Cyberspace Espionage and its Effect on Commercial Considerations

Gabi Siboni and David Israel

Cyberspace is becoming the primary and most effective tool for commercial espionage and the theft of information and intellectual property. It allows the attacker a technological shortcut, giving him the competitive edge over the market in general and the defender in particular. This essay examines whether the need to confront cyberspace threats in general and, more specifically, organizational information security affects the considerations of decision makers in commercial enterprises. Decisions relating to the feasibility of starting development, the costs of protecting the information, the product's life expectancy, and the commercial worth of exploring new fields may all be influenced. This essay also includes some suggestions for helping these fields at the national level.

Keywords: cyberspace, espionage, commercial espionage, intellectual property, cybercrime, cyber theft, technology, information

Background

Commercial espionage is hardly new. It has existed in different incarnations since the dawn of time. Some of the historic industrial revolutions were based on the copying of knowledge. For example, industrial machinery from Great Britain found its way to the United States and helped transform it into an industrial powerhouse at the expense of British patents.[1] In the business world, industrial espionage is usually considered one of the biggest threats to an organization's ability to survive in a competitive market. A fundamental assumption has been that the risk of theft and

Dr. Gabi Siboni is the Director of the Cyber Security Program at the Institute for National Security Studies. David Israel is an information security expert at Motorola Israel and an intern in the Cyber Security Program at the Institute for National Security Studies.

loss of information consisting of intellectual property could result from an internal threat, such as a disgruntled employee, a mole, or even a loyal worker who had been tricked. The threat could also be realized by copying a product through reverse engineering.

Until about a decade ago, protection against industrial espionage focused on physical aspects, such as restricted access areas, entrance checks, and security cameras, in addition to testing the loyalty of employees and others in the development and manufacturing chain, which included security checks, integrity testing, background checks of providers, and so forth. Protection was ensured by denying access to information and intellectual property located within an organization's physical space and by taking steps to prevent this information from being leaked by an internal party or by a foreign party that had breached the physical parameters of protection.

Protection of organizational information and intellectual property relied and continues to rely upon patenting and legal agreements, such as confidentiality agreements between companies and their suppliers, assuming that an organization can sue entities that harm its intellectual property. Sensitive information includes not only intellectual property, but also information that is liable to damage the organization in a myriad of ways, such as contract details, salaries (for headhunting special talents), information about tenders and price proposals, strategic plans, marketing plans, client lists, provider lists, and so forth.

The expanding use of cyberspace for technological development and manufacturing exposes this significant sphere to risks of leakage of sensitive information and intellectual property.[2] In fact, this development has changed the rules of the game in terms of the processes of securing information and intellectual property, making their protection much more complex and resource intensive, while the work processes and the flow of information in the organization has also been affected. Senior management in various organizations understands that the cyber attacker has the edge, and that his chances of success are high compared to the limitations of the organization to defend itself in cyberspace. One study conducted by a large consulting firm claims that some 60 percent of senior managers believe that cyberattacks will increase and become more sophisticated and frequent, exceeding the ability of organizations to defend against them.[3]

As a result, we are now seeing a profound change in decision-making processes affecting research and development and in the considerations of commercial organizations when it comes to investing in R&D. The severity of the threat of information and intellectual property theft requires organizations to take their protection very seriously. Such protection requires the allocation of significant resources, including technological ones, and the application of suitable standards and working procedures. These represent a burden on the human resources and involve high costs, thereby reducing the investment in the product's development. Thus, the organization must ask the following fundamental questions: what are the critical weaknesses in the business process and how should they be protected? What will be the added cost for protecting the information and for the entire security system needed for the R&D process? Will it be possible to construct the required protection system before getting development underway, and does the risk increase because the business enters the market late as a result? Because it is clear that any defense can be breached, it is also important to question the organization's ability to bounce back from damage to the working process during the development stage. What will be the effect of a breach on the overall investment? What delays can be expected during development as a result of limits on information sharing, and what will be the effect of these delays? The whole development process requires partnerships with external entities, even outsourcing. Therefore, one must ask to what extent will it be necessary to invest resources in protection in such situations, or demand that external providers supply additional protection that might increase the cost of their service?

