pwc.com

Cyber Security M&A

Decoding deals in the global Cyber Security industry

Cyber Security M&A review

November 2011

pwc

Contents

Introduction

Welcome to PwC's[1] Cyber Security M&A review. Here we provide a breakdown and analysis of deal activity in the Cyber Security market and examine some of the underlying forces and trends that are driving this rapidly evolving industry.

We review global deal activity for the last three years where total investment exceeded $22 billion.

The market is undergoing significant change in many segments and is attracting investment from many different types of companies including IT companies, defence contractors, technology businesses, professional services firms, telecommunications firms and financial investors. This convergence is driving innovation in the market and, coupled with an increasing awareness of cyber security risks across all organisations, presents significant opportunities for businesses that can address current and emerging issues. This will continue to drive M&A activity by both strategic and financial investors.

Barry Jaber
Director
Security Industry Leader

[1] "PwC" refers to PricewaterhouseCoopers LLP (a limited liability partnership in the United Kingdom), which is a member firm of PricewaterhouseCoopers International Limited, each member firm of which is a separate legal entity.

Cyber Security market overview

The term Cyber Security is relatively new and is commonly thought to be a component of the more familiar Information Security (a slightly broader term that includes non-cyber or offline information) that has been in common use for several decades. Definitions of information security vary but commonly centre on protecting the confidentiality, integrity and availability of information, regardless of the form of the information.

Global Cyber Security spending 2011:

$60 billion

Defining the market

In our view, the definition of Cyber Security needs to be broadened to reflect two distinct characteristics. The first is that Cyber Security includes the development of products and services for offensive applications. These are largely (if not exclusively) designed for government and military use, and are often also referred to as cyber weapons or cyber defence. The second is that Cyber Security not only encompasses the IT domain (primarily Internet Protocol or just 'Internet' connected devices), but also telecoms equipment and industrial equipment.

The Cyber Security market (or industry) therefore is comprised of companies that provide products and/or services for defensive and offensive applications across the IT, telecoms and industrial domains. And that is the definition of the sector that we have used in compiling this report.

Market size and projected growth

Global Cyber Security spending was approximately $60 billion in 2011 and is expected to grow at close to 10% every year over the next 3-5 years. The US accounts for over half of the total. The next largest market is Japan, followed by the UK.

In most countries, the private sector accounts for the majority of Cyber Security spending. The notable exception is the US where government spending is almost equal to that of the private sector.

The main drivers of the Cyber Security market are:

- Increasing cyber threats, both from new actors and new threat vectors (the paths that attacks can take).
- Greater vulnerabilities due to the more pervasive use of technology, particularly mobile devices and Cloud computing.
- Increasing awareness by organisations and consumers of the threats and potential threats.
- Changes in technology driving product and service innovation of security solutions.
- Increasing regulation particularly those enforcing the requirement to secure personal data.
- Changes in outsourcing; some organisations are increasingly relying on partners for security, whilst others are growing internal security spending to maintain greater levels of control.

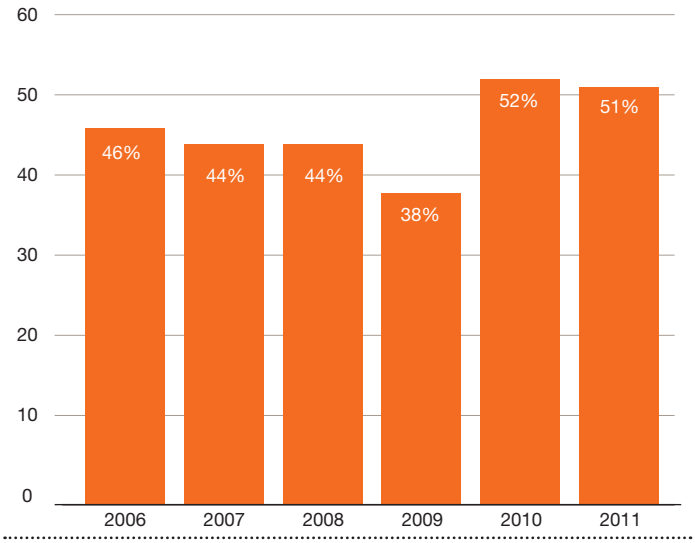
Growing threats and increasing awareness are key

Security breaches and malware attacks have been regular front-page news over the past few years. There have been a number of high profile Cyber Security incidents this year alone, from computer hacking groups, such as LulzSec's attack on the Playstation network to foreign intelligence services, including an attack in March where 24,000 files were stolen from a Pentagon defence contractor. More recently, quasi-political activist groups such as Anonymous have targeted a range of high-profile businesses and organisations. The apparent ease with which some of these activities have taken place has very publicly highlighted the importance of Cyber Security. The costs arising from such breaches have also focused attention on security. Sony reported that the hack of its PlayStation network and the consequent loss of its network availability will cost the business $171 million.

We have also seen the use of viruses developed to attack specific types of equipment. The Stuxnet virus, for example, aimed at industrial control systems, was largely attributed with the problems that hit the Iranian nuclear programme, impacting its uranium enrichment programme. On a more personal – but no less sensational – level, the breach of individuals' mobile phone voicemail accounts by reporters from a News International publication, The News of the World, has also brought home the vulnerability of telecoms and other equipment to unauthorised access.

