Contact:
Don More, Managing Director
dmore@signalhill.com
(646) 312-8686
www.signalhill.com

Signal Hill Year-End 2014 Cyber Security & Risk Review and 2015 Outlook

2014 – The Year of Cyber Insecurity

The Cyber Security & Risk market saw exceptionally strong stock, M&A and investment activity last year, driven by broad recognition that security challenges pose a growing threat to individuals and organizations alike. Surveys show Americans for the first time view cyber risk as the top threat to safety, ahead of national security, terrorism, crime and natural disasters. The U.S. Director of National Intelligence recently ranked cybercrime as the biggest national danger, above terrorism, espionage and weapons of mass destruction. Similar concerns surveyed in the UK, EU and Middle East highlight the global nature of cyber security problems.

Tables 1 and 2 highlight cyber security M&A, investment and public market performance statistics.

Table 1: Cyber Security & Risk M&A and Investment Activity	
Signal Hill M&A Transactions Tracked in 2014	105
Signal Hill Investments Tracked in 2014	87
Signal Hill M&A Transactions Tracked in 2013	97
Signal Hill Investments Tracked in 2013	84
Median M&A Purchase Price/LTM Revs in 2014	4.0x
Average M&A Purchase Price/LTM Revs in 2014	5.2x

Table 2: Cyber Security Stock Valuation and Performance						
Signal Hill Security Index				**Signal Hill New-Gen Security Index**		
	2013	**2014**			**2013**	**2014**
Median EV/Revenue	3.4x	4.7x		Median EV/Revenue	8.0x	9.4x
Median EBITDA/Revenue	15.8x	13.9x		Median EBITDA/Revenue	27.9x	31.2x
Average MRQ YoY Revenue Growth	13.7%	26.7%		MRQ YoY Revenue Growth	36.8%	51.2%
Median EBITDA Margin	10.8%	18.4%		Median EBITDA Margin	0.2%	15.3%
YoY Stock Performance	+24%	+14%		YoY Stock Performance	+27%	+40%

Source: CapIQ
New Gen Security Index: CUDA, CYBR, FEYE, FTNT, IMPV, PANW, PFPT, QLYS
Signal Hill Security Index: KOSDAQ:053800, TSE:4704, ABT, AVG, BKYI, CHKP, CUDA, CYBR, CYRN, FEYE, FTNT, GTO, IMPV, INTZ, PANW, PFPT, QLYS, SYMC, VDSI, WAVX, ZIXI

Signal Hill

Cyber Security and Risk products and services generated $71 billion of spending last year, with demand expected to grow 8.2% to $77 billion in 2015, according to Gartner research. Spending levels pale in comparison to the estimated $373 to $575 billion in damages attributed to security breaches, according to Intel. While hard to quantify, data theft alone (e.g. of trade secrets) may impose damages as great as $2.2 trillion, according to PwC. Target stores estimates its Q1 2014 breach cost $148 million, not including losses due to brand damage and market value impact. Similarly, Sony's 2011 and 2014 hacks cost $271 million. Since 2009, such incidents have grown at an annual average annual rate of 66% to 42.8 million in 2014. Interconnectedness of online activities, data and devices made it easier for attacks to cause greater damage. Consequently, the average cost of a breach to an organization rose to $5.9 million in 2014 from $3.9 million, according to PwC. Reflecting growing board-level concern over security risks, the Economist reported that American firms spent $2 billion on cyber-liability coverage in 2014, up from $1.3 billion in 2013.

Already, Q1 2015 has seen several major breaches, including the theft of millions of medical records from Anthem Health and a coordinated attack on bank ATMs worldwide resulting in theft of an estimated $1 billion. Table 3 lists several of the largest discovered breaches since 2012.

Table 3: Select Major Security Breaches by Records Stolen Since 2012

Target	Records	Technique		Target	Records	Technique
Adobe	152M	Customer Database Hack		Ubisoft	58M	Customer Database Hack
Ebay	145M	Customer Database Hack		HomeDepot	56M	3rd Party Login (Malware)
Anthem	80M	Unencrypted Data Hack (Malware)		Evernote	50M	Customer Database Hack
JP Morgan	76M	Stolen Credentials		Living Social	50M	Customer Database Hack
Target	70M	Customer Database Hack		Sony	10M (100 TB)	Nation-state attack or Insider Threat

Nation-state and organized crime ring attacks rose in 2014, driving propagation of advanced malware such as Regin and Zeus Gameover and major vulnerability exploits including Heartbleed and Shellshock. PwC's recent cybercrime survey, however, found that current and former employees remain the most common source of breaches at organizations, followed by service providers and partners; and ahead of hackers, competitors, activities, organized crime, terrorists and spies. Further, most breaches last year exploited simple mistakes, such as misconfiguration of network devices or clicking on a suspicious email. Dark Reading reports that as much as 95% of successful attacks in fact may be attributable to human error, rather than sophisticated attacks or weak defense technology.

