

## Business Profile

Rev. 2.1

### Contact Information

Mail Address: 4 Druyan st., Rehovot 76574, Israel  
Phone: 972-8-9354152  
Fax: 972-8-9354152  
E-Mail: info@hbarel.com  
Web: www.hbarel.com

### Fields of Activity

Hagai Bar-El is the head of a small group of consultants providing Information Security Consulting services to private and public companies. Services include:

- **Secure Applications Design and Development**  
Active participation in the design and/or deployment phases of applications for handling e-commerce activity, transaction processing, secure local and remote data protection, messaging, wireless communication, and others.  
*More information is available on page 3.*
- **Evaluation of Information Security Products**  
Evaluation of off-the-shelf as well as tailor-made hardware and software applications from the aspects of information security. Evaluation is both in terms of robustness and in terms of cost-effectiveness within a particular environment.  
*More information is available on page 4.*
- **Evaluation of New Technologies**  
Evaluation of proposed solutions and products that employ novel security-related technologies, as a part of the investor's due-diligence process.  
*More information is available on page 6.*
- **Consulting Services**  
Consulting to companies about various Information Security issues, such as: Internet Security, Content Security, E-mail Secrecy, Transactions Secrecy and Integrity, User Authentication Schemes, Digital Signatures, Internal Classification, VPN and Extranet.
- Risk assessment of systems and/or workflow to aid in correct risk management. This includes examination of the system, analysis of possible vulnerabilities, establishment of recommended changes to procedures and products that can increase the level of security to the desired level, according to the sensitivity of the data involved. This also includes presentation of the findings to management and to technical groups.

# Hagai Bar-El Information Security Analyst

4 Druyan st., Rehovot 76574, Israel. Phone: 972-8-9354152, Fax: 972-8-9354152. E-Mail: info@hbarel.com

---

- Composition of corporate Information Security policy documents and Information Security procedures.
- **Lectures and Seminars**  
Provision of lectures and seminars on various information security topics within the fields of expertise.
- **Standardization Activities**  
Participation in standardization bodies on behalf of companies.

## **Fields of Expertise**

The main fields of expertise are:

- Adoption of cryptographic tools for data secrecy, integrity and non-repudiation, including e-mail security, encryption products (hardware and software), authentication devices, methods and protocols, digital signatures, secure storage and standards compliance.
- Secure systems development by integration of cryptography-based protocols and mechanisms for obtaining data secrecy, authenticity and integrity.
- Content security measures.

## **Competitive Advantage**

The competitive advantage of this office over other companies with similar fields of activity is gained mostly by the following facts:

- Past experience involving tens of companies, with highly positive feedback.
- Work is done solely by professionals.
- Highly efficient administrative facilities lead to very low administrative overhead cost. Higher overhead cost is something clients are billed for by this way or the other.
- High security level is retained within the office premises, assuring proprietary information does not leak from within our domain.
- The group does not endorse any product or vendor, is not functioning as a reseller of any product, is not affiliated with or owned by any hardware or software vendor and is not receiving any commission whatsoever from product distributors.

## Secure Product Design Services

Security products require secure design from the top down. This holds for all security products, and especially for those that introduce proprietary mechanisms (not necessarily proprietary algorithms) when implementing cryptography.

We provide assistance in secure design of mechanisms, protocols, and products (software and hardware) in general. Our involvement is offered at all stages of the product design, starting with the top level of risk assessment and threat modeling, all the way down to code review.

Specifically, we provide **consulting, analysis and documentation** in the following areas and stages of development:

1. Threat and risk assessment (*Who are the products enemies? What damage can they cause?*)
2. Security model and Protection model determination (*What approach do we use to protect the assets?*)
3. Evaluation of known protection schemes against the needs of the system (*What adequate mechanisms are already out there and have passed the test of time? How do we deploy them effectively?*)
4. Design of proprietary or case-specific protection schemes (*The mechanisms and flavors we develop to suit our needs best.*)
5. System design assurance (security perspective) at various specification levels.
6. Implementation security assurance and code review.

We may be involved in one, more, or all of these areas in a way that we complement the skills available within the organization. A flexible involvement policy allows us to provide the most cost-effective solution for the customer who can fully utilize its in-house resources. Contracts range from a single-iteration review of security specifications that are received and commented on by secure e-mail to continuous involvement that facilitates weekly meetings throughout the entire product development cycle.