Against this backdrop of growing threats, deal activity continues to increase.

A growing market: Percentage of respondents who believe that information security spending will increase in the next 12 months



Source: PwC 2012 Global State of Information Security Survey

Deal activity

Deal volume and value

	2008	2009	2010	2011H1
Number of deals	77	88	106	37
Total deal value ($millions)	4,155	1,630	5,882	10,175

	2008				2009				2010				2011H1	
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2
Number of deals	21	15	17	24	19	22	17	30	23	13	37	33	24	13
Total deal value ($millions)	149	441	565	3,000	299	137	326	868	661	654	2,179	2,388	9,543	633

Deal value increased sixfold in the last 12 months

Total investment since 2008 has exceeded $22 billion globally

Cumulative spending on Cyber Security deals since 2008 totals nearly $22 billion, an average of over $6 billion in each year. Acquirers have been from a range of sectors including Technology, IT services, Aerospace & Defence as well as financial investors.

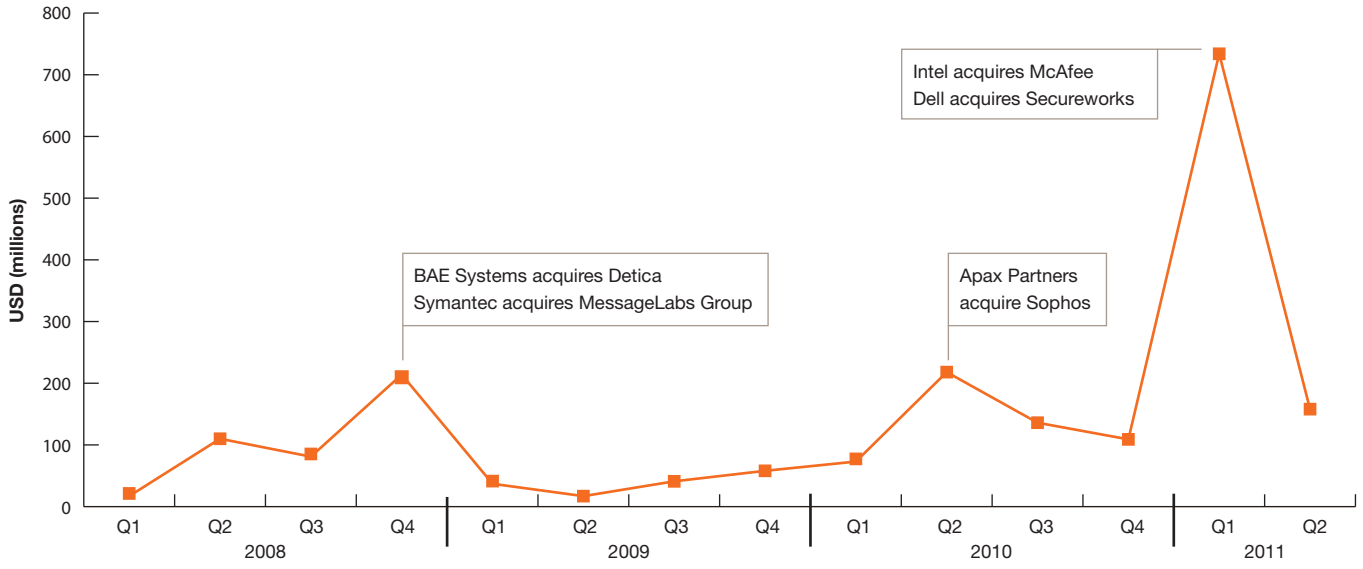
2010 saw an increase in both total deal volume and value of nearly 40% versus 2008, following a marked slowdown in total deal value in 2009. Total deal value increased by over 70% in the first half of 2011 versus full year 2010 to $10.2 billion, driven primarily by Intel's $7.8 billion acquisition of McAfee which was completed in February 2011. Total deal volume in the first half 2011 is slightly ahead of the same period in 2010.

There have been a number of other mega deals (with values of $500 million or above) since 2009, including Dell's acquisition of Secureworks in 2011 and Apax Partners' acquisition of Sophos in 2010.

