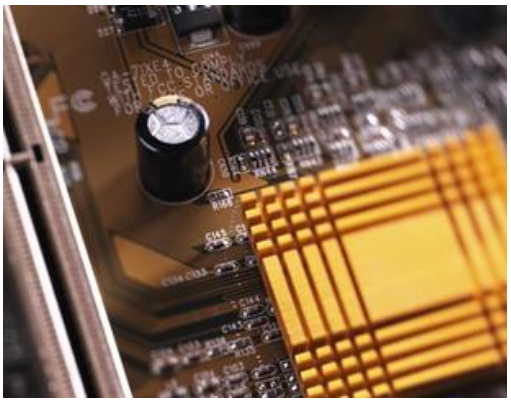
CREDIT SUISSE

Asset Management Equity Business
Security, Safety & Protection Industry

September 2014

IT security industry: Update and overview

Dear Reader,



Despite billions of dollars having been spent over the past decade on firewalls and endpoint solutions such as antivirus software, data breaches are at elevated levels, in our opinion. According to a study, the annual cost of cybercrime is estimated at around USD 400 – 575 billion and represents up to 0.8 percent of the global economy[1]. If cybercrime was a country, it would be the 27th largest economy in the world, with about the same size as Austria[2].

Today's cyber threat landscape is highly targeted and focused on acquiring something valuable and vital such as sensitive personal information or intellectual property. In 2013 there were 253 data breaches, up 62% from 156 in 2012. These breaches resulted in more than 552 million identities exposed, up 493% from 93 million in 2012[3]. The frequency of breaches is accelerating and the magnitude of the damage continues to increase. Such incidents can cost millions of dollars and compromise customer data, intellectual property and business reputation[4]. Therefore it is not surprising that spending for IT security is becoming the top priority for companies and governments. As such we believe IT security is an industry that long-term oriented investors must have exposure to. The aim of this paper is to provide an update and a short overview of this sector in a) describing the types of cyber threats and possible defensive measures, b) to map in a simplified way the various vendors and c) to conclude with the long-term drivers of the IT security sector.

IT security remains a top priority among corporate and government executives

We think IT security will get an increasing share within IT budgets over the next couple of years. In addition, most security solutions have been built from existing technologies, and therefore there is the need to invest just to maintain these legacy systems. Finally, decreasing the vulnerability of corporate networks by traditional solutions results in security gaps because those solutions were not designed to address several major recent developments. Referring to the recent high-profile breaches it seems that traditional network security solutions have insufficient abilities to deal with a complex IT infrastructure and a dynamic and constantly evolving threat environment. According to a

[1] Source: Center for Strategic & International Studies, McAfee (2014): Net Losses: Estimating the Global Cost of Cybercrime, June 2014, URL: http://csis.org/event/2014-mcafee-report-global-cost-cybercrime, 13.8.2014.
The report acknowledges that estimating losses can be difficult, but given "intangibles" such as IP losses, military advantage losses and increased global sales competition, the numbers are more likely to be higher, according to the authors.

[2] Austria is the 27th largest economy with a GDP of USD 415bn (source: IMF (2014): World Economic Outlook, April 2014, URL: http://www.imf.org/external/pubs/ft/weo/2014/01/index.htm, 13.8.2014).

[3] Source: Symantec (2014): Symantec Internet Security Threat Report 2014, April 2014, p. 13, URL: http://www.symantec.com/security_response/publications/threatreport.jsp, 13.8.2014.