Generally, our business model favors concentrated professional work rather than endless retainer contracts, so our involvement in the product design is tightly coupled with the actual need.

## Product Evaluation Services

Companies often refer to third party products to handle their information security needs. Such products can be for data security of e-mails, messaging, local storage, database security, document security, user authentication, etc. Unfortunately, there is very little way for a customer to be sure that the product he uses is indeed secure enough to handle the type of information it is employed to handle. Security products are written by thousands of people and companies worldwide who develop security products with or without having adequate skills and training and with or without taking their products through secure design assurance procedures.

Little or no guarantee is given on the actual robustness of these products and on their ability to support their claimed level of security. Most companies do not give any warranty for the case of a security incident that involves their product. Moreover, for the most part vendors do not provide any documentation that allows the customer to establish an educated trust in the products robustness.

This is not of an evil intent. A formal security proof is practically impossible to obtain for almost all commercial products. It is also unfeasible to test for mitigation of all attacks and threats by a set of go/no-go tests. It is difficult enough to assure that a product correctly supports all of its documented features; it is even more difficult (if not impossible) to assure that a product does not support any risky non-documented features.

Aside of the security issues that may result from poor design, many flaws occur just because the product designer is not a security professional. Experience shows that almost all applications that implement cryptographic mechanisms (for example) and that are written by typical application designers and developers who are not security experts is proven to be flawed shortly after it is introduced or fielded. A quote taken from *Bruce Schneier*, who is one of the experts in this field, says that anyone can design a security system that he himself cannot break.

For summary, following are a few statements that should be considered as facts:

1. Security products are often insecure, due to poor design by people who are skilled, but not necessarily in security.
2. No assurance is given to the customer regarding the robustness of the product. He is typically asked to blindly *trust* its sensitive data to be securely handled by the product.
3. Security products typically handle sensitive data that its exposure may have serious implications, otherwise the security product wouldn't be needed at first place.
4. Usually, the product vendor cannot be found liable for damage caused by data leakage from its products.

The evident conclusion from these is that **it is practically the customer's interest and duty to use any reasonable endeavor to assure that the product it trusts its sensitive data with is indeed worth this trust.** This assumption is the essence of our service.

Our job is to examine a security product to the light of the data it is (or is going to be) trusted to

# Hagai Bar-El Information Security Analyst

4 Druyan st., Rehovot 76574, Israel. Phone: 972-8-9354152, Fax: 972-8-9354152. E-Mail: info@hbarel.com

---

handle. This analysis is performed by security professionals who deal with security assurance for a living, day by day.

The extent to which we perform an evaluation is flexible and is mostly a function of the level of security required, the level of support we can get from the vendor (which typically depends on how much the vendor values the customer), and of course, the projects funding. Our experience shows that even the lowest level of evaluation can usually cross off a significant number of applications, especially of the ones that use cryptography.

## Technology Evaluation Services

Throughout the past eight years we collected knowledge. We evaluated dozens of products and helped develop others. We studied the new advancements in the field of security, and studied each new solution we could get enough information on. We reviewed thousands of documents, standards, specifications, articles and commentary; all are indexed and filed in one digital library.

For the investor this knowledge is power. This power can be translated into money by separating presumably better investments from the rest as part of the due-diligence process. We know the security market, we know the real problems that seek solutions just as we know the widespread solutions that seek problems. We know what can be done today, and we know what problems are probably here to stay (at least for a while). We know many of the ways that were already taken, and in some cases we know where they lead to.

We serve this knowledge to investors who need to evaluate investment opportunities in the field of information security. When presented a new security concept or a new proposed solution to a problem we can help in addressing the following questions:

1. Does the problem (that the proposed solution attempts to solve) actually exist? How meaningful is it? What is the magnitude of the market that seeks solution for this problem?
2. Is the proposed solution effective in solving the problem?
3. Is the proposed solution feasible? Can it be implemented at reasonable cost?
4. Is the proposed solution secure? Does it hold water from the security perspective? Can it be certified?
5. Was it ever tried before? Was a similar concept ever tried before?
6. Are the people involved skillful in the art?

We will attempt to address these questions, as well as any other that will arise during the due-diligence process, so to lead the customer to a position in which he invests his money only after tapping into a large knowledge-base of relevant technologies, experiences, solved and yet unsolved problems.