This list of questions is only partial, but it makes it clear that the decision-making process in the era of cyber threats is changing and the investment in security processes is indeed significant. In addition to other business considerations, cyber threats could cause an organization to decide to refrain from engaging in technological development in fields that are particularly attractive to commercial espionage. Especially sensitive in this regard is the startup industry. These companies are usually on a shoestring budget; having investing all their capital into technological development, they will be hard pressed to invest the necessary resources into sufficiently protecting their intellectual property assets. As a result, the innovation industry is most exposed to cyber threats involving the theft of intellectual property. Israel has a diverse technological infrastructure, including many startups that develop innovative products and solutions. It is therefore important to examine Israel's role in helping to secure the intellectual property developed within it, especially as a result of investments financed by the Office of the Chief Scientist at the Ministry of Economy and Industry.

Companies are exposed to damage in cyberspace as a result of commercial espionage, as well as malicious cyberattacks aimed at causing shut-downs and other harm. Companies need to take into consideration these attacks and protect themselves. This essay will focus on the significance of investing in security and protection of information and intellectual property, as well as the R&D processes, and how such security considerations might affect the scope of R&D investments in general. Furthermore, this essay will examine the tools that may help companies meet their protection needs through shared means and initiatives with different commercial companies. Moreover, the essay examines the state's role in creating a security infrastructure that can help companies, both large and small, improve their protection of intellectual property and increase their willingness to confront cyber threats.

The Complexity of Protecting the Processes of Intellectual Property Creation

One of the most sensitive types of information requiring protection is intellectual property, which is the primary asset of tech companies and startups. In order to understand the complexity of protecting the processes of creating intellectual property – i.e., the complexity of securing the business innovation and its critical competitive edge that justifies the business' existence – the life cycle of the information needs to be analyzed. We will refer to this as the product life cycle in a high-tech company.

The development of a technological product is characterized by the following stages: coming up with the idea, characterizing it, developing a prototype, lab testing, and manufacturing. Needless to say, all the stages of the birth and development of an idea until its maturation as a final product and its manufacturing are digital processes based on different information systems that provide support for each stage of development. As a direct consequence, each stage provides the attacker with motivation and invites a possible cyberattack, whether via the Internet or through an internal party operating either intentionally or inadvertently.

In principle, the organization's objective is to identify the sensitive points in the process and determine cyber defenses for each. In practice, a risk assessment based on information flow and its importance in the development process very quickly turns into a multi-tentacle creature, requiring an in-depth security treatment for each tentacle. Neglecting a particular channel or underestimating its importance might be the weak spot of the defensive system in general. Each development process uses varied tools and technologies, involves different working environments, and always requires information-sharing capabilities, complicating the security of each development stage. At each stage, the organization must assess the need to mitigate risks, which involves confidentiality, integrity, and availability of the information assets.

As an example, we will examine the complexity of protecting sensitive information of an organization interested in developing a technology that can be defined as a strategic project and liable to be the target of a cyberattack. Early in the gestational stage, the company creates documents that are classified and restricted to internal access, such as minutes of meetings, presentations, technological analyses, market scenarios, roadmaps, and so on. These are stored digitally, thus requiring protective means that will ensure authorized access only. Implementing systems designed to prevent information leakage[4] are expensive and complicated to operate. The complexity of protecting sensitive information requires the organization to analyze the processes in which it creates its information; map the systems; understand the life cycle; identify the classified information in the database, the file servers, and end computers; and determine an organizational policy for defining classification. All this must be done before the organization selects the technological tools that will ensure the company's protection, requires users' training, and will accompany the project throughout its duration.

Beyond the need to secure intra-organizational information sharing, it is also necessary to manage and secure the information that leaves the organization. Almost every company shares information with outsiders in order to promote the development processes: from the developing engineer sharing information with some external subcontractor who is an expert in a specific and sensitive field, to the lawyers who have to receive and send business contracts to partners, suppliers or potential customers, and to the logistics and manufacturing personnel who receive and send information to service providers as part of managing the supply chain.[5] Protecting sensitive information that leaves the company is one of the most complex challenges to meet, since digital channels for data transfer from the organization are almost endless. An employee is liable to share information externally via the company's email or by personal email, via a portable device such as a USB flash drive or by burning it onto a CD, by using free file sharing cloud services,[6] and – worst of all – by peer-to-peer services in which the user installs software on an organization's computer that connects directly to a file-sharing computer network. Each of these methods represents a significant risk to the company's intellectual property. Each information channel requires technology that will limit, prevent, block, and monitor all of the information that flows through it.