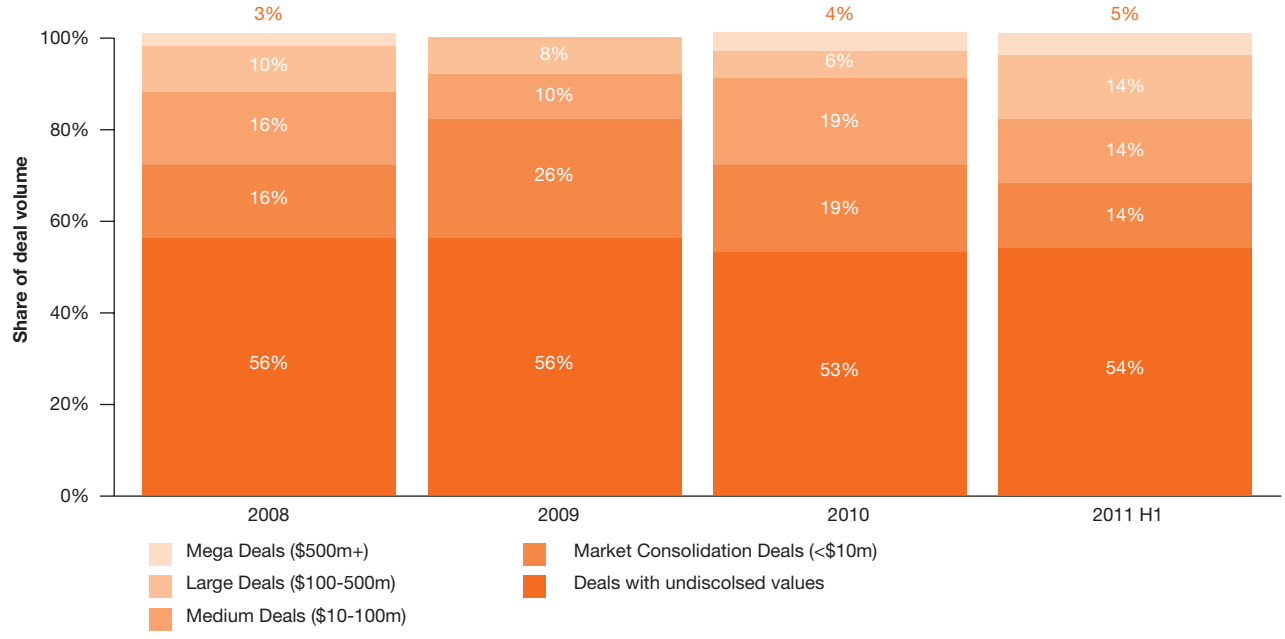
There has been a return to larger deal sizes since 2009 which saw a sharp decline in total deal value. However, the total number of deals in this period increased as the majority of the activity focused on smaller investments (deal valued at less than $10m).

Overall, deal value, deal volume and average deal size have all been trending up over the reviewed period.

Average deal size 2008-2011H1



Deal activity by number and range of deal value 2008-2011H1



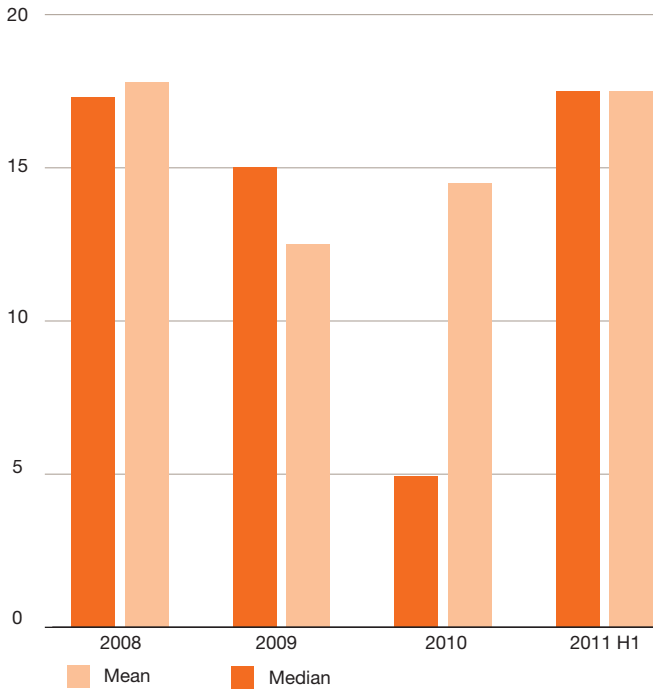
Valuation trends

Deal valuation multiples

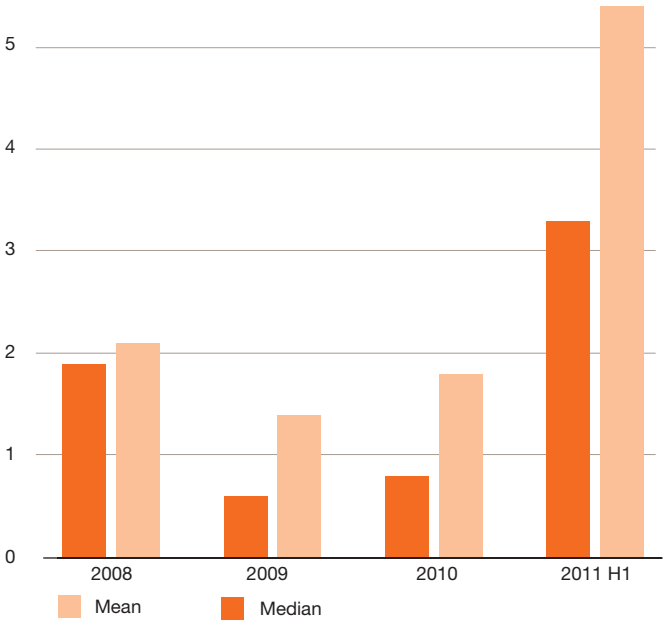
The valuation multiples in cyber security deals are relatively high, with both mean and median deal value-to-EBITDA ratios at around 15 times during the period from 2008 through to 2011H1. Deal value-to-revenue ratios were around 2-3 times over the same period. While these figures have been adjusted to omit some inflated values, they are clear indicators that acquirers are willing to pay a premium to buy Cyber Security companies.

