24 September 2010

Edison tech spotlight

The third pillar

In this issue:

- Why IT security is fast becoming the 'third pillar' of computing
- Innovative technological solutions are needed to keep pace with evolving threats
- M&A activity in this segment accelerates – we expect it to continue
- UK investors have options to play this trend – especially in areas of financial IT security

Is IT security potentially the 'killer app'?

Business and society in general is increasingly being shaped by the globalised communications and information infrastructure. However, this dependence brings vulnerability. With vast quantities of sensitive and mission-critical data being transmitted through the ether and being stored remotely, the rise of IT security as a priority for governments, corporations and consumers is only just beginning.

The segment is ripe for consolidation

The IT security space remains highly fragmented and is ripe for consolidation. Intel's acquisition of virus software developer McAfee for $7.8bn in August marks the largest deal in this segment so far this year but the frequency and diversity of deals remains high. We expect this to continue. Dublin-based financial compliance firm **Trintech**'s announcement this week that it has received "approaches from a number of companies" supports this view.

The UK (and LSE) is well represented

The UK is well represented in IT security – most notably in the area of financial IT security. UK-listed companies such as **Norkom** (compliance systems), **Monitise** (mobile payment systems), **GB Group** and **Intercede** (identity verification), **Endace** (lossless network monitoring) and **Sandvine** (network monitoring, traffic shaping) all feature prominently in their respective niches. We feel they will also feature on the radar of some of the larger consolidators too.

Analysts

Dan Ridsdale 020 3077 5729
Katherine Thompson 020 3077 5730
Richard Jeans 020 3077 5700
tech@edisoninvestmentresearch.co.uk

For institutional enquiries please contact:

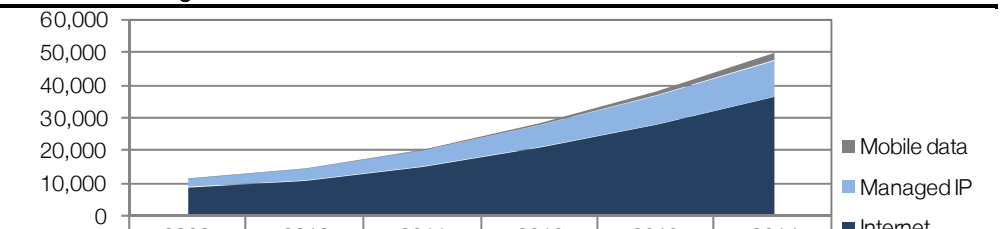
Alex Gunz 020 3077 5746
Gareth Jones 020 3077 5704
institutional@edisoninvestmentresearch.co.uk

Edison's new tech spotlight publication discusses key themes in the sector and is published fortnightly.

A Cyber dependent society

Society is increasingly being shaped by globalised communications and information infrastructure. As a result, vast quantities of sensitive and mission-critical data are being transmitted through the ether and being stored remotely. Global IP traffic volumes are expected to grow nearly fourfold between 2009 and 2014. Meanwhile, corporate and consumer dependence on this data is increasing and the rise of cloud computing, SaaS and smartphone usage will only increase this dependence.

Exhibit 1: Growth in global IP traffic



	2009	2010	2011	2012	2013	2014
Mobile data	66	91	228	538	1,158	2,132
Managed IP	2,606	3,652	4,963	6,771	8,851	11,078
Internet	8,930	10,942	15,205	21,181	28,232	36,709

Source: Cisco

However, this ever-growing cyber-dependence brings vulnerability, and the threats are also on the rise. Cybercriminals are becoming increasingly sophisticated, while the transmission of data at ever faster rates and over wireless networks opens up new vulnerabilities which need to be addressed. Increasingly too, corporations are seeing the need for forensic data monitoring and user authentication within their own networks for both security and compliance reasons.

Upping the ante, government and military leaders have warned that the next world war is likely to be fought at least partly in cyberspace and it seems inevitable that cyber battles raging as we write. We note recent press reports on Stuxnet, a virus that particularly infested high value infrastructure in Iran. The virus has been described as one of the most sophisticated pieces of malware ever detected, so sophisticated in fact that some researchers have claimed it could only have been written by a "nation state".