Companies have invested many resources to block external memory-devices, such as flash drives and alike, preventing browsing on file sharing servers, and more. But the business need for efficiency and the ability to quickly share information from within and outside the office forces the company to create and allow secure and controlled information-sharing channels. One option is using cloud technology, which allows organizations to improve efficiency and make the information accessible from anywhere through cell phones, tablets, and home computers. Cloud services are an excellent solution for the organization, although their level of built-in security does not, at least for now, meet the rigorous needs of protecting information and intellectual property.

The results of a study by McKinsey indicate that the concern for cyberattacks results in a reluctance to adopt cloud technology and mobile services.[7] Some 70 percent of respondents reported that they postponed adopting the use of cloud technology by a year or more because of information-security concerns, and 40 percent reported they postponed the use of mobile services by a year or more for the same reason. In the high-tech field, 50 percent of respondents reported that they will have to make changes in their R&D processes. Another fact reflecting the influence of cyberspace defense on organizational functioning is that 50 percent of the senior high-tech managers who participated in the study reported that the topic of cloud services and mobile services was "a sore point," which limited the employee's ability to share information.

It thus emerges that technologies promising greater business efficiency, such as inexpensive, efficient cloud services, information sharing, and mobile technologies are perceived as a high risk, compelling an organization to spend more rather than to take a risk and wait until these systems can promise rock-solid security. Under these circumstances, organizations are liable to ignore cyberspace risks, preferring process efficiency and time-to-market instead of applying controls and accepting the limitations imposed by the security processes.

Another weak spot related to the organization's necessity to analyze and apply an information-security policy is the need to provide outside parties with access to the company's network. In many cases, the organization sees fit to provide an external provider with remote access to its network, thereby exposing the company to risks emanating with the provider and the level of protection that the provider implements.[8] Companies providing information systems remote support services; providers who have access to update internal logistical information systems; sub-contractors and business partners connected remotely to the company's systems all have possible access to the core of the information systems and the company's network. The access of these parties necessitates that the company builds, maintains, and manages a secure, encrypted communications infrastructure, using a secure logon and authentication process for the organization given access. In addition, the company should limit the network access of these parties to only those resources critical for their work, preventing situations in which they can browse freely through the company network and view sensitive information in its servers and databases. All access by outside parties should require a process analysis, that is, the name of the server to which access is needed; what software and protocols the party must operate; the creation of a designated username; the operation of a control and monitoring system for the whole process of connecting to and working on the server; implementation of firewall rules; and, of course, continuous reassessment of the need for external connection and for handling glitches.

It is essential to ensure that the level of information security on the external party's end is adequate, and to diminish the security risk from any possible weakness in the service provider's end station. Among other steps, it is important to ensure that the external party's computer has an updated antivirus protection. Has the party received the latest security updates? Is the party infected with a Trojan horse or other malware? A supplier's computer connecting to the organization's network becomes an integral part of it. In many cases, it is the weakest link in the system through which a hostile party can penetrate the network for the purpose of carrying out a cyberattack. Under these circumstances, it does not matter if the organization is regulated, has an updated security policy, and secures end stations by routine security updates, antivirus protection, and locking-out software; the moment an external party with an inferior security policy has access to the organization's network, that party becomes a clear and present danger.

Another layer than must be addressed from the security perspective is the process of creating the prototype and the lab testing stage. This is a sensitive stage in which for the first time, the company exposes the innovative technology, the product, and the new capabilities that are supposed to facilitate its business breakthrough. This is where the intellectual property turns into a fixed entity. Were a hostile party to get ahold of it, that party could stand to gain a significant advantage. Therefore, in most cases, the security needs dictate the establishment of restricted development areas and labs that have separate networks, which are severed from the Internet, and have applied added infrastructure and security products parallel to those already on the organization's network. Needless to say, the economic costs of building separate networks of this sort are high, and operational difficulties are great when it comes to moving information to and from the classified networks.

