Sectoral Ability to Manage Cyber Risks in the Supply Chain

Gabi Siboni, Hadas Klein, and Ziv Solomon

This article presents the cyber risks that originate in the supply chain and the challenges that they pose. It examines a number of global methodologies and standards for managing cyber risks in the supply chain and proposes a model for concentrated sectoral management of the challenge so that the process of checking and authorizing suppliers will be streamlined. The proposed model has been found to be feasible in terms of the investment and pooling of resources as well as in increasing the general security level of the various sectors, thus raising the level of cyber protection in the Israeli economy as a whole.

Keywords: Cyber threat, cyber risk management, supply chain, cyberspace

Introduction

In July 2018, a research team from Microsoft identified an attack on a software company that was intended to implant malicious code in a legitimate software product and use it to reach thousands of other customers.[1] In this case, anonymous attackers managed to take control of the shared infrastructure of a software company that provided a PDF editor and another company

Prof. Gabi Siboni is the head of the Cyber Security program at INSS. Hadas Klein is a cyber researcher at INSS. Ziv Solomon is a cyber security consultant. The article is based on a research paper written by Gabi Siboni, Ziv Solomon, and Hadas Klein, "National Cyber Risk Management for the Financial Sector: Reducing Supply Chain Risks," INSS, December 2018.

[1] "Attack Inception: Compromised Supply Chain within a Supply Chain Poses New Risks," Microsoft Defender Research Team, July 2018, https://bit.ly/2UcVsGB.

that provided an installer, so that the installer would install the malicious code along with the PDF editor. An investigation showed that the software company that provided the PDF editor had not been attacked at all. Rather, its product had been replaced through interfering in the process at the second software company, which provided the installer. This example is an indication of the large amount of resources that attackers invest in order to reach their targets through the supply chain.

A "supply chain" is defined here as "a system of factors involved in the supply of a product or service, including service providers, software and information system suppliers, hardware suppliers, and so forth." In the current global era, which is characterized by technologically complex goods and services and support from a wide variety of suppliers for each product or service, it is necessary to ensure cyber protection for the suppliers of each organization. The example provided above is one of many where an attacker exploited security breaches at an organization's supplier in order to penetrate the computer network of the organization it sought to attack.

The optimal handling of cyber challenges in the supply chain requires a concrete response to the needs of the organization and the sector to which it belongs, as well as a response for organizations that are identified as Israeli because of their exposure to cyberattacks of an anti-Israel nature. Many organizations in Israel are subject to guidelines from regulators such as the Banking Supervision Department; the Capital Market, Insurance, and Savings Authority; the Ministry of Health as the regulator of the various healthcare organizations in Israel; and more. Protecting such organizations requires an array of defensive components, among them a level of technological protection and work procedures, including those that relate to cyber threats in the supply chain. The more organizations successfully identify the threats and take the necessary measures to mitigate them at an earlier stage, the more their overall defensive level will increase.

This article discusses the challenge of dealing with cyber risks in the supply chain and provides general recommendations for dealing with them, while also addressing relevant global standards, Israeli regulations, the relevant threat map in the supply chain context, existing methodologies, models for managing suppliers in the supply chain, and possible approaches. The article provides examples from the Israeli economy that could have a possible connection to the subject.

Theoretical Background

A number of models for managing supply chain risks can be found in both industry and in the professional literature. In the book *Purchasing and Supply Chain Management*, three categories of suppliers are outlined: strategic suppliers that are extremely important to the purchasing company and for which it is difficult to find a replacement; preferred suppliers that are important to the purchasing company but can be replaced with some effort; and transactional suppliers, which can be replaced within a short time.[2] In addition to the proposed types of suppliers, this article provides a survey of several supply chain management models in entities relevant to our discussion.

Deutsche Telekom has a four-stage methodology for managing the supply chain for more than 30,000 suppliers in more than 80 countries.[3] Its aim is to mitigate the risks and encourage the company's suppliers to improve their work methods. In the first stage, all potential suppliers with an annual order volume of more than 100,000 euros are surveyed about topics such as human rights, corruption, environmental protection, and employment health. All suppliers are required to be surveyed again after three years. As business relations continue, the company asks the suppliers that are strategically relevant and/or those at high risk to provide wide-ranging information on their work methods through the information system. In the second stage, these declarations are assessed on the basis of additional background information and a focused study. For suppliers at higher risk, additional information is required, and site visits are made. The efficiency of the review increases, and duplicate visits are avoided by cooperating with 13 additional companies that implement the process through Joint Audit Cooperation (JAC).

