Cyber and Medicine – Waging a similar battle

In many respects, cyber security is actually a mirror image of medicine. They are both dedicated to maintaining the health and continued functioning of the organism, while coping with a range of harmful agents both from without and within. On the similarities between the world of cyber and the world of medicine…

By Roni Zehavi

The term Cyber Security, or as it is bantered in everyday language, simply Cyber, has won a place for itself among today's most popular terms used everywhere and in every sphere. This fact is likely a result of the frequency and depth of daily attacks – the commonly agreed number is some million attacks worldwide per day! But it is no less a result of the daily coping that leaves no doubt as to what the future holds.

The fact that the threat is hidden, undetected and unexpected, has heightened the similarity to medicine in the social imagination. The cyber attacker was termed a "virus" already in its early days in the 80s of the previous century, and the rate of its development has only strengthened the natural fear of a fatal attack from something unknown and near impossible to prepare for. For example, in 1985 there were 11 known types of virus, while in 2008 that number has reached a million different viruses. In the first quarter of 2013, the number of viruses had reached a hundred million, and in the first quarter of 2015, 400 million different cyber threats were registered, all developed from malware. The number is increasing exponentially at this very moment as you read about it.

Connectedness and Functionality

On the other hand, the connection and comparison between cyber security and the world of medicine greatly deviate with regard to feelings of fear and threat.

If a visitor from another planet was requested to define the characteristics of a living organism, he would no doubt mention, from his observations, the **connectedness** between various factors and components, from the cellular level to the sub-system level, which allows a unified functionality of the whole system as a single coherent entity. This functionality includes, among other things, data collection, storage, processing, ongoing learning, carrying out integrated activities to achieve common aims, and so on.

Such a description is precisely suited to the modern world we are approaching. Connectedness between people, without regard for geographical borders, nationality or language, as enabled by social networks, between people and machines, and between machines themselves in the world of the "Internet of Things" – all these are weighed in to a unified organism in which integration of local functions of its components result in an inclusive functionality on various levels – local (in company, in the car, the smart home), regional (smart city, smart hospital), or global (network, data cloud, science).

From this analogy between the "human organism" and the "social organism", we can understand how right and representative is the intuitive comparison, and that cyber security is simply the mirror image of medicine, but in the cyber world. They are both dedicated to maintaining the health and continued functioning of the organism, while coping with a range of harmful agents both from without and within, while the result of the activity of these harmful agents is the same – functional and structural damage to the unified system. (It should be mentioned here that the damage caused by the organic attacker is consequential, i.e., it is un-aware or unintentional, and non-focused on the damage it causes, while the cyber attacker is "aware" of its damaging results and in fact, focused on the aim of causing these results, which makes its damage potentially that much more harmful. Still, from the point of view of the system as a whole, this fact is not important with regard to the degree of similarity between the two spheres.)

Data sharing as a necessary condition

From this viewpoint, and with a recognition of the fact that connectedness is the essential and growing characteristic of modern life, we can draw insight that says the daily existence of society will require constant grappling with the presence of cyber attacks, just as our constant battle with viruses and bacteria is part of human life.

Terms such as "basic hygiene", "national awareness", or "safety education", will become increasingly popular in daily life. Cyber security experts are the "doctors" of the social organism. The cyber industry will become known as the new health industry, suggesting a variety of R&D-based medicines (such as anti-viruses). Just as the medical field is divided into specialities and focused areas of expertise (e.g. Orthopedist specializing in joints), so too cyber medicine will become increasingly specialized creating new fields and professions such as network specialist, cloud specialist, or database specialist.

Parallel to the medical Emergency Ward and emergency centers, will be monitoring and cyber response centers, such as CERT (Cyber Emergency Response Team). These teams will be able to evacuate organizations, companies and private individuals with the aim of evaluating threats and providing first aid to ensure the most rapid possible return to work. Such centers will collaborate with each other, sharing information and experience, research and learning about new cyber threats, effective treatment, cures, and the building of systems for protection.

But the medical approach – as meaningful and essential as it may be – is just one view of cyber reality. As in medicine, here too other important factors come in to play, no less vital, such as behavioral culture of knowledge sharing or knowledge hiding among those interconnected. Such cooperation is a necessary condition for the advancement of cutting edge, multi-disciplinary, academic research and is the basis for development of "medicines" and "preventive measures", security and defense technologies, and no less important, a consumer and behavioral culture.

As opposed to the well-known and accepted practices of personal medicine, the sphere of "cyber medicine" still suffers from difficulties emanating from a fear of invading privacy – on a personal level on one hand, and on a business level on the other, where it is seen as a display of weakness, where admission of vulnerability could cause damage to corporate image. Together with this, it seems that the global insight that knowledge sharing is a condition for an all-out war against cyber threat is seeping into awareness with adoption of the phrase: "It is a common problem faced by us all."

Extract:

As in medicine, here too other important factors come in to play, no less vital, such as behavioral culture of knowledge sharing or knowledge hiding among those interconnected. Such cooperation is a necessary condition for the advancement of cutting edge, multi-disciplinary, academic research and is the basis for development of "medicines" and "preventive measures", security and defense technologies, and no less important, a consumer and behavioral culture.