One of the most significant security circuits is the system to control and monitor security events. Without a monitoring system, the organization does not have any ability to identify security events in its systems nor to adhere to its security policy and confront potential cyber events, not to mention the ability to respond to such events and move quickly to reduce the threat. Security information event management (SIEMs) are usually expensive and require constant maintenance and updating to adapt them to new threats, new business processes, and new security systems. A SIEM can receive a security alert usually rooted in the logs of events from intra-organizational systems (audit logs and security logs), such as servers, communications equipment, firewall systems, authentication servers, remote access systems, databases, file servers, and more.

In addition to technological tools, the organization also needs skilled employees who understand the meaning of the events noted by the system and who are capable of analyzing the activity and determining a countermove. Moreover, the use of a SIEM allows the incorporation of outside cyber intelligence information, which provides current information about the nature of known cyberattacks, the sources of the attacks, and the tools used by the attackers. This intel is crosschecked with existing information in the organization's network, allowing early identification and rapid response to the event. The importance of using SIEMs in defending against cyberattacks is evident in a study by the Ponemon Institute. According to this study, companies using these systems were more efficient in identifying and containing cyberattacks. Consequently, those companies saved some $250,000 worth of damage compared to companies not using SIEMs.[9]

The most important step in defending against cyber threats is investing in employee education and awareness of cyber risks. Successful cyberattacks penetrate an organization through its weak links – its employees – and from there implement the attack. From this perspective, a study of phishing-type attacks targeting a company's employees is of particular interest.[10] This, however, does not conclude the activities that organizations must carry out in order to defend their intellectual property. It is not enough to define the sensitive points in the process and protect them; organizations must also invest and develop their network defensive capabilities and build monitoring and control systems that require constant acquisitions, adaptation, and maintenance so as to be able to identify security events and cyberattacks in real time.

It is evident that protecting intellectual property is a complex technological, organizational, and managerial process of great significance to the organization. The process and its financial cost have negative business ramifications, as the analysis below will demonstrate.

Negative Economic Ramifications

Cyberattacks and their potential for damage have negative ramifications on the organization's operational efficiency and its attempts to shorten development and manufacturing processes in order to reach the market before its competition does. According to McKinsey's estimates,[11] as long as cyber threats continue to grow and defensive capabilities fail to provide an appropriate response, they will negatively affect the global economy in the next five to seven years, by harming the value production of the companies, worth $9-21 trillion. This means that the costs of protecting against cyber threats and the loss of information and intellectual property resulting from commercial cyber espionage will significantly damage the global economy. The numbers cited above are, of course, affected by the development of the strength of the defense systems. In addition, there is also the economic cost specific to any given company, mostly because of its need to expand its cyber defense budget at the expense of its R&D budget and, consequently, also because of reduced operational profitability.

Beyond the negative impact of cyber risks – manifested by a global slowdown and the corporate need to increase investments in cyber defense – the damage to intellectual property, which has its own economic ramifications, is a significant risk. Damage to intellectual property is liable to affect the balance of global commercial forces, create unfair competition, and economically harm the profitability of companies to the point of their becoming extinct. Many companies whose intellectual property has been damaged have reported losses of sales, licenses and royalties; decreased profits; and harm to the brand and product's reputation.

One prominent example of intellectual property theft is the Chinese J-31 stealth plane, strikingly similar to Lockheed Martin's F-35. In the past, the American company was the victim of a Chinese cyberattack in the course of which the stealth technology was stolen.[12] The F-35 is considered the most advanced plane in the world. Today, the Chinese possess the costly technological knowledge associated with this plane, such as detailed diagrams of the engine, radar and other systems; advanced manufacturing technologies; and so forth. In this particular instance, the intellectual property, in which billions of dollars had been invested, was revealed to a competitor who used it to create the J-31, stunningly similar to the original. Advanced technological information that falls into a competitor's hands gives the competitor a technological boost and makes it an important player in a market, which, previously was controlled by a limited number of companies.

The main problem is that a company may not even be aware that it had been the victim of a cyberattack designed to steal information or intellectual property, since the information continues to exist on its servers and function as usual. However, it no longer controls the information and must deal with a new competitor who has similar or improved technology and therefore an invaluable relative advantage. Studies show that the time it takes a company to discover it has fallen victim to a cyberattack is 230 days on average.[13] This means that during this period, the attacker is free to inhabit the company's systems – long enough to study the information, analyze it in terms of relevance to the attacker's needs, draw conclusions, and even improve the attack process. The information amassed by the attacker allows it to understand the company's network structure, learn the names of the systems in use, identify the file servers and databases, crack the passwords of employees with access to the most classified materials, and penetrate databases of interest. Moreover, the information copied from the company allows the attacker to understand the organizational structure, become familiar with key personnel and decision makers, and continue to carry out targeted attacks to extract the specific information of interest.