In the third stage, the suppliers are classified and assessed based on the information supplied and the results of the audits. According to Deutsche Telekom, the company cooperates closely with its suppliers in order to deal with serious problems that are identified. In the fourth stage, a development program is implemented and workshops are held for suppliers. In cases where a supplier significantly ignores the company's requirements, higher authorities within the supplier are involved and the process intensifies. More

[2] W.C. Benton, *Purchasing and Supply Management* (Irwin Professional Publishing, 2nd edition, 2009), Ch. 8.

[3] "Corporate Responsibility Report," Deutsche Telekom, 2017.

serious sanctions are occasionally implemented in order to spur the handling and closure of gaps in accordance with Deutsche Telekom procedures.

A document by the Information Technology Infrastructure Library (ITIL) presents a two-dimensional model for classifying suppliers—risk and impact vs. value and importance.[4] The higher the value of the dimensions for a particular supplier, the more significant that supplier is. This model groups suppliers into four classifications:

- Commodity: These are suppliers of goods and services that have a low value and/or are readily available (such as paper or printers).
- Operational: These are suppliers of operational goods or services, generally managed by a junior operations manager, and require infrequent but regular performance reviews of contact people (for example, internet hosting service providers, which provide hosting space for a website that has little influence).
- Tactical: These are suppliers that have significant commercial activity and business interaction, generally led by middle management, and require regular performance reviews as well as ongoing improvement plans (for example, a hardware maintenance supplier who provides solutions for server hardware failures).
- Strategic: These are suppliers with whom confidential or strategic information is shared, who are generally under the responsibility of senior management levels, and require regular and frequent reviews (such as a network services supplier that provides global network services and support).

A more simple pyramid model for classifying suppliers is used by the United Utilities company, which provides water in northwest England, totaling about 1.7 billion liters per day. This model divides suppliers into four groups: partner, strategic, preferred, and approved.[5] The more complex the company's dependency on the supplier is and the higher the value of the goods or services are, the more significant the supplier is. The model makes it possible to define the company's requirements from the supplier against the following performance indices: customers, regulation/law, sustainability, efficiency, safety, and so forth.

[4] "ITIL Service Management," Version 3, § 4.7.5.2, https://www.hci-itil.com/ITIL_v3/books/2_service_design/service_design_ch4_7.html.

[5] "Suppliers," United Utilities, https://www.unitedutilities.com/corporate/about-us/governance/suppliers.

Another methodology for classifying suppliers appears in the Amway—Europe Supplier Information Portal model.[6] According to this methodology, the type of relationship developed between supplier and customer depends on the strategic importance of the product or service being provided, and the talents, abilities, and performance of the supplier. Every supplier is measured and classified according to the model's criteria. This ensures that each supplier will undertake focused activity that is planned especially to develop, improve, or streamline operational performance. The criteria that are used to measure each supplier include performance (order, inventory, supply, service, and quality control); product/service (innovation, development, marketing advantage, economic value); and financial (dependency, alternatives, financial risks, and pricing). The evaluation of these criteria and its results lead to the formulation of specific programs with the supplier to achieve the operational and performance levels required for business purposes.

In Israel, a number of activities have been implemented to improve the management of cyber risks in the supply chain. One of them is the work of the National Cyber Directorate on developing a supply chain protection method. This method includes a suppliers' questionnaire, as well as a control and auditing method accessible through a portal. The intention is that market forces will develop the use of the method and the portal and not to impose it upon suppliers. In addition, the Ministry of Finance relies upon the Unit for Cyber Regulation and Continuity of the Financial Supply Chain[7] to ensure the resilience of the financial system against cyber risks and the continuity in the financial supply chain, maintain the stability of the system, and meet the service targets for the public and the government. Currently, the unit's activity vis-à-vis the financial system's suppliers is voluntary and free of cost. The activity vis-à-vis the suppliers includes a review of their activity, mapping and assessment of risk and existing controls, and formulating a risk mitigation program. It should be noted that this activity vis-à-vis the financial system suppliers is relatively new and still in its early stages.

