Cyber supply chain - description of the methodology of the National Cyber Directorate

Introduction

What is supply chain?

Supply chain is a network of individuals and companies engaged in creating a product or service and delivering it to the consumer.

Factors in the chain begin with the producers of raw materials and end when the finished product or service is delivered to the end user, until the end of the life cycle of the product or service[1].

Cyber protection in supply chain of an organization

In recent years, there has been a significant increase in the number and power of cyber attacks on organizations, whereas a cyber attack through a supply chain is one of the most significant threats to companies and organizations today. In order to manage the cyber risk, to which an organization is exposed in the cyber dimension, from its service providers and suppliers, the organization must examine potential cyber risks arising from engagements with them. During the last year, 2022, there was an increase of more than 650% in the number of attacks through the supply chain against organizations, while these attacks are a significant risk for any business or organization in the world and in Israel. 97% of organizations have already been attacked through supply chain, and it seems that these attacks will only expand and become more sophisticated[2].

Supply chain attacks are aimed directly at one of the suppliers, whether a software supplier or a reliable and well-known service provider working with a business or organization. In fact, such attacks abuse the trust an organization places in its supplier, to penetrate through the supplier into the organization or business.

In order to protect the organization and avoid the consequences of these attacks which may include ransom attacks, phishing, harmful insertions or spying, theft of sensitive information and more, the INCD has developed a national methodology to reduce the risks of cyber attacks resulting from insufficient protection in the security of information in the supply chain.

The methodology is conveniently accessible to organizations on behalf of the INCD in the online YUVAL system, for self-examination of the security level in the organization, which contains the control questionnaire for suppliers[3].

For those who prefer filling the questionnaire manually, it is attached at the INCD's website as an Excel file.

[1] 1 Supply chain definition - link to website
[2] An article on supply chain attacks - link to the article
[3] 3 Yuval system - https://grc.cyber.gov.il/scripts/manage/login.aspx

The method includes indicators and controls defined for testing the resilience of suppliers in questionnaire 1.4. In addition, a database of supplier inspectors for testing the strength of suppliers, who have been certified by institutes authorized for this purpose by the INCD, has been uploaded to the website of the National Cyber Directorate (an explanation of the supplier inspectors is attached below). The mechanism includes a series of steps to test security level in an organization (self-testing of the control questionnaire, bringing in a certified supplier inspector for an organizational examination and certification with a full certificate by a third party) in order to increase the resilience of the Israeli economy and making it easier for companies and organizations to deal with these challenges.

Normative framework – Government Resolution 2443

The background and foundation for promoting the issue of cyber defense in supply chain is Government Resolution 2443.

In accordance with Government Resolution 2443 entitled "Promotion of National Order and Government Leadership in Cyber Defense" of February 15th 2015, the INCD is obliged to initiate and implement general activities, including establishing of infrastructures and operation of mechanisms, the purpose of which is to improve Cyber protection in various sectors.

Hence the importance of assimilating a "supply chain methodology" of the INCD among service providers into entities of the economy, when in addition the INCD recommends to the regulators to anchor the methodology as part of the cyber protection requirements.

It is worth noting that there are government offices that serve as regulators, which have already implemented the supply chain methodology of the Cyber Directorate in their entrusted sectors. For example: already today the Ministry of Transport obliges critical suppliers in the sector to meet the standard required by the method. The Government Cyber Defense Unit in the Ministry of Cyber and National Digital Matters (the YAHAV unit) shall also operate in this way, and other regulators are expected to adopt the methodology as a binding standard.

The purpose of adopting the methodology is to increase the level of resilience of the Israeli economy against cyber attacks and to strengthen the functional continuity of various organizations.

Why produce a uniform standard by the Directorate, when there are international standards?

In 2018, a situation emerged, when the lack of an accepted standard / language between organizations in the economy and their suppliers - in the context of protection from cyber risks, created difficulty among the organizations and required the investment of resources in the development and maintenance of activities with the suppliers. In addition, it became clear that organizations fail to manage and enforce the whole scope of controls regarding the suppliers they work with.

Therefore, it became necessary to establish a fixed and clear standard for requirements to suppliers, one that produces a uniform language for the Israeli economy - a professional and uniform process for suppliers, which includes definition, testing and feedback.

Why is an unsecured supplier dangerous to an organization?

