Enabling innovation with trusted computing

Former CISO of the Israeli Defense Forces Menny Barzilay, also the opening keynote speaker of the upcoming 16th Info-Security Conference, talks about the never-ending debate between innovation and cyber security

By Computerworld Hong Kong editor

MENNY BARZILAY is an evangelist of innovation and strategist in cyber security—two roles that are very much related, but often contradicting each other. As a former CISO of the Israeli Defense Forces and adviser in the global startup community, Barzilay says cyber security is often an innovation enabler, instead of limiter.

He will be visiting Hong Kong to share his views at the 16th Info-Security Conference on May 29, 2015. At an interview with *Computerworld Hong Kong* (CWHK), Barzilay talked about trusted computing and its value to innovation.

***CWHK:* Innovation and cyber security appear to be contradictory concepts. How balance can be achieved between driving innovation and securing such an environment?**

MB: Previously, the world of information security was much simpler. Information security guys were in charge of only proclaiming one of two things: "Yes, you can do it" or "No, it's too risky, you are not allowed to do it." As you can imagine, the latter was used more frequently.

But today, security is no longer about "yes and no" and rather about "how". This means users can tell me what they want to achieve, and together we will find ways to do it. We should stop addressing cyber security as an innovation limiter, and start addressing it as innovation enabler. This makes the job of the CISO a much more complicated one, but also a much more effective one.

***CWHK:* Let's talk about effective security. As technology constantly evolves and hackers find new ways to attack, how can a CISO effectively catch up with the changes? What role does the user play in the process?**

MB: Users have the power to create great damage to the organization. Almost every high profile cyber incident story included users that did something wrong like opening an email attachment or connecting a device that they shouldn't have. It doesn't matter how many security and safety systems are installed in a car, the driver can still crash into a wall.

Investing in user awareness has a high ROI, but only if you do it correctly and effectively. People don't see cyber security as their own problem. They believe "someone" should take care of it. An effective awareness program will not only raise awareness, but will also create partnership with users, who help to protect the organization and identify out-of-the-ordinarily behaviors.

***CWHK:* The military is one of the most popular targets of cyber attacks. What are the lessons learned from your experience that can be applied to the general enterprise environment?**

MB: As technology evolves, it becomes easier to attack and harder to protect. This is called the asymmetry of security. When attacking you can choose one specific target, when protecting you have to secure everything. When attacking you need only to succeed one time, when protecting – all the time. Attacking is very cheap, protecting is expensive.

In today's world scenario, we need to do things differently in many aspects. They include:

- Work together –The hackers and criminals have become very good at sharing information and working together. In order for us to be able to face the rising threats, we too have to work together. Share information and intelligence, and even create in-sector and cross-sector cyber security solutions.
- Invest in detection – Everything is hackable. We need to prepare for the day when we will be hacked. Would we know who did it? How much time will pass until we discover the hack? These are important questions that we need to invest in for answers. This means we should invest in solutions that go beyond security prevention, but also detections.

***CWHK:* What do you think about trusted computing? Does it exist?**

MB: About two years ago someone hacked into AP's Twitter account and published a twit stating that two explosions occurred in the US White House and that President Obama was injured. This fake twit led to a fall in the exchange markets.

More than a year ago I witnessed a POC in which an Asian hacker successfully hacked into a smart TV (remotely) and demonstrated his ability to present a fake "breaking news" about a bomb in the middle of Manhattan.

These events all lead to a loss of trust. And loss of trust is a major business issue and a true enemy of innovation. If people will stop trusting their devices, vendors, applications, progress will stop. Would people use driverless cars? Bitcoins? Biotech? Smart houses? What about Facebook?

Trusted computing means things should work in the same way they are expected to work. This is a general definition which demonstrates that there are many ways to hinder trust.

But does trusted computing exist? The answer is more or less yes. Even though we hear of many incidents that lead to loss of trust, the problem has yet to reach the point where we can say the technology is not trustworthy. But we are not far from that too.

Menny Barzilay will be the keynote speaker at the 16th Info-Security Conference on May 29, 2015—Hong Kong's largest annual security event. He will present on the topic: *Why Cyber Security Needs a Rethink?*