A number of approaches from other spheres in the Israeli economy may be relevant to the discussion here, such as a national classification of suppliers in

[6] "Supplier Segmentation," Europe Supplier Information Portal, http://supplier.amway.com/europeanportal/suppliersegmentation/SitePages/Home.aspx.

[7] "The Unit for Cyber Regulation and Continuity in the Financial Supply Chain," Ministry of Finance, http://mof.gov.il/Units/CyberEmergenciesSafetyDraft/Pages/CyberSeriesUnit.aspx.

other industries (such as building contractors), and an infrastructure process performed or guided by one entity for employees in other entities (such as the government unit for determining security compatibility in the General Security Service). In addition, toward the end of 2018, the National Cyber Directorate in the Prime Minister's Office established a national database,[8] in which any company can check its cyber protection level, information safety, and cyber protection fitness; using the data it obtains, it can receive recommendations on how to prepare, change, and improve. The first module in the system, called YUVAL (Hebrew acronym for organizational targets and controls), is intended to handle the economy's supply chain. The system is based on a defensive doctrine for organizations in the Israeli economy, which was published by the National Cyber Directorate. The challenge facing the officials of the National Cyber Directorate in specifying the system was the need to formulate a methodology to protect the supply chain. The purpose of the initiative was to raise the security level in the Israeli economy, in addition to economic streamlining. As a result, a uniform and orderly system of questions and controls was built, with the aim of creating trust between organizations and suppliers in the economy.

The ISO 27001 standard is a common international information security standard (the standard adopted in Israel is "IS ISO27001"), which institutionalizes the management of organizational information security and deals with the ongoing process involved in establishing and methodically improving the system.[9] Chapter 15 of the standard deals with supplier relations. The controls in this context are detailed in the ISO 27002 standard.[10] Pursuant to this standard, the organization is required to set a documented policy for suppliers to which they will agree. In addition, the policy must focus on the relevant processes that take place at both the organization and the supplier's internet sites. These include identifying the types of suppliers that are allowed access to the organization's information; defining the life cycle for managing supplier relations; defining the types of information accessible to the different types of suppliers; monitoring and controlling access; defining the minimal security requirements according to type of information and type of access so

[8] "The National Cyber Directorate Established a System for Protecting the Supply Chain in the Economy," *People and Computers* (January 2019), https://www.pc.co.il/news/282242 [in Hebrew].

[9] "Information Technology – Security Techniques – Information Security, Management Systems – Requirements," *ISO/IEC 27001*, 2013.

[10] "Code of practice for information security controls," *ISO/IEC 27002*, 2013.

that they serve as a basis for agreements made with every relevant supplier; defining how to handle security incidents and malfunctions connected to the supplier; defining each side's responsibility; and increasing the awareness and training of employees. In addition, a written agreement should be procured of security requirements for each supplier that has the ability to access, process, store, and/or create communication, or provide information or information technology components for the organization. Furthermore, the agreements with the suppliers must include security requirements based on the risks within the goods and services supply chain. The standard also emphasizes the need to manage, monitor, and make changes concerning supplier relations and the supply chain.

Another relevant standard is NIST 800-161, which aims to provide a guide for US federal agencies to help them identify, evaluate, select, and implement risk management processes and controls for the information technology supply chain.[11] The processes and controls published in this comprehensive and detailed standard are subject to change or expand due to regulatory changes, organizational policy, guidelines, and so forth. The standard notes that organizations must develop strategies to mitigate information technology supply chain risks, which are specifically adapted to them and influenced by business needs and tasks, threats, and the operating environment. The standard emphasizes the complexity of the information technology supply chain, and the fact that suppliers have their own suppliers, which makes it difficult for the organization to see, understand, and control the situation. This difficulty increases if the supplier is not a direct supplier. The standard also notes that the handling of risks within the information technology supply chain must be assimilated within the broader organization-wide risk management processes. The controls detailed in this standard relate to the following topics: access control, preparedness and training, expression and responsibility, authorizations, configuration management, continuity, identification and verification, response to events, maintenance, media protection, physical security, planning, application management, employee reliability, control of changes, risk assessment, purchasing of systems and services, protection of systems and communications, and completeness of systems and information.

[11] Jon Boyens, Celia Paulsen, Rama Moorthy, and Nadya Bartol, "Supply Chain Risk Management Practices for Federal Information Systems and Organizations," NIST Special Publication 800-161 (April 2015).