Consequently, we feel that the rise of IT security as a priority for governments, corporations and consumers is only just beginning.

The 'third pillar'

After the company's recent $7.8bn acquisition of McAfee, Intel's CEO coined the phrase that security has become the 'third pillar' of computing (after energy efficiency and mobility). As shown in Exhibit 1, the McAfee deal remains the sector's largest so far in 2010, but the recent surge in M&A activity indicates that he is clearly not alone in that view. Indeed, since we highlighted IT security as a hotbed of M&A deals in the tech sector *(Edison Tech Spotlight, 27 August)*, the pace of M&A has continued unabated – particularly in the US with IBM and HP both being notable serial acquirers especially in the area of cloud computing and security. Given the strategic importance of

the sector, the fragmentation of the supply landscape and the need for innovative technological solutions to keep pace with evolving threats, we feel that the sector remains ripe for consolidation.

Exhibit 2: List of major IT security M&A deals in 2010

Acquirer	Target	Country	Segment	Amount
IBM	OpenPages	US	Risk and compliance software	undisclosed
HP	ArcSight	US	log aggregator of network activity	$1.5bn
IBM	BigFix	US	Network Monitoring	c $400m
HP	Fortify	US	Compliance, business monitoring	N/A
Intel	McAfee	US	virus software	$7.7bn
Private Equity	Sophos	UK	Virus software	$830
Symantec	Verisign	US	Payments, Encryption	$1.28bn
Verisign	PGP Corp	US	Encryption	$370m
Symantec	GuardianEdge	US	Encryption	N/A
Rubicon Project	SiteScout	US	Web ad security	N/A
Private Equity	SonicWall	US	Firewall hardware	N/A
CA Technologies	Arcot Systems	US	'Cloud authentication'	N/A
Private Equity	Avast	US	virus software	N/A
Verifone	Semtek	US	Encryption, payment security	N/A
Jack Henry & Associates	iPay	US	Payment processing	$330m

Source: Edison Investment Research

Key segments

IT security is an incredibly diverse market ranging from traditional virus detection software through to payment authentication and forensic network monitoring. We outline five key areas:

1. Cyber security
2. Network monitoring
3. Cloud computing
4. Mobile security
5. Financial services

Cyber security

Cyber security is probably the most well known area of IT security, such is the prevalence and notoriety of viruses. McAfee estimates this market to be worth $10bn+ and growing at 10% annually. Viruses (or malware), are rogue software programs that can ‘infect’ computers and, at their most basic, can be just a nuisance slowing down computers with unwanted spam messages or adverts. More seriously, others can destroy data or remain hidden within computer systems and can monitor user activity for passwords (so-called ‘phishing’) and other potentially lucrative personal information. For context, according to Intel, there were 10 million new ‘malware’ variants added to the McAfee database alone this year.

Symantec, McAfee and Trend Micro are the largest vendors of virus software – all three are based in the US. In the UK, the largest developer of virus software, privately-held Sophos sold a majority stake to private-equity company APAX Partners, which valued the business at $830m (or 2.5x 2009/10 sales). The corporate anti-virus market is about two-thirds of the market with the remaining one-third derived from sales to consumers. The market grew about 8% in 2009 and market research firms expect an acceleration in 2010. The sector seems relatively defensive and we note recent comments from the UK government that IT cyber security investment is not under threat from the Strategic Defence and Security Review (SDSR) due in coming months.

Intel & McAfee: Software versus hardware virus detection

McAfee's $7.8bn acquisition by Intel in August has set the cat among the pigeons as the industry tries to understand why the world's largest semiconductor manufacturer would buy an application software vendor – seemingly two very distinct businesses. Interestingly, Intel and McAfee had been working together for almost two years prior to the deal (though we have yet to see the fruits of this relationship) and Intel has been increasingly marketing security features in its chipsets. The long-term sales synergies between the businesses lie in the potential to integrate the virus detection algorithms into chipsets, thereby allowing the anti-virus to cope with faster network speeds.

This is a long-term plan – the big vision of incorporating McAfee's security IP onto silicon is only likely to be implemented by middle of the decade (ie 2015). In the short term, McAfee will operate independently within Intel's Software & Services division where it will continue to make 90% of its revenues from traditional virus software.