As noted, the company under attack has no idea it is under attack or how much time the attacker has roamed its network. Even if the company has its suspicions, it will take a long time to learn the details of the attack, its severity, and the quality of the information stolen. The long time lapse before the attack is identified is one of the most important advantages the attacker has, so that shortening the time of discovery becomes one of the most significant challenges in defending against cyberattacks. The ability to identify a cyberattack and respond to it is directly correlated to the company's investment in advanced identification and early warning systems, defense of end stations and databases, implementation of security standards, and employee awareness.

One must also remember that cyberattacks aimed at stealing information are nothing like denial of service (DoS) cyberattacks. In the case of the latter, a company can apply recovery processes when the attack ends and return to normal operations, while drawing conclusions on how to fix the breaches. By contrast, an attack in which knowledge and intellectual property are stolen requires the victim to undertake a complex process of strategizing about future business activity: how to assess the amount of damage caused to the company; whether or not to continue developing the product which depends on a technology that is no longer controlled by the company; whether or not to continue the business strategy outlined in the original plans or to change it radically, and so forth.

According to assessments from various sources,[14] cyberattacks designed for industrial espionage annually cause billions of dollars damage to the global economy. The effects of theft of information and intellectual property are expressed directly upon the organization and also indirectly upon the country's economic situation. In any case, the ability to assess numerically the economic damage is a challenge in itself, and any estimate is no more than conjecture.

The cumulative economic impact of the theft of information and intellectual property has several features. First and foremost, the attacker has the ability to gain a technological advantage and can offer an identical product at a cheaper price because it did not invest in the product's development; at times, the attacker's manufacturing costs are also cheaper. The results for the victim can include reduced sales of the product and having to lower prices, decreased profits, a loss in the value of its shares, and even the demise of the company. Whatever the outcome may be, the costs to the company to handle the attack and improve its defenses are high. A famous example of a company that ceased to exist because of information theft is that of DigiNotar, a Dutch company that went bankrupt after critical information was stolen from it.[15]

At the national level, cyberattacks aimed at stealing information and intellectual property are liable to result in a lowered GDP and the loss of jobs, especially in a country whose economy is driven by technology and R&D. Investments in advanced technology are liable to be lost, translating into an economic boon for the attacker. Moreover, sensitive technological security information is liable to be leaked to enemies, affecting the balance of power vis-à-vis hostile entities and rivals. A quantitative estimate of such an effect could be based on any number of different economic forecasts, but one thing is clear: the economic effect of a cyberattack, both at the company's level and at the national level, must be given profound strategic attention.

In examining the effects of commercial espionage in cyberspace on company business decisions, we must first look at three basic aspects. The first relates to the decision makers' level of awareness of cyberspace espionage risks; the second relates to the question of whether the various companies have the tools to assess the risks and make informed decisions about them; and the third concerns the way in which the decisions made in response to cyber risks are implemented in practice within the organization. Studies show that most companies find it hard to assess the risks and as a result have a difficult time formulating plans to deter them.[16] The unanimous opinion is that cyber risks and sophisticated attacks will only grow as long as companies do not have effective capabilities of defense.

Leakage of intellectual property is one of the main concerns of high-tech companies and is most severe compared to the leaking of product specifications. In contrast, service companies are worried mostly about the leakage of information that identifies their clients, which could damage the service they provide. A survey of companies' cyber-risk maturity – their ability to analyze cyber risks – indicates that large organizations also suffer from significant gaps in their ability to undertake risk management: 90 percent of companies surveyed reported "developing" or "beginning" risk-management processes, while only 5 percent relayed being in an advanced or "mature" risk-management process.[17]

It is interesting to note that no correlation exists between the financial outlay for risk management and the actual maturity of the risk-management process. There are companies that have invested little in the field, but have carried out an effective risk-management process, while others have invested significantly in the process, but have done so without sophistication, thus leaving much to be desired. Senior financial managers lacking technical knowledge have difficulty incorporating cyber risks in their risk-management processes and making informed decisions, all due to the lack of information. Moreover, despite the preoccupation of large organizations with protecting information and spending a significant amount of money over the years on this issue, the data reflect a large gap between the sophisticated risks in cyberspace and the ability of companies to defend against them.