Similarly, the General Data Protection Regulation (GDPR) standard, which was set by the European Parliament, the EU Council, and the European Commission, applies to all EU countries concerning the collection, maintenance, and transfer of individuals' personal data and sets out uniform rules for maintaining privacy.[12] The standard was approved on April 27, 2016 and has been enforced since May 28, 2018. It replaces the European directive on data protection (Guideline EC/95/46), which was established in 1995. The standard applies to all data processing organizations of information carriers in EU territory, even if they do not operate in EU territory. This standard imposes prohibitions and restrictions on the transfer of information outside of EU territory due to concern of violations that may occur in regions where privacy is not properly protected. One of the standard's principles is accountability. In cases of organizations that use suppliers as outsourcing for processing personal information (such as producing salary slips), they must ensure that proper security arrangements are in place and that they are consistent with requirements over the entire supply chain, including their suppliers.

The Bank of Israel issued a directive, requiring the banking corporation to determine which operations are essential in order to ensure that external parties take the required measures to reduce its exposure to cyber risks.[13] The directive also deals with "the banking corporation's responsibility for maintaining a secure working environment vis-à-vis material service providers and its obligation to manage the cyber risks appropriate in regard to these service providers' activity on their own premises, on the banking corporation's premises, and in material providers' interfaces with the corporation." The directive relates to the need to map and identify "material service providers,"[14] giving the banking corporation the ability to demand that a provider fulfills the security guidelines and maintains the banking corporation's enforcement and control capability vis-à-vis the provider.

[12] "GDPR – General Data Protection Regulation," The European Parliament, 2016.

[13] "Supply Chain Cyber Risk Management," Bank of Israel, 2018.

[14] The directive defines "material service providers" as "external entities that belong to a banking corporation's supply chain (such as companies that support capital-market trading services), which are material to its activity and/or expose it to potentially high cyber and information-security risks that, when they eventuate, make it possible to attack the banking corporation or impair its activity." The reference is to outside entities that provide services to the banking corporation only in areas connected with information security.

Similarly, the Capital Market, Insurance, and Savings Authority in the Ministry of Finance published a circular that applies to entities that manage the public's money, such as pension and trust funds, including insurance companies and investment houses.[15] Section E of the circular relates to the issue of outsourcing, specifies the cyber protection requirements in outsourcing agreements, and requires that the entity define a procedure that details the cyber protection requirements vis-à-vis outsourcing risks and in relation to supply chain security. In addition, a service provider must be prohibited from transferring to a third party any information it receives within the framework of its interactions, or from using information to which it is exposed due to interactions for any other purpose that is not connected to its contractual obligations. The circular also sets out that when it is necessary to transfer data, access to itemized data shall be controlled, without copying the entire database.

The Privacy Protection Authority's Privacy Protection Regulations (Information Security), which came into effect in Israel in 2018,[16] are based on the assumption that granting access to an external entity creates unique risks. These regulations require that before implementing any interaction with an external entity, any inherent information security risks must be examined, and if the risks are too high when considering the sensitivity of the information, then outsourcing should be completely avoided. The regulations also determine that the following must be defined between the company and the external entity: the information the external entity is permitted to process and for what purposes; which systems it is allowed to access; the type of processes it is permitted to carry out; the duration of the interactions; how the information will be returned to its owners at the end of the interactions; how the information security regulations will be implemented; and the requirement of the authorized employees of the external entity to maintain information confidentiality.

As shown above, standards and regulations for managing general supply chain risks vary throughout the world, indicating global awareness of this issue. Awareness of cyber threats that originate in the supply chain is also

[15] "Cyber Risk Management at Institutional Investors," Ministry of Finance, August 2016.

[16] "Privacy Protection Regulations (Information Security), Regulation 15—Outsourcing," Knesset, May 2017.

prevalent, and these threats pose a number of challenges that require special attention.

Cyber Threats and Supply Chain Risks

According to the British Computer Emergency Response Team (CERT), four types of threats to the supply chain can be discerned, based on real incidents.[17] The first is an attack on the system through a third-party supplier. In this specific real incident, the attacker attacked an industrial control system (ICT), which a third-party supplier had installed in the organization. The second threat is an attack on commercial websites implemented via website builders and designers. In the specific real incident, the attacker struck financial websites through scripts that were transferred from digitization and design companies. The third threat is an attack on third-party companies that store data, often sensitive information, for other companies. The fourth threat is a "watering hole" attack, which refers to implanting malicious code in sites that are broadly used by the targets of the attack, so that accessing those sites will lead to an attack on the systems of targeted users.