In 2015, incidents will continue to be less the result of new exploits and viruses than weak security hygiene, and growth in points of exposure – IP-addresses, online presences, mobile applications, and cloud-based data.

M&A and Investment Activity Review

M&A

Signal Hill tracked 105 Cyber Security & Risk M&A transactions in 2014 at total announced value of approximately $7.0 billion and 97 deals in 2013 valued at $7.5 billion. Median announced deal value was $40 million. Only 35% of transactions had announced values; including unannounced values, total deal volume rose to an estimated $16 billion in 2013-14 with median deal value of $12-15 million.

The top 30 deal values and Purchase Price/LTM Revenue multiples (excluding not-meaningful multiples) are displayed in Tables 4 and 5 below. The largest and mostly highly-valued deals are listed in Table 6.

Table 4: 2014 Top 30 Announced Sector M&A Deals by Purchase Price/LTM Revenues

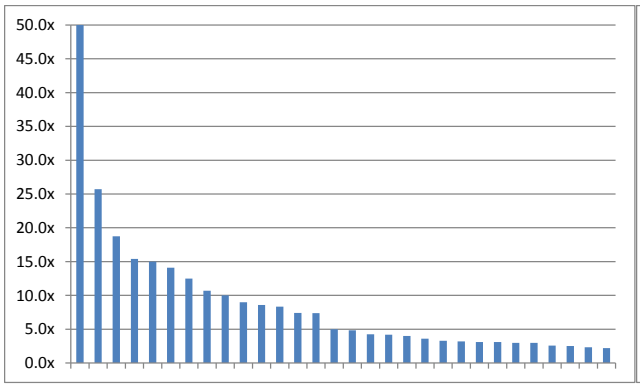


Table 5: 2014 Top 30 Announced Sector M&A Deals by Purchase Price

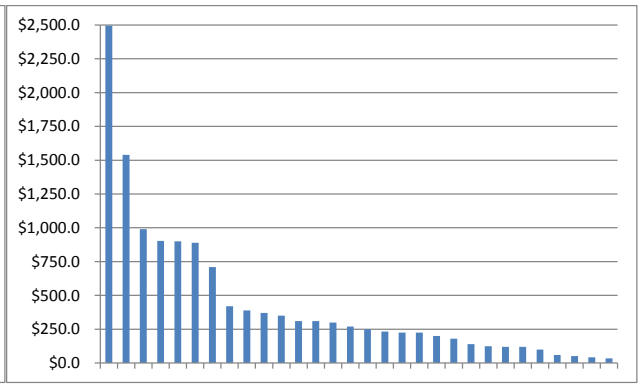


Table 6: Large and High-multiple Cyber Security M&A Deals 2013-2014

Date	Largest M&A Transactions Target / Acquirer	Purchase Price ($mm)	Subsector	Date	Highest Multiple M&A Transactions Target / Acquirer	Purchase Price / LTM Rev	Subsector
23-Jul-13	Sourcefire / Cisco	$2,494.1	Network Security	17-Sep-13	Versafe / F5 Networks	50.0x	Web Security
22-Jan-14	AirWatch / VMware	$1,540.0	MDM	15-Aug-13	Trusteer / IBM	25.7x	Anti-fraud
2-Jan-14	Mandiant / FireEye	$989.4	Penetration Testing and Remediation	22-May-13	Solera Networks / Blue Coat Systems	18.8x	Network Security
20-May-13	Websense / Vista Equity Partners	$902.9	Web Security	22-Jan-14	AirWatch / VMware	15.4x	MDM
15-Aug-13	Trusteer / IBM	$900.0	Anti-fraud	21-May-14	LetMobile / LANDesk Software	15.0x	MDM
8-Aug-14	SafeNet / Gemalto	$890.0	Encryption and IAM	1-Oct-13	41st Parameter / Experian Group	14.1x	Anti-fraud

9-Dec-14	Tripwire / Belden	$710.0	IT Compliance	18-Jul-13	PasswordBank Technologies / Symantec	12.5x	IAM and Authentication
5-Nov-14	Blackbird Technologies / Raytheon	$420.0	MAM	23-Jul-13	Sourcefire / Cisco	10.7x	Network Security
6-May-13	Stonesoft Oyj / McAfee	$389.0	Network Security	2-Jan-14	Mandiant / FireEye	9.7x	Penetration Testing and Remediation
2-Dec-13	Prolexic Technologies / Akamai	$370.0	Cloud Security	8-Jul-13	Aveska / EMC Corporation	9.0x	IAM

Signal Hill divides the Cyber Security & Risk market into 12 subsectors. Table 7 below lists the most active M&A subsectors in order by number of deals, dollar volume, multiples and growth:

Table 7: M&A Momentum Subsectors in Cyber Security & Risk

Most Deals	Highest Volume	Highest Multiples	Greatest Activity Growth 13-14
Identity & Access Management	Anti-malware/ATP	Anti-fraud	Security Services
Services	Services	Anti-malware/ATP	Identity & Access Management
Network Security	Network Security	Mobile Security	Mobile Security
Anti-malware/ATP	Mobile Security	Network Security	Critical Infrastructure Protection
Anti-fraud	Identity & Access Management	Identity & Access Management	Network Security
Mobile + Managed Security	Anti-fraud	Managed Security	Anti-fraud

Tables 8 – 11 below lists and ranks number of deals and purchase price by each subsector for 2014 and 2013.

