Great cybersecurity technologies need great people

By Michael Xie

1 Sep 2016

As chief technology officer, my primary mandate is to develop technologies to help our enterprise customers improve their security postures. As we cross our 300-patent milestone after 16 years in the business, I am encouraged by the good progress we have made.

©alphaspirit via 123RF

In recent times, however, it has dawned on me that powerful as they are, our solutions are not reaching their full potential in all the organisations where they are deployed — due to a dire shortage of cyber security professionals to harness them. This is a global phenomenon, and we have reached a stage where cyber security manpower development cannot be put off any longer.

More manpower needed

One may assume that with greater automation and the advancement of technology in general, the dependency of cyber security on human beings has fallen. The truth is quite the opposite. According to Frost & Sullivan, more manpower is needed for the following reasons:

• **More sophisticated and persistent cyber threats:** The rising sophistication of cyber threats is not just to accomplish a singular goal (e.g. steal sensitive information), but to be persistent and effective over an extended period of time. To achieve these goals, evading detection and, if detected, silently adapting to either continue or reappear later are part of the hacker's operating principles. Consequently, identifying compromises and qualifying their severity requires constant diligence and deep pockets of expertise. A high degree of talent, knowledge, and time is also needed to thoroughly root out discovered compromises.

• **Larger IT footprints:** The growing ubiquity of mobile devices used for business, both corporate-issued and personally-owned, and the increasing adoption of cloud services, contribute to a larger IT footprint to protect. The raft of mobile devices (manufacturers, operating systems and models) and cloud environments (service models and providers) add to the challenge.

• **More security technologies:** Evasiveness of threats and a growing IT footprint require next-generation security technologies to replace and supplement in-place technologies. With this, the security operations team has more dashboards to view, dials to turn, and alerts and reports to examine.

• **Self-inflicted wounds:** No one is perfect and perfection cannot be expected in an IT world of perpetual change. Configuration errors and oversights have and will continue to occur. Similarly, end users will have lapses in judgement (e.g. clicking on an untrusted link). This means re-do and recovery will continue to be a routine part of security professionals' activities.

Combining human and machine

In the face of the cyber security manpower shortage, the industry has made some stop-gap efforts to deal with the issue. Various organisations are developing machine learning and automation technologies that try to substitute human beings in analytical work. There are also attempts to create artificial intelligence to discover and respond to security threats.

In addition, I expect the industry to continue focusing development efforts on technologies that can let businesses deploy security with minimal manpower. Such technologies include cloud-based security platforms that can help resource-lean SMBs manage or increase visibility, as well as security solutions that can be managed remotely by mobile devices.

Commendable as these efforts are, they are no replacement for the flesh and blood of real IT personnel. Intelligent cyber security technologies can only take the place of human decision making as an initial filter (take a look at what trading algorithms have done to the modern stock market) — at the end of the day both artificial intelligence and human operators need to work together. Without the human element, larger and larger swaths of the world will suffer from poorly implemented cyber security — security tasks will be sub-optimally done, leading to greater vulnerabilities in cyber defences and inefficiently run security departments.

On the security technology provider front, we can expect to see more consolidation in the near term. A dearth of security practitioners will make it hard for small vendors to both develop their technology and expand headcount, putting pressure on them to merge with larger solution providers.

Grooming talent

To successfully groom cyber security talent, all stakeholders in the industry must come together – not just technology providers, but governments, regulators, educational institutions, services providers and end-users. There must be more concerted setting of the security education agenda, curriculum development and knowledge transfer, funding and internship programs. For young aspiring cyber security professionals, it will be immensely helpful if you could reach out to the industry to signal your interest.

And if you aren't sure you will make a good cyber sleuth? Just ask yourself a few questions. Did you grow up reading Agatha Christie? Do you have a natural inclination for investigation and discovery? Do you love connecting dots and reading minds? Is good triumphing over evil important to you? Do you enjoy using technology to solve everyday issues and improve lives? If you have answered yes to all these, the industry needs you.

ABOUT THE AUTHOR

Michael Xie, founder, president and CTO of Fortinet,