RƎDDAL

Cyber security - more complexity, more business

Reddal Insights — 29 January 2015
Per Stenius

The total number of security incidents has increased by 48% from 2013 to 2014. It comes as no surprise then that global IT security is expected to grow at a pace of 10% annually. The World Economic Forum ranked cyberattacks among the top 5 most likely global risks in 2014.

This article originally appeared as a post in LG CNS BLOG (www.lgcnsblog.com) on 29.01.2015. Reproduced here with the kind permission of LG CNS.

A recent survey finds that the total number of security incidents climbed to over 42 million in 2014, suggesting a growth of 48% from 2013. Somewhere in cyberspace someone is attacking someone else roughly once every second, or over 115 000 times every day. While the estimates of the impact of these attacks vary, industry sources indicate the total cost of these attacks is on the order of 500 billion USD annually. It comes as no surprise then that global IT security spending by corporations to combat cybercrime is estimated at about 75 billion dollars currently, and expected to grow at a pace of 10% annually. The World Economic Forum ranked cyberattacks among the top 5 most likely global risks in 2014.

Cyber… what?

Cyberspace, a term originating from 80s science fiction literature, is today a term referring to the domain covered by global information networks, into which computers, mobile devices and increasingly various machines and sensors are connected. This is no longer a matter of basic information technology equipment used for organizational data transfer and transactions. Key technology types now also include operational technology (systems and automation controlling physical processes that create and deliver products and services) and consumer technology (things like smart TVs, household appliances, domestic automation, cars and even baby monitors).

As cyberspace expands, the environment of security breaches is also becoming more complex. No longer can a wall be erected around a company. Business is increasingly dependent on cloud computing, mobility, social computing, big data and analytics. These technological trends are providing such powerful business opportunities that companies have had to abandon the closed wall and must fight the battle in a more open, multiple entry point environment. This calls for new security strategies, and is a key driver in the ever increasing complexity and fragmentation of cyber security solutions. The same challenge of how to stay secure in this open environment is now spreading due to the internet of things, and is already reaching many personal devices and homes.

The villains in the story are no longer the same either. While the popular view blames malicious hackers and criminal organizations for cybercrime, increasingly the perpetrators include governments, terrorist organizations and company insiders. In many cases the enemy is not even known, and there are multiple opinions on the source of the attack. The recent breach into SONY Pictures internal data has been blamed on North Korea, or potentially groups associated with the North Korean government, but some industry experts suggests the actual culprit may have been a disgruntled employee. The discussion in media is often distorted, and blame can be assigned based on political motives, rather than actual evidence. The actual target may be unclear as well, as attacks often involve complex indirect paths. In the case of Stuxnet, a malware infection that targeted Iranian uranium enrichment facilities, the attack was systematically and patiently orchestrated through the supply chain until it finally reached the true target. Similarly, a recent credit card information theft focused on Target seems to have originated by stealing network credentials from a supplier.

While most of the big media stories are about credit card information theft (an issue plaguing especially the US, since swipe type cards are still used there), cyber security issues now touch a much broader space. Banks, retailers, media companies, factories (including a German steel mill and a Korean nuclear plant), stock exchanges, government installations and even home appliances like baby monitoring cams are breached. Recently even the internet access of a country (that being North Korea) was brought down.

Cyber security is big, diverse and growing

Given the intensity of malicious activity in cyberspace, cyber security business is brisk and stock prices are expected to continue rising. Most of the analysts following the space seem very bullish on the prospects of the cyber security sector, and both consolidations among the bigger ones, as well as rapidly growing startups provide value creation opportunities for investors.

If we look at the overall market, it can be broken down into a set of sub-segments:

- Defense and intelligence; covering both military, security, and intelligence, this market focuses on the most advanced technology, but in sheer size it is relatively small and entry to this market is difficult due to its complexity and special requirements.

- Government; including health, education, crime, justice and other governmental areas. This market is fragmented and the requirements vary considerably; the technology is not necessarily state of the art, and the volume is considerably larger than that of defense and intelligence.
- Enterprise; this is the bulk of the cyber security market, and covers large businesses (manufacturers, retailers, banks, travel, service companies). Some of these companies, such as telecom companies, energy and utilities, and transportation and logistics companies are part of critical national infrastructure although the threat is not quite the same as in the defense sector.
- SME and consumers; while the requirements in this segment are less complicated, the market is substantial in volume and the threat perceived considerable (and increasing, given that the internet of things extends deeply into this segment, with many users completely unaware of the threats they are exposed to).

