Achieving ROI in security investment

Security expert Guy Ron talked about the lessons learned from securing military and mining organizations, the ROI of security strategy and more

By Computerworld Hong Kong editor

GuyRon, InfoSec

CYBER SECURITY expert Guy Ron practiced in the most sensitive and high risk organizations in the world. With experiences in running security organizations for government agencies and the military in Israel, as well as consulting for the mining, banking and technology organizations, Ron will be visiting Hong Kong to share his experience at the *16th Info-Security Conference* on May 29, 2015.

At an interview with *Computerworld Hong Kong* (CWHK), Ron talked about the lessons learned in securing these high risks organizations, the ROI of security strategy, intelligence in cyber security and more.

***CWHK:* What are the lessons learned from running security in the highly targeted organizations that can be applied to general businesses?**

Guy Ron (GR): One of the major lessons learned from the mining industry is securing the OT (operational technologies) environment. Mining operations rely heavily on physical equipment, which is becoming automated, computerized and often being controlled by an operator hundreds of kilometers away. Security in OT is becoming a concern for organizations in the mining, oil, resources and even the manufacturing industries.

Historically, most cyber security measures are placed around the IT environment. Only a handful of companies will protect the equipment, like a drilling machine. But with the automation of physical equipment and more of them being operated via the Internet, more attackers are seeing them as the easy targets. The level of security and awareness among the OT environment is way behind of the IT environment. Most organizations still have lots to invest for the right measures and standards. This is not to match with their IT environment, but just to put them into a more reasonable position.

***CWHK:* Talking about investment, how do you find the ROI of security technologies?**

GR: Technologies that we used to spend a lot of money, like antivirus, IPS and IDS, are arguably not giving us the best ROI. These technologies used to protect the organizations, but they are no longer effective. They can only tackle yesterday's threat, but they cannot protect us from tomorrow's or today's threats. Organizations are spending money in protecting threats and risk that are often no longer relevant. Their investments are wasted.

One of the reasons for a low ROI in security technologies is the mismatch between investments and threats. Most organizations are investing in millions of dollars to protect everything from everyone. But attackers are growing at an accelerating pace to develop sophisticated and complex attacks. They are always one-step ahead of the enterprises. The attackers are using new tactics. They have moved into a new war, but the enterprises are still playing catchup. This has come to a point that enterprises need to reevaluate their security strategies, to become much smarter in technology investments. They need to prioritize their budget based on cyber threat intelligence (CTI).

***CWHK:* How do they become smarter? How does CTI help?**

GR: CTI is becoming rucial in organization's security strategy. The traditional security operation tends to gather logs and data to provide basic monitoring and analysis to identify patterns. But such analysis is very limited and they are missing the weak signals in the pattern, which are often signs of the real attacks.

More organizations are moving to the next level of analysis by correlating security incidence data with the organization's system logs and operational data to identify the weak signals that are specific for the organization.

By matching vulnerability data from the security vendors with the organization's information, the security organization is also able to generate real-time alert of the relevant threats. Organizations can then apply immediate measures to remediate the situation.

With CTI, organizations are also able to identify the relevant risk that are specific to the organization ahead of the attack, so they can allocate more resources to the high risk areas and be prepared for potential attacks. CTI will allow organizations to be ahead of the game and be proactive in protecting the organization.

***CWHK:* You also have a background in software development. How does the development stage help enterprises to reduce vulnerabilities?**

GR: I am a big supporter for secure software development, but I'm very disappointed with how little has been done in this area. Only a few software vendors invest in putting security methodology in the development stage. Very often they will only invest in this area after incidents happens. This is found even less amang the in-house developed software. Almost none of the large corporations use any secure development process.

Cyber criminals are becoming aware of this. They are currently going after the low hanging fruit, the major package software, but they will, someday, go after enterprises and the vulnerabilities in their in-house software.

Guy Ron 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: The Prosecution: The Trusted Computing is an Oxymoron.