State of the Healthcare Cybersecurity Industry 2018 User Survey Results

Black Book Market Research LLC annually evaluates leading health care /medical software, information exchanges and service providers across 18 operational excellence key performance indicators completely from the perspective of the client experience. Independent and unbiased from vendor influence, more than 606,000 health care IT users are invited to contribute. Suppliers also encourage their clients to participate in producing current and objective customer service data for buyers, analysts, investors, consultants, competitive suppliers and the media.

For more information or to order customized research results, please contact the Client Resource Center at +1-.800.863.7590 or surveyresearch@BlackBookMarketResearch.com

For more information, visit www.blackbookmarketresearch.com

Black Book's Annual Cybersecurity Survey Reveals Healthcare Enterprises Are Not Maturing Fast Enough, Processes Continue Underfunded and Understaffed in Q2 2018

The industry is deluged with new applications, challenging systems, new devices and innovative approaches to handling and sharing data.

Black Book Market Research LLC surveyed over 2,464 security professionals from 680 provider organizations to identify gaps, vulnerabilities and deficiencies that persist in keeping hospitals and physicians proverbial sitting ducks for data breaches and cyber attacks. 96% of IT professionals agreed with the sentiments that data attackers are outpacing their medical enterprises, holding providers at a disadvantage in responding to vulnerabilities.

A fragmented mix of 410 vendors offering data security services, core products and solutions, software, consulting and outsourcing received user feedback including large IT companies, mid and small security vendors and start-ups in the polling period Q3 2017 to Q2 2018.

Over 90% of healthcare organizations have experienced a data breach since Q3 2016 and nearly 50% have had more than 5 data breaches during the same timeframe. Not only has the number of attacks increased, more than 180 million records have been stolen since 2015, affecting about 1 in every 12 healthcare consumers.

The dramatic rise in successful attacks by both criminal and nation-state backed hackers illustrates how attractive and vulnerable these healthcare enterprises are to exploitation. Despite these wake-up calls, the provider sector remains exceedingly susceptible to ongoing breaches.

Budget constraints have encumbered the practice of replacing legacy software and devices leaving enterprises more susceptible to an attack. “It is becoming increasingly difficult for hospitals to find the dollars to invest in an area that does not produce revenue,” said Doug Brown, Founder of Black Book. According to 88% of hospital representatives surveyed, IT security budgets have remained level since

2016. As a percentage of IT organizational budgets, cybersecurity has decreased to about 3% of the total annual IT spend.

Despite the lack of earmarked funds by US buyers, Black Book projects the global healthcare cybersecurity spend to exceed $65 billion cumulatively over the next five years.

A third of hospital executives that purchased cybersecurity solutions between 2016 and 2018 report they did so blindly without much vision or discernment. 92% of the data security product or service decisions since 2016 were made at the C-Level and failed to include any users or affected department managers in the cybersecurity purchasing decision. Only 4% of organizations had a steering committee to evaluate the impact of the cybersecurity investment.

“The dilemma with cybersecurity budgeting and forecasting is the lack of reliable historical data,” said Brown. “Cybersecurity is a newer line item for hospitals and physician enterprises and budgets have not evolved to cover the true scope of human capital and technology requirements yet.”

Last year’s Black Book cybersecurity survey revealed 84% of hospitals were operating without a dedicated security executive. As a solution to unsuccessfully recruiting a qualified healthcare chief information security officer, 21% of organizations opted for security outsourcing to partners and consultants, or selected security-as-a-service options as a stop gap measure.

That shortage of healthcare cybersecurity professionals is forcing a rush to acquire services and outsourcing at a pace five times more than cybersecurity products and software solutions. Cybersecurity companies are responding to the labor crunch by offering healthcare providers and hospitals with a growing portfolio of services.

“The key place to start when choosing a cybersecurity vendor is to understand your threat landscape, understanding the type of services vendors offer and comparing that to your organization’s risk framework to select your best suited vendor,” said Brown. “Healthcare organizations are also more prone to attacks than other industries because they persist at managing through breaches reactively.”

57% of IT management respondents report their operations are not aware of the full variety of cybersecurity solution sets that exist particularly mobile security environments, intrusion detection, attack prevention, forensics and testing.

58% of hospitals did not select their current security vendor in advance of a cybersecurity incident.

32% of healthcare organizations did not scan for vulnerabilities before an attack.

"Providers are at a severe disadvantage when they are forced to hastily retain a cybersecurity firm in the midst of an ongoing incident as the ability to conduct the necessary due diligence is especially limited," said Brown.

16% of healthcare organizations reported they felt intimidated by a vendor to retain services when the vendor identified a vulnerability or security flaw. "While the intrinsic nature of cybersecurity radiates pressures and urgency, hospitals shouldn't let this dictate the vendor selection process," said Brown.

60% of healthcare enterprises have not formally identified specific security objectives and requirements in a strategic and tactical plan. Without a clear set of security goals, providers are operating in the dark and its impossible to measure results.

83% of healthcare organization have not had a cybersecurity drill with an incident response process despite the skyrocketing cases of data breaches in the healthcare industry.

Only 12% of hospitals and 9% of physician organizations believe that a Q2 2019 assessment of their cybersecurity will show improvement. 23% of provider organizations believe their cybersecurity position will worsen, as compared to 3% in other industries.

In 2018, 24% of providers still do not carry out measurable assessments of their cybersecurity status. Of those that did, 7% used an objective third party service to benchmark their cybersecurity status, 6% used an objective software solution to benchmark their cybersecurity status, and 78% self-assessed with own criteria.

29% of respondents currently report they do not have an adequate solution to instantly detect and respond to an organizational attack.

74% of surveyed CIOs did not evaluate the total cost of ownership (TCO) before making a commitment to sign their current cybersecurity solution or service contract. 89% reported they bought their cybersecurity solution to be compliant, not necessarily to reduce risk when the IT decision was made.

Healthcare organizations are hyper-focused on patient care and reimbursement. "Cybersecurity risks are not on the forefront of executives' minds," said Brown. "Medical and financial leaders also wield more influence over organizational budgets making it difficult for IT management to implement needed cybersecurity practices despite the existing environment."

BLACK BOOK ANNOUNCE THE 2018 TOP CYBERSECURITY SERVICES & SOLUTIONS VENDORS

Black Book Market Research LLC conducts polls and surveys with healthcare executives and frontline users about their current technology and services partners and awards top-performing vendors based on performance based on 18 qualitative indicators of client experience and solution/service satisfaction and 3 indicators of customer loyalty. Black Book surveyed users of eighteen categories of cybersecurity vendors, consultants and advisors which produced the 2018 rankings of #1 performing suppliers.

AUTHORIZATION & AUTHENTICATION SOLUTIONS – FIREEYE

Other Top Authorization & Authentication Solution Vendors include: SAILPOINT, AVATIER, SECUREAUTH, AUTH0, OPTIMAL IDM, CROSSMATCH & IMPRIVATA.

BLOCKCHAIN SOLUTIONS – HASHED HEALTH

Other Top Blockchain Solution Vendors include: POKITDOK, IBM BLOCKCHAIN, HEALTHCOMBIX, MEDICAL CHAIN, HEALTH LINKAGES, GEM & BLOCK MD.

COMPLIANCE & RISK MANAGEMENT SOLUTION – CLEARWATER COMPLIANCE

Other Top Compliance & Risk Management Solution Vendors include: EY, DELOITTE, SERA-BRYNN, KPMG, COALFIRE, CYNERGISTEK & BAE SYSTEMS.

CYBERSECURITY ADVISORS & CONSULTANTS – LEIDOS

Other Top Compliance & Risk Management Solution Vendors include: KPMG, EY, SECURE DIGITAL SOLUTIONS, CYNERGISTEK, IBM, ATOS & IMPACT ADVISORS.