The ISO 27036-1 standard also provides examples of threats in this context:[18] A supplier's physical access to the customer's sites; access to the customer's information or information systems at their sites by the supplier's employees; remote access of the supplier to the customer's information or information systems; processing the customer's information by the supplier outside of the customer's sites; using the customer's applications on the supplier's infrastructure; hosting the customer's equipment at the supplier's sites, and storing the customer's data (including backups) at the supplier.

A report by a cyber intelligence company reviewing significant cyberattacks that took place between 2016 and 2018 in Israel and abroad noted that the financial sector (banks) is a main target for skilled criminal and government hackers, while core banking systems, such as Swift and the ATM network, have in recent years become a preferred target for hackers.[19] The report also notes that in the past decade, companies and organizations have developed front-end protection systems vis-à-vis the internet but have invested less in

[17] "Cyber-Security Risks in the Supply Chain," CERT UK, 2015.

[18] "Information Technology – Security Techniques – Information Security for Supplier Relationships," *ISO 27036*.

[19] "Report on Cyber Events, 2016–2018: Exploiting the Swift Supply Chain," Clearsky, March 2018.

protecting their contacts with suppliers. In this way, a cyberattack originating in one of the links in the supply chain has become an efficient way to gain a foothold into penetrating strategic organizations. The hackers exploit the relative ease of accessing small companies and organizations with a weaker cyber defense system and use them to penetrate target organizations of critical importance. Hackers also exploit the fact that some secondary suppliers of the critical organizations have direct or easier access to the organization and through them penetrate the critical organization. An attack via the supply chain has become more sophisticated and includes the use of legitimate software updates to distribute malware. Since organizations are unable to inspect software updates, the level of risk of damage to the core systems of organizations and countries has increased significantly.

According to the report by the cyber intelligence company, three main insights can be made from the current situation in terms of how organizations deal with the threats:

1. Building a new defensive model: The traditional model, which mainly involves increasing security of the organization's external "boundaries" while leaving the core of the organization unprotected, is no longer appropriate. In recent years, this concept has led to a lack of security for the internal systems. Currently, many organizations are investing tremendous resources in strengthening their defensive parameters but do not sufficiently budget or invest in their internal security. The lack of balance in investment leads to a situation where if a hacker succeeds in penetrating the organization, he can easily spread out and operate within it.

2. Strengthening protective mechanisms between organizations and secondary suppliers: It is extremely difficult to protect the connection between organizations and companies and the secondary suppliers who provide them with services and information. This is even more true when protecting information against companies that provide cloud-based computing services. Some information providers in the banking sector are international entities (such as Bloomberg and Reuters); clearly, the ability to affect their information protection systems is relatively inferior. Banks and regulators have a greater ability to affect and control the security systems of suppliers in Israel, but this requires the setting of clear standards and defensive systems for the information security systems that are required of the secondary suppliers who connect directly to the core banking systems. At the same time, the protective systems must be strengthened, and the internal systems of the banks and financial institutions need to have limited exposure to secondary suppliers.

3. Deploying a back-end protection system similar in nature to the front-end protection system: It is recommended to build a monitoring and protection system vis-à-vis secondary suppliers, similar in nature to the company's front-end protection system, including the establishment of a DMZ, a strong identification system that includes multi-factor identification, an information filter system, a "sandbox" system to test the results of software update installations, and a monitoring system that includes keeping data for a long period and constantly monitors the connection with the secondary suppliers. This defensive system should also be deployed against the company's subsidiaries, as working with subsidiaries that have separate protection systems and separate software systems puts the company at risk just like with a secondary supplier.

The National Cyber Directorate's document on "Outsourcing Risks in the Supply Chain" lists the following risks as unique to the supply chain: the insertion of software or hardware that is infected with malware; malicious action by a maintenance worker; and malicious action through a remote maintenance channel.[20] The document proposes means to mitigate the risk by integrating it into the organization's risk management; supervising maintenance people by monitoring their network activity, accompanying them while they are on-site, requiring incoming personnel to wear identification tags, monitoring the remote maintenance channel, and disconnecting it when no longer needed; and concealing the specific end-target as part of purchasing for large organization—for instance, when purchasing for a very large organization, of which only parts of the organization are sensitive, it is possible to eliminate the destination of the purchase on the order.

