CYBERSECURITY MARKET REPORT

FROM THE EDITORS AT CYBERSECURITY VENTURES

Q3 2015

The Cybersecurity Market Report is published quarterly by Cybersecurity Ventures. We cover the business of cybersecurity, including market sizing and industry forecasts from consolidated research by IT analyst firms, emerging trends, employment, the federal sector, hot companies on the Cybersecurity 500 list, notable M&A, investment and IPO activity, and more.

MARKET SIZING & PROJECTIONS

The worldwide cybersecurity market is defined by market sizing estimates that range from $77 billion in 2015 to $170 billion by 2020.

Sponsored by the Cybersecurity 500 list of the world's hottest and most innovative cybersecurity companies.

- Market research firm Gartner says global spending on IT security is set to increase 8.2 percent in 2015 to $77

billion, and the world will spend $101 billion on information security in 2018.

- The cyber security market is estimated to grow to $170 billion (USD) by 2020, at a Compound Annual Growth Rate (CAGR) of 9.8 percent from 2015 to 2020, according to a report from Markets and Markets. The aerospace, defense, and intelligence vertical continues to be the largest contributor to cybersecurity solutions.

- North America and Europe are the leading cybersecurity revenue contributors, according to a report from TechSci Research. Asia-Pacific is rapidly emerging as a potential market for cyber security solution providers, driven by emerging economies such as China, India and South-East Asian countries, wherein, rising cyber espionage by foreign countries is inducing the need for safeguarding cyber space.

- The "PwC Global State of Information Security Survey 2015" found that U.S. information security budgets have grown at almost double the rate of IT budgets over the last two years.

- According to 451 Research's new "Voice of the Enterprise: Information Security" quarterly study, based on responses from over 1,000 IT professionals, primarily in North America and EMEA, spending on security remains strong with 37 percent of enterprise security managers expecting to increase their budget in the next 90 days. Only 4 percent of enterprises are decreasing security spending.

- Million dollar plus cybersecurity deals (vendors selling to end-users) are on the rise. In a recent research note, analysts at FBR & Co., an Arlington, Va. based investment banking and M&A advisory firm, indicate that the number of seven-figure (cybersecurity) deals have increased by 40 percent year-over-year.

Who's HOT in cybersecurity? GO HERE to see "The List".

- "Given the ongoing, evolutionary nature of cyber-attacks, coupled with the relatively low share of total IT spend security accounts for, we believe industry growth

rates will remain stronger than industry forecasts" states Columbia Threadneedle Investments. We expect 10-15 percent growth over the next 3-5 years versus the 8-10 percent forecasted by industry analysts like Gartner. This creates immense opportunities for innovative cybersecurity companies as well as potentially outsized investment returns for those capitalizing on the theme.

- Cybersecurity is predicted to be the fastest growing homeland security market as North America, Asia and Europe invest in cyber defenses, according to ASDReports in its "The Homeland Security Market Forecast 2014-2024". ASDReports says the global homeland security market size was $238 billion in 2014.

- India has the world's second largest population, and a very small cybersecurity economy. But they are a nation to watch for cybersecurity market growth. According to a PwC report cited in The Economic Times, India's cyber security market size will jump to $1 billion USD in 2015 (from an estimated $500 million USD last year). That is a whopping 100 percent year-over-year growth.

Cybersecurity market by international (non-U.S.) regions

MicroMarketMonitor publishes reports including cybersecurity revenue and growth forecasts by international region. They forecast the following numbers:

- The Europe Cyber Security Market is expected to grow to $35.53 billion by 2019, with an expected CAGR of 7.2 percent for the period 2014-2019. This market contributes 26.95 percent of the global market and will slightly fall down to 22.81 percent by 2019.

- The Middle East and Africa Cyber Security Market is expected to grow to $13.43 billion by 2019, with an expected CAGR of 13.7 percent for the period 2014-2019. This market contributes 7.19 percent of the global market and will slightly grow to 8.62 percent by 2019.

Cybercrime Evolves in Russia

- The Asia Pacific Cyber Security Market is expected to grow to $32.95 billion by 2019, with an expected CAGR of 14.1 percent for the period 2013-2019. This market contributes 17.21 percent of the global market and will slightly grow to 21.16 percent by 2019.

- The Latin America Cyber Security Market is expected to grow to $11.91 billion by 2019, with an expected CAGR of 17.6 percent for the period 2013-2019. This market contributes 5.18 percent of the global market and will slightly grow to 7.65 percent by 2019.

Cybersecurity hot and emerging markets, data points by sector.

- According to IDC, the hot areas for growth are security analytics / SIEM (10 percent); threat intelligence (10 percent +); mobile security (18 percent); and cloud security (50 percent). According to a report from Markets and Markets, the cloud security market is expected to be worth $8.7 billion by 2019.

- The network security sandbox market, which barely existed a few years ago, is set to grow immensely as advanced persistent threats (APTs) necessitate a behavioral approach to detecting malware. New analysis from Frost & Sullivan, “Network Security Sandbox Market Analysis”, finds that the market earned revenues of $537 million in 2014 and estimates this to exceed to $3.5 billion by 2019.

- IDC predicts that by the end of 2015, 20 percent of proprietary data in the cloud will be encrypted – and by 2018, that will quickly rise to 80 percent. The encryption software market is forecasted to be worth $4.82 Billion by 2019, according to Markets and Markets.

- ABI Research calculates that total revenues for the global digital forensics market will reach $3.7 billion

global digital forensics market will reach $2.7 billion (USD) by the end of 2015, and they estimate the market to reach $4.7 billion in 2020.

- High growth in the adoption of cloud computing, virtualization and increasing attacks on data centers, are some of the key factors that are fueling the growth of the data center security market – projected to be worth $8.13 billion by 2020, according to Markets and Markets.

- Technology market research firm Infonetics Research (now part of IHS Inc.), recently reported that global network security appliance and software revenue climbed 6 percent in 2014, to $6.9 billion, as enterprises and network operators deployed security solutions aimed at protecting data and network infrastructure. The report tracks integrated security appliances, secure routers, SSL VPN gateways, VPN and firewall software, and intrusion detection and prevention products.

CYBERCRIME

Cyber attacks costing businesses $400 billion to $500 billion + a year.

Sponsored and co-published by SmartBrief on Cybersecurity, security and risk management news that matters to the C-suite

- The British insurance company Lloyd's estimates that cyber attacks cost businesses as much as $400 billion a year, which includes direct damage plus post-attack disruption to the normal course of business. Some vendor and media forecasts put the cybercrime figure as high as $500 billion and more.

- According to the "World Economic Forum (WEF) Global Risks 2015 Report", most cybercrime incidents go unreported, and few companies come forward with information on their losses. That is not surprising given the risk to an organization's reputation and the prospect of legal action against those that own up to cybercrime.

- The World Economic Forum (WEF) says a significant portion of cybercrime goes undetected, particularly industrial espionage where access to confidential documents and data is difficult to spot.

documents and data is difficult to spot.

- TechSci Research says the banking and financial services sector has been the prime target of cyber criminals over the last five years, followed by IT & telecom, defense, and the oil and gas sector.

- Cybercriminals stole up to $1 billion from approximately 100 financial institutions in the U.S., Germany, Russia, Ukraine, and China over a two-year period, according to researchers from security firm Kaspersky Lab.

- The Federal Communications Commission (FCC) has entered a $25 million settlement with AT&T Services, Inc. to resolve an investigation into consumer privacy violations at AT&T's call centers in Mexico, Colombia, and the Philippines. The data breaches involved the unauthorized disclosure of almost 280,000 U.S. customers' names, full or partial social security numbers, and unauthorized access to protected account-related data, known as customer proprietary network information (CPNI). This is the FCC's largest privacy and data security enforcement action to date.

- Ransomware has cost $18 million over the past 15 months. Ransomware scams involve a type of malware that infects computers and restricts users' access to their files or threatens the permanent destruction of their information unless a ransom— anywhere from hundreds to thousands of dollars—is paid. An advisory from the FBI's Internet Crime Complaint Center said more than $1 million a month, on average, was paid to recover computers from ransomware incidents.

- Alcatel-Lucent's Motive Security Labs estimates that last year 16 million mobile devices worldwide have been infected by malicious software – or "malware" – used by cybercriminals for corporate and personal espionage, information theft, denial of service attacks on businesses and governments, and banking and advertising scams.

- The IRS, which is increasingly being called into identity theft cases involving tax fraud, has set up a new cybercrime investigation team of about a dozen agents.

  According to a recent Wall Street Journal article, the Washington-based unit will tackle a nearly fourfold jump in identity theft cases since 2011, many of which involve hackers stealing information in order to collect victims' tax refunds.

- **DF Labs**, a data breach and incident response firm, reports that Harvard University has just recently faced its second data breach within four months. Whether planning to blackmail wealthy families, future leaders, or gain access to various research information (as many Ivy Leagues schools are host to research projects for military and other various organizations), Universities are growing in popularity among cyber criminals and it's not just the Ivy Leagues.

- According to "Verizon's 2015 Data Breach Investigations Report", which analyzes security incidents that happened last year, the top five affected industries by number of confirmed data breaches were: public administration, financial services, manufacturing, accommodations and retail.

- At the end of last year, Joseph Demarest, assistant director of the FBI's cyber division told a U.S. Senate hearing that the cyberattack that crippled Sony Pictures would probably get past 90 percent of internet defenses that are out there today in private industry – and would have challenged even state government.

CYBER INSURANCE

Cyber insurance market grows from $1 billion to $2.5 billion over the past two years.

Sponsored by Cavirin, a leading provider of cloud security and GRC services.

- According to BITS, the technology policy division of the Financial Services Roundtable, 2014 marked an important milestone in the growth of cyber insurance with a significant jump in both the number of companies offering cyber insurance and the number of

companies offering cyber insurance and the number of firms buying cyber insurance. Demand for that insurance rose by 21 percent across all industries, with financial institutions representing the biggest increase of 29 percent in coverage buying.

- Inga Beale, CEO at Lloyd's, recently told Fortune that demand for cyber insurance has grown considerably in recent years. Last year, the insurance industry took in $2.5 billion in premiums on policies to protect companies from losses resulting from hacks. That was up from around $2 billion a year before, and less than $1 billion two years before that.

- PwC says adoption of cyber insurance as a tool to help manage security risks continues to rise. More than half (51 percent) of respondents say they have purchased cybersecurity insurance, according to the "PwC 2015 Global State of Information Security Survey". And among those that have done so, many are taking steps to enhance their security posture in order to lower their insurance premium.

- Fortune recently reported that about 90 percent of cyber insurance is being purchased by U.S. firms, leaving other companies around the world exposed.

- Forrester Research recently predicted "$100 million cyber-insurance policies will become the norm."

- "Cyber insurance policies are offered by more than 70 carriers according to a Gartner Research report, and include liability coverage for exposing confidential information, paying to notify customers of a breach and providing them with credit-monitoring services", stated Lou Shipley, CEO at **Black Duck Software**, which helps companies securely manage open-source software, in a recent article he wrote for The Wall Street Journal. Shipley advises that small businesses should consider buying cyber insurance to help fend off hackers, given that percent of cyberattacks hit companies with fewer than 100 employees. At present, most cyber insurance buyers are large corporations.

JOB MARKET

Cybersecurity workforce shortage to reach 1.5 million by 2019.

Sponsored by DB Networks, Assuring Database Security through Intelligent Continuous Monitoring

- "The demand for the (cybersecurity) workforce is expected to rise to 6 million (globally) by 2019, with a projected shortfall of 1.5 million" stated Michael Brown, CEO at Symantec, the world's largest security software vendor.

- The "Cisco 2014 Annual Security Report" warns that the worldwide shortage of information security professionals is at 1 million openings, even as cyberattacks and data breaches increase each year.

- More than 209,000 cybersecurity jobs in the U.S. are unfilled, and postings are up 74 percent over the past five years, according to a Peninsula Press (a project of the Stanford University Journalism Program) analysis of numbers from the Bureau of Labor Statistics. The demand for information security professionals is expected to grow by 53 percent through 2018.

- A recent CNBC story quotes a Rand Corporation study which estimates there are around 1,000 top-level cybersecurity experts globally vs. a need for 10,000 to 30,000.

Cybersecurity Careers: FireEye is hiring in N. America, EMEA, APAC, LATAM – Apply now

- "The cybersecurity job market is on fire" says Veronica Mollica, founder and executive information security recruiter at **Indigo Partners, Inc.** in Fairfield CT. "Our candidates are facing competing offers from multiple companies with salary increases averaging over 30 percent. Current employers are scrambling to retain talent with counter offers including 10 percent and higher salary increases for information security team members to remain on board" adds Mollica.

- According to a recent report from DICE, a leading IT job board, the top five IT security salaries are: No. 1 – lead software security engineer at $233,333; No. 2 – chief security officer at $225,000; No. 3 – global information security director at $200,000; No. 4 – chief information security officer at $192,500; and No. 5 – director of security at $178,333.