In fact, one might conclude that the greatest problem in dealing with cyber risks is the ability to assess the risk, and consequentially, the difficulty in providing an appropriate security response. The difficulty in confronting complex cyber risks – and the poor record of success to date – has led to the conclusion that increasing cyber expertise within the organizations themselves is imperative. At present, there is a growing trend in large American companies to hire cyber experts for senior positions.[18] Companies included on the Fortune 500 list have appointed cyber experts who report directly to the CEO, compared to the widespread structure in which the chief information security officer – CISO – reports to the chief information office – the CIO. Moreover, the demands currently made of cyber experts include not only a technical understanding in the field of information security, but also extensive familiarity with business processes and an understanding of risk management.

Although large companies make strategic decision about cyber security and establish bodies with the requisite knowledge and technologies designed to analyze the risks and improve the level of security around the information assets, mid-sized and small companies find it hard to do so on their own. These companies lack the resources needed to apply the range of processes, technologies, and frequent adaptations required in the field of cyber defense. Companies with limited resources face several options. Applying minimal cyber defenses to the best of their understanding and budgetary allowance consequently leaves them at risk of information and intellectual property theft as a determined attacker will, in all probability, be able to penetrate the company's network. Many small, resource-poor companies will appoint a system administrator as the professional in charge of information security. In many cases, that person's work will focus on issues within his or her technical responsibility, such as security of servers and end stations, user management, mail server security, and network infrastructure security. Such a person will not be able to build an information security system that takes into consideration the professional analysis of potential cyber risks facing the organization.

A second option is for the company to increase its cyber defense budget in order to provide an appropriate response to the risks and, accordingly, to risk management. One may assume that this will involve significant investing in a cyber security infrastructure, the acquisition of relevant products, setting up a team of experts, professional training, meeting standards, and so on. Investing in the field will affect the company's profitability and its ability to compete, in the expectation that the investment will pay for itself first and foremost by reducing the probability of cyberattacks while increasing the company's ability to develop business processes in a properly-secured environment.

A third option involves relying on managed security services via outsourcing, although in many cases the providers do not see the whole organizational picture and are not part of the critical processes described above. The primary advantage of relying on outsourced security services is that it enables a company that does not have any knowledge or technological and economic ability to receive professional security services. Moreover, the price tag will be lower because the service provider distributes its costs over a large number of customers. On the other hand, an external entity is not part of the company's day-to-day functioning and is not privy to business processes that change regularly and has limited ability to provide an integrative response that is tailored precisely to the organization's needs. Furthermore, outsourcing usually provides a range of priced, defined, and generic services so that it can appeal to most of its customers, which makes it difficult to receive security services that are both dynamic and specific to the company's needs. Managed security services can be a real improvement for small companies with clear security needs, but only up to the point where the business processes become complex.

It seems that small companies, which are founded entirely on their intellectual property, will find it difficult to protect their information – their chief asset – and their working processes against sophisticated cyberattacks. These companies will settle for a partial security solution on the assumption that they are not a preferred target of sophisticated attacks. This type of solution will then place them at the top of the ladder of companies at high risk of cyberattacks, business espionage, and information and intellectual property theft.

The situation is especially difficult for Israeli startup companies. Israel's R&D industry is widespread. Hundreds of companies rely on the R&D budget of the Office of the Chief Scientist at the Ministry of Economy and Industry and on raising capital from all sorts of funds in order to develop knowledge, technology, and products. The intellectual property is the most important asset in the existence and development of the Israeli startups. These companies will have to choose one of the three alternatives described above. One can assume that, because of budgetary constraints and possibly also because of a lack of awareness, they will opt for minimal cyber security. This means that the most advanced information assets and the largest potential growth engine for the nation's economy will receive the lowest form of cyber defense on the market. This is a disturbing realization, requiring profound attention at the national level.