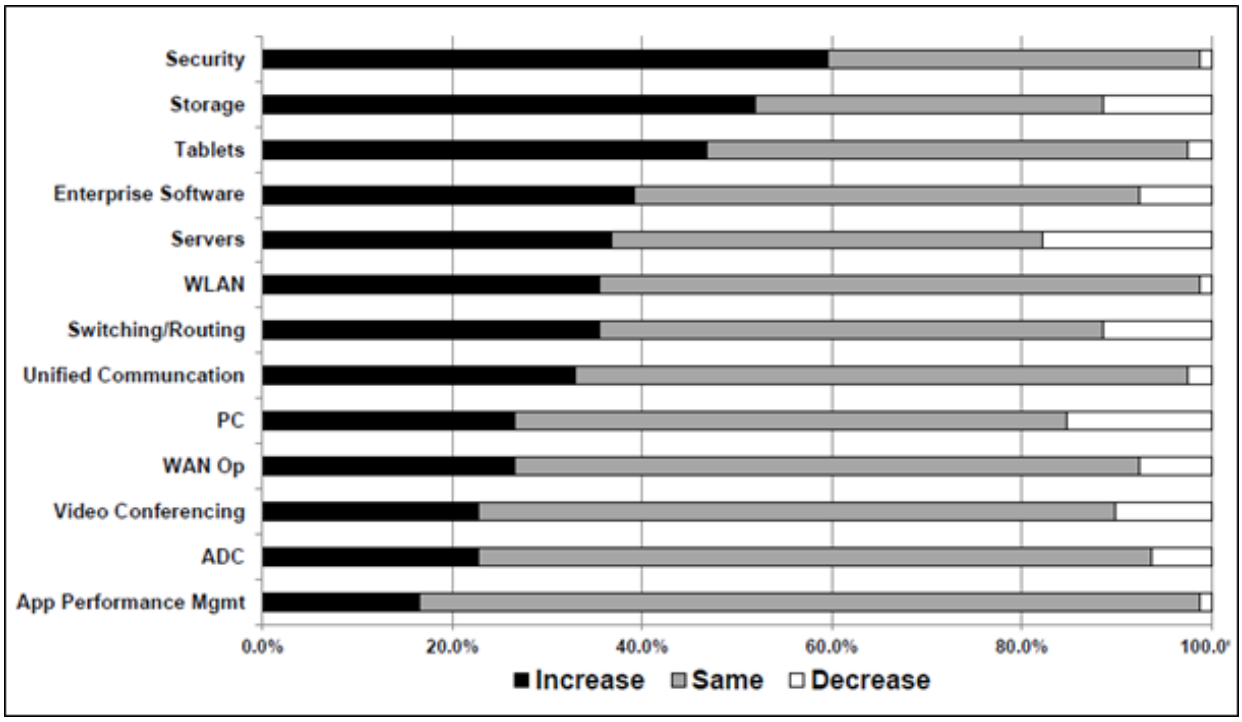
[4] When US retailer Target admitted last year that credit card details of at least 40 million customers had been stolen, US banks lost about USD 200 million (source: Financial Times (2014): Cyber attacks, The Lex Column, Aug. 26th 2014, p. 12).

report by Verizon, there are some interesting findings[5]:

- 75% of breaches were driven by financial motives,
- 66% of breaches took months to discover,
- 92% of breaches were perpetrated by outsiders,
- 37% of breaches affected a financial organisation, and
- 71% of breaches targeted devices.

In our opinion cybersecurity risks have increased significantly with the adoption of new trends such as cloud-based applications, social networks or virtualization, because they might generate more weaknesses in an organization's network. The big challenge for IT security administrators is to find a balance between enhancing the productivity of the employees, and securing their networks and sensitive data. Therefore it is not surprising that IT security has always been a top priority among Chief Information Officers (CIOs). According to a survey ~60% of CIOs are expecting to increase the spending on security-related products in 2014 (fig. 1).

Fig. 1: Which technologies will increase of decrease within your 2014 IT budget?



Source: Piper Jaffray, June 2014.

Types of cyber threats

Fig. 2 provides a short overview of the types of cybersecurity threats facing consumers, enterprises and governments[6]:

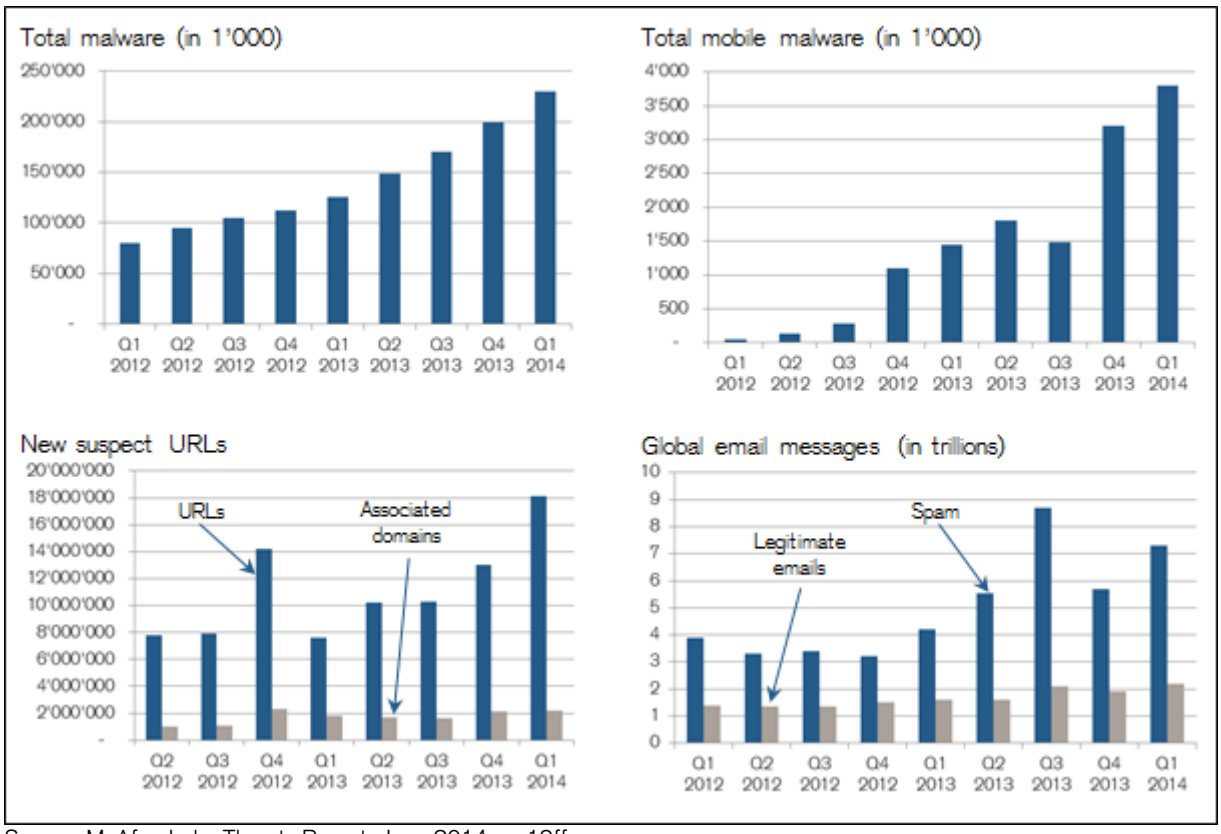
- Malware: Malware stands for "malicious software", which can be used to disrupt applications, steal sensitive data or gain access to a networked server. It can take many forms including viruses, trojans, worms and others. In Q1 2014 the total sample count broke the 200 million level, this was a 19% sequential increase from Q4 2013.
- Mobile malware: Mobile malware is similar to traditional malware, but it resides within an application running on mobile devices. Mobile malware has been noted to have the following capabilities, all of which do not require the user's permission such as make calls, install additional applications, monitor, record and send SMS, read user's contact data and

[5] Source: Verizon (2013): 2013 Data Breach Investigations Report, p. 19ff, URL: http://www.verizonenterprise.com /resources/reports/rpdata-breach-investigations-report-2013_en_xg.pdf, 13.8.2014.
[6] Source: McAfee (2014): McAfee Labs Threats Report, June 2014, p. 19ff, URL: http://www.mcafee.com/de/ mcafee-labs.aspx, 13.8.2014.

others. The total number of mobile malware increased by 167% to almost 4 million as of Q1 2014.

- Web threats: A web threat is simply any threat that uses the web to facilitate a crime, typically leveraging internet communication protocols such as HTTP, email, attachments or web servers. Examples are spams, phishing or clicking on dangerous links (URLs). According to McAfee, 18 million new suspicious URLs were noted in Q1 2014, which was up 19% sequentially from Q4 2013.

Figure 2: Types and amount of cyber threats



Source: McAfee Labs Threats Report, June 2014, p. 19ff.

- Messaging threats: Messaging threats are the use of electronic messaging systems to send unsolicited bulk messages (spam). The most common form of spam is via email, but it can also be delivered in other forms such as SMS, blogs, forums etc. As shown in fig. 2, the volume of spam exceeded 7 trillion messages in Q1 2014, which is up from 5.5 trillion in Q4 2013.
- Network threats: A network threat is any threat that leverages a network to gain access to an enterprise's server or storage infrastructure in order to steal data or intellectual property. It can also target the network itself in order to disrupt traffic to/from a website, often referred to as a Distributed Denial of Service (DDoS). Alternatively these DDoS-attacks could also be used as a diversion to conceal other activities, such as an Advanced Persistent Threat (APT).

Traditional vs. next-generation security tools

Traditional security tools such as firewalls, IPS (Intrusion Prevention Systems), Secure Web and Secure Email Gateways as well as anti-virus programs are effective against the traditional array of threats. As the business usage of the internet evolves, the threats continue to develop as well. In previous years, simple website defacements or DDoS-incidents were the most damaging forms of attacks. However, in 2008 traditional security tools began to fail against newer forms such as advanced targeted attacks (also known as Advanced Persistent Threats, APTs). APTs bypass

traditional security tools because they start outside of the network before traditional security tools can detect them. The motivation is usually financial gain, trying to obtain, destroy or modify information or selling stolen information to criminal groups. The major advance in new threats has been the level of tailoring and targeting. Targeted attacks aim to achieve a specific impact against specific enterprises, and have three major goals[7, 8]:

- Information compromise: Stealing, destroying or modifying business-critical information.
- Theft of service: Obtaining use of the business product or service without paying for it.
- Disrupting business operations.