- IDC predicts that "by 2018, fully 75 percent of chief security officers (CSO) and chief information security officers (CISOs) will report directly to the CEO, not the CIO". This will arguably push those positions higher up in to the salary stratosphere.

Machine learning and behavioral analysis from DB Networks frees up cybersecurity staff, LEARN HOW

- U.S. News and World Report ranked a career in information security analysis eighth on its list of the 100 best jobs for 2015. They state the profession is growing at a rate of 36.5 percent through 2022.

- "Traditional manual approaches to cybersecurity are proving to be unsustainable." said Brett Helm, Chairman and CEO of **DB Networks**. "Intelligent IT security automation through machine learning and behavioral analysis is faster, more accurate, and frees up skilled professionals to focus on more critical issues."

- According to a 451 Research Q2 2015 study, based on responses from over 1,000 IT professionals, primarily in North America and EMEA, security managers reported significant obstacles in implementing desired security projects due to lack of staff expertise (34.5 percent) and inadequate staffing (26.4 percent). Given this challenge, only 24 percent of enterprises have 24×7 monitoring in place using internal resources.

InfoSEC Job Board – for Employers and Job Seekers, provided by Information Security Buzz

- "Signature-based security products fire hose an endless stream of insignificant alerts and false positive alerts to the SOC overwhelming the staff," said Steve Hunt, President and COO of **DB Networks**. "The lost time and

productivity of that approach is staggering. Behavioral analysis is field proven to be extremely accurate identifying attacks, substantially reducing false positives, resulting in far less staffing requirements."

SECURITY SOFTWARE

IBM Security: fastest growing vendor in the security software market

Sponsored by SandHill.com, the business strategy destination for cloud, mobile, IoT, cybersecurity, and big data software

- Worldwide security software revenue totaled $21.4 billion in 2014, a 5.3 percent increase from the prior year, according to Gartner, Inc. Low growth in endpoint protection platforms and a decline in consumer security software — markets that together account for 39 percent of the market — offset the strong performance of high-growth areas, such as security information and event management (SIEM), secure Web gateway (SWG), identity governance and administration (IGA) and enterprise content-aware data loss prevention (DLP).

- Gartner recently listed the top five security software vendors by 2014 revenues (USD), market share, and growth. IBM leads the pack with a 17 percent growth rate, more than three times the nearest competitor. The top five by revenues: Symantec with $3.69 billion in revenues, 17.2 percent market share, and a (- 1.3 percent) decline in growth; Intel Security with $1.825 billion in revenues, 8.5 percent market share, and 4.5 percent growth; IBM Security with $1.486 billion in revenues, 6.9 percent market share, and 17 percent growth; Trend Micro with $1.052 billion in revenues, 4.9 percent market share, and a (-5.9 percent) decline in growth; EMC (includes its RSA business) with $798 million in revenues, 3.7 percent market share, and 5 percent growth.

- IBM Security has ascended to the No. 8 position on the **Cybersecurity 500**, a list of the world's hottest and most innovative cybersecurity companies, and it is the top listed firm in the professional services category. Gartner has called IBM the largest security vendor selling

has called IBM the largest security vendor selling exclusively to enterprises. IBM Security grew three times faster than the entire cybersecurity market in 2014.

- "IBM is ushering in an intelligence-driven era of security with our clients" says Brendan Hannigan, General Manager at IBM Security. "We are outpacing the competition because we help clients safeguard the full spectrum of a risk framework – people, data, applications and infrastructure – by deploying the industry's broadest portfolio of security consulting, services, and software" adds Hannigan.

The business of cybersecurity at SandHil.com, STORIES HERE

- Ginni Rometty, IBM Corp.'s Chairman, President and CEO, had the following to say at the recent IBM Security Summit in New York City, when she addressed CISOs (Chief Information Security Officers), CIOs, and CEOs from 123 companies in 24 industries. – "We believe that data is the phenomenon of our time. It is the world's new natural resource. It is the new basis of competitive advantage, and it is transforming every profession and industry. If all of this is true – even inevitable – then cyber crime, by definition, is the greatest threat to every profession, every industry, every company in the world… That's why IBM created a Security Business Unit, marshaling the knowledge of 6,000 experts."

- Speaking at the IBM Security Summit, IBM's CEO Ginni Rometty went on to say "We announced that more than 1,000 organizations across 16 industries are participating in our X-Force Exchange threat intelligence network. We only launched the network a month ago, so its rapid growth speaks to significant need. And we're bringing a potent weapon to the fight – a 700 terabyte threat database including two decades of malicious cyberattack data from IBM's security operations, as well as anonymous threat data from more than 4,000 organizations, which have contributed 300 new collections of data in the last month."

Security industry failing to keep pace with hacker innovation, Cisco warns

- According to an article in The Wall Street Journal, IBM

reported second-quarter (Q2 2015) revenue fell 13.5 percent. That adds to a string of quarterly declines that now spans 13 periods despite company efforts to scale back on legacy hardware and push into cloud-based software and services. Technology services revenue was down 10 percent; business services fell 12 percent; software dropped 10 percent; and overall hardware revenue sank 32 percent.

- "IBM's security business is hot and innovative according to our criteria which includes the security sectors they cover, CISO and corporate security staff feedback, research and analyst firm observations and findings, investigative media coverage, demos and presentations at conferences, notable implementations, and revenue growth" says Steve Morgan, Editor-In-Chief of the **Cybersecurity Market Report**. "If there's a concern, it's that IBM's security business only makes up 1 to 2 percent of IBM's total revenues (before the recent revenue declines it was closer to 1 percent). If the company isn't able to execute on its corporate strategy to reinvent itself around next generation technologies – then does it start to pull back on resources to a unit that contributes a tiny fraction to the bottom line?

MANAGED SECURITY SERVICES

Global managed security services market exploding from $8 billion in 2015 to $30 billion by 2020.

SOLUTIONARY, an NTT Group Security Company, is the Next Generation Managed Security Services Provider (MSSP)

- The "Global Managed Security Services Market Report" by Frost & Sullivan states that the MSS sector is expected to reach $12.78 billion by 2018. They found that in 2014, the MSS market was $7.83 billion.

- The global managed security services market is projected to reach $29.9 billion by 2020, with a compound annual growth rate (CAGR) of 15.8 percent over the next five years, according to a recent report from Allied Market Research (AMR).

- ABI Research says most organizations lack the security expertise to manage security solutions from a wide variety of vendors. Rising threats, government regulations, and a lack of internal resources are driving businesses to turn to managed security service providers (MSSP) which offer expertise and dedicated security personnel.

- IDC stated "enterprises will be utilizing security software as a service (SaaS) in a greater share of their security spending. By the end of 2015, 15 percent of all security will be delivered via SaaS or be hosted and by 2018 over 33 percent will be".

- At the most recent Gartner Security & Risk Management Summit in Sydney, Australia, Gartner analysts stated "A significant portion of organizations are shifting existing resources away from the operational aspects of security technologies, such as security device administration and monitoring, toward mitigation and incident response. This new dynamic has given rise to significant growth throughout the globe for managed security services."

- Frost & Sullivan notes that the fastest growing regions in the managed security services sector will be Europe, the Middle East and Africa. Senior Analyst Beatriz Valle points to the enforcement of the EU Data Protection Legislation as being the catalyst for the rapid uptake in managed security services. Valle mentions, "In North America too, stringent regulations and increasing governance complexity will spur MSS uptake, particularly in healthcare, banking and retail."

- "Gartner's Magic Quadrant for Managed Security Services, Worldwide", features MSSPs which are evaluated on their completeness of vision and ability to execute, and lists the following companies as "Leaders": Dell SecureWorks, IBM, Verizon, AT&T, and Symantec. Right behind the Leaders are the "Challengers": NTT (Solutionary), BT, HP, and CSC". For CISOs and others deciding on managed security services and MSSPs, it may be valuable to buy the **report** and learn about

vendor strengths and cautions.

Alert: Cyber-shark sighting … MSSP firm Herjavec Group in CSO's Cybersecurity Business Report Blog

- "The Forrester Wave: Managed Security Services: North America", is an evaluation of managed security service providers (MSSPs) including the 13 most significant vendors in the North American market. The vendors include AT&T, CenturyLink, CSC, Dell SecureWorks, HP, IBM, Leidos, SilverSky, Solutionary/NTT, Symantec, Trustwave, Verizon, and Wipro. This **report** details how well each vendor met Forrester's criteria and where they stand in relation to each other, and can be useful to help choose the right partner for outsourced security services.

- International Data Corporation (IDC) Canada has published a new IDC MarketScape research report that comprehensively covers the 12 most prominent Managed Security Service Providers (MSSPs) in the Canadian market. TELUS, IBM, CGI, and Bell earned the distinction of placing in the Leaders category. Dell, Herjavec Group, IPS, Above Security, eSentire, Allstream, Wipro, and Scalar were placed in the Major Players category. The **report** highlights the evolution within the managed security services space while offering valuable guidance for organizations examining domestic security solutions providers.

GOVERNANCE, RISK & COMPLIANCE

Risk consulting shifting from Big Four to cyber consultancies and the cloud.

Sponsored by Cavirin, a leading provider of cloud security and GRC services.

- An alarming finding in a 2015 Ponemon Institute report commissioned by Dell SecureWorks was that 58 percent out of the 1,825 IT security and IT leaders surveyed said they did not think or were unsure if their organization possessed sufficient resources to achieve compliance with security standards and laws.

- Fortune conducted a poll of CEOs at Fortune 500

- Fortune conducted a poll of CEOs at Fortune 500 companies and got dozens of responses when asking them what they thought their greatest threats were, or challenges. The No. 1 response was the pace of technological change. Cybersecurity was the No. 2 response.

- The "2015 Travelers Business Risk Index" identifies computer-related issues as the second concern for all businesses (58 percent), as opposed to 2014 when it was ranked fifth. 70 percent of large businesses now see cyber risk as a major threat, compared with 60 percent of mid-sized businesses, and 45 percent of small businesses.

- The global enterprise governance, risk and compliance (GRC) market is expected to grow from $5.81 billion in 2014 to $11.50 billion by 2019, at a CAGR of 14.6 percent for the period 2014 to 2019, according to MicroMarketMonitor.

- Gartner ranked "Risk based security and self-protection" as a top 10 strategic trend for 2015. Compliance and risk management tasks are a huge burden on corporate resources. Automated tools can save time and money, and reduce the number of staff dedicated to GRC.

- "Significant operational improvements and cost reduction are a direct result of automating security and compliance efforts" says JD Sherry, CEO at **Cavirin** and an industry expert on corporate security. "All organizations, regardless of size are looking for innovative platforms that allow them to automate how they analyze operational risk across their infrastructure without adding significant headcount and resource drain. This includes streamlined GRC solutions that continuously assess operational risk for both the traditional data center as well as public cloud infrastructures."

- "As organizations leverage third parties for growing their business, assessing the compliance/risk of those partners and providers on a continuous basis will be paramount" says JD Sherry, CEO at **Cavirin**, who advises CISOs at corporations globally on risk and compliance. In the end, compliance liability almost always is the

responsibility of the end-user.

- EMC's inaugural "RSA Cybersecurity Poverty Index" that compiled survey results from more than 400 security professionals across 61 countries, states the greatest weakness of the organizations surveyed is the ability to measure, assess and mitigate cybersecurity risk with 45 percent of those surveyed describing their capabilities in this area as "non-existent," or "ad hoc," and only 21 percent reporting that they are mature in this domain.

- A recent survey of more than 1,000 directors at public companies conducted by the National Association of Corporate Directors (NACD) showed more than half (52.1 percent) of directors say they are not satisfied with the quantity of the information provided by management on cybersecurity and IT risk.

- A new report from Source Information Services (Source) has found that the global market for risk consulting has risen by over $1 Billion (9 percent) to just under $14 billion in 2014. The report says that although regulation and compliance work has been the driver of most of the (risk consulting) growth to date, cybersecurity is set to have a significant impact in the near future.

- Big Four firms carry out the majority of global risk consulting, accounting for 61 percent. However, Source warns that they may be set to miss out on the next stage of growth if they don't react to the growing demand for cybersecurity expertise. Dr. Fiona Czerniawska, founder of Source, said: "Big Four firms aren't seen by clients to have the specialist expertise required to capitalize on this wave of increased investment in cyber security. These firms now have a limited window of opportunity to either recruit or acquire organisations with these skills."

SECURITY ANALYTICS

Security analytics market expected to exceed $3 billion by 2018

The FireEye Threat Analytics Platform detects and responds to threats discovered through event and data stream analysis

- The big data and analytics market will reach $125 billion worldwide in 2015, according to research firm IDC. Big data analytics tools will be the first line of defense, combining machine learning, text mining and ontology modeling to provide holistic and integrated security threat prediction, detection, and deterrence and prevention programs, according to recent predictions by The International Institute of Analytics (IIA).

- The global security analytics market will be worth $3.22 Billion by 2018, according to Markets and Markets.

- The North American security analytics market is expected to grow from $835.6 million in 2014 to $1.2 billion + in 2019, at a CAGR of 7.8 percent from 2014 to 2019, according to a report from MicroMarketMonitor.