Deal value/EBITDA ratio recovered in 2011 to over 15x

Deal valuation trends, 2008-2011H1, Deal value/EBITDA ratio



Deal valuation trends, 2008-2011H1, Deal value/Revenue ratio



Listed Cyber Security companies valuations and share price trends

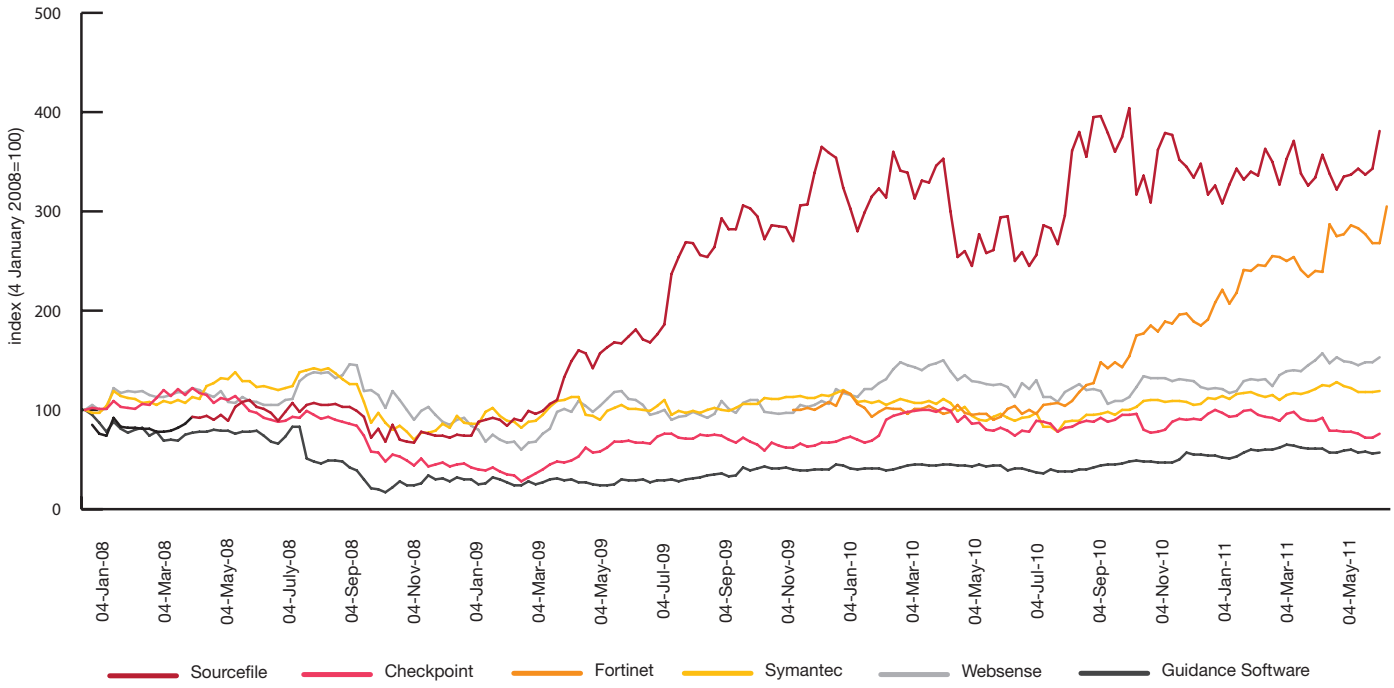
Price-Earnings multiples for listed pure-play security businesses, all US-based, range from 14-51x.

The market in cyber security stocks divides between pure plays and software/hardware providers that have a strong security offering as part of their products and services. Prices for pure play stocks are volatile, with large swings often accompanying news items relating to specific breaches. As the graph below shows, prices in some stocks have significantly outpaced market averages. For example, Sourcefire, one of the leading providers of security software to large businesses and governments, has seen a four-fold increase in its share price since May 2009. Many stocks trade at very high earnings multiples and have ratios of ten times or more.

	Operating income multiple	Profit before tax multiple	Revenue multiple
Checkpoint	20.6	19.5	10.0
Sourcefire	51.5	36.1	5.5
Fortinet	51.1	51.1	8.7
Symantec	14.1	16.7	2.0
Websense	25.1	29.4	2.3

Note: Share price on 24 August 2011; financial data for last reported full financial year

Share price (indexed) of pure play Cyber Security companies, January 2008-August 2011



Note: Fortinet indexed at 100 in November 2009 when first listed.

Deal makers

Overview

Strategic investors accounted for c.70-80% of deal volume from 2008-2011 H1 and include companies from a range of sectors including Technology, IT services and Aerospace & Defence.