A document by the SANS Institute addresses the required organizational preparedness given the cyber risks from the supply chain.[21] The document proposes that organizations build a supplier management program based on four components: identifying and defining the important suppliers; precisely defining the agreements for each supplier; setting and implementing guidelines and controls; and organizational integration. The document also proposes

[20] "Outsourcing and Supply Chain Risks," National Cyber Directorate**,** May 18, 2017.

[21] "Combatting Cyber Risks in the Supply Chain," SANS Institute, 2015.

that organizations act according to best practices (in terms of personnel, processes, and technology) in order to minimize their exposure to supply chain risks. Finally, the document summarizes the main components of the supply chain security program according to basic and comprehensive components, cross-referencing each of the three components as in the following table:

Table 1: Main Components of the Supply Chain Security Program

Component	Basic	Comprehensive
Personnel	Background checks	Security requirements appearing in contracts
Processes	Basic surveys and control and risk surveys of the suppliers	Implementation of the full supplier management program
Technology	Network segmentation and monitoring	Code review and inspection of vulnerabilities of third parties, in-depth monitoring, security threat analysis, and reliance on intelligence

A threat to the organization through an attack on its supply chain can occur through a wide variety of mechanisms. These include penetration of the systems of a supplier with relatively low-level protection (but with access to the organization's systems), through which the organization's systems are breached; use of legitimate software updates to distribute malware; and so forth. These are not theoretical threats for organizations but are based on a large number of actual incidents that occurred in Israel and abroad and damaged the organizations by exploiting their supply chains. The complexity of the threat, the wide variety of possible scenarios, and the increasing power of the hackers necessitate organizations to take significant defensive measures to deal with the challenge and mitigate the risks.

The above survey shows that there is much discussion of cyber threats in the supply chain. However, this discussion is inefficient, since each entity must fulfill the guidelines and recommendations on its own, and each supplier must fulfill his customer's requirements separately and invest a tremendous amount of resources in implementing the various requirements, which by nature are not uniform.

The Proposed Model

A critical component in supply chain risk management is the ability to survey cyber risks among suppliers and build a work plan that will make it possible to close gaps through the appropriate controls. In general, this article focuses on formulating a broad, sectoral process that will enable suppliers to receive certification from a central testing entity. The article is based on the assumption that organizations belonging to the same business sector have many common suppliers. For instance, most banks in Israel use the same printing supplier, but currently each bank separately surveys the same printing supplier.

The proposed model is all organizations that use the supplier will finance the certification processes, thereby making it possible to pool resources and invest greater resources in the entire certification process. Different levels of certification will take place according to the characteristics of the supplier and the requirements of the organizations in that sector. This way the organizations will rely on the work of the testing entity, and the suppliers will be saved repeated inspections each time by a different entity. The proposed model can serve as a basis only; if necessary, the various organizations can expand their requirements of their material service providers in the supply chain, for example by imposing more stringent requirements or even requirements to install additional monitoring systems at the supplier's premises.

The risk survey of the suppliers of addressing cyber risk in the supply chain can be carried out through two main operational alternatives:

1. *Self-management by each organization in the sector:* This is essentially the current situation, wherein each organization acts independently vis-à-vis the suppliers on its supply chain. Each organization also determines its requirements from each supplier or group of suppliers.

2. *Central sectoral management (for all or most of the organizations in the sector):* To realize this, it will be necessary to establish a main entity that will be jointly owned by the companies operating in a single sector. The purpose of this entity will be to implement cyber risk surveys and monitor performance among the sector's suppliers. This entity will be responsible for managing the surveyors (whether they carry out the survey directly or through surveyors working for the entity, or external surveyors); dictating the survey requirements; monitoring and tracking the implementation of programs to correct the gaps raised in the surveys; and revising the

inspection methodologies and tools used according to the concurrent needs and developments in the field. In addition, the entity will need to discuss the question of controlling foreign suppliers and how to implement the inspections and controls for them as well. One example is the MASAV/Shva company that was established by the large banks in Israel and provides services to the entire banking sector.