CYBERSECURITY TRAINING & EDUCATION – KNOWBE4

Other Top Cybersecurity Training Solution Vendors include: INSPIRED ELEARNING, DIGITAL DEFENSE, THE SANS INSTITUTE, (ISC)2, OPTIV, VANGUARD & CIRCADENCE.

DDOS ATTACK PROTECTION – IMPERVA

Other Top Cybersecurity DDOS Attack Protection Vendors include: CLOUDFLARE, F5 NETWORKS, FORTINET, ARBOR NETWORKS, NEXUSGUARD, AKAMAI TECHNOLOGIES & ROOT9B.

END POINT SECURITY SOLUTIONS – CARBON BLACK

Other Top End Point Security Solutions include: SYMANTEC, FORTINET, CHECKPOINT SOFTWARE, FORTINET, DUO, ABSOLUTE SOFTWARE, COUNTER TACK, TREND MICRO & MCAFEE.

ENTERPRISE ACCESS MANAGEMENT – BOMGAR

Other Top Access Management Vendors include: IMPRIVATA, TREND MICRO, MICROSOFT, CISCO, SAILPOINT, RSA SECURITY & MICRO FOCUS.

ENTERPRISE FIREWALL NETWORKS – FORTINET

Other Top Firewall Network Vendors include: SONICWALL, ZSCALER, CHECKPOINT SOFTWARE, PALO ALTO NETWORKS, CISCO, HUAWEI, FOREPOINT & SOPHOS.

HEALTHCARE DATA ENCRYPTION – ONPAGE

Other Top Data Encryption Vendors include: SENETAS, THALES, DATA LOCKER, SYMANTEC, SOPHOS, CHECKPOINT SOFTWARE, TREND MICRO, FLEXENTIAL, VIRTRU & APRICORN.

INTRUSION PROTECTION SOLUTIONS – IMPERVA

Other Top Intrusion Protection Solution Vendors include: CISCO, INTEL SECURITY (MCAFEE), TREND MICRO TIPPING POINT, IBM, PALO ALTO NETWORKS, ALERT LOGIC, HEWLETT PACKARD & EXTREME NETWORKS.

MEDICAL DEVICE & INTERNET OF THINGS SECURITY – FORTIFIED HEALTH SECURITY

Other Top Medical Device & IoT Security Solution Vendors include: BAYSHORE NETWORKS, SENRIO, RUBICON, SECURERF & BASTILLE.

OUTSOURCING & NETWORK MANAGED SERVICES – TRUSTWAVE

Other top Outsourcing & Managed Services Vendors include: CYTELLIX, SECUREWORKS, DXC TECHNOLOGIES, ARMOR, BOMGAR, NTT, OPTIV, LEVEL3, AT&T & SECUREWORKS.

PATIENT PRIVACY MONITORING – FAIRWARNING

Other Top Patient Privacy Monitoring Solution Vendors include: CONVERGEPOINT, HAYSTACK, IATRIC, CYNERGISTEK, MAIZE ANALYTICS, JERICHO SYSTEMS & TRUE VAULT.

RANSOMWARE PROTECTION – ZIX CORPORATION

Other Top Ransomware Protection Solution Vendors include: IBOSS, ZSCALER, DIGITAL GUARDIAN, WEBSENSE, CISCO, SYMANTEC & BARKLY.

SECURE COMMUNICATIONS PLATFORMS – DOC HALO

Other Top Secure Communications Platform Vendors include: PERFECTSERVE, PATIENT SAFE SOLUTIONS, VOCERA, IMPRIVATA, SPOK, ONPAGE, TIGER TEXT & TELEMEDIQ.

THREAT DETECTION & CYBER ATTACK PREVENTION – DIGITAL GUARDIAN

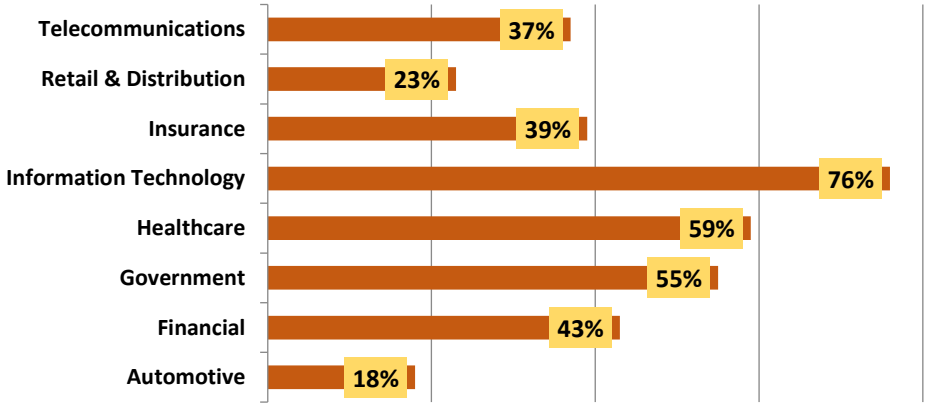
Other Top Threat Detection & Prevention Vendors include: SYMANTEC, FORCEPOINT, CROWDSTRIKE FALCON, CARBON BLACK, TRAPX SECURITY, MCAFEE, FIREEYE, IBM, FORTINET & CYLANCE.

THREAT INTELLIGENCE & ANALYTICS – JVION

Other Top Threat Intelligence & Analytics Vendors include: EY, RAYTHEON, RAPID7, CSC, HAYSTACK, NOVETTA, REDSEAL & SAS INSTITUTE.

Global healthcare cyber security market size is expected to reach nearly USD 10,848.87 million by 2022, according to a new report by Grand View Research, Inc. Key factors attributing to the growth of the market include the increasing incidences of cyber attacks for misuse of electronic patient health records (E-PHR), social security records, IP theft, and others. Cyber attacks are constantly increasing across the globe. On previous encounters it was witnessed that cyber attacks were focused on stealing, financial information, billing information, and bank account numbers using stolen devices with un-encrypted data, phishing and spam mails. Technological advancements have led to advanced cyber warfare using SQL injections, advanced persistent threats (APT), zeroday attacks, and advanced malware. Lack of adequate IT spending by healthcare organizations and lack of awareness about cyber crime have exposed the vulnerabilities of healthcare organizations. The overall impact of cyber attacks on the hospitals and healthcare systems is estimated to be nearly six billion per year. Furthermore, these organizations face internal threats due to factors such as the use of cloud services, unsecure networks, employee negligence, bring your own device (BYOD), lack of internal identification and security systems, stolen devices with un-encrypted files.

Security Market Breakdown in 2018



Healthcare cyber security market is segmented by, type of threat into malware, DDoS, advanced persistent threat (apt), spyware, lost and stolen devices, others. In the second quarter of 2017, the McAfee Labs Global Threat Intelligence network registered notable trends in cyber threat growth and cyberattack incidents across industries. McAfee Labs counted 311 publicly disclosed security incidents in Q2, an increase of 3% over Q1. 78% percent of all publicly disclosed security incidents in Q2 took place in the Americas.

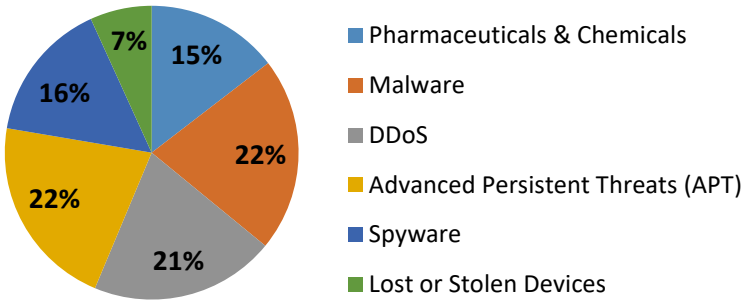
The health, public, and education sectors comprised more than half of total incidents in 2017-2018 worldwide. And, in North America, the health sector attacks led vertical sectors in Q2 security incidents in the Americas. Security information and event management (SIEM), risk and compliance management, DDoS mitigation, antivirus, antimalware, identity and access management, intrusion detection system (IDS)/intrusion prevention system (IPS) and others are the solutions included in the scope of the study. These solutions can be used individually or can be used as a suite of products providing layer wise security.