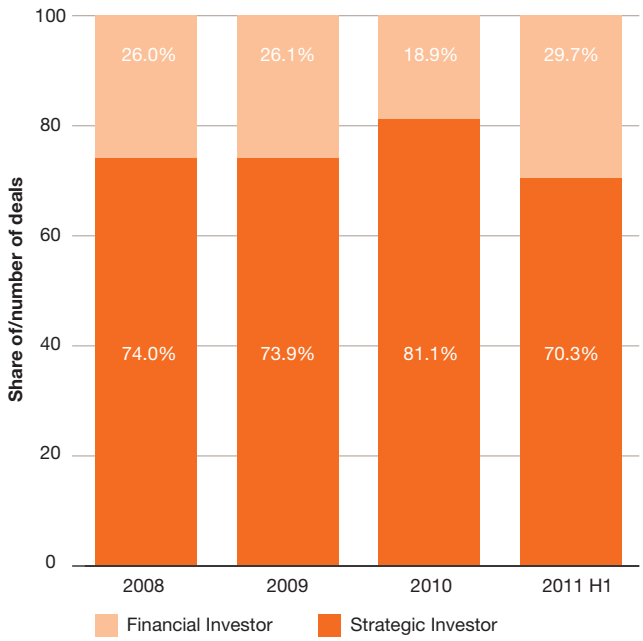
Top 10 deals

A number of features characterise the top ten deals in the period we have looked at between 2008-2011 H1. Technology and IT software/services businesses (eg Intel, Symantec Dell and Hewlett Packard) have dominated. The only defence contractors to feature in the top ten are BAE Systems and Raytheon. All of the top ten deals featured only UK and US based targets and acquirers.

The two biggest deals in H1 2011 were Intel's acquisition of McAfee for $7.8 billion and Dell's $612 million acquisition of Secureworks. This contrasts with 2010 which saw Hewlett Packard purchase ArcSight for $1.6 billion and Symantec's $1.3 billion acquisition of VeriSign. Overall the top ten deals in 2011 so far have been worth $10.1 billion up from $5.0 billion in 2010 and $1.5 billion in 2009 and in each year the top ten deals have accounted for more than 85% of total deal value in that year.

The only large-scale financial investors to date have been Apax Partners with their acquisition of Sophos in 2010 for $580 million and Thoma Bravo's acquisition of SonicWall also in 2010 for $633 million.

Deal activity by investor group
Measured by total number of deals 2008-2011H1



All of the top ten deals featured only UK and US based targets and acquirers

Top10 Cyber Security deals, 2008-2011H1

Date effective	Target name	Target nation	Acquirer name	Acquirer nation	Value of transaction (USDm)
02/28/2011	McAfee Inc	United States	Intel Corp	United States	7,828
10/22/2010	ArcSight Inc	United States	Hewlett-Packard Co	United States	1,569
08/09/2010	VeriSign Inc-Indentity Business	United States	Symantec Corp	United States	1,280
10/23/2008	Detica Group PLC	United Kingdom	BAE Systems (Holdings) Ltd	United Kingdom	1,021
11/14/2008	MessageLabs Group Ltd	United Kingdom	Symantec Corp	United States	695
07/20/2010	SonicWALL Inc	United States	Thoma Bravo Fund	United States	633
02/08/2011	SecureWorks Inc	United States	Dell Inc	United States	612
03/05/2010	Sophos PLC	United Kingdom	Apax Partners LLP	United Kingdom	580
31/01/2011	Applied Signal Technology, Inc.	United States	Raytheon Co	United States	490
11/18/2008	Secure Computing Corp	United States	McAfee Inc	United States	476

Financial investors

Over 2008-2011 H1, around 25% of deal volume was attributable to financial investors, accounting for 15% of total deal value. In terms of share of deal value, financial investors have started 2011 at a relatively slow rate compared to 2009 and 2010 where they contributed 30% and 25% of total deal value respectively.

Top10 Cyber Security deals with financial acquirers, 2008-2011H1

Date effective	Target name	Target nation	Acquirer name	Acquirer nation	Value of transaction (USDm)
07/20/2010	SonicWALL Inc	United States	Thoma Bravo Fund	United States	633.64
05/03/2010	Sophos PLC	United Kingdom	Apax Partners LLP	United Kingdom	580.00
10/05/2009	AVG Technologies CZ sro	Czech Republic	TA Associates Inc	United States	200.00
09/05/2008	Tumbleweed Communications Corp	United States	Tornado Acquisition Corp	United States	141.46
03/24/2009	Aladdin Knowledge Systems Ltd	Israel	Investor Group	United States	137.12
01/25/2010	ExteNet Systems Inc	United States	Investor Group	United States	128.40
07/28/2009	Entrust Inc	United States	Thoma Bravo LLC	United States	123.87

Deal rationale

The rationale for acquisitions of Cyber Security companies differs by the type of acquirer:

- **Defence contractors** are seeking to diversify away from core defence markets as i) the near term outlook for defence spending in Western Europe is negative; ii) there is a structural trend in government spending away from defence and towards security, and iii) the Cyber Security market is expected to experience strong growth. Defence contractors have targeted acquisitions that provide access to new customers (primarily government agencies e.g. CIA, FBI, GCHQ, MI5/6), new capabilities and access to scarce security-cleared personnel.
- **IT companies** see Cyber Security as a necessary capability to have in-house in order to provide customers with end-to-end solutions. As threats and incidents proliferate, Cyber Security is increasingly being seen as a source of differentiation for their products and services.
- **Technology companies** have been broadening their product portfolios and driving security features into existing products.
- **Private equity investors** are attracted to the high growth potential available from the Cyber Security sector and, as deals continue to flow, the clear path to future exit opportunities. Venture capitalists have been active and are making smaller investments, particularly in the US.