The two biggest segments, government and enterprise, offer a wide range of opportunities. For some customers, such as banks, maturity is high and there is a long list of legacy and regulative requirements, whereas others are less advanced. Nevertheless, companies serving enterprise and government typically have skill sets that can be applied across, and the core requirements have considerable similarities.

The defense and intelligence segment may seem attractive, but entering it is difficult and the requirements can be extremely complex and cumbersome. Often the revenue flow is also quite slow and limited, and the scalability of sales restricted. While companies have used this segment successfully to expand to other markets, it is today perhaps not the easiest entry point. This market is quite mature, technological sophistication high, and entry costs high (and business cycles slow), making the rewards quite uncertain.

The SME and consumer segment provides considerable growth opportunities, not only because cyberspace is reaching so deep into this segment in various ways and platforms (personal computers, laptops, pads, mobile handsets, internet of things across a plethora of devices), but also because the end users have limited understanding of the ways to protect themselves and failure to do so has such dramatic consequences. A big challenge is usability, since having to deal with multiple platforms and solutions will probably exhaust most average users. Suffice it to say that few companies have found yet a convincing way to handle security on the SME and consumer level in a simple, elegant and exhaustive way.

It is no longer about hackers and computers

Cyber security has come a long way, and the market continues to grow. Today it touches nations, government agencies, big corporations, SMEs and consumers alike, and the cyber attacks come from a wide range of sources. Cyberspace has become a military theater, but at the same time its threats extend very much into our homes, vehicles and devices alike.

The market demands are broad, offering opportunities to both small and large players. However, as the industry matures, the key question is which companies will master the integration of the various areas and become the major global players. Today global technology vendors, system integrators, major global consultancies, defense contractors, local IT service specialists, telecom operators, technology startups and niche specialists all compete in the space. While the era of "build a protective wall around the target" is over, and solutions must survive open multiple entry point environments, it is nevertheless clear that all but expert end users will demand solutions that are simple to use and provide exhaustive protection.

The players who are able to provide an integrative easy-to-use solution, and consolidate the key technologies to do so (most likely by focused acquisitions), will find considerable value creation opportunities in this market.

Further reading and references

Cyber security is a complex topic, and a good way to follow the very latest events in a deeper way than what mass media can provide is to follow some of the best bloggers in the area:

www.krebsonsecurity.com
www.schneier.com

Recent news illustrating the opportunity provided the range of threats, and some of the key players in the cyber security space:

http://rt.com/business/164804-cybercrime-445-billion-year/
http://www.itproportal.com/2014/12/18/syrian-state-sponsered-cyber-terrorists-hack-international-business-times/
http://rt.com/news/205235-stuxnet-kaspersky-iran-companies/
http://www.businessweek.com/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data
http://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/
http://www.businessinsider.com/home-depot-confirms-hack-2014-9
http://www.businessweek.com/articles/2014-01-23/low-tech-thief-steals-data-for-100-million-korean-credit-card-accounts
http://rt.com/news/216379-germany-steel-plant-hack/
http://rt.com/news/216599-korea-nuclear-plant-hacked/
http://www.usatoday.com/story/money/business/2014/10/04/jpmorgan-chase-cyberattack-russians/16717499/
http://www.govtech.com/security/12-Startups-Poised-to-take-on-the-Latest-Cybersecurity-Threats.html
http://www.forbes.com/sites/truebridge/2014/09/24/why-startups-are-the-new-super-heroes-of-cyber-security/
http://www.ft.com/cms/s/0/63d7798e-5b03-11e4-b449-00144feab7de.html#axzz3O0GIiGVA
http://seekingalpha.com/article/2448825-why-investing-in-cyber-security-stocks-is-a-steal-now
http://247wallst.com/technology-3/2014/11/24/5-game-changing-cybersecurity-stocks-to-buy-now/
http://www.marketwatch.com/story/the-three-best-cybersecurity-stocks-you-can-buy-today-2

014-09-15?page=2