Market dynamics in this sector are dependent on the type of threat, effectiveness, and frequency of attack, ability to detect and destroy. New types of threats are detected each day, hence, the solutions need to be upgraded constantly to provide adequate firewall security and prevent data breach.

Cyber attacks are increasing at a rapid pace across the globe. The type of threat, frequency of attack and impact of each attack varies across different organizations based on their internal security controls. Earlier these attacks were focused more on stealing credit card details, billing information, bank account numbers using spam mails, phishing, or by using stolen devices with un-encrypted data. The time taken to identify security breaches can be very long if adequate internal systems, firewalls are not used and it can create a huge impact to the company's credibility and accountability.

Furthermore, using advanced malware, DDoS, SQl injections, advanced persistent threats (APT), zero-day attacks, rootkits, clickjacking and others, the cyber criminals have been able to easily bypass the protocols, resulting in loss of intellectual property, patient records, and other valuable information. The threat from internal sources is also very high owing to company policies such as bring your own device (BYOD), use of cloud services. Lack of internal identification and systems, use of insecure networks, employee negligence, loss of devices with un-encrypted files or data theft by the employee are also some of the key aspects contributing to the increasing crimes. In 2017, malware held the largest market share and is expected to continue its strong growth over the forecast period.

Healthcare Security Threats Breakdown in 2018



To tackle the various threats, cyber companies have been developing multiple products which can be used individually or can be used as a suite of products providing layer-wise solutions. Some of the key solutions used for protection are identity and access management, risk and compliance management, security information and event management (SIEM), and intrusion detection system (IDS)/intrusion prevention system (IPS), data encryption software, firewalls, antivirus, antimalware software, and others. Ideally, organizations implement more than 2 layer or 3 layer security frameworks to better identify the threats and control the flow of data, information and monitor the various other transactions performed by each user.

In 2017, identity and access management held the maximum market share of nearly 12%. However, risk and compliance management is expected to be the most lucrative solution type growing at a CAGR of over 14% over the forecast period. Rising trend of security lapses, data breaches, is expected boost the overall; IT spending by healthcare organizations and especially in the field. Furthermore, technological advancements, increasing criminal attacks and the challenges of the digital world are expected to significantly boost the usage rates of these solutions over the next seven years.

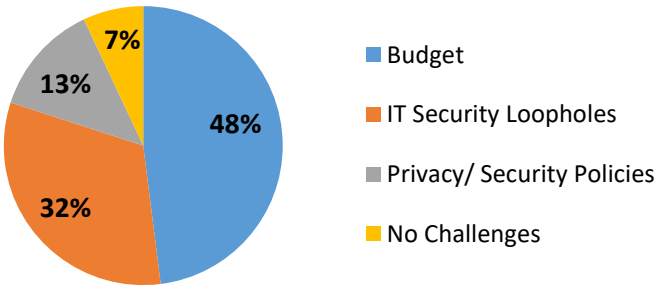
Technological advancements have led to advanced cyber warfare using SQL injections, advanced persistent threats (APT), zero day attacks, and advanced malware. As security breaches become more common and costly, medical device cyber security has emerged as a major issue in 2017, requiring device companies and

healthcare providers to take preemptive action to maintain trust in medical equipment and to prevent breaches that could cripple the industry. Security information and event management (SIEM), risk and compliance management, DDoS mitigation, antivirus, antimalware, identity and access management, intrusion detection system (IDS)/intrusion prevention system (IPS) and others are the solutions included in the scope of the study. These solutions can be used individually or can be used as a suite of products providing layer wise security.

Healthcare Security Solutions Breakdown in 2018

Lack of adequate IT spending by healthcare organizations and lack of awareness about cyber crime have exposed the vulnerabilities of healthcare organizations. The overall impact of cyber attacks on the hospitals and healthcare systems is estimated to be nearly six billion per year. 48% providers revealed that lack of budget was the major obstacles to properly securing and protecting health information. Healthcare facilities' own employees are another roadblock for some organizations. 13% said that employees who don't comply with privacy and security policies limit their ability to protect health information. A somewhat surprising finding is that 7% of providers felt there were no obstacles to securing healthcare data.

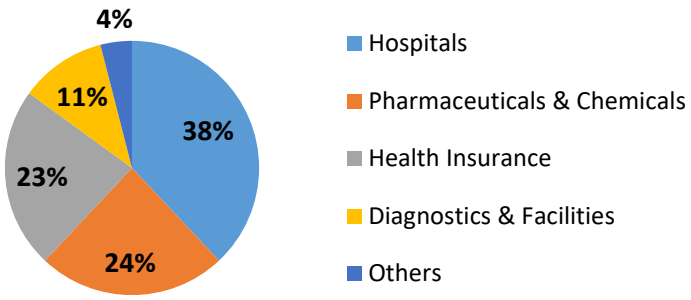
Challenges to Healthcare Security in 2018



The healthcare industry is one of the world's largest and fastest-growing industries. Consuming over 10 percent of gross domestic product (GDP) of most developed nations, health care can form an enormous part of a country's economy. The Global Industry Classification Standard and the Industry Classification Benchmark further distinguish the healthcare industry as several sectors, and the need of security in each. This vertical is highly diverse, which gives an opportunity to build a strong and growing business that specializes in healthcare. Today, there are four key healthcare segments that can benefit greatly from physical security technologies: Hospitals (including everything from large, enterprise healthcare networks to small, stand-alone facilities); Pharmaceuticals & Chemicals; Health Insurance Firms; Diagnostics & Facilities. Because the healthcare market includes so many different types of facilities, it provides the chance to start small and then

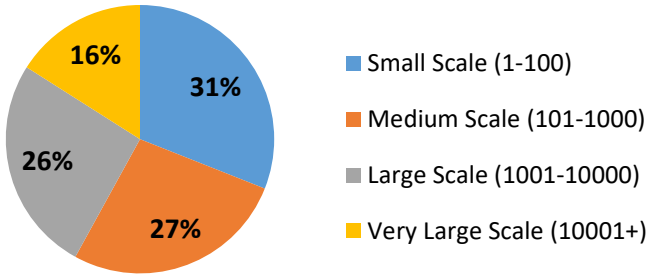
work their way up to larger clinics and hospitals. With such a diverse customer base, you're likely to find plenty of potential clients within your local area, regardless of where you live.

Healthcare Sector Market Breakdown in 2018



Majority of healthcare vendors lack minimum security practices, well short of HIPAA standards. Healthcare organizations are often unaware of how many of their vendors have access to protected health information. There are an overwhelming number of small and niche healthcare vendors for organizations to manage. Healthcare organizations do little to gain assurances or enforce security requirements for vendors. Most healthcare organizations focus due diligence on their largest vendors but breach data shows that over half of breaches are attributed to smaller companies. Existing vendor security programs have significant blind spots.