Table 8: 2014 Subsector M&A-Number of Deals

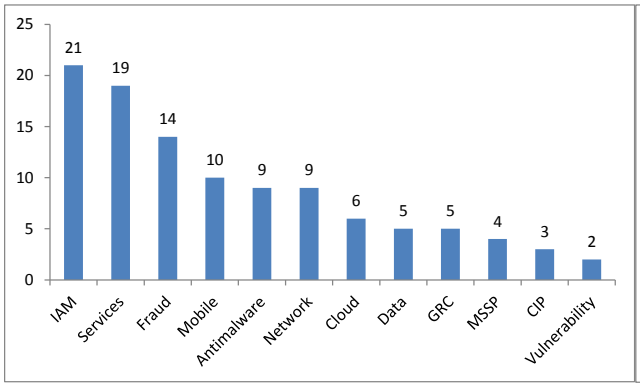
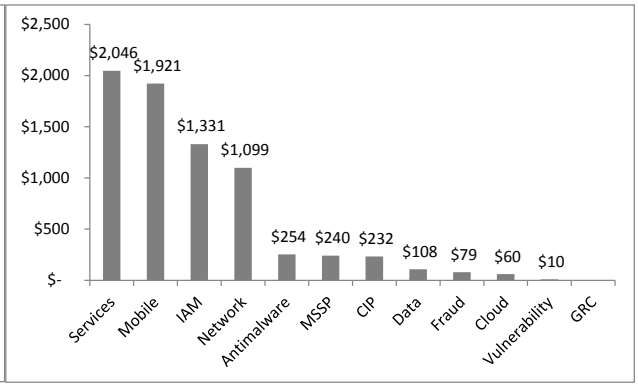


Table 9: 2014 Subsector M&A-Deal Volume $mm



Signal Hill

Table 10: 2013 Subsector M&A-Number of Deals

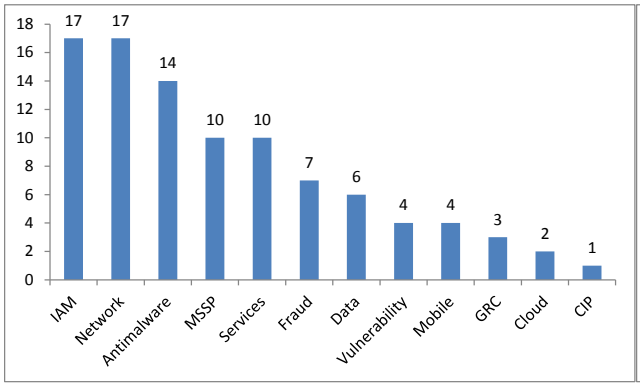


Table 11: 2013 Subsector M&A-Deal Volume $mm

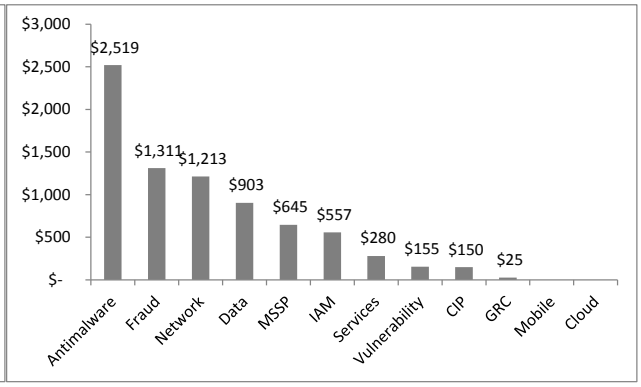
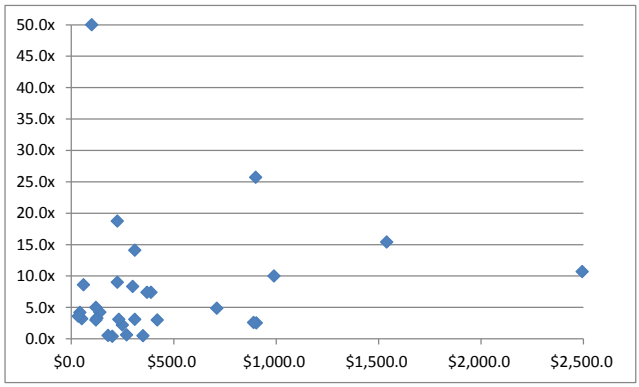


Table 12: Subsector M&A Size vs Valuation



Regression analysis of acquisitions of publicly-traded security companies over the past decide shows that the primary determinant of M&A deal value in the sector is the most recent quarter over prior-year quarter revenue growth rate. Analysis of security stock trading valuations similarly shows the largest determinant of value is recent revenue growth rate. Profitability is a distant second in terms of valuation impact. Size/scale in itself show almost no correlations with valuation, as a scatter chart of the 30 largest M&A transactions since 2013 shows in Table 12.