Nevertheless, the deal does illustrate the increasing role that hardware is likely to play in enabling security systems to keep up with the accelerating pace of computing and networking speeds. In particular as 10Gb networks become mainstream, the need for faster, hardware-based cyber security systems is likely to increase rapidly. Intel is not alone in bridging the hardware/software divide – in May, Oracle acquired Secerno, a supplier of database firewalls implemented in hardware. We note that Russian-based Kaspersky Lab, the fourth largest anti-virus software vendor has been granted a patent (Patent No. 7,657,941) for a hardware anti-virus system in February this year. The case within monitoring is just as strong, and we highlight Endace, the UK-listed (New Zealand-based) supplier of hardware based network monitoring equipment as a company which should benefit from this trend.

Network monitoring

This leads us neatly into network monitoring, a high growth market adjacent to security. Through capturing and analysing network traffic, monitoring tools are becoming an increasingly key part of the security strategies of homeland security agencies and large corporates alike. However, uses span far beyond security – it is increasingly being used by banks to enhance their compliance efforts as well as to detect threats. As a business tool, monitoring is being used by high frequency traders to gain milliseconds of time advantage in exchange trading. Monitoring plays a crucial role in enabling operators to understand usage patterns and optimise their networks. It is also key to enabling traffic shaping, the process whereby network traffic is optimised though analysing the packets flowing through it and delaying some to allow priority data to flow more easily.

The monitoring sector has also significant levels of activity of late. HP reportedly outbid at least two rivals to clinch its $1.5bn acquisition of AcrSight – an aggregator of network logging activity – last week. On a smaller scale, Narus (an OEM customer of Endace) was acquired by Boeing Defense in July, while earlier this month Arbor Networks was bought by Tektronix, part of Danaher. Preceding all this, Detica's acquisition by BAE highlighted how expertise in this field is being coveted by industry majors.

Within the UK-listed universe, we again highlight Endace, which has a hardware-based solution, enabling 100% packet capture on high speed (10Gb/s+) networks as a company which could be approaching a sweet spot. Also on AIM (but based in Canada), Sandvine is a play on both network

monitoring and shaping. We also note Digital Barriers, the homeland security roll-up vehicle, although we suspect recent M&A activity could be raising valuation expectations of potential targets.

SaaS/cloud computing

Cloud computing (or 'Software as a Service' – SaaS) presents a clear security challenge. Unlike traditional (Local Area Network) architectures, with SaaS the storage and manipulation of data is not only physically separate from the end-user's location but crucially is often located outside the company itself at a third-party vendors' location. Furthermore, with true SaaS, data from multiple customers are shared on vendor storage hardware, thereby putting a burden on the vendors to protect the data and ensure these proprietary data sets are isolated from each other. The necessity to transmit those files from storage to the user creates a vulnerability both to cyber criminals and and poor network performance. To illustrate, in 2007 leading SaaS CRM software provider Salesforce.com acknowledged that a spate of targeted email virus and phishing attacks against its customers resulted from one of its own employees falling for a phishing scam and turning over the keys to the company's customer database. While no major security breaches have appeared in the headlines since then, security concerns remain one of the main barriers to SaaS adoption and, as a result, this area will remain a focus of investment.

Cloud/SaaS M&A activity

For this reason the worlds of storage and security are converging rapidly as clearly shown when Symantec acquired Veritas (a storage software company) some years ago in a mega deal worth over $13bn. This deal made Symantec (a security company) the largest supplier of backup, recovery and archiving software. Symantec was clearly ahead of the trend. In a similar but smaller move earlier this year, US-based Trend Micro acquired UK-based Humyo, which specialised in online file storage and backup.

Several other high profile acquisitions have taken place in this area – for example Google's acquisition of Postini and Cisco's acquisition last year of Scansafe are clearly intended to placate end users who are concerned about the integrity and safety of data (whether emails or other data traffic) transmission. Radware with its Application Delivery Controller has recently been much touted as a potential takeover target too. In a much publicised attack in January 2010 (later dubbed 'Operation Aurora' by McAfee), Google was one of up to 34 companies which were subject to a cyber attack originated in China. McAfee attributed the vulnerability of the attack to a flaw in Microsoft's Internet Explorer.