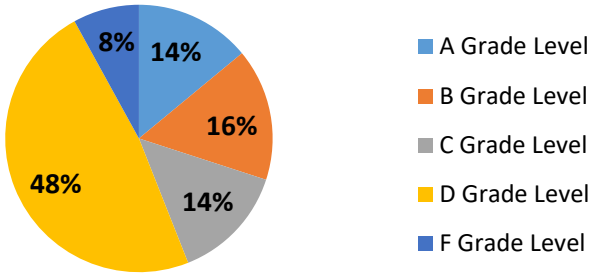
Healthcare Security Vendors Size Breakdown in 2018



According to CORL Technologies Annual Report on Healthcare Security Vendors, even after thousands of efforts 48% of security vendors fail to protect healthcare data. The score definitions for vendors defined under as:

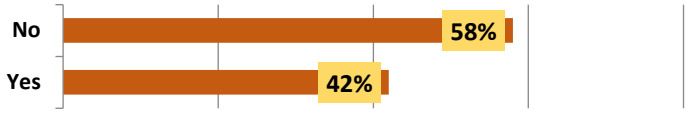
A Grade Level - High confidence that vendor demonstrates a strong culture of security
B Grade Level - Moderate confidence that vendor demonstrates a culture of security
C Grade Level - Indeterminate confidence that vendor demonstrates a culture of security
D Grade Level - Lack of confidence based on demonstrated weaknesses with vendor's culture of security
F Grade Level - No confidence in vendor's ability to protect information

Healthcare Security Vendors Score Breakdown in 2018



Research states that only 42% healthcare organizations hold the security certification. A major percentage: 58% of the organizations are not holding vendors accountable for meeting minimum acceptable security standards. Security certifications provide third party validation of security practices. Examples for the industries include: HITRUST, AICPA SOC 2 and 3 reports, ISO 27001, and FedRAMP. It is important for organizations to understand the scope and baseline criteria used for certifications to boost the security arena.

Healthcare Vendors with Security Certification in 2018



2017 was the year of the healthcare breach, with many organizations falling victim to malicious attacks.

January 2017: Many servers, accessible via the internet, are vulnerable to TLS/SSL attacks such as Drown, Triple Handshake, SMACK, FREAK, Logjam, and SLOTH. While weak or misconfigured TLS/SSL is not a new problem, so many websites and other services accessible via the internet are insecure. Many academics have called for a revamp of internet architecture to ensure better security. Some researchers have even suggested a new way to map the internet.

February and March 2017: We saw waves of attacks by cyber weapons such as Shamoon 2.0 and Stonedrill and increases in malspam attributable to botnets such as Necurs. It is likely that we will see the rise of offensive cyber maneuvers, including the use of cyber weapons, by nation state, non-state, and other actors in 2018. But, one does not need to be a sophisticated cyber-attacker to access and use such technology. Indeed, many of these resources are easy to use and hiding in plain sight.

April 2017: Many entities have been failing to address SMB vulnerabilities, thus making things such as remote code execution a fairly trivial endeavor. On a related note, research continued to show that the Conficker worm was alive and well after all of these years. While the state of healthcare Cyber Security is improving, there will continue to be many entities with vulnerable machines to SMB attacks.

May 2017: The most significant event this month was WannaCry, which exploited an SMB vulnerability, in a global cyberattack campaign. However, SMB vulnerabilities are not just a Windows problem. We also took note of SambaCry which allows for remote code execution via a writable SMB share.

June 2017: While WannaCry was still somewhat of a problem in June, NotPetya surfaced as a new issue and yet another global cyberattack campaign. Although WannaCry was a ransomworm, NotPetya was characterized as a destructive wiper malware. In addition, NotPetya was largely attributed to a supply chain software problem.

July 2017: Analysts anticipated a rise in malware specifically targeting specialized types of industrial control systems. One such example is known as Industroyer. According to analysts, such malware is designed with what almost appears to be “insider knowledge” of the exact workings of these industrial control systems. Yet others state that such malware has been around for quite a while and is not new. There is general consensus, however, around the fact that such targeted, specific malware for pinpointing specific types of industrial control systems will continue to increase over time.

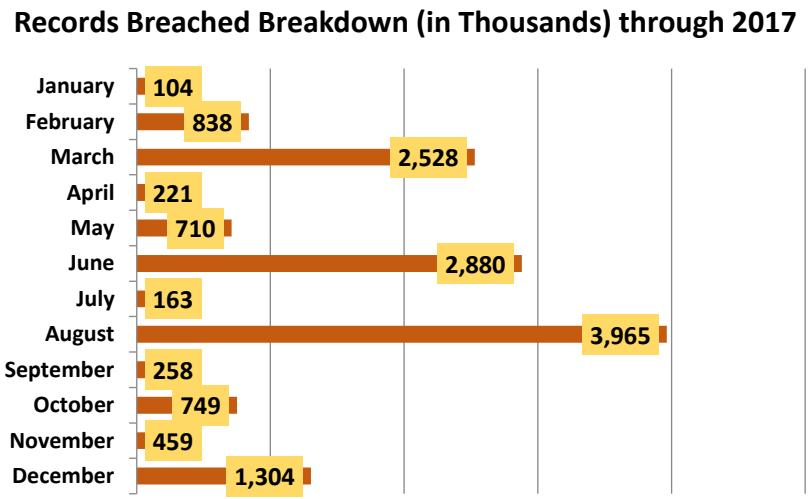
August 2017: The telnet protocol is not new, nor should it be “news” that telnet communications are not encrypted and that credentials can be easily stolen. However, with the rise in the Internet of Things (IoT), we noted the work of a researcher that had disclosed information about this problem and thousands of credentials to IoT devices having been uncovered through the course of such research.

September 2017: Just about every organization has a website, and web technology is always changing. But, as we have noted previously in this blog post, website security is not something that everyone has mastered. Thus, while entities may patch their back-office systems and in-house IT infrastructure, their websites may be ignored. Web applications may have significant vulnerabilities such as directory traversals which may result in unauthorized disclosure of potentially sensitive files. In addition, if you have a back-end database which your web application can query, you need to keep in mind problems such as, but not limited to, SQL injection vulnerabilities.

October 2017: Wireless-connected devices are quite ubiquitous. Yet, many do not give much thought to the insecurity of such devices. Researchers disclosed a method for attacking the WPA2 protocol. In addition, advanced persistent threat actors continued to target critical infrastructure sectors with ongoing campaigns.

November 2017: We saw significant vulnerabilities affecting products that many thought, once upon a time, were far more secure than their counterparts. Yet, we now know that, just like any other technology, there have been significant flaws in MacOS, Linux, and other platforms. Furthermore, medical device security remains problematic with significant insecurity found in connected infusion pumps and other types of medical devices.

December 2017: While the healthcare sector has been in the news in regard to cyber attacks and reported breaches, some analysts have found that the healthcare sector is not the worst in terms of sheer numbers of breaches.



Perhaps we need more of a multi-dimensional approach to how we understand and address cyber risks. Cyber security and healthcare both touch virtually everything. These are things that we cannot afford to ignore. The clock is ticking.

Essential Functions of IT & Data Security Products and Services

*Functions (also) specific to healthcare security are highlighted in bold red.

Function	Definition
Access Control Mechanism	Security safeguards (i.e., hardware and software features, physical controls, operating procedures, management procedures, and various combinations of these) designed to detect and deny unauthorized access and permit authorized access to an information system.
Accountability	The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity. This supports non repudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action.
Active Security Testing	Security testing that involves direct interaction with a target, such as sending packets to a target.
Advanced Encryption Standard (AES)	The Advanced Encryption Standard specifies a U.S. government approved cryptographic algorithm that can be used to protect electronic data. The AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information. This standard specifies the Rijndael algorithm, a symmetric block cipher that can process data blocks of 128 bits, using cipher keys with lengths of 128, 192, and 256 bits.
Advanced Key Processor (AKP)	A cryptographic device that performs all cryptographic functions for a management client node and contains the interfaces to 1) exchange information with a client platform, 2) interact with fill devices, and 3) connect a client platform securely to the primary services node (PRSN).
Anomaly-Based Detection	The process of comparing definitions of what activity is considered normal against observed events to identify significant deviations.
Anti-Jam	Countermeasures ensuring that transmitted information can be received despite deliberate jamming attempts.
Anti-Spoof	Countermeasures taken to prevent the unauthorized use of legitimate Identification & Authentication (I&A) data, however it was obtained, to mimic a subject different from the attacker.
Antispyware Software	A program that specializes in detecting both malware and non-malware forms of spyware.
Anti-Virus Software	Software designed to detect and potentially eliminate viruses before they have had a chance to wreak havoc within the system. Anti-virus software can also repair or quarantine files that have already been infected by virus activity.
Approved Security Function	A security function (e.g., cryptographic algorithm, cryptographic key management technique, or authentication technique) that is either a) specified in an Approved Standard; b) adopted in an Approved Standard and specified either in an appendix of the Approved Standard or in a document referenced by the Approved Standard; or c) specified in the list of Approved security functions.