Investment

Signal Hill tracked 87 non-change-of-control investments in 2014 in Cyber Security and Risk totaling approximately $1.2 billion and 84 investments in 2013 valued at $1.5 billion. The total number, dollar value and median investment size by round is shown at Tables 13 and 14.

Table 13: 2013-14 Investments by Round

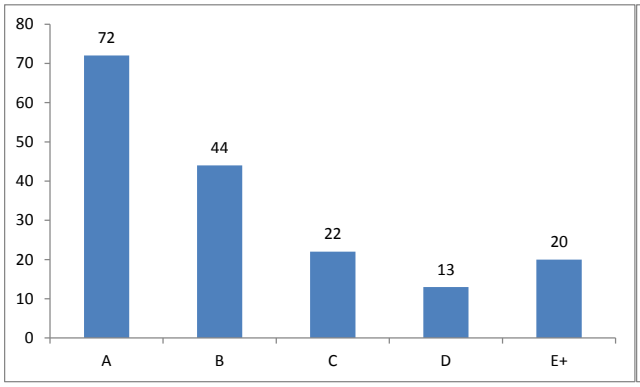
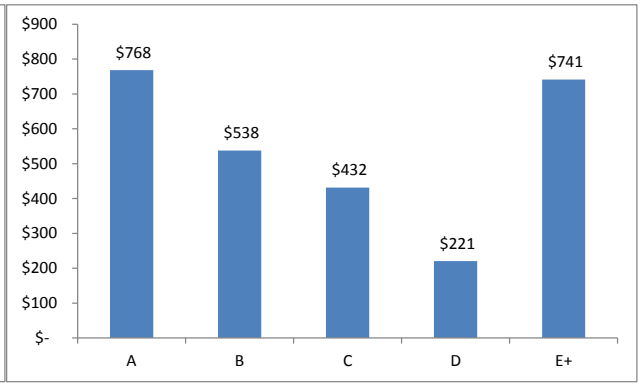


Table 14: 2013-14 Investment Volume by Round $mm



Signal Hill

Table 15 below lists the most active investment subsectors by number of deals and dollar volume:

Table 15: M&A Momentum Subsectors in Cyber Security & Risk		
Most Investments	**Highest Volume**	**Greatest Activity Growth 2013-14**
Anti-malware	Anti-malware/ATP	Data Security
Cloud Security & IAM	Mobile Security	Vulnerability Management
Data Security	Data Security	GRC
Network and Mobile Security	Network Security	Network Security
Vulnerability Management	Services	Anti-fraud
GRC	Cloud Security	Critical Infrastructure Protection

Tables 16 – 19 summarize number and total value of financial investments by each subsector for 2014 and 2013.