Supporting the need to formulate a national response and strategy for the cyber defense of Israeli startups is the Office of the Chief Scientist at the Ministry of Economy and Industry. The chief scientist facilitates the establishment of technological hothouses by financing of up to 85 percent of their budgets, for an annual total of ILS 1.5 billion. The government's financing is expected to be returned through royalties paid to the state from any income generated by the product itself or a related product, including services that are ancillary to the product or involved in it. The chief scientist's investment in R&D is thus a highly risky venture because of the exposure of developing technologies to the theft of their intellectual property. The damage might be inestimable as the companies risk their ability to realize the products of their R&D, and, as a consequence, they also risk their ability to pay back the state for having funded the R&D process.

Concluding Insights

Protecting information and intellectual property is a critical need for any private, commercial or national organization. The process of protecting information and intellectual property is complex, both technologically and process-wise, and has significant ramifications for the organization's development budgets. The successful implementation of an effective defensive shield around the information and intellectual property depends mostly on the organization's awareness of the risks and its ability to optimally protect itself. All of this is a direct consequence of the organization's economic capabilities, the maturity of the organizational culture regarding information security, the existence of organizational functions, and the presence of skilled manpower. It seems that the economic ability to realize advanced security solutions is one of the major obstacles that small and mid-sized companies face when trying to confront the risk of information and intellectual property theft. But the existence of economic ability – while certainly a necessary condition – does not alone ensure effective handling of the risk of cyberattacks.

It is clear that organizations find it hard to assess their cyber risks because of the lack of current knowledge, the complexity of the issue, the lack of economic resources, insufficient skills, or an inappropriate organizational structure (such as the lack of a position in charge of cyber defense and risk-management). This situation affects an organization's awareness of cyber risks and its preparedness to operate against them. Even organizations rich in resources and professional manpower do not always succeed in implementing optimal defenses against cyber risks, which can provide an effective response using different means information security. The situation is particularly dire for startups notable for their groundbreaking intellectual property and tremendous economic potential, and, at the same time, for their limited budgets that keep them from effectively defending their valuable intellectual property. Moreover, startups by their very nature are focused on technological development and tend not to set up significant IT and information security entities.

Israel's government security organizations and critical infrastructure companies in the private sector are defined as bodies guided by the National Agency for Information Security and the director of security of the defense establishment. By contrast, Israel's private sector sphere is left without guidance or help at the national level, and is, in fact, expected to conduct itself to the best of its understanding and ability. The National Cyber Bureau may be tasked with determining a comprehensive policy for protecting Israel's computerized systems (the so-called "national cyberspace policy") and with developing a state-wide operational approach that is suitable for routine times.[19] Protecting information and intellectual property in private sector institutions not considered critical infrastructures, however, is not a significant part of the bureau's work.

It is incumbent upon the State of Israel to improve its defense of knowledge that is supported with the state's R&D funds, and to ensure the protection of information and intellectual property in the technological and business sectors, as damage to these two sectors would directly affect the Israeli economy and market competition. Furthermore, the State of Israel needs to establish a consulting body for the protection of knowledge and intellectual property within the private sector in general and technological companies, such as startups, in particular. The National Cyber Bureau might be responsible for this body.

One response, albeit only partial, to the challenges described herein is to demand that the state protect its investments in R&D. Such a demand could cause private sector business initiatives to respond with an appropriate level of expertise and at a reasonable cost for companies financed by the Office of the Chief Scientist. It is therefore advisable that the government assist in constructing a security infrastructure for needy companies. An example would be helping with development capabilities and activity within a secure cloud, applying high-level security standards.

A business enterprise that seeks to provide security solutions and development capabilities in a secure infrastructure will only do so if it assumes it has a profitable business model and enough clients. This will occur if the companies financed by the Office of the Chief Scientist are urged to secure their intellectual property using professionally-determined standards. This necessary action will match the financing body's demands to operate in a secure environment together with the response of private sector companies that will provide such an environment to a captive market.