Attack Sensing and Warning (AS&W)	Detection, correlation, identification, and characterization of intentional unauthorized activity with notification to decision makers so that an appropriate response can be developed.
Attack Signature	A specific sequence of events indicative of an unauthorized access attempt. A characteristic byte pattern used in malicious code or an indicator, or set of indicators that allows the identification of malicious network activities.
Authentication	Confirming the correctness of the claimed identity of an individual user, machine, software component or any other entity.
Authorization	The approval, permission or empowerment for someone or something to do something.
Authorized Vendor Program (AVP)	Program in which a vendor, producing an information systems security (INFOSEC) product under contract to NSA, is authorized to produce that product in numbers exceeding the contracted requirements for direct marketing and sale to eligible buyers. Eligible buyers are typically U.S. government organizations or U.S. government contractors. Products approved for marketing and sale through the AVP are placed on the Endorsed Cryptographic Products List (ECPL).
Backup	File copies that are saved as protection against loss, damage or unavailability of the primary data. Saving methods include high-capacity tape, separate disk sub-systems or on the Internet. Off-site backup storage is ideal, sufficiently far away to reduce the risk of environmental damage such as flood, which might destroy both the primary and the backup if kept nearby.
Bastion Host	A special-purpose computer on a network specifically designed and configured to withstand attacks.
Blacklisting Software	A form of filtering that blocks only websites specified as harmful. Parents and employers sometimes use such software to prevent children and employees from visiting certain websites. You can add and remove sites from the “not permitted” list. This method of filtering allows for more full use of the Internet, but is less efficient at preventing access to any harmful material that is not on the list.
Block Cipher	A symmetric key cryptographic algorithm that transforms a block of information at a time using a cryptographic key. For a block cipher algorithm, the length of the input block is the same as the length of the output block.
Boundary Protection	Monitoring and control of communications at the external boundary of an information system to prevent and detect malicious and other unauthorized communication, through the use of boundary protection devices (e.g., proxies, gateways, routers, firewalls, guards, encrypted tunnels).
Bulk Encryption	Simultaneous encryption of all channels of a multichannel telecommunications link.
Canister	Type of protective package used to contain and dispense keying material in punched or printed tape form.
Capstone Policies	Those policies that are developed by governing or coordinating institutions of Health Information Exchanges (HIEs). They provide overall requirements and guidance for protecting health information within those HIEs. Capstone Policies must address the requirements imposed by: (1) all laws, regulations, and guidelines at the federal, state, and local levels; (2) business needs; and (3) policies at the institutional and HIE levels.

Clear Desk Policy	A policy that directs all personnel to clear their desks at the end of each working day, and file everything appropriately. Desks should be cleared of all documents and papers, including the contents of the "in" and "out" trays —not simply for cleanliness, but also to ensure that sensitive papers and documents are not exposed to unauthorized persons outside of working hours.
Clear Screen Policy	A policy that directs all computer users to ensure that the contents of the screen are protected from prying eyes and opportunistic breaches of confidentially. Typically, the easiest means of compliance is to use a screen saver that engages either on request or after a specified short period of time.
Chain of Custody	A process that tracks the movement of evidence through its collection, safeguarding, and analysis lifecycle by documenting each person who handled the evidence, the date/time it was collected or transferred, and the purpose for the transfer.
Chain of Evidence	A process and record that shows who obtained the evidence; where and when the evidence was obtained; who secured the evidence; and who had control or possession of the evidence. The "sequencing" of the chain of evidence follows this order: collection and identification; analysis; storage; preservation; presentation in court; return to owner.
Challenge and Reply Authentication	Prearranged procedure in which a subject requests authentication of another and the latter establishes validity with a correct reply.
Challenge-Response Protocol	An authentication protocol where the verifier sends the claimant a challenge (usually a random value or a nonce) that the claimant combines with a secret (often by hashing the challenge and a shared secret together, or by applying a private key operation to the challenge) to generate a response that is sent to the verifier. The verifier can independently verify the response generated by the Claimant (such as by re-computing the hash of the challenge and the shared secret and comparing to the response, or performing a public key operation on the response) and establish that the Claimant possesses and controls the secret.
Check Word	Cipher text generated by cryptographic logic to detect failures in cryptography.
Checksum	Value computed on data to detect error or manipulation.
Cipher Block Chaining-Message Authentication Code (CBC-MAC)	A secret-key block-cipher algorithm used to encrypt data and to generate a Message Authentication Code (MAC) to provide assurance that the payload and the associated data are authentic.
Cipher Text Auto-Key (CTAK)	Cryptographic logic that uses previous cipher text to generate a key stream.
Ciphony	Process of enciphering audio information, resulting in encrypted speech.
Clearance	Formal certification of authorization to have access to classified information other than that protected in a special access program (including SCI). Clearances are of three types: confidential, secret, and top secret. A top secret clearance permits access to top secret, secret, and confidential material; a secret clearance, to secret and confidential material; and a confidential clearance, to confidential material.
Cold Start	Procedure for initially keying crypto-equipment
Common Configuration Enumeration (CCE)	A SCAP specification that provides unique, common identifiers for configuration settings found in a wide variety of hardware and software products.

Common Platform Enumeration (CPE)	A SCAP specification that provides a standard naming convention for operating systems, hardware, and applications for the purpose of providing consistent, easily parsed names that can be shared by multiple parties and solutions to refer to the same specific platform type.
Common Vulnerability Scoring System (CVSS)	An SCAP specification for communicating the characteristics of vulnerabilities and measuring their relative severity.
Communications Cover	Concealing or altering of characteristic communications patterns to hide information that could be of value to an adversary.
Communications Security (COMSEC)	A component of Information Assurance that deals with measures and controls taken to deny unauthorized persons information derived from telecommunications and to ensure the authenticity of such telecommunications. COMSEC includes crypto security, transmission security, emissions security, and physical security of COMSEC material.
Compartmentalization	A nonhierarchical grouping of sensitive information used to control access to data more finely than with hierarchical security classification alone.
Compensating Security Control	A management, operational, and/or technical control (i.e., safeguard or countermeasure) employed by an organization in lieu of a recommended security control in the low, moderate, or high baselines that provides equivalent or comparable protection for an information system.
Comprehensive Testing	A test methodology that assumes explicit and substantial knowledge of the internal structure and implementation detail of the assessment. Also known as white box testing
Computer Forensics	The practice of gathering, retaining, and analyzing computer-related data for investigative purposes in a manner that maintains the integrity of the data.
Computer Network Defense(CND)	Actions taken to defend against unauthorized activity within computer networks. CND includes monitoring, detection, analysis (such as trend and pattern analysis), and response and restoration activities.
Configuration Control	Process of controlling modifications to hardware, firmware, software, and documentation to protect the information system against improper modification prior to, during, and after system implementation.
Cross Certificate	Certificate issued from a CA that signs the public key of another CA not within its trust hierarchy that establishes a trust relationship between the two CAs.
Content Filtering	The process of monitoring communications such as email and Web pages, analyzing them for suspicious content, and preventing the delivery of suspicious content to users.
Controlled Cryptographic Item (CCI)	Secure telecommunications or information system, or associated cryptographic component, that is unclassified and handled through the COMSEC Material Control System (CMCS), an equivalent material control system, or a combination of the two that provides accountability and visibility. Such items are marked “Controlled Cryptographic Item,” or, where space is limited, “CCI”.
Cooperative Key Generation	Electronically exchanging functions of locally generated, random components, from which both terminals of a secure circuit construct traffic encryption key or key encryption key for use on that circuit.
Cover-Coding	A technique to reduce the risks of eavesdropping by obscuring the information that is transmitted.