Aerospace & Defence companies

BAE Systems entered the market by acquiring Detica plc in 2008 for c.$1 billion. BAE Systems has since acquired part of L-1 Identity Solutions in a three-way deal with Safran for $297m and two Scandinavian businesses, ETI and Norkom, for $210 million and $290 million respectively.

Raytheon has been acquiring in the last few years with the $211 million acquisition of Oakley Networks in 2007 and of SI Government solutions and Telemus Solutions in 2008. Further acquisitions included the $350 million purchase of BBN technologies in 2009 and the $490 million purchase of Applied Signal Technologies in 2011.

Outside the top ten, Mantech has made a number of sub-$100 million acquisitions and QinetiQ has been active, completing a number of acquisitions including the $40m acquisition of Cyveillance in 2009.

Technology companies

The major technology businesses accounted for six of the top ten deals over the review period. Intel acquired McAfee for $7.8 billion in 2011 which was the largest deal in the sector during our review period. Symantec acquired VeriSign in 2010 for $1.28 billion and MessageLabs in 2008 for $695 million. Symantec also made a number of smaller acquisitions

including GuardianEdge Technologies, Mi5 Networks, SoftScan and PC Tools. Dell bought SecureWorks in 2011 for over $600 million, HP acquired ArcSight in 2010 for nearly $1.6 billion and McAfee acquired Secure Computing in 2008.

Outside the top ten, IBM has made a number of smaller acquistions including BigFix in 2010, Guardium and Ounce Labs in 2009.

BAE Systems acquires L-1 Intelligence Services Group

BAE Systems acquisition of US company L-1 Identity Solutions' consulting business in September 2010 for a total consideration of $297 million provides a clear example of defence businesses' strategies to deepen their capabilities in offering cyber security advice and services to government clients. BAE Systems acquired three divisions from L-1 that together made up its Intelligence Services Group. In a release, the president of BAE Systems Intelligence and Security sector described the deal as "all about building our capabilities to better meet the dynamic and changing and security needs of our US government customers".

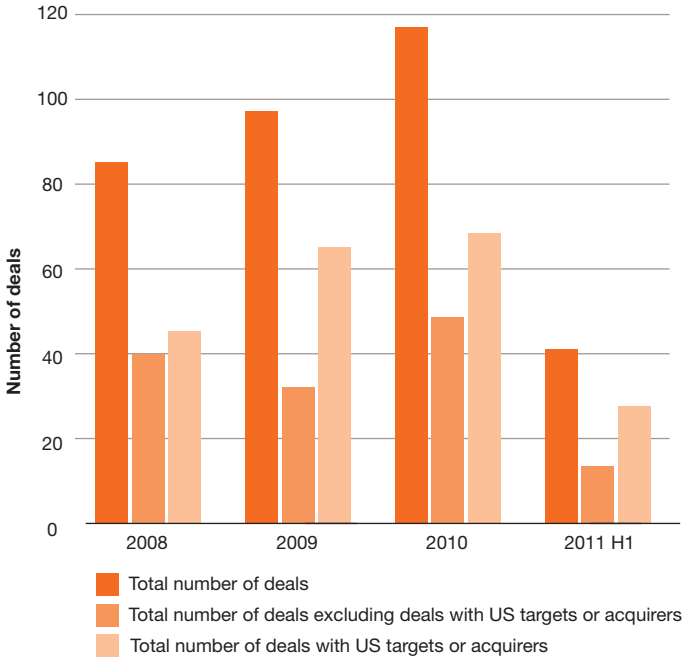
Intel acquires McAfee

The largest deal in the sector to date, Intel's acquisition of McAfee for $7.8 billion, highlights the importance of security for large established technology businesses. However, the market remains divided in its views about the rationale behind Intel's decision to buy and the extent to which the value of the deal will generate the right level of returns. While some commentators have attributed the deal to Intel's long-term plan to embed security in its chipsets, others have questioned the feasibility of this in the medium term. Other views include Intel's desire to move further into the high-growth mobile market, where McAfee has a range of security products, and others believe the acquisition will allow Intel to have specific software written for its chips to provide additional security.