- MicroMarketMonitor says the security analytics market is expected to grow significantly in the North American region due to the increasing number of security breaches, continued line of sophisticated attacks, and the existence of obsolete cyber defense systems in organizations. Vendors in the security analytics market are constantly innovating and remodeling their existing architecture to develop better and more secure systems.

- By 2016, 25 percent of large global companies will have adopted big data analytics for at least one security or fraud detection use case, according to Gartner.

FireEye ComplImentary REPORT: The Numbers Game: How Many Alerts are too Many to Handle?

- Anton Chuvakin, Research Vice President with Gartner, recently stated “As many organizations continue to struggle with utilizing traditional security tools… the expectation that they will magically adopt security analytics approaches as well as big data technologies is questionable at best — the emerging tools make some tasks easier, but come with their own skill

requirements".

- "A big challenge in the cybersecurity analytics space is sifting through all the vendor hype to find the right tool… since each company has its own unique needs and the market is crowding with new entrants ranging from major tech vendors to startups flush with lots of VC cash to power their marketing spin" says Steve Morgan, Editor-In-Chief of the **Cybersecurity Market Report**. "An even bigger challenge is finding security practitioners who have real-world big data analytics experience in the context of combating cyber-threats. There's a small universe of cyber-pilots who have seen active duty in this space".

- Microsoft will make its Advanced Threat Analytics (ATA) cybersecurity software – based on technology Microsoft acquired when it bought Israeli cybersecurity startup Aorato last year – available starting in August (2015), according to a ZDNet article.

- SAS Institute, the $3 billion plus business analytics software and services company, and the largest independent vendor in the business intelligence market, is a new entrant in the cyber analytics space with its SAS Cybersecurity solution.

APPLICATION SECURITY

Poor software development practices may be the biggest cyber-threat of all

Sponsored by Code Dx, a next-generation security tool used by Software developers, security analysts, security auditors and CISOs to manage software vulnerabilities

- The "Forrester Wave: Application Security Report", which evaluates vendors for security and risk professionals, says many firms have rushed to bring applications online, building out consumer-facing websites, buying commercial off-the-shelf (COTS) products, and developing mobile applications to enable and engage with their customers and partners without thinking about the security of the application itself. As a consequence, businesses are exposing their most

consequence, businesses are exposing their most sensitive corporate and customer data to possible external threats and breaches.

- Bessemer Venture Partners (BVP) – one of the most well respected tech industry venture capital firms – authored a white paper that states application software development is the most critical business function in the early days of most startups today. The paper states "the most important feature of secure development is written and periodic in-person (security) training by your senior developers".. and "the second basic feature of secure development is source code analysis – the automated discovery of vulnerabilities".

- "The SANS Institute 2015 State of Application Security Report" states that many information security engineers don't understand software development—and most software developers don't understand security. Developers and their managers are focused on delivering features and meeting time-to-market expectations, rather than on making sure that software is secure. SANS indicates only a small amount of security testing is done by the development team (21.6 percent) or quality assurance personnel (22.percent) – while the internal security team accounts for most (83.2 percent) of the testing.

- "The security industry is overly-focused on testing and scanning for known vulnerabilities in software after it's been released, and under-focused on poor software development practices that lead to vulnerable applications that hackers can exploit. Application security has to be part of the early stages of the SDLC; not tacked on at the end when finding and fixing the vulnerabilities is far more costly." says Frank Zinghini, CEO of **Applied Visions, Inc.**, a software development company providing innovative solutions in cyber security, business applications, and command and control systems to government and commercial customers worldwide.

- "Many organizations have significant network security in place but it's not enough as 84 percent of all cyber-attacks are happening on the application layer" said Tim Clark, Head of Brand Journalism at SAP, in a recent Forbes blog.

- The U.S. Department of Homeland Security (DHS) states that 90 percent of security incidents result from exploits against defects in software.

- CNET recently reported that programmers are copying security flaws in to your software. Programmers don't write all of their code. They routinely borrow code from others, and they're not checking the code for security flaws. This widespread practice opens the door for hackers to have broad impact with just a few exploits.

Find, prioritize and visualize software vulnerabilities – fast and affordably, with Code Dx

- In a recent CIO Journal, published by the Wall Street Journal, James Kaplan, a partner at McKinsey & Co. and co-author of "Beyond Cybersecurity: Protecting Your Digital Business" said "A far better model (for software development) would be if you were teaching your developers how to write secure code, were including security architects in the development process from day one of the project, and investing in tools for secure development. Then you have many fewer flaws at the end of the process." He added "Most developers have not been trained on secure coding practices."

- "Most software developers and security analysts don't realize that when they run only one application security testing tool, even the best on the market, they miss most of the weaknesses in their code. This is the dirty little secret that is just starting to get out of the bag: no single tool does a very good job" says Anita D'Amico, CEO at **Code Dx**.

- According to a study done by the National Security Agency's (NSA) Center for Assured Software (CAS) the average application security testing tool covers eight of the 13 weakness classes (e.g. buffer handling, file handling, initialization and shutdown, and number handling), which is 61.5 percent. This study also found that the average tool covers only 22 percent of the flaws in each of the 13 weakness classes. If the percentage of the flaws is multiplied by the percentage of weakness classes covered, the total coverage of the average tool is only 14 percent.

- "The NSA study is eye opening for many software developers who have assumed that their vulnerability scanners cover a much larger area" says Ken Prole, CTO at **Code Dx**. "Missing more than 80 percent of the weaknesses in the application code should not be acceptable for any organization."

- According to market researcher ReportsnReports, North America is the largest market for security testing services. Markets and Markets expects this market alone to grow from $2.47 billion in 2014 to $4.96 billion by 2019, at an estimated Compound Annual Growth Rate (CAGR) of 14.9 percent from 2014 to 2019. More than half of respondents to a SANS Institute survey expect spending on application security programs to increase over the next year (more than a quarter expect spending to increase significantly), and only 3 percent expect to spend less.

MOBILE SECURITY

Mobile security market exploding with 30 percent + growth projected through 2019

Sponsored by AVG Technologies (NYSE:AVG), the online security company for devices, data and people.

- The total mobile security market is expected to grow from $1.5+ billion in 2014 to $5.75 billion by 2019, at an estimated Compound Annual Growth Rate (CAGR) of 30.7 percent from 2014 to 2019, according to a report by Markets and Markets.

- According to a 2015 Silicon Valley Bank report, there will be more than 1 billion employee-owned smartphones and tablets in the workplace by 2018.

- According to Gartner, portable, wirelessly-connected consumer devices are everywhere. By 2018, 70 percent of mobile professionals will conduct all of their work on personal smart devices.

- The "PwC 2015 Information Security Breaches Study on UK Corporations" reports that 15 percent of

UK Corporations" reports that 15 percent of organizations suffered from a breach caused by use of a smartphone or tablet device, more than doubling last year's figure of 7 percent.

- The "2015 Alcatel Lucent Motive Security Labs Report" – found that malware infections in mobile devices increased 25 percent in 2014. Android devices have now caught up with Windows laptops, which had been the primary workhorse of cybercrime, with infection rates between Android and Windows devices split 50/50 in 2014.

- According to the "HP 2015 Cyber Risk Report", 97 percent of the mobile applications examined had significant flaws in their security features, leaving user data at risk. The report states "Not only do the same issues that affect web applications impact their mobile counterparts, but mobile applications have the added bonus of also having unique security concerns. 80 percent of mobile applications unintentionally revealed information of potential benefit to malicious attackers. 71 percent stored data in an unsecure manner. 66 percent didn't protect data via encrypted communication or other means. And 31 percent had the potential to reveal geo-location information."

- Malware growth continues to be aided by the fact that a vast majority of mobile device owners do not take proper device security precautions. The Motive Security Labs survey found that 65 percent of subscribers instead expect their service provider to protect both their mobile and home devices.

- According to a recent Ponemon Institute study commissioned by IBM, 40 percent of companies do not scan their mobile apps for cybersecurity vulnerabilities before making them available, creating huge windows of opportunity for data breaches. The average company tests less than half of the mobile apps they build, and 33 percent never test their apps.

- The Ponemon study indicates 50 percent of companies

dedicate zero ($0) budget towards securing the mobile apps they build for customers, who use those apps to enter and upload confidential data including billing and personal identity information.

- Subbu Sthanu, Director of Mobile Security and Application Security at IBM, said the Ponemon study found that 67 percent of large organizations allow their employees to download unverified, personal apps on their work devices, the same phones and tablets that can also access highly confidential customer records and business data.

- Apple is adding security to mobile devices with its new iOS9, adding two-factor authentication for user ID and stronger encryption to ward off hackers.

- "Mobile security spending is trending up rapidly – due in part to the sheer number of new mobile devices entering the market and growing mobile risk awareness from corporate security people" says Steve Morgan, Editor-In-Chief of the **Cybersecurity Market Report**. "But the market is just cracking open and mobile security is only a fraction of the total security spend. Analysts and research firms indicate the real opportunity in mobile security is still ahead of us".

- Gartner has stated that there is a lack of penetration of security tools among users of new mobile platforms, and they do not expect to see new demand for this type of capability to emerge before 2016. Most consumers do not recognize that antivirus is important on mobile devices and therefore have not yet established a consistent practice of buying mobile device endpoint protection software. This purchasing trend and market shift away from PCs will have significant repercussions on the consumer security market. However, as mobile devices gain in mass popularity and as security is likely to be a higher priority from 2017 onward, then new market opportunities are likely to emerge.

DATA BREACH

Only one-third of corporations have a data breach response plan.

Sponsored by DFLabs – Cyber Incidents Under Control

- According to the "2015 Travelers Business Risk Index", 29 percent of all businesses list cyber threats as one of the risks they are least prepared to face. While 53 percent of companies say they review their data security plans and practices, only 33 percent have a cyber or data breach response plan. Larger companies, which worry most about cyber issues, are also the most prepared.

- At least 60 percent of brands will discover a breach of sensitive data in 2015, with the actual number of breached entities being as high as 80 percent or more, according to Forrester's annual predictions research.

- The "PwC 2015 Information Security Breaches Survey of UK corporations" states that nearly 9 out of 10 large organizations surveyed now suffer some form of security breach – suggesting that these incidents are now a near certainty. Staff-related breaches feature notably in the survey. 75 percent of large organizations suffered a staff-related breach; 50 percent of the worst breaches in the year were caused by inadvertent human error, up from 31 percent a year ago.

How to calculate your own custom costs of a data breach – includes direct and indirect costs, and damage depreciation

- According to a World Economic Forum (WEF) report published earlier this year, in the U.S., 47 states have have enacted laws that require security breaches involving personal data to be reported. The European Union and several of its member states have introduced similar regulations.

- Forrester said that most firms will botch the data breach responses, and we'll quickly see million-dollar fines and suits become the norm. Why? Forrester finds that only 21 percent of global security technology decision-makers report that improving incident response is a critical priority.

- Michael Siegel, a Principal Research Scientist at the MIT

Sloan School of Management shared some alarming statistics at the ARC Advisory Group's 19th Annual Industry Forum earlier this year: Over 80 percent of breaches involved systems where security patches had been available for at least one year; 75 percent of breaches go undiscovered for weeks or months; 67 percent of breaches were aided by significant errors from employees of the victimized firm.

CostPerBreach.com

- Out of 1,425 respondents (including 142 CSOs and CISOs), 56 percent have named data breach protection their top security priority, according to a survey conducted by Vanson Bourne on behalf of CA Technologies.

- In a joint Cebr/Veracode survey entitled "Business and Economic Consequences of Inadequate Cybersecurity," more than 200 British C-level executives shared top concerns were breach costs (e.g., forensics, clean-up, legal), reputation and brand damage, and lost revenue due to downtime.

- According to Gartner, Inc., 75 percent of enterprises' information security budgets will be allocated for rapid detection and response approaches by 2020, up from less than 10 percent in 2012. "Breach detection is top of mind for security buyers and the field of security technologies claiming to find breaches or detect advanced attacks is at an all-time noise level," said Eric Ahlm, research director at Gartner.

- "One might assume that once an organization experiences a data breach, the response is to secure defenses to make sure that history does not repeat itself", according to Marsh & McLennan Companies, a $12 billion global professional services firm. "However, an analysis of prior data breaches indicates that the statistical likelihood that an organization will suffer a data breach in the next year actually increases if that organization has previously suffered a breach."

- There's a dramatic difference between two prominent reports on the cost of a data breach: Ponemon Institute says the cost per data breach is $154; Verizon's RISK

Team calculates the cost per breach at 58 cents.

THE COSTS OF A DATA BREACH – Customize your own cost-per-breach formula

- "In the cases of the Verizon and Ponemon estimates, we see two formulas answering the same question (cost-per-breach) yet yielding different results" says Dario Forte, CEO at **DF Labs** and an industry expert on data breach and incident response. "We would rather challenge analysts to approach the problem from a different angle; that is to apply a custom formula to one's own organization or industry".