Mobile security

In many ways, mobile IT security faces similar challenges to cloud security as, in each case, the data storage and the user are physically separate. Mobile adds another layer of complexity however – the data is transmitted wirelessly, which on the face of it could make transmission even more vulnerable to interception or loss. Furthermore, a key issue with mobile devices is that they get carried everywhere by users and can be physically intercepted, thereby allowing access to sensitive emails, contact information or proprietary corporate information.

In addition to the rationale outline earlier, Intel's bid for McAfee was also motivated by the need to bolster its security offerings in mobile chipsets, stating on the call that there is an "explosive growth opportunity" for security in mobile. Nokia's E-Series division (of business phones) already cite a "wide range of in-built security features such as device encryption, device locking and remote wiping", while bundling anti-virus software from most of the major vendors such as F-Secure, Kaspersky, RSA, Symantec and Trend Micro.

Another adjacent area of growth is in the field of mobile commerce and payments, the rise of which will unquestionably bring mobile security further to the fore. As no one platform has yet gained critical mass (outside of Japan), more aggressive moves by industry power brokers look afoot. Reports suggest that AT&T, Verizon and T-Mobile USA are in talks to conduct pilots of wireless payment chips embedded in phones in four US cities, while Apple has recently recruited Benjamin Vigier, an NFC veteran as a product manager of mobile commerce.

Within the UK, Monitise looks to be in a strategically strong position. It develops and manages mobile banking and payment transactions for banks, generating its revenues based on a transaction commission. In a domain where critical mass and strong partners are a prerequisite, Monitise notably has Visa as a strategic development partner and investor. As an aside, Monitise is one of very few UK-listed companies that we can identify as clear beneficiaries of the rise of mobile applications.

In a related area, Innovision Research & Technology, an NFC IP provider, was bought by Broadcom for £32m (an 84% premium) in June.

Financial services security

All businesses today face a trade-off between liberating the flow of data while ensuring data protection and conforming to regulatory standards. Nowhere is this balance more finely met than in financial services IT security. Given the obvious sensitivity and value of the data being exchanged, the financial services industry often operates at the cutting edge of technology development. It is also one of the most diverse segments of IT security as it encapsulates areas from financial crime and compliance through to ID fraud, encryption and payment systems – the most common requirement here being user authentication. Many of the major banking corporations run a complex web of proprietary and off-the-shelf IT security systems. Employee access to personal/proprietary data is on the increase. For example, call centre employees often have access to a wide range of customer personal info.

Unlike the two earlier market segments, the UK is well represented here.

- Norkom sells scalable software platforms addressing most aspects of compliance and financial crime, including enterprise investigation management, anti-money laundering, and customer due diligence (CDD) etc, while its fraud management solutions include online fraud and debit card fraud. Regulatory regimes are clearly a factor here (although, interestingly, were partly attributed as a cause of Norkom's profit warning last week). We do note that the Dodd-Frank Financial Reform Act in the US will likely mean increased IT compliance and data monitoring.

- GB Group provides identity management software and services for a range of uses such as combating ID fraud, money laundering and even under-age gambling. A peripheral use of the technology is that it allows corporations to analyse their customer base for sales-targeting etc.
- Intercede has developed a range of smartcard and associated platforms to manage ID and access rights. In effect, this technology is not about data security but about physical security for buildings in the corporate, government and public service space.
- Trintech is NASDAQ-listed and Dublin based. It is a provider of integrated financial governance, risk management, and compliance (GRC) software solutions for commercial, financial, and healthcare markets.

Conclusion

IT security has rapidly become an extremely important application for most industries across the globe. Data has become distant, global, mobile and pervasive – so protecting the ownership rights of the data is becoming a major industry in its own right.

Some trends are clear:

- Ongoing network speed increases are necessitating shifts to hardware architectures.
- Mobile opens up a completely new world of threats and business opportunities.
- Monitoring by both government agencies and corporates is on the up, driven by security threats, compliance obligations and commercial motivations.
- User authentication (not just for financial transactions) will become pervasive.
- We expect this segment to remain a hive of (M&A) activity for the foreseeable future. The strategic importance of the sector and the need for innovative technological solutions to keep pace with evolving threats mean that strategic premiums will continue to be paid.