The requirements can be based on accepted standards or on the classification of suppliers as proposed by the National Cyber Directorate. These two options address a number of additional aspects:

Improved sectoral cybersecurity: The first aspect addresses the question of which alternative will increase the level of cybersecurity and stability in the specific sector. Given the analysis conducted, the answer is clear. Centralized management of the suppliers cyber risk survey has a variety of advantages: establishing a specialized professional entity will enable it to methodically develop knowledge and to improve and enhance its abilities for the entire sector; a uniform survey of suppliers will allow for setting cybersecurity benchmark requirements for the entire sector, while normalizing the requirements from suppliers in the supply chain; intensifying the requirements from suppliers will better enable the sector to enforce improved controls, since the requirements will be developed by a centralized entity; the burden on suppliers, who are currently dealing with separate risk surveys and requirements from each organization in the sector, will be significantly lightened; and the pooling of resources will increase the quality and depth of the survey and as a result, will improve the risk management level of the suppliers.

Economic aspects: The economic aspects are worth examining and will be particular to each sector. Establishing the capability of conducting a centralized risk survey could lower the costs for each organization while also improving the survey's effectiveness, given the increased professionalism of the surveying entity in the sector.

Anti-trust considerations: In this context, we must examine the extent to which joint activity by the organizations in the sector vis-à-vis suppliers in the supply chain will deviate from anti-trust regulations. According to our analysis, establishing a centralized surveying entity does not affect this component and rather would improve the level of security and stability of the specific sector. In addition, the survey process can ascertain that sensitive organizational information is not shared with other organizations. This is already happening today, for instance in the Financial Cyber Center in Beer Sheva, as well as in organizations within the global financial system, such as Federal Financial Institutions Examination Council (FFIEC) and others. Clearly, when establishing the centralized body, it will be necessary to regulate a variety of restrictions that will apply to the survey process. As we understand, it will be possible to create regulations that will respond to the requirements of the various regulators.

The opening of new suppliers: Various organizations are already dealing with long processes that involve the opening of new suppliers in the system. These processes last for quite a number of months. A centralized entity could shorten the process and even enable suppliers to request a risk survey and qualification in advance.

The above shows that establishing a centralized entity will significantly improve the level of cybersecurity in a given sector and enable the constant development of knowledge of cyber risks. Moreover, centralized management will increase the strength and impact that the surveying entity has on the suppliers (since it will represent all or most of the organizations in the sector, and not just one), improve the professionalization of the staff (a specialized entity at the sector level), lower overhead (management, physical, and so forth) for each organization, and lead to significant savings in the resources required to survey all components of the supply chain. It should be emphasized that the responsibility for a cyberattack due to a failure in the supply chain will remain with the entity using the supplier, since the aim of the proposed model is only to streamline and improve the process and its associated costs.

Conclusion and Recommendations

From an economic perspective, it is recommended that the surveying of cyber risks in the supply chain be managed by a centralized body by sector. An entity that surveys cyber risks will represent all organizations in the sector and their requirements, and not just one organization, although a single organization will be able to add specific requirements for a certain supplier, if necessary. In order to establish and operate the central entity, a differential pricing mechanism among the organizations in the sector is proposed, reflecting each organization's volume of activity in the initiative.

The proposed model also has risks, which will need to be comprehensively examined and managed accordingly. These risks include, inter alia, potential harm to the market of the companies that currently provide cyber surveys (it is possible that they may stop providing these services, since fewer companies will be required once the "testing entity" is selected in each sector), which will reduce competition in the industry. When one entity conducts the entire survey process, there is a risk that not all vulnerabilities will be discovered. This is in contrast to having various surveyors that provide an additional "eye" and sometimes discover vulnerabilities that are not discovered by a single centralized surveyor. Another risk concerns the level of protection of this entity and its possible penetration by a malicious actor, which could endanger the entire sector. Finally, there is the potential of a conflict of interests, should the inspecting entity also be responsible for correcting the vulnerabilities. Obviously, this risk is relevant only in a case where the central entity chooses to use outside suppliers to conduct the survey on its behalf.

Within the context of Israel, it is recommended that the National Cyber Directorate conduct an in-depth process examining the proposed model. It is preferable that the process begin with mapping the sectors for which the model is relevant (sectors where it is assumed that a significant portion of the suppliers are shared suppliers). It is then worthwhile to conduct a feasibility study, similar to the financial sector, as presented in this article. After that, we recommend defining the relevant requirements from the various suppliers and the risk survey processes for each sector.