- **DF Labs** encourages corporations to consider these criteria when assessing total cost-per-breach or per record: Direct Costs + Indirect Costs + Projected "Damage Depreciation" Costs = Total Cost of Breach. For more information on this criteria, go **HERE**. "Indirect costs should vary from industry to industry and company to company, therefore resulting in varying data breach costs specific to one's own organization rather than basing security plans on one global figure" says Dario Forte, CEO at DF Labs.

IOT SECURITY

Multi trillion dollar global Internet of Things market will lift security research and spending through 2025.

Sponsored by Nexusguard, the global leader in DDoS defense – protecting enterprises from malicious internet threats to their sites, services and reputations

- In a McKinsey & Company report 'Unlocking the potential of the Internet of Things', their bottom-up analysis for the applications they size estimates that the IoT has a total potential economic impact of $3.9 trillion to $11.1 trillion a year by 2025. At the top end, that level of value would be equivalent to about 11 percent of the world economy. The report states "with policy actions to encourage interoperability, ensure security, and protect privacy and property rights, the Internet of Things can

begin to reach its full potential."

- The Internet of Things (IoT) Security Market is expected to grow from $6.89 Billion (USD) in 2015 to $28.90 Billion by 2020, according to a new market research report published by Markets and Markets.

- Research and advisory firm Technavio's analysts forecast the global IoT security market to grow at a CAGR of nearly 55 percent over the period 2014-2019.

- Gartner states "The Internet of Things (IoT) is a key enabling technology for digital businesses. Approximately 3.9 billion connected things were in use in 2014 and this figure is expected to rise to 25 billion by 2020. And while deployment is growing, there are factors slowing down the rate of adoption. Security and privacy are among the top key concerns among enterprises. Existing ideas and approaches to identity management will not be entirely effective for the IoT. IAM and other security leaders must rethink and rearchitect to be successful."

- "IoT will increasingly have sensing, analytics and visualization tools that may be accessed on a personal, community or national level. Information sharing and ease of accessibility via the IoT makes businesses vulnerable to targeted cyber attacks, so the huge benefits must be weighed against the growing risks" states EY in its 2015 "Cybersecurity and the Internet of Things" report.

- "By its very design, the Internet of Things is built with lightweight security," explains Terrence Gareau, Chief Scientist, **Nexusguard**. "These devices rely heavily on shared libraries and a rapid development cycle. Because of their constraints, many IoT devices have limited options for firmware upgrades and other risk management features. The fact that they are also "always-online" makes them highly susceptible to intrusion and attacks."

  MORE about IoT security in the "Nexusguard 2015 Internet Security Trend Report"

- According to an HP study, 70 percent of the most

commonly used IoT devices contain vulnerabilities.

- "Computerworld's Forecast Study 2015" predicts spending on security technologies will increase by 46 percent, ahead of all other IT categories, and that Internet of Things (IoT) will be the top new area of spending in 2015.

- By year-end 2017, over 20 percent of businesses will employ digital security services devoted to protecting business initiatives in IoT, according to Gartner research.

- Google is providing Carnegie Mellon University (CMU) $500,000 to launch a project that will turn its campus into a living IoT laboratory – where Internet-connected sensors, gadgets and buildings communicate with each other. A second CMU team will develop technology to further protect the privacy of IoT users. The mission is to fulfill the IoT's promise by creating a complete system of interoperable IoT technology and finding answers to key research questions, such as how to preserve privacy and ensure security in an increasingly sensor-filled environment.

- Spurred by private sector awareness, political turmoil, and cybercrime, Asia-Pacific organizations will spend $22 billion on critical infrastructure technologies by 2020, ABI Research estimates. The lucrative OEM market – which ties Asia-Pacific to electronic manufacturers worldwide – also is an attractive target for hackers and malware creators. And as demand grows for Internet of Things (IoT) solutions, OEM vendor spending on security must increase to meet customers' concerns. After all, more businesses will turn to Asia-Pacific's expanding roster of OEMs and original design manufacturers (ODMs) for partnerships and joint research and development agreements, according to IDC.

WEB SECURITY

Web applications are the weakest point in corporate cyber defense.

Sponsored by ImmuniWeb, the award-winning web application security testing platform providing on-

demand manual penetration testing in parallel with managed vulnerability scanning

- The market for global corporate web security was sized at over $1.7 billion (USD) in 2014, and is anticipated to reach a value of $3.2 billion by 2020, according to a report from Future Market Insights (FMI).

- "Cloud based Web Security solutions are seeing stronger demand" according to the "Corporate Web Security Market 2014-2018 Report" from technology research firm The Radicati Group, Inc.. "Organizations that traditionally deployed on-premises solutions are increasingly moving all their services to the cloud."

- A survey in "The SANS Institute 2015 State of Application Security Report" indicates that public-facing web applications are rated as the major concern by 74 percent of respondents.

- Web application attacks, point-of-sale intrusions, cyber espionage and crimeware were the leading causes of confirmed data breaches last year, according to findings based on data collected by Verizon Enterprise Solutions and 70 other organizations from almost 80,000 security incidents and over 2,000 confirmed data breaches in 61 countries.

Think your website isn't worth anything to hackers? Think again. READ THE STORY

- More than one-quarter — 27 percent — of all security breaches at banks last year involved web app attacks, according to the most recent "Verizon Data Breach Investigations Report". In web app attacks, cybercriminals use a variety of tactics to interfere with web applications.

- A recent InformationWeek / DarkReading article states "According to numerous studies, the preferred method for attacking businesses' online assets is via their Web applications".

- "Web attacks are everybody's scourge," stated Dr. Anton Chuvakin, Research Vice President, Security and Risk Management at Gartner, in a recent Bank Technology

News article. "As the Internet is growing, all sorts of less-skilled programmers are deploying applications. You have fewer security-minded programmers. In five years, we'll all still be talking about web app attacks".

- The "HP 2015 Cyber Risk Report" finds that 86 percent of web applications tested had serious issues with authentication, access control, and confidentiality, an increase over the previous year's rate of 72 percent. The report, which looked at 6,500 web applications, found that 52 percent of them suffered from long-known security issues.

- Researchers from KU Leuven University in Belgium and The State University of New York at Stony Brook recently tested websites "protected" with various trust seals provided by reputable security vendors (including Symantec, McAfee, Trust-Guard, and Qualys) delivering automated vulnerability and malware scanning services. The research showed "that seal providers perform very poorly when it comes to the detection of vulnerabilities on the websites that they certify." This is a weakness inherent in almost all fully-automated solutions – they can only go so far before their output needs to be analyzed by a qualified pentester.

- According to security firm Tripwire, "The mammoth rise in cybercrime has made organizations revise their application security strategy and implement new techniques to safeguard their software. This is largely because traditional security methodologies, such as Manual Testing and Web Application Firewalls (WAF), have been rendered irrelevant due to evolving hacking techniques."

- "Web applications remain the weakest point in corporate cyber defense and they require special attention" says Ilia Kolochenko, founder and CEO at **High Tech Bridge** – a global provider of information security services in the areas of penetration testing, computer forensics, malware analysis and source code review, and provider of **ImmuniWeb**, an on-demand web security testing service provided in partnership with PwC.

GET THE SCOOP on the top mistakes banks make

defending against hackers

- "The SANS Institute 2015 State of Application Security Report" states external security consultants are used by 29.6 percent of organizations, and security-as-a-service providers are used by 15.2 percent of organizations, when asked – who tests application security?

- "We expect the percentage of corporations turning to outside providers for web application scanning to trend way up" says Steve Morgan, Editor-In-Chief of the **Cybersecurity Market Report**. "Web applications have become a security choke point and enterprises can not adequately manage the exploits. They need third parties to help".

- A report by Bessemer Venture Partners (BVP), a multi-national $4 billion venture capital firm, taps cybersecurity as one of three areas within cloud as particularly high growth. Referring to the importance of securing cloud applications – and the potential staggering market impact of not securing them, BVP stated "If Salesforce went down for two days, the whole industry would lose 20 percent off its valuations".

OPEN SOURCE SECURITY

Open source software reaches near 100% adoption by mainstream IT organizations, increases demand for security solutions

Sponsored by Black Duck Software, who helps the world's most innovative companies streamline, safeguard, and manage their use of open source software.

- According to Gartner, 95 percent of all mainstream IT organizations will leverage some element of open source software (OSS) – directly or indirectly – within their mission-critical IT systems in 2015.

- Gartner says that through 2020, security and quality defects publicly attributed to OSS projects will increase significantly, driven by a growing presence within high-profile, mission-critical and mainstream IT workloads.

- The "2015 Future of Open Source Survey" sponsored by **Black Duck Software** and venture capital firm North Bridge reveals 78 percent of companies run on open source, yet many lack formal policies to manage legal and security risks.

  How Small Businesses Can Fend Off Hackers – Black Duck CEO Lou Shipley shares cyber security tips in this WSJ article

- Intruders are increasingly targeting the application stack for exploitation, according to the "Cisco 2015 Annual Security Report". Cisco says the rise of cloud apps and the ubiquity of do-it-yourself (DIY) open-source content management systems (CMS) has created a landscape of vulnerable websites and SaaS offerings. Underlying systems/networking layers managed by IT operations may withstand malicious attacks, but application-level components built by developers are often riddled with vulnerabilities.

- "Attackers have become more proficient at taking advantage of security gaps" says Jason Brvenik, Principal Engineer, Security Business Group, at Cisco. "We observed that 56 percent of all OpenSSL versions still remain vulnerable to Heartbleed". According to Dark Reading, three out of four global 2000 companies are still vulnerable to Heartbleed one year after its discovery.

- The Core Infrastructure Initiative (CII), a project managed by The Linux Foundation that enables technology companies, industry stakeholders and esteemed developers to collaboratively identify and fund critical open source projects in need of assistance, recently announced financial support of nearly $500,000 for three new projects to better support critical security elements of today's global information infrastructure.

- The New Stack recently reported that the Linux Foundation and job board DICE polled 1,010 hiring managers and 3,446 Linux professionals to report on the state of the Linux job market. Their recent annual survey states security vulnerabilities such as the 2014 Heartbleed bug have fueled a need for Linux-savvy

security pros.

- Bill Ledingham, CTO at **Black Duck Software**, says 40 percent of the 8,000 vulnerabilities disclosed last year were in open source projects. The software upon which (it turns out) a whole of organizations depend on is, all too often, insecure. It contains vulnerabilities that may lie dormant for years (and years and years) but upon discovery can have devastating effects due to its expansive use.

- Manufacturing & Logistics IT Magazine recently reported that Stuart J. Mackintosh, who previously supported the UK Cabinet Office on its Open Source and standards strategy, has launched a global crowdfunding campaign to perform a full network security penetration testing of the Odoo ERP open source solution. Such a test would be the first time Odoo, one of the most widely used ERP

VULNERABILITY MANAGEMENT

Heartbleed exploits persist due to sloppy practices in $9 billion security and vulnerability management market.

Sponsored by Digital Defense, Inc., which provides the Vulnerability Management as a Service (VMaaS) to CISOs and InfoSEC teams.

- Vulnerability management is a key area where defenders (internal security teams) and builders (software development teams) must work together to identify and repair serious security vulnerabilities as quickly as possible, according to "The SANS Institute 2015 State of Application Security Report". In their survey, SANS states 26 percent of internal security teams took two to seven days to deploy patches to

critical apps in use, while another 22 percent took eight to 30 days, and 14 percent needed 31 days to three months to deploy patches satisfactorily.

- The SANS Institute report indicates that for nearly half of organizations – vulnerabilities in production apps are patched through quick-and-dirty fixes or other short-term workarounds, such as disabling a feature or function in the app – a very troubling statistic.

- 7,038 new security vulnerabilities were added to the National Vulnerability Database (NVD) database in 2014. That was an average of 19 new vulnerabilities per day. NVD is a federally funded repository of cyber-vulnerability data maintained by the National Institute of Standards and Technology (NIST).

- NVD statistics indicate 24 percent of the vulnerabilities added in 2014 were rated as high severity. Third-party applications were the source of 80 percent of vulnerabilities. Operating systems were responsible for 13 percent of vulnerabilities, and hardware devices for 4 percent. The top 3 operating systems by number of vulnerabilities: Apple Mac OS (147); Apple iOS (127); and Linux Kernel (119). It is interesting to note that Microsoft operating systems are no longer in the top 3. The top 3 applications by number of vulnerabilities were web browsers: Microsoft IE (242); Google Chrome (124); and Mozilla Firefox (117).

Digital Defense's VMaaS – Vulnerability-Management-as-a-Service – unites Security, R&D, and IT Operations teams with patented scanning technology, proprietary project management services, and trademarked assessment scoring methodology to rapidly reveal and remediate security vulnerabilities

- A report by 451 Research states that in some industries, the average time to fix a vulnerability is 176 days. As a result, the window of opportunity for hackers remains wide open.

- "Heartbleed was a landmark and catastrophic security bug that corporate security managers got stung by, and the entire IT community is now intimately familiar with — and surprisingly (or maybe not so surprisingly) there

are still a lot of unprotected web servers at risk of further exploit by Heartbleed." says Steve Morgan, Editor-In-Chief of the **Cybersecurity Market Report**.