Many suppliers are asked by an organization to provide details on their level of protection. Sometimes a supplier does not fully understand the requirements, or the organization does not bother to verify the data transferred to it by the supplier. Moreover, the supplier often acts by a substantial contract with another supplier - support and / or maintenance of information systems, storage of sensitive data outside the organization, technological outsourcing services and more, when damage to the supplier through that same additional supplier may cause significant and irreversible damage to the organization and its customers.

Supplier inspectors

• **Supplier inspectors** – those certified to audit suppliers in the economy to verify that they comply with the organizational supply chain method.

• **The following 3 colleges administer certification for supplier inspectors:**

- o "The Technion" - Sarona Tel Aviv branch
- o "Ha-Michlala" - The Standards Institution of Israel
- o The "INT" college - WE WORK complex

These colleges were selected as part of a Call for proposal by the Directorate and were authorized to train the supplier inspectors.

A certified supplier inspector is the one who tests the supplier and its level of resistance using the methodology of the INCD. In addition, the supplier inspector helps the supplier implement all the controls in his organization, and then builds a 'supplier file' for him when he meets all the required controls, and transfers it to one of the competent certification institutes.

Why should an organization disclose information / security practices to a supplier inspector?

Supplier inspectors, who have been successfully certified after completing the supply chain cyber compliance inspectors' course on behalf of the Directorate, are the ones who shall conduct compliance tests for suppliers in the Israeli economy according to the method of the INCD for testing supply chains.

The method includes checks to examine the strength of the supplier's supply chain facing cyber attacks on various issues.

Certification methods

* Suppliers with certification method A (Platinum)	* Suppliers with certification method B (Gold)
The suppliers were required to answer the questionnaire with the help of a supplier inspector certified on behalf of the INCD, along with a third party audit carried out by an authorized compliance testing institute on behalf of the INCD.	This is a self-declaration by a supplier, which means that this method of certification includes a statement authorized to sign (usually the VP/CEO of the organization) on behalf of the supplier on its compliance with the supply chain methodology of the Directorate. Beyond what has been said, although it is not mandatory, **the Directorate recommends conducting an internal organizational test by the method with the help of a supplier inspector certified on behalf of the Directorate.**

(An in-depth explanation of the certification methods is attached hereby.)

Certification bodies

In the certification method A, confirmation of suppliers' compliance with the supply chain method is carried out by the following certification bodies:

• The Standards Institution of Israel (SII) - certification services on the SII website.

• The Institute for Quality Control - IQC Certification services on the IQC website.

These bodies are entrusted with rating the suppliers and issuing a certificate confirming the compliance with the supply chain methodology of the INCD.

Upon certifying the suppliers, the list of "approved suppliers who met the supply chain method of the National Cyber Directorate" is published in the database of the INCD's website for public use (Certified A).

https://www.gov.il/he/departments/guides/supply_chain_guide?chapterIndex=4

A supplier that carries out the process according to the A certification method is the most secure in terms of the method, because it has passed all the comprehensive tests and received all the approvals from the supplier inspectors and the certification body.

In addition to the fact that his organization will have a high level of security - entities in the Israeli economy will be able to contact him if they want to work with a secure organization, as published in the database of the "Suppliers with the A certification" on the website of the National Cyber Directorate.

Explanation of the form of the new methodology

What does the methodology consist of? Details of the meaning of risk levels and modules

The methodology addresses 3 different levels of risk, which make up the total of general requirements. As a rule, the choice of which level of risk to demand is up to the client, at his discretion as part of a risk management process or according to the guidance of his regulator if applicable.

These are the three levels of risk:

Basic level (1); a level with a significant risk for the customer (2); and a critical risk level for the customer (3).