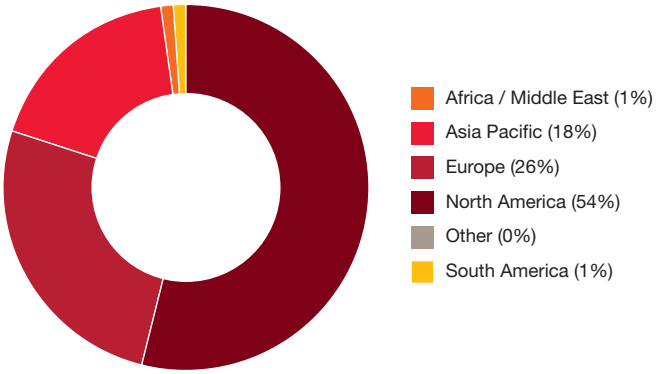
US is key

As expected, when looked at in terms of value, the majority of deals (over 50%) involve acquirers or targets that are based in North America. However, the spread is more global when it comes to the volume of deals. There are two reasons for the focus of value in North America. First, the US has a very strong technology industry, and secondly, the US defence and intelligence budgets are significantly larger than in any other country. By comparison, Europe accounted for approximately a quarter of deal value and a third of deal volume over the same period.

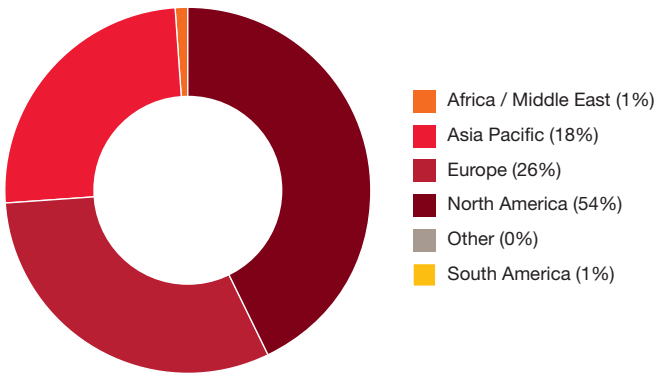
Deal activity 2008-2011H1
Measured by total number of deals



Regional distribution of deals by acquirer region 2008-2011H1
Measured by number of deals with disclosed values



Regional distribution of deals by acquirer region 2008-2011H1
Measured by number of deals



Future deal prospects

There are a number of key trends that are likely to drive Cyber Security deals in the future. As the use of the internet becomes increasingly mobile (with smart phones and tablets already accounting for a high proportion of internet activity), the perceived vulnerability of those technologies will add to the demand for higher levels of security. The adoption of Cloud computing for personal, corporate and government use will also drive the need for greater protection. And both of these come against a backdrop of heightened awareness of hacks, malware and deliberate attacks on institutions and companies by semi-organized groups such as the Anonymous group of hackers.

Defence contractors increasingly perceive the need to expand their offerings to governments, both to provide additional security services and in the development of a wide range of cyber weaponry that will be used for both offensive and defensive purposes against others' networks and technology.

As consumers and organisations become more aware of the wide and growing array of threats that are ranged against their data and services, they will demand more from the companies that they select for hardware and software. Existing providers are likely to seek acquisitions that can give them rapid access to differentiating their offerings with enhanced levels of security.

The graphic below shows some of the main long term drivers shaping information technology and its uses. These are key reasons for the increasing interest in Cyber Security and the development of an active and growing M&A market. As the world becomes ever more connected and appreciative of the many benefits that unprecedented information sharing and communications creates, there is also a growing awareness of how vulnerable such extensive and complex networks can be. Vast amounts of data are available more readily to more people than ever before, but there is an equal recognition that managing and securing the data explosion is an increasingly difficult. The divide between work and home is blurring, with constantly connected mobile users now working in ways that create challenges for corporate IT in securing their systems without damaging productivity.

Added to these broad trends are the specific impacts of e-finance with transactions increasingly taking place online, tough regulatory standards for data protection and privacy and the development of new 'internets' large private networks and walled garden models for media and other forms of distribution. Overall, then, it is not hard to see why Cyber Security is seen an as a major growth area and a market that many businesses are seeking to enter.

Long term drivers shaping the cyber security market

1	Infrastructure revolution	• Increase in penetration of high speed broadband and wireless networks • Centralisation of computing resources and widespread adoption of cloud computing • Proliferation of IP (internet protocol) connected devices and growth in functionality • Improved global ICT (Information and Communications Technology) infrastructure enabling greater outsourcing • Device convergence and increasing modularisation of software components • Blurring work/personal life divide and 'Bring Your Own' approach to enterprise IT • Evolution in user interfaces and emergence of potentially disruptive technologies
2	Data explosion	• Greater sharing of sensitive data between organisations and individuals • A significant increase in visual data • More people connected globally • Greater automated traffic from devices • A multiplication of devices and applications generating traffic • A greater need for the classification of data
3	An always-on, always-connected world	• Greater connectivity between people driven by social networking and other platforms • Increasingly seamless connectivity between devices • Increasing information connectivity and data mining • Increased Critical National Infrastructure and public services connectivity
4	Future finance	• Rising levels of electronic and mobile commerce and banking • Development of new banking models • Growth in new payment models • Emergence of digital cash
5	Tougher Regulation and Standards	• Increasing regulation relating to privacy • Increasing standards on Information Security • Globalisation and net neutrality as opposing forces to regulation and standardisation
6	Multiple Internets	• Greater censorship • Political motivations driving new state/regional internets • New and more secure internets • Closed social networks • Growth in paid content
7	New Identity and Trust Models	• The effectiveness of current identity concepts continues to decline • Identity becomes increasingly important in the move from perimeter to information based security • New models of trust develop for people, infrastructure, including devices, and data

Source: PwC / Technology Safety Board Information Security 2020 report

Case study
Entering the Cyber Security market

PwC recently helped a client develop an entry strategy for the Cyber Security market.