- OpenSSL is used by over 60 percent of websites worldwide to encrypt personal data, according to **Digital Defense, Inc. (DDI)**, a leading provider of vulnerability management solutions to corporations globally. Michael Cotton, Vice President, Research and Development for DDI says "the SSL Heartbleed flaw was a 'once-a-decade' critical security flaw that will have a lasting impact for years to come. Because OpenSSL is so widely used in various software and hardware applications, nearly all organizations were (and still may be) impacted in some way."

- The "Cisco 2015 Annual Security Report" contains results from the "Cisco Security Capabilities Benchmark Study", which surveyed Chief Information Security Officers (CISOs) and Security Operations (SecOps) executives at 1,700 companies in nine countries, and revealed that 56 percent of all installed OpenSSL versions are still over four years old. This startling data indicates that many corporations remain vulnerable to Heartbleed.

- The security and vulnerability management market is forecast to be worth over $9 billion USD by 2019, at a CAGR of 10.7 percent during the forecast period, according to Markets and Markets.

OSINT / CYBER INTELLIGENCE

Open source intelligence is a "must-have" solution for corporate security staffs.

Sponsored by Silobreaker, provider of cyber threat intelligence solutions for CSOs, CISOs, cyber-responders, C-level executives, and corporate stakeholders.

- The threat intelligence security market size is expected to grow from $3 billion in 2015 to $5.8 billion + by 2020, at a Compound Annual Growth Rate (CAGR) of 14.3 percent from 2015 to 2020, according to Research and Markets.

- According to research from IDC, worldwide threat

- According to research from IDC, worldwide threat intelligence security services spending will increase from $905.5 million in 2014 to more than $1.4 billion in 2018.

- "Dark Reading's 2014 Threat Intelligence Survey" reveals that 66 percent of respondents say they use threat intelligence regularly to guide IT security strategies, with 60 percent of those security pros saying it plays a vital role, even shaping their entire security strategies.

- Forrester Research states that Investors are eager to capitalize on the strong demand for CTI solutions and services: Since October 2014, Cyberthreat Intelligence (CTI) vendors have raised $102.5 million (USD), and there have been three acquisitions. The vendor landscape is overwhelming, and security and risk pros must separate fact from hype when it comes to investing in CTI offerings, according to Forrester.

Why cyber should not be limited to cyber – a 'must read' for CIOs and CISOs

- By 2017, 75 percent of large enterprises will receive custom threat intelligence information tailored to their industry, company, brand, and environment, according to IDC.

- Samuel Culpepper III, a former U.S. military and contract intelligence analyst, a combat veteran, and executive editor of Forward Observer Magazine, summed up OSINT in a Guerillamerica blog post stating "Open Source Intelligence (OSINT) information makes up 80-90 percent of all intelligence information because there are so many sources and collectors. Every website, news report, magazine article, and speech produces OSINT information. A good intelligence analyst doesn't have to know everything, he just has to know where to find it. The entire internet is our intelligence repository."

- "As intelligence agencies spend billions of dollars on covert programs that sweep up private data, they're neglecting … open-source research… some former intelligence officials say" according to an article in the Pittsburgh Times. "Some answers that spies hunt are broadcast on blogs, not stashed on hidden flash drives".

- "A good OSINT platform used by skilled cybersecurity

analysts is a must-have solution for corporate enterprises who need to defend themselves against against a growing community of cyber outlaws and evildoers" says Steve Morgan, Editor-In-Chief of the **Cybersecurity Market Report**. "An OSINT app will cull data from blogs, newsfeeds, social media, and even temporary websites on the dark web… and the OSINT app will also keep up on new data sources. CISOs should not be asking "Why use OSINT?" They should be asking "Why NOT use OSINT?" If a corporate IT staff is not using OSINT directly, then they should be using a commercial cyber threat intelligence platform that does."

- "Many emerging intelligence needs are not addressed by the offerings of the traditional IT security industry. Assessing a company's reputation and how it may prompt attacks, understanding the motivations and beliefs of a threat actor, and discovering how a geopolitical event triggers the use of a new attack type promoted on social media all require access to and analysis of non-technical data that IT or product companies don't provide. There is a full spectrum of information that is being overlooked. Making sense of data from publicly available sources is as relevant for cyber security as it is for other purposes but can only be managed effectively with the right tools and processes" said Kristofer Mansson, **Silobreaker** CEO.

- The dark web – which is not indexed by search engines – is a cybercriminal hangout. Some OSINT tools can help keep an eye on the hackers-for-hire, spam and phishing campaigns-for-hire, malware and vulnerabilities-for-sale, stolen intellectual property, cyber investigators-for-hire (competitors who could be watching you), cyber insiders-for-hire (perhaps even inside your own company), hacktivist forums that talk about things like new DDoS attacks about to launch, and more.

- Strategic cyber intelligence will play a crucial role in defending private companies and government sectors by providing the necessary intelligence to prevent potential incidents that could cripple our security as well as our economy, according to the Intelligence and National Security Alliance (INSA) Cyber Intelligence Task Force.

BANKING

Banking and financial services is fastest growing non-government cybersecurity market

Sponsored by Easy Solutions, a security provider focused on the comprehensive detection and prevention of electronic fraud across all devices, channels, and clouds

- According to the "Banking & Financial Services Cybersecurity: U.S. Market 2015-2020 Report", published by Homeland Security Research Corp. (HSRC), the 2015 U.S. financial services cybersecurity market will reach $9.5 billion, making it the largest non-government cybersecurity market. In addition, the report concludes that this market will be the fastest growing non-government cybersecurity market, exceeding $77 billion in cumulative 2015-2020 revenues.

- Consulting firm PwC stated that financial services companies will increase their cybersecurity spending by $2 billion over the next two years. PwC surveyed 758 banks, insurers, and other financial services companies, and stated they collectively spent $4.1 billion on cybersecurity in 2014.

- In a recent live on-air interview from Davos Switzerland on Bloomberg's Market Makers, Bank of America Corp. CEO Brian Moynihan said the nation's second largest lender will spend $400 million on cybersecurity this year… and it is the first time in 20 years of corporate budgeting he has overseen a business unit with no budget. Moynihan said the only place in the company that doesn't have a budget constraint is cybersecurity.

- The Wall Street Journal recently reported that J.P. Morgan Chase & Co. is going to accelerate its timeline for a cybersecurity spending boost – and the bank expects cybersecurity spending to double to $500 million in 2016. In an earlier article, WSJ reported that Citigroup Inc.'s annual cybersecurity budget has risen to more than $300 million, and Wells Fargo spends roughly $250 million annually on cybersecurity.

- A recent article in Infosecurity Magazine stated that financial services firms are hit by security incidents a

  staggering 300 times more frequently than businesses in other industries.

  The online activities of more than 75 million users from over 280 leading financial services companies and banks, security firms, retailers, airlines and other entities in the U.S. and abroad are protected by Easy Solutions fraud prevention systems

- Deloitte states that the financial services sector faces the greatest economic risk related to cybersecurity. In the "Deloitte 2015 Banking Outlook", they say to improve cybersecurity in 2015, banks will be forced to devote greater resources to enhancing the security, vigilance, and resilience of their cybersecurity model and should consider: Adopting new methods, such as war gaming, attracting specialized talent, and increasing collaboration with other members of the ecosystem; Beefing up their intelligence apparatus to detect new threats in a timely manner; Expanding the role of the CISO to include clear and prompt communications with the board.

- The Wall Street Journal reported that in his testimony at a congressional hearing recently, Frank Cilluffo, Director of the Center for Cyber and Homeland Security at George Washington University, cited figures that he said were provided to him recently by a major, unnamed U.S. bank. He said that in just the last week (at that time), this firm had faced 30,000 cyberattacks. "This amounts to an attack every 34 seconds, each and every day," Mr. Cilluffo said. He added that about 22,000 of them came from criminal organizations and about 400 from nation-states.

- The biggest security threats to banks last year were web app tampering, distributed denial-of-service attacks, and the increased use of payment card skimmers, according to "Verizon's Data Breach Investigations Report". These three categories of attacks made up three-quarters of security incidents targeting banks.

- According to the "Semiannual Risk Perspective from the

National Risk Committee", published in Spring 2015 by the Office of the Comptroller of the Currency (OCC) in Washington, D.C., operational risk is high as banks adapt business models, transform technology and operating processes, and respond to increasing cyber threats. Banks may not incorporate resiliency considerations, including recovery from cyber events, into their overall governance, risk management, or strategic planning processes, increasing their vulnerability (to cyber-attacks). Banks and their employees, customers, and third-party service providers continue to be vulnerable to cyber attacks that can compromise data or systems or allow criminals to illegally obtain personally identifiable information.

- According to the "2015 Travelers Business Risk Index", published by The Travelers Companies, Inc.: Cyber risks are the top concern in the banking and financial services sector; 80 percent of these business leaders say they are worried about this risk; This is far ahead of the 58 percent average across all other sectors; The industry has addressed risks with written business continuity plans (78 percent), data security review procedures (68 percent), and data breach response plans (63 percent).

Fraud Intelligence for Bank CISOs and IT Security Staff

- The Depository Trust & Clearing Corporation (DTCC) recently announced that almost half of the respondents (46 percent) in its most recent "Systemic Risk Barometer Study" cited cyber security as their top concern and 80 percent of respondents rated it as a top 5 risk overall. The cyber security rating has almost doubled in just one year as security incidents continue to rise across the financial markets, with specific respondent feedback citing the growth in the "frequency and sophistication of cyber attacks".

- The Federal Financial Institutions Examination Council (FFIEC), on behalf of its members, has issued a Cybersecurity Assessment Tool that institutions may use to evaluate their risks and cybersecurity preparedness. The Office of the Comptroller of the Currency (OCC) examiners will gradually incorporate the Assessment into examinations of national banks, federal savings

associations, and federal branches and agencies (collectively, banks) of all sizes. The Assessment helps banks and examiners determine a bank's inherent risk profile and level of cybersecurity preparedness.

- JD Supra recently reported that with data breaches and cyber crime on the rise, the FFIEC has made cybersecurity a top priority. The Cybersecurity Self-Assessment Tool is just one piece of the cybersecurity puzzle being considered by the FFIEC in the wake of a survey conducted last year on more than 500 institutions to assess their current data security practices. Based on those findings, the FFIEC and its member regulators are also working on incident analysis, crisis management, training and policy development with respect to cybersecurity preparedness, as well as improvements in the area of collaborations with other agencies to communicate the importance of and best practices for cybersecurity.

FEDERAL SECTOR

U.S. Federal Government has spent $100 billion on cybersecurity over the past decade, $14 billion budgeted for 2016.

- With a cumulative market valued at $65.5 billion (2015 – 2020), the U.S. Federal Cybersecurity market will grow steadily at about 6.2 percent CAGR, according to a report from Market Research Media, Ltd. The report states "the annual cyber security spending of the US Federal government is bigger than any national cyber security market, exceeding at least twofold the largest cybersecurity spending countries."

- Demand for vendor-furnished information security products and services by the U.S. federal government will increase from $7.8 billion in FY 2014 to $10.0 billion in 2019 at a compound annual growth rate (CAGR) of 5.2 percent, according to "Deltek's Federal Information

Security Market Report" (published Oct. 2014) – which examines the trends and drivers shaping the federal information security marketplace and provides a forecast for the next five years.

- "Federal agencies have spent more on cyber security than the entire GDP of North Korea, who some have speculated is to be involved with some of this cyber attacks," said Senator Thomas. L. Carper. "The issue of Cyber Warfare is not science fiction anymore. It's reality."

- In an effort to combat the growing threat of cybercrime, the U.S. Department of Homeland Security (DHS) increased its cyber security budget 500 percent during the past two years; and President Obama included $14 billion for cyber security spending in his 2016 budget, according to GCN.

- In an effort to help replace the password as our primary means of security online – through the National Strategy for Trusted Identities in Cyberspace – the U.S. Government has invested more than $50 million over the past four years to advance the Multi-Factor Authentication market in partnership with the research and development community and technology firms.

- President Obama issued an executive order on April 1, 2015, declaring "the increasing prevalence and severity of malicious cyber-enabled activities… constitute an unusual and extraordinary threat to the national security, foreign policy and economy of the United States. I hereby declare a national emergency to deal with this threat."

- TIME recently reported that the U.S. Director of National Intelligence ranks cyber crime as the No. 1 national security threat, ahead of terrorism, espionage and weapons of mass destruction. The TIME article said the federal government suffered a staggering 61,000 cyber-security breaches last year alone.

- The recent hack on the U.S. Office of Personnel Management exposed the records of up to 20 million current and former government employees, some dating back to 1985. Compromised data includes Social

Security numbers, job assignments and performance evaluations, background check and fingerprint information. In the aftermath of the breach, the Agency Director stepped down.

- Reuters recently reported that nearly every U.S. weapons program tested in fiscal 2014 showed "significant vulnerabilities" to cyber attacks, including misconfigured, unpatched and outdated software, according to the Pentagon's chief weapons tester in his annual report.