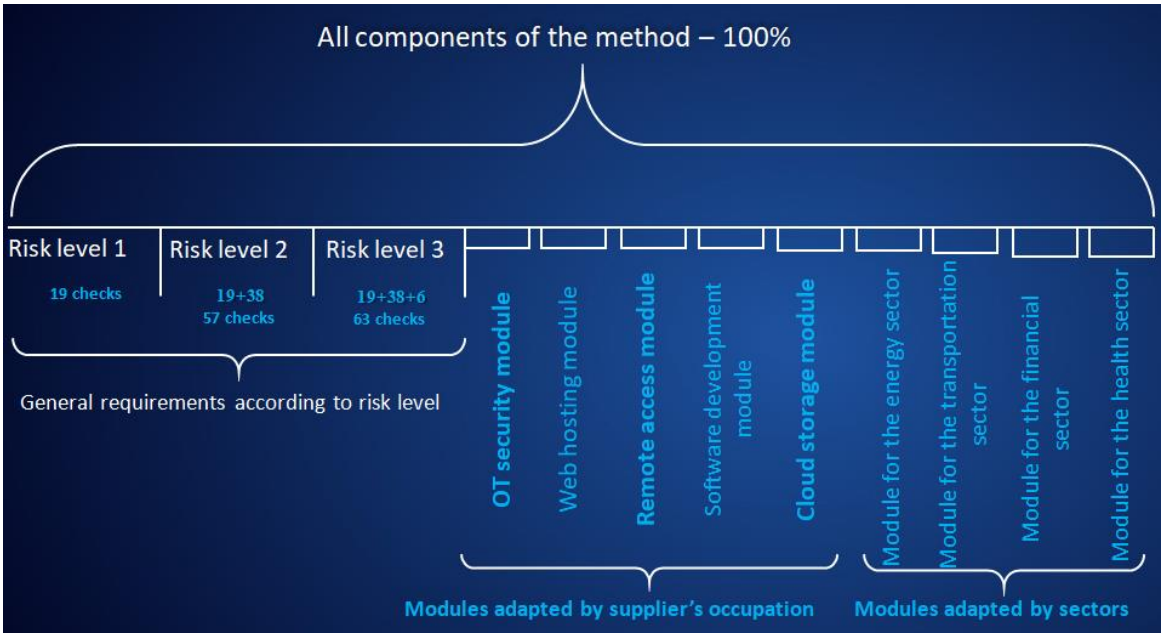
(The use of each level is explained on the next page).

Also, there are dedicated modules (types of contracts) adapted to the supplier's business - which are added to the general requirements:

- OT security.
- Web hosting.
- Remote access.
- Software Development.
- Cloud system.

The modules will be added in the questionnaire to the general requirements based on the supplier's occupation.

(In addition to this, a new section will be expanded, in which dedicated modules will be added to the method, for each sector that wishes to manage according to the supply chain method of the Directorate.)



What level of risk will we use for a supplier?

Risk level	1 – Basic	2 – Significant	3 - Critical
Explanation	The most basic risk level, which every supplier is absolutely required to apply. This level is suitable for suppliers who pose low digital risk to their clients (19 checks).	Usually applied when a supplier poses a significant risk to the organization. By default SMB organizations shall apply this level. (Contains 19 checks of level 1 and 38 additional checks for level 2, i.e. 57 checks in total).	The most secure one, for implementation at suppliers that pose a significant and even critical risk to the customer, will often be implemented in large organizations. (Contains all the checks of the general requirements, i.e. all the risk levels 1, 2, and 3; making 63 checks in total).
Occupation of the supplier	A supplier who does not possess the organization's information and does not have access to the organization's information or infrastructure, as well as a supplier who possesses the organization's information but publishing the information or disrupting it will not cause damage to the organization.	A supplier that holds the organization's information or has access to the organization's information or infrastructure, the attack of which could constitute substantial damage to the organization.	A supplier that holds the organization's information or has access to the organization's information or infrastructure, the attack of which could constitute substantial damage to the organization.

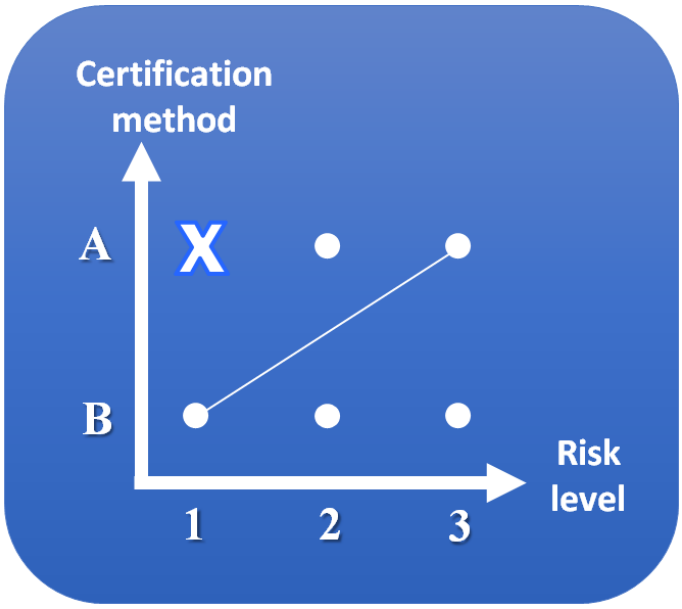
Difference between the certification methods - and when each of them is to be used?