Covert Channel Analysis	Determination of the extent to which the security policy model and subsequent lower-level program descriptions may allow unauthorized access to information.
Cryptography	The discipline that embodies the principles, means, and methods for the transformation of data in order to hide their semantic content, prevent their unauthorized use, or prevent their undetected modification.
Cryptographic Hash Function	A function that maps a bit string of arbitrary length to a fixed length bit string. Approved hash functions satisfy the following properties: 1) (One-way) It is computationally infeasible to find any input which maps to any pre-specified output, and 2) (Collision resistant) It is computationally infeasible to find any two distinct inputs that map to the same output.
Cryptographic Logic	The embodiment of one (or more) cryptographic algorithm(s) along with alarms, checks, and other processes essential to effective and secure performance of the cryptographic processes.
Cyclical Redundancy Check (CRC)	A method to ensure data has not been altered after being sent through a communication channel.
Data Origin Authentication	The process of verifying that the source of the data is as claimed and that the data has not been modified.
Defense-in-Breadth	A planned, systematic set of multidisciplinary activities that seek to identify, manage, and reduce risk of exploitable vulnerabilities at every stage of the system, network, or sub-component life cycle (system, network, or product design and development; manufacturing; packaging; assembly; system integration; distribution; operations; maintenance; and retirement).
Defense-in-Depth	Information security strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and dimensions of the organization.
Device Distribution Profile	An approval-based Access Control List (ACL) for a specific product that 1) names the user devices in a specific key management infrastructure (KMI) Operating Account (KOA) to which PRSNs distribute product, and 2) states conditions of distribution for each device.
Digital Certificate	The electronic equivalent of an ID card that establishes your credentials when doing business or other transactions on the Web. It contains your name, a serial number, expiration dates, a copy of the certificate holder's public key (used for encrypting messages and digital signatures) and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is real.
Electronic Authentication (E-authentication)	The process of establishing confidence in user identities electronically presented to an information system.
Electronic Key Entry	The entry of cryptographic keys into a cryptographic module using electronic methods such as a smart card or a key-loading device. (The operator of the key may have no knowledge of the value of the key being entered.)
Emanations Security (EMSEC)	Protection resulting from measures taken to deny unauthorized individuals information derived from intercept and analysis of compromising emissions from crypto-equipment or an information system.
Enclave	Collection of information systems connected by one or more internal networks under the control of a single authority and security policy. The systems may be structured by physical proximity or by function, independent of location.

Encryption	A data security technique used to protect information from unauthorized inspection or alteration. Information is encoded so that it appears as a meaningless string of letters and symbols during delivery or transmission. Upon receipt, the information is decoded using an encryption key.
Encryption Certificate	Certificate containing a public key that can encrypt or decrypt electronic messages, files, documents, or data transmissions, or establish or exchange a session key for these same purposes. Key management sometimes refers to the process of storing, protecting, and escrowing the private component of the key pair associated with the encryption certificate.
Entrapment	Deliberate planting of apparent flaws in an IS for the purpose of detecting attempted penetrations.
Error Detection Code	A code computed from data and comprised of redundant bits of information designed to detect, but not correct, unintentional changes in the data.
Fail Safe	Automatic protection of programs and/or processing systems when hardware or software failure is detected.
Fail Soft	Selective termination of affected nonessential processing when hardware or software failure is determined to be imminent.
Failover	The capability to switch over automatically (typically without human intervention or warning) to a redundant or standby information system upon the failure or abnormal termination of the previously active system.
False Acceptance	When a biometric system incorrectly identifies an individual or incorrectly verifies an impostor against a claimed identity.
Firewall	A hardware or software link in a network that inspects all data packets coming and going from a computer, permitting only those that are authorized to reach the other side.
Firewall Control Proxy	The component that controls a firewall's handling of a call. The firewall control proxy can instruct the firewall to open specific ports that are needed by a call, and direct the firewall to close these ports at call termination.
Firmware	The programs and data components of a cryptographic module that are stored in hardware within the cryptographic boundary and cannot be dynamically written or modified during execution.
Flaw Hypothesis Methodology	System analysis and penetration technique in which the specification and documentation for an information system are analyzed to produce a list of hypothetical flaws. This list is prioritized on the basis of the estimated probability that a flaw exists, on the ease of exploiting it, and on the extent of control or compromise it would provide. The prioritized list is used to perform penetration testing of a system.
Focused Testing	A test methodology that assumes some knowledge of the internal structure and implementation detail of the assessment object. Also known as gray box testing.
Formal Access Approval	A formalization of the security determination for authorizing access to a specific type of classified or sensitive information, based on specified access requirements, a determination of the individual's security eligibility and a determination that the individual's official duties require the individual be provided access to the information.

Full Disk Encryption (FDE)	The process of encrypting all the data on the hard disk drive used to boot a computer, including the computer's operating system, and permitting access to the data only after successful authentication with the full disk encryption product.
Functional Testing	Segment of security testing in which advertised security mechanisms of an information system are tested under operational conditions.
Graduated Security	A security system that provides several levels (e.g., low, moderate, high) of protection based on threats, risks, available technology, support services, time, human concerns, and economics.
Handshaking Procedures	Dialogue between two information systems for synchronizing, identifying, and authenticating themselves to one another.
Hash-based Message Authentication Code (HMAC)	Hash-based Message Authentication Code – (HMAC) A message authentication code that uses a cryptographic key in conjunction with a hash function.
High Assurance Guard (HAG)	An enclave boundary protection device that controls access between a local area network that an enterprise system has a requirement to protect, and an external network that is outside the control of the enterprise system, with a high degree of assurance.
Hot Site	A fully operational offsite data processing facility equipped with hardware and software, to be used in the event of an information system disruption.
Hybrid Security Control	A security control that is implemented in an information system in part as a common control and in part as a system-specific control.
Identity Certificate	Certificate that provides authentication of the identity claimed. Within the National Security Systems (NSS) PKI, identity certificates may be used only for authentication or may be used for both authentication and digital signatures.
Incident Response Plan	The documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of a malicious cyber attacks against an organization's information system(s).
Information Security Continuous Monitoring (ISCM)	Maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.
Information Assurance Vulnerability Alert (IAVA)	Notification that is generated when an Information Assurance vulnerability may result in an immediate and potentially severe threat to DoD systems and information; this alert requires corrective action because of the severity of the vulnerability risk.
Internal Security Testing	Security testing conducted from inside the organization's security perimeter.
Interoperability	For the purposes of this standard, interoperability allows any government facility or information system, regardless of the PIV Issuer, to verify a cardholder's identity using the credentials on the PIV Card.
Intrusion Detection Systems (IDS)	Hardware or software product that gathers and analyzes information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organizations) and misuse (attacks from within the organizations.)