- The National Law Review reports that as part of a series of cyber security bills enacted last year, Congress passed the DHS Cybersecurity Workforce Recruitment and Retention Act of 2014. The law is intended to help the Department of Homeland Security (DHS) recruit and retain cybersecurity professionals. For DHS, which is responsible for securing civilian government computer systems, a top-flight and expertly trained cybersecurity workforce is an absolute necessity to carry out its security mission.

- Earlier this year The White House announced it will establish a new Cyber Threat Intelligence Integration Center, or CTIIC, under the auspices of the Director of National Intelligence. Currently, no single government entity is responsible for producing coordinated cyber threat assessments, ensuring that information is shared rapidly among existing Cyber Centers and other elements within the government, and supporting the work of operators and policymakers with timely intelligence about the latest cyber threats and threat actors. The CTIIC is intended to fill these gaps.

- To keep pace with training demands of the Army's growing cyber force, the U.S. Army Communications-Electronics Command, or CECOM, is standing up a new training range to help Soldiers validate their cyber security skills. CECOM's Logistics and Readiness Center Cyber Battlefield Range, expected to open in summer 2015, is part of a larger training program designed to re-invest in Soldiers and enhance the cyber security skills

of the Army's digital warriors.

- The U.S. Federal Financial Institutions Examination Council has recently mandated that its members formulate contingency plans to address the threat of DDoS attacks – which have become a key weapon of choice for cyber-criminals – according to **Nexusguard**, a leading cybersecurity firm whose customers include Federal agencies and commercial enterprises.

- A recent article in the National Law Review states "the devastating attacks, ongoing risks, and intense government focus on cybersecurity are expected to create ample opportunities for skilled and experienced cybersecurity professionals to work as contractors for DHS and other government agencies. In addition, the government's need for specialized systems will continue to present enviable opportunities for qualified cybersecurity experts to provide their services and expert advice. For example, the government recently announced that $98 million in contracts were being awarded for work on the U.S. Air Force's network defense and enemy cyber deception."

- At the RSA Conference in April, the U.S. Department of Homeland Security (DHS) announced they are opening a Silicon Valley office. According to a recent Fortune article, the office is a bid to improve relations between tech companies and the government, spread the government's ideology on cybersecurity throughout the tech industry, and recruit top talent that might otherwise head to the private sector.

- A recent San Jose Mercury News story signaled Silicon Valley's importance in cyberwarfare stating "In one of the most overt displays of the federal government's growing dependence on Silicon Valley, the Department of Defense late last month announced it will start providing venture capital funding to valley startups that can help the Pentagon develop more advanced cybersecurity and intelligence systems to fend off nation states and hackers targeting everything from top-secret military correspondence to public power grids."

- "Over the past decade, in the United States alone, more than $100 billion has been spent on cyber-security at

the federal level" according to a recent contribution to The Mantle by Benjamin Dean, a Fellow for Cybersecurity and Internet Governance at Columbia University. "This spending has been justified by the need to bolster defenses against an amorphous set of cyber-criminals and cyber-attackers. Following the money tells a story of why cybersecurity has not improved, despite so much investment over the past two decades. Rather than defense, a significant proportion of these funds have actually been used to develop sophisticated offensive cyber-capabilities, in other words, state-sponsored hacking."

PROFESSIONAL SERVICES

A new breed of pure-play cybersecurity professional services firms emerges

Sponsored by root9B, provider of the The Adversary Pursuit Center (APC) – a manned information security operations center, providing clients 24/7/365 remote computer network defense

- Deloitte recently stated the market for information security consulting grew by 8.1 percent to $15.3 billion in 2014, from $14.2 billion in 2013, citing Gartner research that analyzes and publishes its market share and rankings for the previous calendar year across all security-related capabilities.

- Gartner has stated 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 to enhance their security postures.

- In an interview recorded at the 2015 RSA Conference, Cisco Security Services SVP Bryan Palma told SearchSecurity "If you look at what's happening in the services market, it grows twice as fast as the security product market. It's bigger than the security product market."

- According to research from International Data Corporation (IDC), worldwide threat intelligence security services (TISS) spending will increase from $905.5

services (TISS) spending will increase from $905.5 million in 2014 to more than $1.4 billion in 2018. The TISS market is made up of several distinct facets,

including data feeds and publications, consulting security services, and managed security services (MSS). IDC has expanded its definition of the intelligence security services market to include what it calls iterative intelligence. This iterative process learns from past experiences and mistakes, and incorporates this new knowledge at a more rapid pace, which often results in better long-term solutions.

MANNED INFORMATION SECURITY – We send specialized cyber operators into your network to hunt for and stop the intruders your existing solutions are no match for

- The "2015 PwC US State of Cybercrime Survey" asked whether organizations have the expertise to address cyber-risks associated with implementation of new technologies, only 26 percent said they have capable personnel on staff. Most rely on a combination of internal and external expertise to address cyber-risks of new solutions.

- "We expect to see a new breed of cybersecurity professional services firms emerge over the next two years, driven by rising cybercrime, new types of cyber-threats, and a severe cybersecurity labor shortage" says Steve Morgan, Editor-In-Chief of the **Cybersecurity Market Report**. "We anticipate new entrants around micro-specializations in fields like proactive adversarial pursuit services and other niches. The companies who are first to market in these categories have an opportunity to differentiate themselves and win big contracts during the early stages of market development. First movers will even define some of the cybersecurity specialty service market categories."

- "The average network compromise goes undetected for more than 200 days" says Eric Hipkins, CEO of **root9B**. "The cyber threat requires a proactive manned information security solution, providing superiorly trained and equipped defenders to focus on active defense and adversary pursuit" adds Hipkins.

EDUCATION & TRAINING

Billion dollar plus security awareness training market driven by factors including breaches tied to employees.

Sponsored by Digital Defense, Inc., which provides the SecureED security awareness training program that educates employees on how to fend off attacks that target human vulnerabilities.

- Gartner, Inc. research Vice President Andrew Wells said the security awareness training market exceeds $1 billion in annual revenue (globally), it is growing approximately 13 percent year, and CISOs are increasingly turning to educational security awareness solutions to help improve organizational compliance, expand security knowledge and change poor security behaviors.

- The "PwC 2015 US State of Cybercrime Survey" states that employee training and awareness continues to be a critical—and often neglected—component of cybersecurity. Only half (50 percent) of survey respondents said they conduct periodic security awareness and training programs, and the same number offer security training for new employees.

- More than 800 IT security officials—representing U.S. and European companies and organizations with at least 500 employees—responded to a 2015 survey by the CyberEdge Group. Survey respondents said employees are to blame for breaches, and ranked "low security awareness among employees" as the No. 1 reason why their companies and organizations were unable to defend against cyber threats.

Most security education programs lack the "Stickiness Factor" required for effective retention of key security principles by all employees, putting organizations at increased risk for security breaches. MORE

- The PCI Security Standards Council states that one of

the biggest risks to an organization's information security is often the action or inaction by employees that can lead to security incidents.

- Market growth is driving many new local, national and global entrants with a variety of programs and approaches to security awareness training. **Digital Defense, Inc.** (DDI) is helping companies protect vital business data with **SecurED**, an engaging training program that delivers expert information – with a dash of humor to make it fun and memorable – dramatically strengthening employee awareness and building a culture of security.

- "Employees who do not understand their responsibility in safeguarding confidential and sensitive information are putting their company at great risk" stated Dr. Larry Ponemon, Chairman and Founder of Ponemon Institute, in a commissioned study by Digital Defense. "As revealed in this research, quality security training programs that are relevant and engaging can make a tremendous difference in reducing the threat and likelihood of a data breach."

- A community reminder from **Digital Defense**: Every October since 2004, **National Cyber Security Awareness Month**—administered by the Department of Homeland Security (DHS)—reminds us of the importance of protecting not only our individual identities, finances, and privacy but also our country's national security, critical infrastructure, and economy. Cyber security is a responsibility shared by all—the public sector, the private sector, and the general public.

ISRAELI MARKET

Israel is second only to the United States as the largest exporter of cyber products.

Gartner Israel is a Gartner, Inc. Company – the largest global information technology (IT) research and advisory company.

- Israeli companies exported some $6 billion (USD) in cyber-related products and services last year, a peak figure which surpasses the amount of Israeli defense contracts signed in 2014, according to the Cybersecurity

contracts signed in 2014, according to the Cybersecurity Review, which is published by Delta Business Media in London. The latest data from Israel's National Cyber

Bureau (NCB) shows a surge in cyber exports from $3 billion (USD) in 2013 to $6 billion last year. According to NCB, that constitutes about 10 percent of the global cyber market.

- Globes Online, an Israeli business news media property, reported that figures collected by the Israel Export and International Cooperation Institute show that over 200 cyber security companies are operating in Israel in a field that is growing at 8 percent a year. Their main market is the U.S., and most of the technologies exported there are designed to protect government, military, and financial infrastructure, in addition to protection of strategic facilities.

- Eviatar Matania, Head of the Israeli National Cyber Bureau in the Prime Minister office of Israel, was at the U.S. Chamber of Commerce speaking to The Wall Street Journal about the future of cyber security, where he said investors have poured $500 million into Israeli cyber security startups in the past few years.

- "The Israeli cybersecurity market is a very exciting and dynamic market with hundreds of cybersecurity startups—and new ones crop up every quarter" says Nancy Shapira-Aronovic, Business Development Manager with **Gartner Israel**, which works with startups in different stages from seed to IPO and connects them with Gartner security analysts – to help them gain exposure to the global security market, and to get input on their go-to-market and product strategies.

There were 8 Israeli Security Vendors recognized as "Cool Vendors" by Gartner

- There were 16 Israeli companies listed on the Q2 2015 **Cybersecurity 500** list of the world's hottest and most innovative cybersecurity companies, which is published by Cybersecurity Ventures. More are expected to be added in Q3 and Q4 2015.

- In a recent VentureBeat article, Jerusalem Venture Partners (JVP) stated that the last couple of years have

demonstrated that significant public companies are being created in the cyber-security space in Israel, from Imperva to Varonis to the most successful Israeli IPO of 2014 – CyberArk.

- Glilot Capital Partners, an Israel-based venture capital fund investing in early-stage cybersecurity and enterprise software start-ups, recently announced the successful closing of a $77 million fund. “The fund places a strong focus on “rule-breaking” companies in the cyber-security and enterprise software spaces, with a lean expense structure and a rapid time-to-market.

- “Based on our research, more than 150 cyber security companies were founded in Israel since 2012,” stated Yoav Leitersdorf, Managing Partner at YL Ventures, a San Francisco-based venture capital firm that is focused on cyber security and invests primarily in Israeli companies, in a press release from The California Israel Chamber of Commerce (CICC).

- “The increased activity in the M&A of Israeli cyber security companies has shown the technological competitiveness of Israel in the hyper growth security market. We believe this is only the beginning and we will see large substantial cyber security companies emerge out of Israel” stated Ronen Nir, General Partner at Carmel Ventures, in a press release from CICC.

- Microsoft (Redmond, Wash.) has signed a letter of intent to acquire Israeli cloud security firm Adallom for $320 million cash, according to The Wall Street Journal.

- The California Israel Chamber of Commerce (CICC) announced that more than 40 cyber security companies from the Israeli high-tech hotbed – a record number of companies from Israel – were showcasing their technology at the RSA Conference 2015, held earlier this year in San Francisco.

- Cyberweek (held last month) and **CyberTech** (Jan 26-27, 2016) are the nation’s two major cybersecurity events held annually which have significant international participation, according to Nancy Shapira-Aronovic, Business Development Manager with **Gartner Israel**.

THE CYBERSECURITY 500

Breaking news from the world's hottest and most innovative cybersecurity companies.

Menlo Park, Calif. – Mon. Aug 3, 2015 – Announcing the Q3 2015 Edition of the Cybersecurity 500 list of the world's hottest and most innovative cybersecurity companies

- **Easy Solutions** (Doral, Fla.), No. 5 on the Cybersecurity 500 and a security provider focused on the comprehensive detection and prevention of electronic fraud across all devices, channels and clouds, recently announced the availability of the Easy Solutions Customer Portal, designed to bring together the power of threat detection, malware management and attack takedown all within a single, unified view. For the first time, external threat management and anti-fraud teams can visualize the current threat environment facing millions of end-users, track incidents and manage takedown of those all within a single workflow.

- **AVG Technologies** (Amsterdam, The Netherlands), No. 6 on the Cybersecurity 500 and the online security company for more than 200 million monthly active users, announced the establishment of its global Center of Excellence for mobile in Tel Aviv, Israel. The new office comprises a 3,200 square meter facility, supporting more than 120 employees working across state-of-the-art mobile innovation, emerging mobile threats research, and Internet of Things technology development.

- **Code Dx, Inc.** (Northport, N.Y.), No. 15 on the Cybersecurity 500 and a provider of a robust suite of fast and affordable tools that help software developers and security analysts find, prioritize and visualize software vulnerabilities, announced the addition of CM-Logic to its reseller program. CM-Logic, a United Kingdom-based consulting firm with strong expertise in the software development lifecycle, will expand Code Dx's market presence to the European market.