• Certification method: A - Implementing the method + an inspector on behalf of the supplier + a third party inspector (certification).

• Certification method: B - Implementing the method + self-declaration of the supplier.

It is important to note that the choice of certification type to require from each supplier as a rule is up to the customer, at his discretion as part of a risk management process or according to the guidance of his regulator if applicable.

The following diagram shows response options for the method, which combines the 2 certification methods: A and B, and the three risk levels: 1, 2, and 3.



• In other words, a self-declaration is possible at all risk levels (1, 2, 3) for the supplier's decision. At levels 2 and 3, a full certification process can also be carried out.

• The methods of certification do not constitute relief or aggravation in terms of the requirements themselves, as they are reflected in the risk levels, but only in the way they are proven.

• Finally, supply chain management has to correspond with procurement cycles of organizations, and with specific circumstances of suppliers, some of which are international, and some of which operate in other special circumstances.

• Certification method B (self-declaration) can be used as a temporary step in favor of meeting the threshold conditions of a tender, for example; or it can also, in general, be a starting step to accustom suppliers to using the method and make it easier for small and medium-sized businesses.

• With certification method B, to declare an organization as complying with the Directorate's method, the Cyber Directorate recommends using supplier inspectors trained for this purpose on behalf of the Directorate in order to carry out an internal organizational inspection of the supplier.

• Regarding international suppliers, for which at this stage requiring compliance with an Israeli third-party inspection would be unrealistic, it is possible to direct them towards compliance with method B certification (self-declaration of compliance with the method).

Advantage of the A certification method in accordance with the recommendations of the National Cyber Directorate for secured suppliers

Along with better protection of the organization and preservation of the interests that stand at the foundation of the company, implementation of the methodology in the organization as a supplier may allow it a relative advantage compared to suppliers who do not act in accordance with the recommendations.

The fact that it is secure against cyber attacks in accordance with the recommended national standard should definitely improve the ability to work safely with customers, has the power to strengthen the customer's desire to enter into a contract, and may even increase the number of customers.

Today, many business contracts and tenders are conditional on various information security checks, a situation that forces suppliers to adapt to competing in tenders.

Adherence to the method enables suppliers to have a better starting point in each tender, since the supplier does not have to make additional adjustments to the same process declared / documented in the organization, per tender, but in a broad and comprehensive manner.

Also, the name of each supplier that complies with the method, whether it has been fully certified or reported in a self-declaration, will be published with contact details in the secure supplier database located on the INCD's website and brought to the attention of the public and the economy, subject to the supplier's consent.

An explanation regarding the use of the YUVAL system

It is important to note that the use of the YUVAL system is not mandatory!

The supplier questionnaire addressing the supply chain methodology of the National Cyber Directorate is accessible in the system with the purpose to help the supplier to fill out the questionnaire.

However, there is no obstacle to submitting a supplier file using the Excel questionnaire manually.

Reading and using the checklist questionnaire 1.4 in the Excel file

• Those that choose not to use the YUVAL system can use a dedicated Excel file.

• In the questionnaire there are several central columns according to which the filtering will be carried out for each supplier.

• An initial filter shall be applied - by the column called the type of contract (indicating the general requirements intended **for all suppliers** according to the level of risk required from the client, in addition to modules adapted to the type of the supplier occupation - including software development, website hosting, remote access, cloud system and OT security).

• The next filter shall be applied by the column called risk level rating -
according to the customer / regulator requirement for that supplier.

• Then, of course depending on the level of risk, we will examine the depth of application according to rating column to determine the depth of application required for each level; we can see the details of the application in the column called depth of control application.

• After applying the filters we will examine the control, the depth of the control application, and the required evidence columns, which are critical.

With their help, we will know how to address the checks relevant to that supplier in the correct way.

Clarification - as mentioned above, the questionnaire can be filled out manually in Excel – filling it using the YUVAL system is not mandatory, the system is created to provide users a convenient access to the questionnaire – in other words, the supplier will usually prefer to self-check using the YUVAL system that contains the questionnaire itself, and produces a report at the end.

But if the preference is to fill out the questionnaire manually - there is no problem.

The changes introduced when updating questionnaire 1.3 to questionnaire 1.4

• Change in contract types, added “OT security" module.

• Most checks have been rewritten to reduce ambiguity.

• The requirement for mandatory data clearance station was removed at this stage.

• The certification methods were reduced to A and B only (as indicated above).

• 3 new risk levels were defined to replace the substantial / non-substantial from the previous questionnaire (as indicated above).