Intrusion Prevention System (IPS)	System(s) which can detect an intrusive activity and can also attempt to stop the activity, ideally before it reaches its targets.
Kerberos	A widely used authentication protocol developed at the Massachusetts Institute of Technology (MIT). In "classic" Kerberos, users share a secret password with a Key Distribution Center (KDC). The user, Alice, who wishes to communicate with another user, Bob, authenticates to the KDC and is furnished a "ticket" by the KDC to use to authenticate with Bob. When Kerberos authentication is based on passwords, the protocol is known to be vulnerable to off-line dictionary attacks by eavesdroppers who capture the initial user-to KDC exchange. Longer password length and complexity provide some mitigation to this vulnerability, although sufficiently long passwords tend to be cumbersome for users.
Key Escrow System	A system that entrusts the two components comprising a cryptographic key (e.g., a device unique key) to two key component holders (also called "escrow agents").
Link Encryption	Link encryption encrypts all of the data along a communications path (e.g., a satellite link, telephone circuit, or T1 line). Since link encryption also encrypts routing data.
Manual Cryptosystem	Cryptosystem in which the cryptographic processes are performed without the use of crypto-equipment or auto-manual devices.
Media Sanitization	A general term referring to the actions taken to render data written on media unrecoverable by both ordinary and extraordinary means.
Memory Scavenging	The collection of residual information from data storage.
Message Authentication Code (MAC)	A cryptographic checksum on data that uses a symmetric key to detect both accidental and intentional modifications of the data. MACs provide authenticity and integrity protection, but not non repudiation protection.
Multifactor Authentication	Authentication using two or more factors to achieve authentication. Factors include: (i) something you know (e.g. password/PIN); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric).
Mutual Authentication	Occurs when parties at both ends of a communication activity authenticate each other.
Network Sniffing	A passive technique that monitors network communication, decodes protocols, and examines headers and payloads for information of interest. It is both a review technique and a target identification and analysis technique.
Non-repudiation	Assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the information.
Off-line Cryptosystem	Cryptographic system in which encryption and decryption are performed independently of the transmission and reception functions.
Operating System (OS) Fingerprinting	Analyzing characteristics of packets sent by a target, such as packet headers or listening ports, to identify the operating system in use on the target.

Patch	A patch is a small security update released by a software manufacturer to fix bugs in existing programs. Your computer's software programs and/or operating system may be configured to check automatically for patches, or you may need to periodically visit the manufacturers' websites to see if there have been any updates.
Peer Entity Authentication	The process of verifying that a peer entity in an association is as claimed.
Penetration Testing	A test methodology in which assessors, using all available documentation (e.g., system design, source code, manuals) and working under specific constraints, attempt to circumvent the security features of an information system.
Periods Processing	The processing of various levels of classified and unclassified information at distinctly different times. Under the concept of periods processing, the system must be purged of all information from one processing period before transitioning to the next.
Print Suppression	Eliminating the display of characters in order to preserve their secrecy.
Profiling	Measuring the characteristics of expected activity so that changes to it can be more easily identified.
Public Key Cryptography	Encryption system that uses a public-private key pair for encryption and/or digital signature.
Public Key Enabling (PKE)	The incorporation of the use of certificates for security services such as authentication, confidentiality, data integrity, and non-repudiation.
Quarantine	Store files containing malware in isolation for future disinfection or examination.
Remediation	The act of correcting a vulnerability or eliminating a threat. Three possible types of remediation are installing a patch, adjusting configuration settings, or uninstalling a software application.
Resilience	The ability to quickly adapt and recover from any known or unknown changes to the environment through holistic implementation of risk management, contingency, and continuity planning.
Resource Encapsulation	Method by which the reference monitor mediates accesses to an information system resource. Resource is protected and not directly accessible by a subject. Satisfies requirement for accurate auditing of resource usage.
Risk Analysis	The process of identifying the risks to system security and determining the likelihood of occurrence, the resulting impact, and the additional safeguards that mitigate this impact. Part of risk management and synonymous with risk assessment.
Root Cause Analysis	A principle-based, systems approach for the identification of underlying causes associated with a particular set of risks.
Sandboxing	A method of isolating application modules into distinct fault domains enforced by software. The technique allows untrusted programs written in an unsafe language, such as C, to be executed safely within the single virtual address space of an application. Untrusted machine interpretable code modules are transformed so that all memory accesses are confined to code and data segments within their fault domain. Access to system resources can also be controlled through a unique identifier associated with each domain.

Scoping Guidance	A part of tailoring guidance providing organizations with specific policy/regulatory-related, technology-related, system component allocation-related, operational/environmental-related, physical infrastructure-related, public access-related, scalability-related, common control-related, and security objective-related considerations on the applicability and implementation of individual security controls in the security control baseline.
Secure Erase	An overwrite technology using firmware-based process to overwrite a hard drive. Is a drive command defined in the ANSI ATA and SCSI disk drive interface specifications, which runs inside drive hardware. It completes in about 1/8 the time of 5220 block erasure.
SSL (Secure Socket Layer)	An encryption system that protects the privacy of data exchanged by a website and the individual user. Used by websites whose URLs begin with https instead of http.
Security Fault Analysis (SFA)	An assessment, usually performed on information system hardware, to determine the security properties of a device when hardware fault is encountered.
Security Impact Analysis	The analysis conducted by an organizational official to determine the extent to which changes to the information system have affected the security state of the system.
Security Information & Event Management (SIEM) Tool	Application that provides the ability to gather security data from information system components and present that data as actionable information via a single interface.
Signature Validation	The (mathematical) verification of the digital signature and obtaining the appropriate assurances (e.g., public key validity, private key possession, etc.).
Signature Verification	The use of a digital signature algorithm and a public key to verify a digital signature on data.
Spam Filtering Software	A program that analyzes emails to look for characteristics of spam, and typically places messages that appear to be spam in a separate email folder
Strong Authentication	The requirement to use multiple factors for authentication and advanced technology, such as dynamic passwords or digital certificates, to verify an entity's identity.
Super Encryption	Process of encrypting encrypted information. Occurs when a message, encrypted off-line, is transmitted over a secured, online circuit, or when information encrypted by the originator is multiplexed onto a communications trunk, which is then bulk encrypted.
Suppression Measure	Action, procedure, modification, or device that reduces the level of, or inhibits the generation of, compromising emanations in an information system.
Tabletop Exercise	A discussion-based exercise where personnel with roles and responsibilities in a particular IT plan meet in a classroom setting or in breakout groups to validate the content of the plan by discussing their roles during an emergency and their responses to a particular emergency situation. A facilitator initiates the discussion by presenting a scenario and asking questions based on the scenario.
Tailoring	The process by which a security control baseline is modified based on: (i) the application of scoping guidance; (ii) the specification of compensating security controls, if needed; and (iii) the specification of organization-defined parameters in the security controls via explicit assignment and selection statements.
Threat Analysis	The examination of threat sources against system vulnerabilities to determine the threats for a particular system in a particular operational environment.

Trusted Identification Forwarding	Identification method used in information system networks whereby the sending host can verify an authorized user on its system is attempting a connection to another host. The sending host transmits the required user authentication information to the receiving host.
Tunneling	Technology enabling one network to send its data via another network's connections. Tunneling works by encapsulating a network protocol within packets carried by the second network.
Validation	The process of demonstrating that the system under consideration meets in all respects the specification of that system.
Verification	Confirmation, through the provision of objective evidence, that specified requirements have been fulfilled (e.g., an entity's requirements have been correctly defined, or an entity's attributes have been correctly presented; or a procedure or function performs as intended and leads to the expected outcome)
Web Content Filtering Software	A program that prevents access to undesirable Web sites, typically by comparing a requested Web site address to a list of known bad Web sites.
Whitelisting Software	A form of filtering that only allows connections to a pre-approved list of sites that are considered useful and appropriate for children. Parents sometimes use such software to prevent children from visiting all but certain websites. You can add and remove sites from the "permitted" list. This method is extremely safe, but allows for only extremely limited use of the Internet.
Zeroization	A method of erasing electronically stored data, cryptographic keys, and CSPs by altering or deleting the contents of the data storage to prevent recovery of the data.