- **DF Labs** (Lombardy, Italy), No. 17 on the Cybersecurity

DFLabs (Lombardy, Italy), No. 47 on the Cybersecurity 500 and a leading data breach and incident response firm, has added three new Fortune 500 corporations to its client portfolio. DFLabs' new customers are comprised of top-tier firms within the Retail, Oil and Gas, and Financial Services industries.

- **Cavirin** (Santa Clara, Calif.), No. 20 on the Cybersecurity 500, announced their Automated Risk Assessment Platform (ARAP) just became the first platform to earn an Adaptive Compliance PCI Continuous Compliance Certification. As IT and Information Security audits are becoming the new norm, now more than ever before organizations are scrambling to stay compliant. In response to that growing need, ARAP helps companies pass their PCI audits and protect themselves from a catastrophic security breach, as well as avoid the financial penalty costs associated with a failure to pass their audit.

- **Black Duck Software** (Burlington, Mass.), No. 38 on the Cybersecurity 500 and a leader in securing and managing open source software, launched a broader, multi-faceted Global Partner Program, which will see the company's footprint expand further across EMEA. The U.S.-based company has named successful channel architect Kevin Bland as Director of Channels and Alliances to build an ecosystem of strategic partners with complementary products and services.

PwC and High-Tech Bridge launch innovative web security solution

- **Nexusguard** (San Francisco, Calif.), No. 24 on the Cybersecurity 500 and the worldwide leader in Distributed Denial of Service (DDoS) security solutions, announced they were included in The Forrester Wave: DDoS Services Providers, Q3 2015 report. The report presents analysis and scoring of multiple DDoS industry vendors.

- **root9B** (Colorado Springs, Colo.), No. 45 on the Cybersecurity 500, announced a first-of-its-kind adversary pursuit center (APC). The APC will serve as the nerve center of root9B's manned cyber security HUNT operations, creating an always-on environment where

highly-trained security operators will actively monitor client's proprietary networks, searching for malicious activity and closing the response gap from nearly a year to just a few days.

- **Digital Defense, Inc.** (San Antonio, Texas), No. 46 on the Cybersecurity 500 and a leading provider of security risk assessments, awareness education and security intelligence has been named as one of the 20 Most Promising Cyber Security Solutions for 2015 by CIOReview.

- **DB Neworks** (Carlsbad, Calif.), No. 47 on the Cybersecurity 500 and a leading database security company, was honored as The Best Data Center Security Product winner in the 3rd Annual 2015 Cyber Defense Magazine Awards.

- **High-Tech Bridge** (Geneva, Switzerland), No. 65 on the Cybersecurity 500, and PricewaterhouseCoopers (PwC) Switzerland have announced a joint business relationship to bring a new and innovative set of web application security services to their clients. The joint business relationship will provide clients with access to High-Tech Bridge's innovative **ImmuniWeb** application security testing service as part of PwC's market leading Threat and Vulnerability Management services. In other news, High-Tech Bridge announced they have opened a U.S. office in San Francisco.

- **Morphick** (Cincinnati, Ohio), No. 70 on the Cybersecurity 500, was formed out of Cincinnati Bell's fast-growing cybersecurity business earlier this year. Brian Minick, CEO, started up the new business and hired 30 people from Bell to hit the ground running. Minick was previously chief information security officer (CISO) for GE's aviation, energy and transportation units.

- **Coalfire** (Louisville, Colo.), No. 74 on the Cybersecurity 500, announced that it has completed the independent assessment of the Virtustream Federal Cloud under the Federal Risk and Authorization Management Program (FedRAMP). Virtustream, the enterprise-class cloud software and services provider, received their Provisional Authority to Operate (P-ATO) from the Joint Authorization Board for the Federal Risk and

Authorization Management Program (FedRAMP).

- **BRI – Business Risk Intelligence** (Nordrhein-Westfalen, Germany), No. 85 on the Cybersecurity 500 and a leading risk intelligence provider, was listed as one of the top 10 hottest European cybersecurity firms in Channelnomics, which featured an analysis of the world's hottest and most innovative cybersecurity companies as reported by Cybersecurity Ventures.

- **Silobreaker** (London, United Kingdom), No. 132 on the Cybersecurity 500 and a leading provider of OSINT and cyber intelligence tools wins the Excellence Award for Best Newcomer Security Company of the Year at SC Magazine Awards Europe 2015.

VENTURE CAPITAL

VC firms invest over $1 billion into cybersecurity startups during the first half of 2015.

Join the Cybersecurity Ventures mailing list to stay on the cutting edge

- Globally, venture-backed cybersecurity companies raised $1.9 billion last year, a record, according to Dow Jones VentureSource.

- CB Insights reported that in the first half of 2015, venture firms invested $1.2 billion into cybersecurity startups.

- Google Capital, Google's growth equity fund, made its first cybersecurity investment into Crowdstrike, leading a $100 million round.

The Wall Street Journal Venture Capital Dispatch reported Allegis Capital has closed on $100 million toward a new fund that will emphasize investments in cybersecurity startups

- Venky Ganesan, Managing Director at Menlo Ventures, told The Wall Street Journal that in 2011 Menlo directed about 5 percent of a $400 million fund toward security

startups, and its current fund has dedicated about 20 percent to the field.

- Factor Advisors LLC, a subsidiary of the ETF Managers Group LLC, the Advisor and Manager to the PureFunds ISE Cyber Security ETF (NYSE: HACK), announced that HACK has been recognized as the Most Innovative ETF of 2014 at the Capital Link Annual Closed -End Fund & ETP Awards. HACK ETF is the first exchange - traded fund to provide specific exposure to the cyber security sector by using a passive, index approach to provide investment results, before fees and expenses, that correspond generally to the ISE Cyber Security Index.

- **Allegis Capital**, a leading seed and early stage venture capital investor in companies building disruptive and innovative cybersecurity solutions for the global digital economy, has raised a $100 million fund to back cybersecurity startups. “There is a substantial need for new and promising cyber security startups and a huge investment opportunity in them” said Allegis Founder and Managing Director Robert Ackerman.

MERGERS & ACQUISITIONS

Recent Cybersecurity M&A Activity

Read CSO’s Cybersecurity Business Report Blog

- Auxilio, Inc (Mission Viejo, Calif.), a leading provider of Information Security Services for the healthcare industry, acquires Redspin, Inc., a penetration testing firm. The Carpinteria, Calif.-based company will be integrated into Auxilio’s Security Solutions Group.

- AVG Technologies (Amsterdam, The Netherlands), the online security company for more than 200 million monthly active users, acquires Privax, a leading global provider of desktop and mobile privacy services for consumers. AVG will add Privax’sHMA! Pro VPN to its existing portfolio of security software and services that will be immediately made available to AVG’s global customer base. Privax has more than 250,000 paying subscribers worldwide using its VPN encryption service, while its popular free web-based browser proxy service regularly attracts a global audience of over eight million

unique visitors per month.

- Baidu (Beijing, China), the Chinese web giant, acquires online security startup Anquanbao for an undisclosed sum, according to QQ Tech. Anquanbao, also based in Beijing, is a cloud-based protection service that guards websites from malware and distributed-denial-of-service attacks.

- Blue Coat Systems, Inc. (Sunnyvale, Calif.), a market leader in enterprise security, acquires Perspecsys, Inc., a leader in enterprise cloud data protection solutions. With this acquisition, Blue Coat significantly expands its cloud security offerings while enhancing the industry's most robust hybrid cloud portfolio.

- Check Point Software Technologies Ltd. (San Carlos, Calif.), the largest pure-play security vendor globally, acquires Lacoon Mobile Security. Lacoon is leading the industry in providing a solution to secure the entire mobile device, with the best advanced threat catch-rate for enterprise-grade mobile security platforms. Lacoon was founded in 2011 by experts from the mobile cyber security and defense industries with R&D operations in Tel Aviv, Israel and a sales team in San Francisco, Calif.

AVG Acquires PriVax, a Global Leader in Personal Privacy…

- CipherCloud (San Jose, Calif.), a leader in cloud security, expands its platform through the acquisition of core technology from Anicut Systems, a privately held provider of adaptive security as a service. This acquisition complements the company's commitment to delivering a holistic cloud security platform that enables enterprise cloud adoption. The transaction has closed. Financial terms of the acquisition are undisclosed.

- Cisco (San Jose, Calif.) acquires OpenDNS, a privately held security company based in San Francisco. OpenDNS provides advanced threat protection for any device, anywhere, anytime. The acquisition will boost Cisco's Security Everywhere approach by adding broad visibility and threat intelligence from the OpenDNS cloud delivered platform. Cisco paid $635 million in cash

plus other considerations to acquire Open DNS.

- CounterTack (Waltham, Mass.), the leader in Big Data Endpoint Detection and Response (EDR), acquires ManTech Cyber Solutions International (MCSI), a commercial software division of ManTech International Corporation. The acquisition enhances CounterTack's leadership position in the EDR market, and will enable CounterTack to deliver truly unprecedented value to its market-leading 200+ customers, by combining real-time operating system-level behavioral threat detection with in-memory threat analysis that maps to the entire cyber kill chain and scales enterprise-wide. ManTech will become an equity investor in CounterTack as well as a global distribution partner.

- DigiCert (Lehi, Utah), a global Certificate Authority and leader of trusted identity solutions, acquires the CyberTrust Enterprise SSL business from Verizon Enterprise Solutions. Financial terms of the deal were not disclosed. The acquisition makes DigiCert the second-largest Certificate Authority (CA) for high-assurance SSL certificates.

- Digital Guardian (Waltham, Mass.), the only endpoint security platform purpose built to stop data theft, acquires Savant Protection, a provider of advanced application whitelisting solutions.

- Early Warning (Scottsdale, Ariz.), a trusted leader in fraud prevention and risk management, acquires Authentify Inc. Founded in 1999, Authentify is a worldwide leader in phone-based, multi-factor authentication solutions. It currently serves more than 1,200 financial institutions and e-commerce companies.

- Elbit Systems Ltd. (Haifa, Israel), an international high technology company which develops and supplies a broad portfolio of airborne, land and naval systems and products for defense, homeland security and commercial applications, acquires the Cyber and Intelligence division of NICE Systems.

Splunk acquires Caspida for $190 million

- Fidelis Cybersecurity (Bethesda, Md.) acquires

Resolution1 Security. The Resolution1 platform delivers real-time insight and analysis, and automated response and remediation of security incidents, enabling security analysts and operations teams to more rapidly and effectively find and eliminate threats at the endpoint device. Fidelis Cybersecurity is a privately held company backed by Marlin Equity Partners, a global investment firm with over $3 billion of capital under management.

- Fortinet (Sunnyvale, Calif.), a global leader in high-performance cyber security solutions, acquires Meru Networks, a leader in intelligent Wi-Fi networking, for roughly $44 million.

- F-Secure (Helsinki, Finland) acquires nSense – a privately held Danish company providing security consultations, vulnerability assessment services and related products to large enterprises. The acquisition strengthens F-Secure's position as a prominent security vendor in Europe, and lays a foundation for the company's growth as a cybersecurity leader in the region. The terms of the acquisition were not disclosed.

- Global Defense and National Security Systems Inc. (Reston, Va.) acquires STG Group Inc., a cybersecurity provider to the U.S. federal government, for $165.5 million in cash and equity. Global Defense will pay $75 million in cash and 8.58 million of its shares, valued at $10.55 each, to Reston, Va.-based STG. Global Defense, a special purpose acquisition company, said in a Securities and Exchange filing that it intends to fund a portion of the purchase with debt financing.

- Level 3 Communications, Inc. (Broomfield, Colo.), acquires privately held Black Lotus, a provider of global Distributed Denial of Service (DDoS) mitigation services. The acquisition of Black Lotus represents another step in Level 3's continued commitment to provide leading security product capabilities. Level 3 acquired the outstanding equity of Black Lotus in an all-cash transaction on July 1, 2015. Terms of the transaction were not disclosed.

- ManTech International Corporation (Fairfax, Va.) acquires Knowledge Consulting Group (KCG), a rapidly growing cyber security advisor in both the public and

private sectors focused on anticipating threats and implementing defensive countermeasures. ManTech will fund the acquisition from cash on hand with additional funding from its existing line of credit.

Microsoft (Redmond, Wash.) has signed a letter of intent to acquire Israeli cloud security firm Adallom for $320 million cash, according to The Wall Street Journal.

- Opera Software (Oslo, Norway) acquires SurfEasy Inc., a leading Toronto-based company that provides an easy-to-use VPN solution for protecting customers' online privacy and security on smartphones, tablets and computers. The two companies envision a powerful collaboration and venture into joint products, expanding on Opera's product footprint.

- Raytheon Company (Waltham, Mass.) and Vista Equity Partners have completed a joint venture transaction creating a new company that combines Websense, a Vista Equity portfolio company, and Raytheon Cyber Products. Raytheon owns 80.3% of the new company. Vista Equity Partners owns 19.7%. Raytheon has invested $1.9 billion (net of cash acquired) to acquire Websense, of which $600 million is in the form of an intercompany loan to the joint venture. Raytheon has also contributed the assets of Raytheon Cyber Products and related intellectual property, which is valued at $400 million. Vista Equity Partners has made a new cash investment of approximately $335 million for 19.7 percent of the equity interest in the joint venture.