Table 16: 2014 Subsector Investment-# of Deals

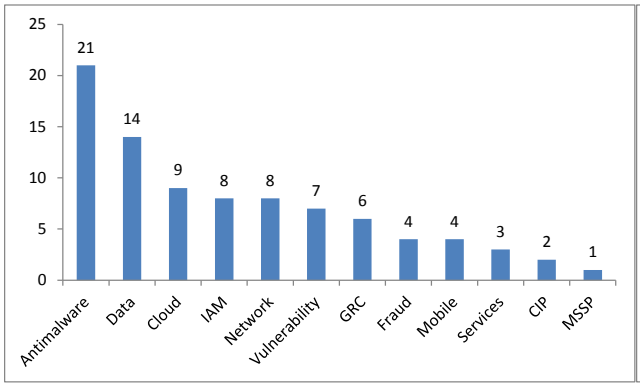


Table 17: 2014 Subsector Investment-Deal Volume $mm

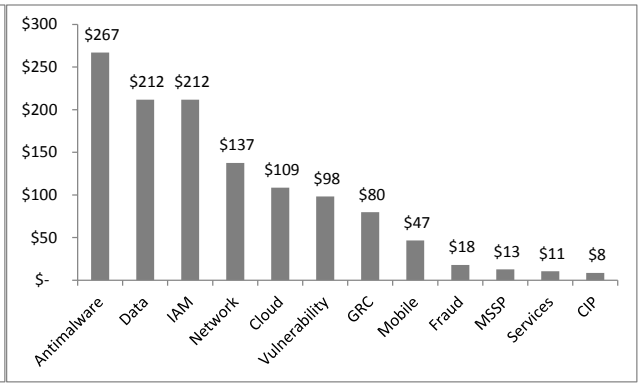


Table 18: 2013 Subsector Investment-# of Deals

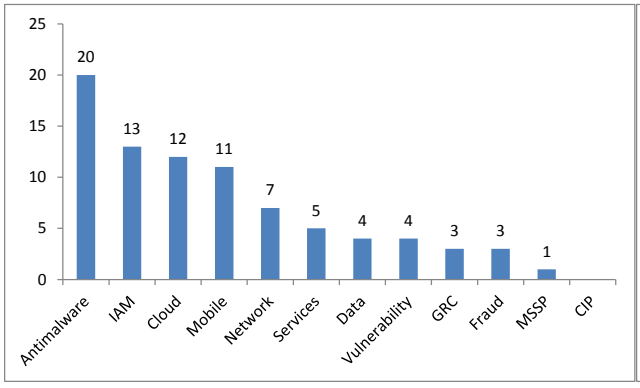
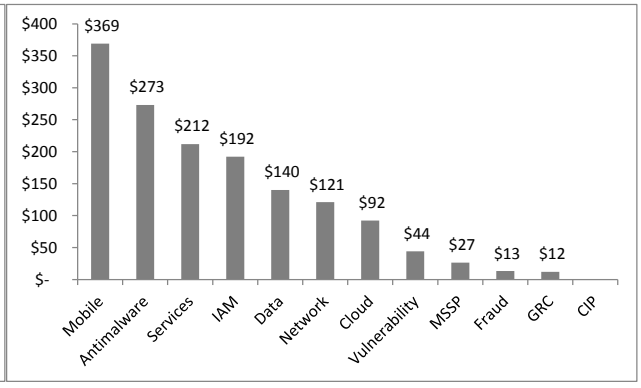


Table 19: 2013 Subsector Investment-Deal Volume $mm



Signal Hill

Subsector Assessment and Trends

Signal Hill divides Cyber Security and Risk into 12 subsectors (within which are 46 segments), classified by solution type. Six of the 12 subsectors are Primary categories, listed on the left side of Table 20 below. Another six, on the table's right side, are Derivative categories with distinct technologies and practices that incorporate the Primary categories. For example, Cloud Security can encompass any of the six Primary subsectors. For purposes of deal and investment analysis, we place a vendor in the Derivative category when its main function and value proposition is defined by the Derivative category; however when the Primary category best describes the vendor's function, it is classified as Primary though it may have Derivative category capabilities. Among subsectors there is a degree of overlap, for example with respect to software suites and appliances. As a result, market spending estimates shown include some double-counting.

Table 20: Cyber Security and Risk Subsectors

Primary Subsectors	2014 Market Size	Projected Annual Growth		Derivative Subsectors	2014 Market Size	Projected Annual Growth
Anti-malware/ATP	$10.0B	7.7%		Critical Infrastructure Protection	$70.5B	10.7%
Identity & Access Management	$9.2B	15.0%		Managed Security Services	$13.8B	15.4%
Network Security	$8.3B	3.0%		Security Services	$11.2B	8.0%
Data Security	$4.9B	16.0%		Cloud Security	$2.7B	22.0%
Vulnerability Management	$2.6B	12.0%		Mobile Security	$4.5B	41.0%
Anti-fraud	$1.3B	10.0%		Security GRC	$1.0B	9.0%

Brief discussion of subsector parameters and trends follow.

Primary Subsectors

Anti-malware/Advanced Threat Protection

The global endpoint security market, $10B in 2014, is expected to grow 7.7% annually, $14.5 billion by 2019 (Markets and Markets)

Malicious code is the cyberattack weapon of choice, deliverable via websites, email/SMS, files, application stores, and attached devices. Malware is the most common breach method, followed by hacking and social engineering. Malware threats are growing quantitatively and qualitatively as attackers share tools and techniques online. The average number of emails containing malware increased by 50% in 2014, according to security vendor Cyren, which also found a 159% increase in malware URLs in 2014. Increasingly, blended threats combine methods such as phishing and hacking to introduce malware. Subsector solutions overlap most closely with Vulnerability Management, Network Security and Data Security; for example large antivirus vendors also offer data loss prevention, and several firewall vendors integrate endpoint protection products.

In 2014, consumers drove about two-thirds of subsector spending. Organizations purchase solutions as suites and appliances, which Gartner research defines as Endpoint Protection Platforms.

Advanced Threats (also called APT for Advanced Persistent Threats) are distinguished from regular malware by the fact they are typically signature-less, multi-faceted, targeted and customized – thus, not reliably addressable through traditional antivirus products. This form of malware is harder to prevent and detect, as it often is deposited deep into a computing system and does not leave files. APT is the fastest growing segment within the subsector with projected 42% annual spending growth from $617 million in 2014, according to IDC.

In addition to anti-virus and APT, analytics technologies figure prominently in the subsector. Analytics is a diffuse space describing vendors that leverage big data techniques and threat intelligence feeds to find previously unseen anomalies indicative of an attack.

Areas of investment and acquisition interest include zero-day and polymorphic attack protection, social-engineered attack prevention, browser-based malware detection, advanced protection of web-facing applications, real-time attack intelligence and incident remediation.

Major public vendors in this sector include Cisco, FireEye, Intel, Proofpoint, Symantec and Trend Micro.