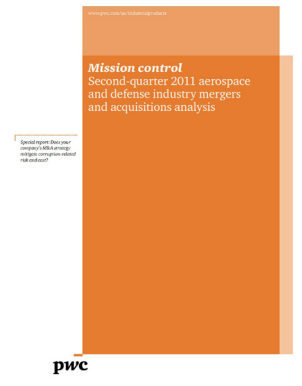
We started our work by reframing the question and breaking it down into a number of key issues:

- What is the most useful way to define and segment the Cyber Security market?
- Which segments are the most attractive?
- What choices need to be made to ensure the right strategic focus?
- What is the right approach to enter these markets successfully (e.g. organic growth, partnership, JV or acquisition)?
- What changes does the organisation need to make to enable this?

Our analysis provided our client with an assessment of the attractiveness of various areas of the Cyber Security market, based on external research and interviews with buyers of Cyber Security solutions. We also compared various market entry options and formulated a shortlist of clear approaches to entering the identified segments.

This provided our client with a robust and fact-based analysis that enabled them to formulate an entry strategy that was both deliverable and provided a platform for future growth.

Other relevant thought leadership

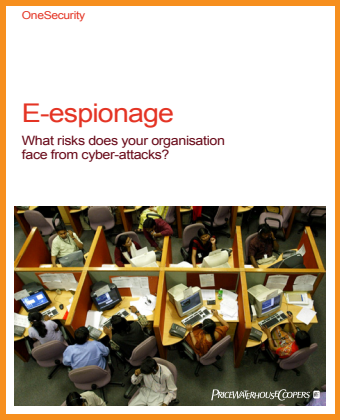


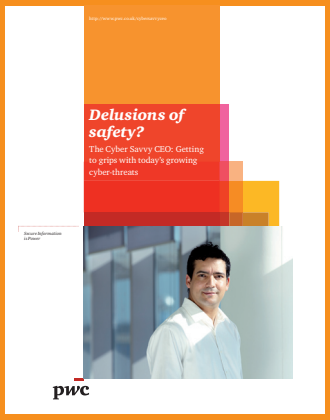
Methodology

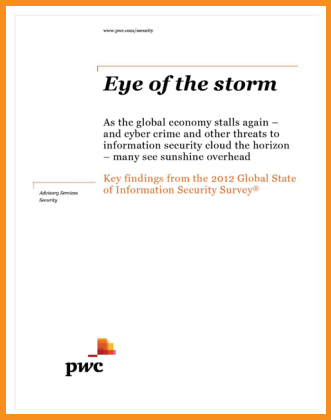
Cyber Security M&A is an analysis of mergers and acquisitions in the Cyber Security industry. Information was sourced from Thomson Financial and includes deals where the target is defined as a cyber security business definition in this report.

This analysis includes all individual mergers and acquisitions for disclosed or undisclosed values, leveraged buyouts, privatizations, minority stake purchases, and acquisitions of remaining interest announced between January 1, 2008 and June 30, 2011, with a deal status of completed. The term deals, when referenced herein, is used interchangeably with transactions.

Regional categories used in this report approximate United Nations (UN) Regional Groups as determined by the UN Statistics Division, with the exception of the North America region (includes North America and Latin and Caribbean UN groups), the Asia and Oceania region (includes Asia and Oceania UN groups), and Europe (divided into United Kingdom, plus Eurozone and Europe ex-UK and Eurozone regions). The Eurozone includes Austria, Belgium, Cyprus, Finland, France, Germany, Greece, Ireland, Italy, Luxembourg, Malta, Netherlands, Portugal, Slovenia, and Spain. Oceania includes Australia, New Zealand, Melanesia, Micronesia, and Polynesia. Overseas territories were included in the region of the parent country.







Contacts

Barry Jaber
Director, Security Industry Leader
barry.n.jaber@uk.pwc.com
+44 (0)20 721 31567

Neil Hampson
Partner, UK and Global Aerospace & Defence Leader
neil.r.hampson@uk.pwc.com
+44 (0)20 7804 9405

Andrew McCrosson
Partner, Transaction Services
andrew.mccrosson@uk.pwc.com
+44 (0)20 7213 5334

Michelle Ritchie
Director, Transaction Services
m.ritchie@uk.pwc.com
+44 (0)20 7212 2502

Rob Morgan
Director, Corporate Finance
rob.morgan@uk.pwc.com
+44 (0)20 7212 3670

Philip Shepherd
Partner, TMT
philip.a.shepherd@uk.pwc.com
+44 (0)20 7804 9366

William Beer
Director, OneSecurity
william.m.beer@uk.pwc.com
+44 (0)20 7212 7337

Scott Thompson
US Aerospace and Defence Leader
scott.thompson@us.pwc.com
+1 703 918 1976

Bob Long
US Aerospace and Defence Transaction Services Leader
bob.long@us.pwc.com
+1 703 918 3025

pwc.com

HB-2011-09-14-1705-CG_Cyber Security