- Salesforce.com (San Francisco, Calif.) bolstered its mobile security when it recently acquired Toopher, a four-year-old two-factor authentication startup out of Texas. Although terms of the deal were not disclosed, Business Insider reported that Salesforce granted a total of 37,408 shares to Toopher's seven employees – worth approximately $2.5 million at the time.

Blue Coat acquires the cloud-crypto monkeys at Perspecsys

- Splunk Inc. (San Francisco, Calif.), provider of the leading software platform for real-time Operational Intelligence,

acquires Caspida, Inc., a leading innovator in machine learning and behavioral analytics. Under the terms of the agreement, Splunk has acquired all of the outstanding stock of Caspida for an aggregate purchase price of approximately $190 million, including approximately $127 million in cash and $63 million in restricted Splunk securities.

- Splunk, Inc. (San Francisco, Calif.) acquires Metafor, the Vancouver-based provider of anomaly-detection and behavioral-analytics technology for IT and security operations. The value of the transaction was not disclosed.

- Singtel (Singapore), Asia's leading provider of infocomm technology (ICT) solutions, acquires Chicago-based data security and compliance solutions firm Trustwave for $810 million in cash. Following the close of the acquisition, Trustwave will operate as a standalone Singtel business unit and continue to be headquartered in Chicago, the company said.

- Synopsys, Inc. (Mountain View, Calif.) acquires Codenomicon, a global software security company based in Finland with a focus on software embedded in chips and devices. Codenomicon is known for independently discovering and reporting the Heartbleed bug. The additional talent, technology and products will expand Synopsys' presence in the software security market segment.

DEAL WATCH

Recent Cybersecurity Investment & IPO Activity

Looking for Cybersecurity C-Suite, Sales or Marketing Executives? Look no further… these Cybersecurity Search Firms can help

- Barkly (Boston, Mass.), an endpoint security startup, closes a $12.5 million Series A financing round, led by New Enterprise Associates (NEA) and including Sigma Prime Ventures. Barkly has now raised a total of $17 million since the company was co-founded in 2013 by Mike Duffy and Jack Danahy, longtime colleagues

Mike Duffy and Jack Danahy, longtime colleagues, information security industry veterans and serial entrepreneurs. The funding will be used to expedite the company's recruiting, product development, and go-to-market initiatives in the healthcare and financial services industries.

- BitSight Technologies (Cambridge, Mass.), the standard in Security Ratings, closes a $23 million round of Series B financing. Comcast Ventures joins as a new investor together with current investors Globespan Capital Partners, Menlo Ventures, Commonwealth Capital Ventures, Shaun McConnon and Flybridge Capital Partners, all participating in the round of funding. New funding will be used to extend sales and marketing into Europe and APAC, expand engineering and data science teams to accelerate the company's new data analytics products, and fund potential acquisitions of key data source partners. BitSight has raised $49 million to date.

- Checkmarx (Tel-Aviv, Israel), a global leader in software application security, secures a $84 million investment from New York-based venture capital and private equity firm, Insight Venture Partners. The new round of capital will be primarily used to further accelerate growth through product innovation and global expansion.

- CounterTack (Waltham, Mass.), the leader in Big Data Endpoint Detection and Response (EDR), closes a $15 million Series C round of funding, led by TenEleven Ventures, with other new investors in the round including EDBI (the corporate investment arm of the Singapore Economic Development Board), along with the participation of existing investors.

- CrowdStrike Inc. (Irvine, Calif.), provider of the first true Software-as-a Service (SaaS) based next-generation endpoint protection platform, completes a $100 million Series C financing round, led by Google Capital. Rackspace (NASDAQ: RAX), a CrowdStrike customer, also participated in the round along with existing investors Accel and Warburg Pincus. This brings the company's total funding raised to $156 million.

IPO Watch: Sophos goes public on the London Stock Exchange with a market cap of $1.59 billion,

according to The Wall Street Journal

- Cryptzone (Waltham, Mass.), a provider of dynamic, context-aware network, application and content security solutions, closes a $15 million Series B round of funding. The round was led by Kayne Partners, the growth private equity group of Kayne Anderson Capital Advisors, L.P., an approximately $29-billion alternative investment firm. Additionally, existing investor Medina Capital and a number of its limited partners participated in the round. The funding will accelerate Cryptzone's go-to-market strategy and fuel its global expansion.

- Cybereason (Cambridge, Mass.), a provider of threat detection solutions, closes a $25 million Series B funding round, with defense contractor Lockheed Martin participating as a strategic investor. Led by Spark Capital with existing investor CRV also participating in the round, the startup said the funds would be used to expand its research and development and support sales and marketing efforts.

- Cylance Inc. (Irvine, Calif.), the first next-generation endpoint protection company to successfully apply artificial intelligence to predictively identify and stop cyber attacks before they ever execute, has closed more than $42 million in Series C funding. Led by DFJ Growth, the round includes investments from KKR, Dell Ventures, Capital One Ventures and TenEleven Ventures.

- Cyphort (Santa Clara, Calif.), a pioneer of Advanced Threat Defense (ATD) solutions, secures $30 million in Series C funding. Sapphire Ventures led the round and was joined by all existing investors: Trinity Ventures, Foundation Capital and Matrix Partners. The latest round of funding will be used to help with the security company's rapid growth and expansion into new markets. The new funding brings Cyphort's total investment to more than $53 million since inception.

- Distil Networks (Arlington, Va.), a company that analyzes website traffic and blocks malicious bots, closes a $21 million Series B round. Bessemer Venture Partners led the round. Investors Foundry, TechStars, ff Venture Capital, Idea Fund and Correlation Ventures also

participated. The investment brings the total raised to $38 million.

- E8 Security (Redwood City, Calif.), provider of cyber security analytics solutions to help enterprises detect and manage malicious insider threats and targeted cyber attacks, closes $9.8 million in series A funding led by March Capital Partners, with participation from Allegis Capital and The Hive. The funding will be allocated to furthering product development, currently in private beta with several large domestic and international organizations, while also expanding the organization's engineering and development teams.

- enSilo, (San Francisco, Calif.), an Israeli cybersecurity startup which has relocated its corporate headquarters to the west coast, raises $10 million in Series A financing. The round was led by Lightspeed Venture Partners with additional investment from existing backer Carmel Ventures. The new investment will be used to expand the company's global operations, in particular in the North America market, and to open U.S. offices on the West Coast.

- HackerOne (San Francisco, Calif.), the vulnerability management and bug bounty platform, secures a Series B financing of $25 million led by New Enterprise Associates (NEA). The round includes participation from existing investors, including Benchmark, as well as numerous angel investors including Salesforce Chairman and CEO Marc Benioff, among others.

- HyTrust (Mountain View, Calif.), the cloud security automation company, raises $25 million in a Series D round, plus $8 million in venture debt and credit facilities from a syndicate of venture capital firms and strategic investors. This brings the total investment in HyTrust to $84.5 million from 11 investors.

- Illusive Networks (Tel-Aviv, Israel) raises $5 million in Series A funding from cybersecurity think tank Team 8, which is a partner with Innovation Endeavors, the VC firm founded by Google Chairman Eric Schmidt.

- Keybase (New York City, N.Y.) raises a $10.8 million Series A, led by VC firm Andreessen Horowitz. Keybase

started as a PGP keyserver hobby project, aimed at making key lookups as easy as knowing someone's username. The company has gotten more ambitious

and they have a new goal – to bring public key crypto to everyone in the world, and they are are building open source apps that anyone can use.

- Menlo Security (Menlo Park, Calif.) closes a $25 million Series B funding round led by new investor Sutter Hill Ventures and joined by existing investors General Catalyst, Osage University Partners and Engineering Capital to support the company's rapid growth.

- Niara (Sunnyvale, Calif.), a stealth security analytics company, closes a $20 million Series B financing round led by Venrock, with additional participants including New Enterprise Associates (NEA) and Index Ventures.

IPO Watch: Rapid 7 to Become Latest Stock in Hot Cybersecurity Sector, according to The Wall Street Journal

- Recorded Future (Somerville, Mass.), a real-time threat intelligence vendor, raises $12 million in Series D funding, led by Reed Elsevier Ventures.

- RedSeal, Inc. (Sunnyvale, Calif.), a security analytics company, secures $17 million in a Series C round, bringing their total investment to $56.1 million in five rounds from 11 investors.

- RedOwl (San Francisco, Calif.), a leader in insider risk management and security analytics, raises $17 million in Series B funding led by Allegis Capital. The company will use the new funds to continue its expansion, further build out the product development and data science teams, and to begin broadening its go-to-market efforts.

- SafeBreach (Tel-Aviv, Israel), an Israeli cybersecurity company, raises $4 million from Sequoia Capital and serial entrepreneur and angel Shlomo Kramer. The investment is the first for SafeBreach, which plans to use the money from the financing round to expand its development in Israel and its North American business.

- Signifyd (San Jose, Calif.), the fastest growing provider of

fraud protection for e-commerce businesses, raises $7 million in a Series A round of financing led by Allegis Capital with participation from Resolute Ventures, IA Ventures, QED Investors, Lucas Ventures and Tekton Ventures. This brings the company's total funding to $11.2 million since its founding by two PayPal veterans.

- Tanium (Emeryville, Calif.), the company that has redefined security and systems management, announced that Andreessen Horowitz invested an additional $52 million in the company. This subsequent investment in Tanium is a follow-up to Andreessen Horowitz's initial financing of $90 million in May 2014 and constitutes one of its largest investments to-date.

- ThreatQuotient Inc. (Sterling, Va.), a cyber security software firm, raises $1.5 million in a seed round of funding led by Blu Venture Investors, Center for Innovative Technology, and the Virginia Tech Investor Network (VTIN) which includes angel investor Todd Headley, the former Chief Financial Officer at Sourcefire. This initial funding will be used to expand the company's go-to-market reach through both direct and channel partner activities and to further enhance ThreatQ, the company's threat intelligence platform (TIP).

- Twistlock (Tel-Aviv, Israel), an enterprise security suite for virtual containers, raises $2.5 million in funding from YL Ventures.

- TrapX Security (San Mateo, Calif.), a global leader in deception-based cyber security defense, raises $9 million in its Series B round, led by investors Intel Capital and Liberty Israel Venture Fund together with current investors BRM Group and Opus Capital. The investment will be used to accelerate growth across the business, spanning the development of deception technology, the hiring of engineering and marketing talent, and the expansion of global sales initiatives. Headcount is expected to grow by 40 percent globally within the next year to accommodate the increase in customer demand.

- Venafi (Salt Lake City, Utah), the Immune System for the Internet and leading provider of Next Generation Trust Protection, receives $39 million in additional funding.

The financing was led by QuestMark Partners and other new investors Intel Capital and Silver Lake Waterman and existing investors. The investment will accelerate development of the Venafi Trust Protection Platform to secure more Global 5000 businesses and governments and support its fast-growing worldwide customer base.

- VS2, a.k.a. Virtual Software Systems (Waltham, Mass.), raises $2 million in seed funding to develop a new way to neutralize cyberattacks after a breach. Investors in the round included Bulldog Investors and Sequel Capital Management.

- WireX (Yehud, Israel), a network forensics company, raises $9.3 million led by Vertex Venture Capital. The financing round also included participation from existing investors Magma Venture Capital, Entrée Capital and a group of serial entrepreneurs Mickey Boodaei, co-founder of Imperva and Trusteer, Rakesh Loonkar, co-founder of Trusteer and Idan Plotnik, founder of Aorato (acquired by Microsoft). Funding will be used to expand the Israeli-based R&D center and establish headquarters in the U.S.

- Ziften (Austin, Texas), a leader in continuous endpoint visibility, raises $24 million in funding led by Spring Mountain Capital, with significant participation from Fayez Sarofim, an early investor in Ziften. The equity financing round will accelerate Ziften's go-to- market strategy and extend its global reach as it delivers on the demands of organizations for a security solution that swiftly discovers, analyzes, and plugs security exposures to harden corporate resiliency.

ARCHIVES

Don't miss an issue of the Cybersecurity Market Report

Join our mailing list and get notified when we publish each issue of the Cybersecurity Market Report

- The **Cybersecurity Market Report, Q2 2015 edition** has been archived for our readers.

- The **Cybersecurity Market Report, Q1 2015 edition** has been archived for our readers.

Stay tuned for the Cybersecurity Market Report, Q4 2015 edition, coming in October.

CYBERSECURITY VENTURES

Steven C. Morgan, Editor-In-Chief

Steve Morgan is Founder and CEO at Cybersecurity Ventures, and Editor-In-Chief of the Cybersecurity Market Report and the Cybersecurity 500 list of the world's hottest and most innovative cybersecurity companies. Steve writes the weekly Cybersecurity Business Report for IDG's CSO, and he is a contributing writer for several business, technology, and cybersecurity media properties.

CYBERSECURITY VENTURES