Identity & Access Management

Sector spending was estimated at $9.2 billion in 2014, growing 15% annually through 2019 to $18.3 billion (Markets and Markets)

In 2014, Forrester research placed IAM as the highest-ranking enterprise security spending priority, reflecting the simultaneous opportunities and challenges of managing distributed digital identities that enable access from anywhere to anything. Most serious breaches in 2014 involved unauthorized administrative access, so locking secure identity management is critical to protecting organizations. Effective IAM also improves business performance by streamlining trusted interactions among stakeholders. IAM also ties closely to compliance and risk management in areas of authorization and governance, which relates to onboarding, provisioning and other account lifecycle tasks. For consumers and consumer-facing businesses, identity theft is the highest-profile cyber security concern.

Active areas within the subsector include cloud-based IAM enabling single sign-on access across devices and applications. Most enterprise SSO systems are network-based and increasingly inadequate to manage mobile identities and cloud applications. Advanced and multi-factor authentication, including biometrics and mobile context-based smart authentication, are also high growth segments. Interest in advanced authentication technologies reflects overdue need for replacement of password-based authentication and rapid advent of mobile and wearable devices as potential universal authenticators. Identity analytics is another active area as IAM data feeds will increasingly get integrated into next generation firewalls, malware detection, antifraud and data loss prevention solutions to improve efficacy.

Further out on the horizon is what Gartner terms IdoT, for Identity of Things. As Internet of Things becomes mainstream, IAM will need to be designed around managing identities of entities – people, things and services – within a single framework.

Public IT infrastructure vendors including CA, Dell (Quest), IBM and Oracle have built and bought IAM suites, and are expected to expand into cloud and mobile access management, as well as identity analytics. Authentication-focused players such as RSA (EMC) and Gemalto will likely seek to also expand cloud-based offerings, broaden forms of authentication and expand into authorization.

Network Security

Sector spending is estimated at $8.3 billion in 2014, growing in the low single-digits through 2018 (IDC)

Network Security remains a necessity for organizations' extended perimeters. Forrester research's 2014 business security needs survey found three of the five highest priorities to be network security-related, namely Firewall Management (#2), SIEM (#4) and Intrusion Management (#5). Though no longer a static, centralized set of access points, the network boundary between private and public IT environments requires protection to supplement endpoint, application and data security. There is arguably a greater need for network security solutions in a BYOD world, as less control over users and devices increases the need for security from the network.

While overall sector spending is flat, this reflects increased overlap of network spending with solutions in the vulnerability management, anti-malware, mobile and cloud security segments. Also, the larger sub-segments of Network Security that are flat-to-declining – i.e. traditional firewall, VPN and intrusion detection – mask high growth segments that include: SIEM (security information and event management) growing 12% annually according to Research Markets; all-in-one appliances including SMB UTM (unified threat management) growing 24% annually according to IDC research; network device configuration management growing 17% annually; and DDoS (Distributed Denial of Service) security. DDoS attacks, still the most widely used method of taking down websites, increased 240% in 2014, according to security firm Incapsula.

As network security becomes more closely tied to both application-level and cloud security, integrated solutions see high demand. Increasingly powerful UTM devices also are of interest. Other active areas within the sector include proactive network threat intelligence and next-generation firewalls.

Major network security public players are Cisco, Check Point, IBM, Splunk, HP, Palo Alto, Intel, EMC, Barracuda and Fortinet. These vendors actively seek to enhance their cloud-based offerings and augment analytics capabilities.

Data Security

Data security has estimated spending of $4.9 billion in 2014, with expected growth of 16% annually (IDC, Forrester, Radicati)

Solutions that filter and encrypt digital data at rest and in motion will see accelerating demand growth as de-perimeterization and data mobility expose online information to theft and tampering. Last year saw a 49% rise in data breaches and 78% increase in data records stolen or lost, according to Gemalto. Email remains the most vulnerable vector for sophisticated data attacks on organizations and individuals. Cybercriminals in 2014 increasingly focused on phishing individuals with access to valuable data or credentials that could be hijacked and used for cyberattacks. Rapid expansion of unprotected Wifi, SMS and Dropbox-type cloud services add to the necessity for directly securing data.

With data protection and data privacy compliance becoming a high priority, organizations are increasingly incorporating pervasive encryption to achieve compliance and data security, and mitigate data breach risks associated with adoption of advanced technologies, particularly cloud services and mobility.

Other areas of high interest include secure messaging gateways utilized by carriers and public cloud services, demand for which is forecast to grow 55% annually to $363 million by 2017, according to Infonetics. Data loss prevention from the cloud, for mobile and for deployment in public clouds are also of interest; overall DLP demand is forecast by Gartner research to grow 22% annually. There also will be more demand for persistent digital rights management, driven by cloud adoption, bring-your-own-IT and the Internet of Things (IOT). Within communications, voice and video transmission encryption are also gaining attention.

Large public or recently-public players include Blue Coat, Dell, Barracuda, Gemalto, Intel, Proofpoint, Symantec, TrendMicro and Websense.

