tests. This process enables the organization to assess the level of risk it faces, to methodically define the organization's means of defense, and to determine whether the level of exposure to risk is compatible with that defined and stipulated by the board of directors, the organization's management, and the various interested parties.

Implementing the guidelines described above are not a guarantee for preventing cyber events. They will, however, ensure that those responsible for the organization's defense systems will acquire a deeper understanding of the cyber risks with which they must contend. Thus, implementing the guidelines can go a long way in reducing the risks that an organization faces within the framework of its business needs. According to expert assessments, the systemic problem discovered in the Kmart corporation during the cyberattacks discussed above was due to poor implementation of risk management processes.[16] Implementing a systematic and orderly risk management process can help reduce an organization's exposure to risks, as well as diminish the reputational and financial damage that may result from events of this kind.

[16] Minsky, "Kmart Cyber Breach."