In order to effectively defend against the entire risk continuum, which includes both traditional threats and APTs, the users need to address a broad range of attack vectors with next-generation technologies that operate everywhere the threat can manifest: On the network, on endpoints, on mobile devices and in virtual environments.

A simplified approach to map the vendors

Due to the fact that it is very difficult for investors to get an overview of this dynamic area, we provide a simplified mapping of the product areas where each vendor participates (fig. 3). The purpose is to visualize which vendor has in our opinion the most comprehensive security portfolio capable of defending against all types of cyber threats.

Fig. 3: Vendor mapping (simplified)[9]

Security product		Vendor					
Traditional technologies	SWG/SEG	Symantec	Fortinet	FireEye	Palo Alto Networks		
	FW/IPS	Symantec	Fortinet	FireEye	Palo Alto Networks		
	Network Segmentation	Symantec	Fortinet				
	Endpoints	Symantec	Fortinet	FireEye	Palo Alto Networks		
Next-generation technologies	NAC	Symantec					
	Mobile Devices	Symantec	Fortinet	FireEye	Palo Alto Networks		
	App White-/Blacklisting	Symantec		FireEye			
	SIEM			FireEye			
	NGFW		Fortinet		Palo Alto Networks		
	WAF	Symantec	Fortinet			Imperva	Qualys
	Forensics/Compliance	Symantec		FireEye	Palo Alto Networks		Qualys
	Threat Intelligence	Symantec	Fortinet	FireEye	Palo Alto Networks	Imperva	Qualys
	Sandboxing	Symantec	Fortinet	FireEye	Palo Alto Networks		
	DLP/DAM	Symantec	Fortinet			Imperva	
	DAST						Qualys

Source: Piper Jaffray, Credit Suisse, 19.8.2014.

[7] The term „Advanced Persistent Threat" war originally coined by the US military in reference to a specific group called „APT1". According to Gartner, APTs are defined as follows: 1) Advanced: It gets through the existing defense, 2) Persistent: It will keep trying until it gets in, and once done, it succeeds in remaining hidden from the current level of detection until it attains its objective, 3) Threat: It can cause harm, source: D'Hoinne, Orans (2013): Strategies for Dealing with Advanced Targeted Attacks, Gartner, Nov. 15th 2013, p. 2.

[8] This is not to say that state-sponsored attacks do not occur. The majority of these cases are using techniques that were first seen in financially motivated attacks. As an example Mandiant (2013) published an interesting report about this topic (source: Mandiant (2013): APT1 - Exposing One of China's Cyber Espionage Units, URL: http://intelreport.mandiant.com/, 19.8.2014).

[9] Explanation of the abbreviations: SWG: Secure Web Gateway, SEG: Secure Email Gateway, FW/IPS: Firewall/Intrusion Prevention System, NAC: Network Access Control, Mobile Devices: Mobile Device Management, SIEM: Security Information and Event Management, NGFW: Next Generation Firewall, WAF: Web Application Firewall, DLP: Data Loss Prevention, DAM: Digital Asset Management, DAST: Dynamic Application Security Testing. Due to the fact that the current product environment is very dynamic, ***we do not claim that fig. 3 can be viewed as complete***. Additionally, before evaluating the various vendors, it is imperative to understand the definition of each of the security product categories.

CREDIT SUISSE

To conclude

In the last couple of months we had the opportunity to meet several management teams of small- to large-size companies and asked them for a brief overview of their IT security infrastructure. These meetings confirmed what we had suspected, that most enterprises use a wide range of vendors across the entire spectrum of IT security products. This is not surprising as they want to avoid becoming dependent on a single IT security provider. Additionally, it also seems to us that no vendor might be able to provide a comprehensive "one-stop-shop IT security solution".

Historically, IT security stocks have acted like insurance companies, tending to outperform during recessions and underperform in good economic times. While it is still too early to tell, we think innovation as well as new and stricter regulatory trends could position leading vendors in attractive market positions. In our opinion key long term drivers for IT security companies include:

- IT security threats are always evolving.
- The budgets for IT security solutions are non-discretionary by nature and will continue to grow.
- Finally, we believe the industry is operating in an attractive and structural growth market.

For long-term oriented investors we think this investment theme is very appealing and is still early in its attractive secular growth cycle. We therefore believe investments in this area will increase going forward due to its structural nature. As a consequence, we are shareholders of leading companies in the field of next-generation innovative security solutions.

Service

If you have any questions please do not hesitate to contact me by phone +41 (0)44 344 69 90 or e-mail:
Dr. Patrick Kolb: patrick.kolb@credit-suisse.com