The establishment of a secure cloud infrastructure should create a safe space for the needs of technological development companies, including startups. Such an infrastructure would be based on security systems that specialize in protecting information and intellectual property and allow those companies to manage their sensitive information within much tighter security parameters than they could make for themselves. The Office of the Chief Scientist, which budgets millions of shekels to technological hothouses, is accelerating the use of the secure cloud. The Office of the Chief Scientist is also a partner in the Kidma Program to Advance the Cyber Security Industry in Israel,[20] along with the National Cyber Bureau, and gives preferential budgeting to R&D in the field of cyberspace in order to promote and position Israel as a global leader in the field. Getting funds from the Office of the Chief Scientist at present is not conditional upon presenting a plan to protect the information and intellectual property; thus, million-dollar companies that are developing technologies designed to fuel Israel's economic growth are, in practice, exposing themselves to cyberattacks and potentially tremendous damage.

In a world in which sophisticated cyberattacks focus on the theft of information for the sake of taking technological shortcuts, the establishment of a professional body that consults for private sector technological companies and the development of a designated cloud infrastructure with a high level of security should dramatically improve the survival rate of the startups and ensure the successful protection of their intellectual property. By making such a move, Israel would be able to maintain an obligatory security mechanism and ensure a return on its R&D investments.

Notes

[1] Doron S. Ben-Atar, *Trade Secrets: Intellectual Piracy and the Origins of American Industrial Power* (New Haven: Yale University Press, 2004).

[2] In many cases, manufacturing plans for product components (sets, printed circuits, electronics, and so forth) are sent to subcontracted manufacturers via magnetic media, whether physically or through telecommunications.

[3] Tucker Bailey, Andrea Del Miglio, and Wolf Richter, "The rising strategic risks of cyberattacks," *McKinsey Quarterly*, May 2014, http://www.mckinsey.com/insights/business_technology.

[4] Such systems are known as data leakage prevention systems.

[5] The organization's supply chain manages processes of acquisitions, manufacturing, storage, distribution, and shipping, and its function is to connect the manufacturers, suppliers, and end clients. Supply chain management requires great flexibility and coordination capabilities vis-à-vis external entities, and represents an important component in creating the company's value.

[6] Cloud services include DropBox, Google Drive, Jumbo Mail, and the like.

[7] Bailey, Del Miglio, and Richter, "The rising strategic risks of cyberattacks."

[8] The attack on the North American retail chain Target, in which millions of credit card numbers were stolen, started with the theft of access permissions from a maintenance-systems provider that Target had contracted. See Brian Krebs, "Target Hackers Broke in via HVAC Company," *Krebs on Security*, February 14, 2015, http://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/.

[9] "2013 Cost of Cyber Crime Study: United States," Ponemon Institute, October 2013.

[10] "APT1 Exposing One of China's Cyber Espionage Units," *Mandiant Report*, February 2013, http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

[11] Bailey, Del Miglio, and Richter, "The rising strategic risks of cyberattacks."

[12] Franz-Stefan Gady, "New Snowden Documents Reveal Chinese Behind F-35 Hack," *Diplomat*, January 27, 2015, http://thediplomat.com/2015/01/new-snowden-documents-reveal-chinese-behind-f-35-hack/.

[13] Mandiant, "Mtrends: Beyond the Breach: Mandiant 2014 Threat Report, https://dl.mandiant.com/EE/library/WP_M-Trends2014_140409.pdf.

[14] McAfee, "The Economic Impact of Cybercrime and Cyber Espionage," Center for Strategic and International Studies, July 2013, http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime.pdf.

[15] See the detailed analysis of this attack in Gabi Siboni and Sami Kronenfeld, "Iran and Cyberspace Warfare," *Military and Strategic Affairs* 4, no. 3 (December 2012): 77-100, http://www.inss.org.il/uploadImages/systemFiles/MASA%20-%204.3.pdf.

[16] Bailey, Del Miglio, and Richter, "The rising strategic risks of cyberattacks."

[17] Ibid.

[18] Nadia Damouni, "U.S. companies seek cyber experts for top jobs, board seats," *Reuters*, May 30, 2014, http://www.reuters.com/article/2014/05/30/us-usa-companies-cybersecurity-exclusive-idUSKBN0EA0BX20140530.

[19] From the homepage of the National Cyber Staff at the website of the Civil Service Commission http://www.csc.gov.il/DataBases/NewsLetters/NewsLetters3/Pages/CyberHeadquarters.aspx.

[20] See circular issued by the Office of the Chief Scientist: "The Kidma Program to Advance the Cyber Security Industry in Israel," November 21, 2012.