Vulnerability Management

Vulnerability Assessment and Application Security Test spend was $2.6 billion in 2014 growing 12% yearly (IDC)

The most serious distributed attacks last year came from exploited vulnerabilities, such as Heartbleed and Shellshock, which impacted two-thirds of web servers, Microsoft Office, Adobe Reader and other applications. Effective vulnerability assessment, patch and configuration management, application security testing, and forensics solutions are critical to preventing a broad array of breaches.

The need for vulnerability management is further heightened by explosion of mobile computing and, in 2015 and beyond, the Internet of Things. HP recently found 70% of network-accessing devices contain vulnerabilities, while a majority of mobile applications have not been adequately tested. A growing number of vulnerabilities last year were also found in virtual environments, which heighten risks by creating a single point of failure.

In addition to directly preventing exploits, vulnerability assessment solutions provide threat intelligence feeds that benefit anti-malware and SIEM, as well as incident remediation services. Vulnerability exploitation is often

followed by a targeted malware attack so vulnerability assessment can break the attack chain. In addition vulnerability assessments help maintain PCI and other types of compliance.

The most active public companies in the sector include HP, IBM, Intel, Qualys and SolarWinds.

Anti-fraud

North American Fraud Detection/Prevention spending is forecast to grow 10% yearly, to $2.1 billion in 2019 (Micro Market Monitor)

This segment focuses on technology solutions that detect, predict or prevent fraudulent transactions over the internet. While estimates vary widely, according to one survey e-commerce losses due to cyber fraud exceeded $200 billion in 2014 and are expected to rise 20% annually with online transactions. The problem is widespread – one in four US consumers received data breach notifications, according to ACI Worldwide.

This area's technology integrates with other subsectors including IAM (as authentication is the primary defense against online fraud, which typically involves identity compromise) and Anti-malware (which often stop attacks that aim to perpetuate financial fraud). Fraud occurring from stolen identities accounts for nearly 85% of ID thefts in the US, according to the Federal Trade Commission. Anti-malware is also connected as breaches often are utilized by cybercriminals to advance cyber fraud attacks. Similarly, Data Security combats fraud utilized to steal digital information.

Areas of high interest in the subsegment include fraud analytics tools that review data from different data sources across a wide range of channels to discover trends, patterns, and anomalies in transactions. Mobile fraud detection is also a focus area as devices will be a prime target for fraud in 2015 according to experts, as mitigation systems and models are still not robust. In addition, health record protection is a major market opportunity given pending digitalization of the healthcare industry. A recent study by the Medical Industry Fraud Alliance reported medical identity theft to be the fastest growing identity crime, as highlighted by the March 2015 Anthem breach.

Anti-fraud also includes E-signature verification solutions, which have seen recent strong interest in support of online commerce. Increasingly, anti-tampering protection solutions for financial services, software publishers, games companies and device manufacturers are becoming an area of focus.

Key public players in this market include SAP, FICO, Fiserv, Experian, EMC, CSC, IBM and ACI.

Derivative Subsectors

Critical Infrastructure Protection

Security spending to protect critical infrastructures will grow 10.7% through 2020 from $63.8 billion in 2014 (ABI)

CIP addresses several major related developments in technology use – IoT, IP-enablement of industrial control systems and convergence of physical and IT security. Actual subsector size, while large, is more difficult than

others to estimate and separate from other cyber security areas, such as anti-malware, network security and vulnerability management, due to significant technology and functional overlap.

Protecting high-value physical targets against cyber-attacks is becoming an acute priority as high-profile breaches become more common, and as more devices and industrial control systems become IP-enabled. For example, there has been a rapid rise in hacks against systems controlling energy stations. Other discovered hacks include stock exchanges, utilities, air traffic control systems and railways. Research vendor IOActive has shown how hackers can commander new automobile electronic control units.

Subsector areas of interest include event management automation, threat intelligence management, and cyber-attack vulnerability and anomaly testing software for oil and gas, manufacturing, medical, chemical, pharmaceutical and water treatment markets.

Managed Security Services

North American MSS revenues of $1.8 billion in 2013 are forecast to reach $3.3 billion in 2018 (Frost & Sullivan)

Managed security refers to cloud-based delivery of combined security solutions-as-a-service and traverses all Primary subsectors. It is an alternative to deployment of security "behind the firewall", i.e. within the organization. Gartner research predicts MSS will become the primary means by which mid-size and smaller organizations purchase cyber security and risk solutions. ABI research predicts demand will reach $32.9 billion in 2020. Cloud based services vary by vendor and range from basic firewall monitoring to advanced analytics and delivery of a full range of services across every primary subsector. Managed security services providers are differentiated as well by whether they serve enterprises or smaller organizations. Vendors also vary in the extent to which they use third-party security vendors versus their own technologies.

Managed security services are provided by pure-play MSSs, consultancies and VARs, telcos and traditional security vendors offering cloud-delivered versions of their products and specialty vendors.

Security Services

Security services spending totaled $11.2 billion in 2014 and is forecast to increase 8% annually (Gartner)

Professional security services represent a major horizontal subsegment that crosses the Primary subsectors. It includes security consulting, integration, monitoring, ethical hacking, training, testing, development and remediation services. According to online recruiter Dice, cyber security help-wanted ads increased 77% in December 2014 over 2013; experts cite a recurring shortage of security-trained services personnel.

Complex security needs have been heightened due to the rapid rate of technology change. Gartner predicts that by 2018 more than half of organizations will use security services firms that specialize in data protection, security risk management and security infrastructure management.

While most security services are delivered by larger consultancies including the Big Four Accountancies, large system integrators and Big IT publics such as IBM and HP, the highest growth is among specialty firms that are experiencing rapid expansion.

Mobile Security

$4.5 billion of total mobile security spending in 2014 expected to rise 41% annually to $34.8 billion by 2020 (Infonetics)

Mobile security traverses all Primary security sectors and is the fastest growing subsector, reflecting rapid evolution toward an IT world dominated by mobile devices. Subsector areas include data encryption, device authentication, mobile application vulnerability management and messaging security. The client-side mobile device security software market represents about $1.4 billion of spending in 2015 and is projected to rise to $3.4 billion in 2018.

Areas of highest concern among businesses include data loss protection, application security, unauthorized device access and misconfiguration and mobile payment fraud. Mobile malware will become a major focus as incidents and variants grow alongside usage. During 2014 there was a 61% increase in mobile malware targeting Android devices. Mobile device authentication also is expected to be an area of focus in 2015.

Cloud Security

Cloud security spending was $2.7 billion in 2014, predicted to grow 22% annually to $3.6 billion in 2016 (Gartner)

Like other derivative subsectors, cloud security traverses all Primary subsectors. It refers to solutions that protect applications run from and data stored in the cloud, whether data centers or public cloud services. Areas of interest include security event monitoring, anti-malware for virtualized environments and data security solutions that continuously manage access to and encrypt content residing in the cloud. Cloud infrastructure vulnerability and compliance management solutions are also active focus areas – Gartner research predicts more than 30% of small or midsize businesses will need to adopt cloud-based security controls by the end of 2015.

Governance, Risk & Compliance Management

Security policy and compliance spending of $1.0B in 2014 is forecast to grow 9% annually to $1.4B in 2018 (IDC)

Within the broader GRC market, security policy and compliance management automates monitoring and maintenance of risk controls that assure adherence to regulations and policies meant to maintain security. Policy and compliance management also helps organizations optimize their cyber security spending for greater return on investment. In 2014, according to a PwC survey, only 38% of organizations reported having a methodology to prioritize security investments based on risk and impact to business strategy.

Cyber security GRC is a preventive solution that complements Vulnerability Management (IDC research characterizes the subsegment as a part of VM) and often involves Security Services. There is heightened interest in compliance monitoring solutions to reduce security vulnerabilities, and in specialized vendors that address the

compliance needs of particular industry verticals. Regulatory demands are growing to help improve the state of cyber security. As examples, the US SEC is evaluating implementation of greater security risk disclosure requirements, and stringent EU Data Protection regulations are expected to be finalized in 2015.

2015 Forecast: Continued Sector Strength

Evidence strongly suggests that high levels of cyber security & risk M&A and financing activity will continue, and perhaps accelerate, through 2015-16.

- Signal Hill's canvassing of strategic buyers and financial investors suggest broad interest in investing into security this year – particularly among firms that have yet to invest in the sector. The interest is both thematic and specifically focused on gap filling in areas of perceived need.

- Public markets continue rewarding cyber security companies and acquirors with above-average valuation multiples, and the IPO window is open, with a growing backlog of companies filing this year.

- Business IT spending surveys suggest cyber security and risk remain high near-term investment priorities.

- Security investment refresh cycles are generally expected to accelerate due to rapid adoption of newer cloud and mobile technologies, and introduction of next-gen security solutions.

- There is an emerging view among regulators and organizations that security spending is better viewed in the context of organization risk levels, rather than percent of IT budget; this suggests security budgets will increase. As the Wall Street Journal has noted, "What companies finally are recognizing is they are paying $50,000 to protect their business and all the data on their systems. It's not a percentage of IT spend, it's a percentage of risk of the company at large."

- Large IT consulting and integration firms see increased customer demand for expansion of their cyber security consulting capabilities. This is due to the complexity associated with rapidly evolving enterprise security technologies and increasingly regulated environments.

- Both the quality and quantity of cyber-attacks continue to rise, and awareness of the challenge is high.

- We see some increase in divergence of valuations; median multiples are likely to remain stable, however with greater dispersion.

Signal Hill, named *2014 Boutique Investment Bank of the Year* by the Global M&A Network, is a leading independent advisory boutique serving the M&A and private capital raising needs of growth companies. Signal Hill's experienced bankers provide deep domain expertise and an unyielding commitment to clients in our sectors: Internet & Digital Media, Internet Infrastructure, Services and Software. With more than 600 completed transactions and offices in Baltimore, Bangalore, Boston, Mumbai, Nashville, New York, Reston and San Francisco, Signal Hill leverages deep strategic industry and financial sponsor relationships to help our clients achieve Greater Outcomes®.