Absolute (Vancouver, Canada). Absolute offers near real-time security breach remediation. The company's Absolute Persistence product, a self-healing endpoint security technology, provides IT personnel control over devices and data. The company's cloud-based visibility allows for remote IT asset management and security for healthcare providers, including support from its healthcare information security and privacy practitioners and ASIS-certified protection professionals.

Agari (San Mateo, Calif.). Agari allows companies to secure themselves and customers from advanced phishing attacks. The Agari Email Trust Platform helps healthcare organizations verify trusted email identities and stop threats of identity deception.

AlienVault (San Mateo, Calif.). AlienVault is the provider of Unified Security Management, a comprehensive approach to security monitoring, and the AlienVault Open Threat Exchange, an open threat intelligence community enabling collaborative defense with community-powered threat data. USM is designed to monitor cloud, hybrid cloud and on-premises environments. AlienVault is the champion of mid-size organizations that lack sufficient staff, security expertise, technology or budget to defend against modern threats. The Unified Security Management (USM) platform provides all of the essential security controls required for complete security visibility, and is designed to enable any IT or security practitioner to benefit from results on day one.

AllClear ID (Austin, Texas). AllClear ID provides breach response and customer identity protection services. The company notifies customers in the event of identity theft and assigns a dedicated investigator to initiate any dispute processes, recover financial losses and restore credit reports to the pre-fraud state.

Arxan (San Francisco). Arxan offers application attack-prevention and self-protection products for the internet of things with mobile and desktop applications. The company aims to protect customers from financial loss, fraudulent transactions, stolen credentials and internet protocol theft. In the healthcare space, Arxan offers protection for embedded apps in medical devices.

AT&T Security Solutions (New York City, NY). AT&T Security Solutions help provide the first line of defense for your network from external and internal attacks. The portfolio of managed and consulting solutions help you take a proactive, comprehensive approach to security, compliance and business continuity.

Attivo Networks ThreatDefend (Fremont, Calif.). The ThreatDefend™ Deception and Response Platform is a powerful security control for an active defense, which provides early threat detection and changes the asymmetry against attackers. The Attivo Networks deception solution takes an innovative approach to detection by dynamically setting traps and lures to create a virtual hall of mirrors, altering an attacker’s reality and imposing increased cost as they are forced to decipher what is real versus fake. The ThreatDefend platform is unique in that it provides visibility throughout the attack lifecycle and detects activity that has bypassed traditional security controls. Designed for the most sophisticated human and automated attackers, the Attivo Networks deception technology is proven at global scale by Fortune 500 customers to accurately and efficiently detect threats. High-interaction engagement technology is used to substantiate each detection, provide high-fidelity alerts,

automate attack analysis. Extensive 3rd party integrations complete the cycle of an active defense with attack information sharing and automation to simplify incident response.

Auth0 (Bellvue, Wash.). Auth0 is a HIPAA-compliant service that healthcare organizations can use with their business associates when handling protected healthcare information. The company provides authentication for third-party business associates and ensures all data transfers are HIPAA-compliant.

Avast. Going from strength to strength, Avast adds 30 million new users to reach a total of more than 230 million active users worldwide. Avast Mobile Security reaches 100 million downloads faster than any mobile security app in Google Play history, and AV-Comparatives ranks Avast as the most popular mobile security provider in North America, South America, and Europe, and third in Asia. New product launches: Avast 2015, with four new features (Home Network Security, Secure DNS, HTTPS Scanning, and Smart Scan), Avast SecureLine VPN for Android and iOS, Avast GrimeFighter, and Avast Ransomware Removal.

Axway (Phoenix). The Axway Amplify Platform is a data and engagement platform that can provide real-time operational intelligence and API lifestyle management. In the healthcare space, the Axway Amplify can help eliminate silos, overcome interoperability challenges, accelerate meaningful use and promote patient engagement with health information.

BAE Systems. Consulting services help clients to prepare for Cyber Attacks by understanding and managing cyber exposure, enabling them to make informed investment decisions and to put pragmatic, cost-effective protection in place.

Barracuda Networks (Campbell, Calif.). Barracuda Networks offers solutions to solve IT problems including content security, networking and application delivery and data storage, protection and disaster recovery. The Barracuda Web Application Firewall provides secure access to patient portals while the Barracuda NextGen Firewall F secures network devices against persistent threats, malware and zero-day exploits.

Barrier1 (Minneapolis). Barrier1's Real-Time Intelligent Threat Management and the Advanced Analytics Reactive Engine platforms are designed to protect against security breaches. The technology inspects traffic type and dataflow to stop malware and viruses; analyzes the real time data flow; and inspects the network with multiple methods of authentication. The company's customers include hospitals, clinics and specialty providers with MRI and CT Scans from multiple hospitals and clinics.

Battelle (Columbus, Ohio). Battelle is a nonprofit research and development organization that includes a team of experts devoted to medical device cybersecurity. The team members, led by a certified ethical hacker, hacks into medical devices to help manufacturers identify vulnerabilities in the software, mitigate cybersecurity risks and help design new products.

Bayshore Networks (Bethesda, Md.). Bayshore offers solutions for a variety of cyber initiatives, including industrial asset visibility, cybersecurity protection and managed remote access. The company aims to help clients eliminate cyber threats and risks while preparing to achieve industrial internet of things maturity.

BeyondTrust (Phoenix). BeyondTrust delivers cybersecurity solutions designed to reduce risks and act against internal and external data breach threats. The company offers an integrated risk intelligence platform to identify critical risks and provide information for the company. In the healthcare space, BeyondTrust's PowerBroker privileged account management solution enforces

lbest practices; its Retina vulnerability management solutions allows the healthcare IT security team to identify exposure, analyze the business impact and conduct remediation.

BIO-key (Wall Township, N.J.). BIO-key offers biometric software and hardware solutions to strengthen user authentication. The company's products include finger scanning devices for authentication in addition to passwords, PINs tokens and cards for customers to secure their devices.

Bitglass (Campbell, Calif.). The Bitglass Cloud Access Security Broker solution enables organizations to ensure security and regulatory compliance when using cloud apps. Founded in 2013, the company aims to protect corporate data on managed and unmanaged devices. Bitglass's platform can help healthcare professionals with multiple hospital affiliations access files on any device and maintain visibility and control of their data.

BlueCat (Grapevine, Texas). BlueCat centralizes and automates domain name server services so organizations can leverage the DNS data for increased visibility, control and compliance. The company takes a software-centric approach to information security and promotes interoperability to manage complex network structures. In the healthcare arena, BlueCat allows organizations to centrally manage and track wired and wireless networks and devices.

Booz Allen Hamilton (Washington DC). Booz Allen Hamilton has a Commercial Cyber team that healthcare organizations could potentially benefit from, as it works to create tailored cybersecurity options that can anticipate attacks. Booz Allen states its approach to cybersecurity also includes identifying the external risks, quickly responding to identify, triage, respond, and learn from cyber incidents. From there, they assist organizations in detection and the recovery process, so normal operations can be restored quickly and efficiently.

Bradford Networks (Boston). Bradford Networks' network entry solution is designed to continuously assess risks of all users and endpoints. The technology integrates with existing endpoint security, firewall and threat detection solutions through the SmartEdge Platform.

Bromium (Cupertino, Calif.). Bromium focuses on the global enterprise security market and its Bromium Secure Platform protects against all advanced malware. The company's solution can secure patient data and minimize breaches across the healthcare industry.

BT (London UK). BT provides the full range of cyber security consultancy and services. It can conduct ethical hacking exercises to identify weaknesses, and then undertake continuous vulnerability scanning and threat monitoring. Managed security services enable you to transmit sensitive information around the world using secure document delivery and email. It can implement message scanning and virus protection services, and provide file encryption or public key infrastructure services.

CA Technologies (New York City). CA Technologies works with healthcare organizations on digital transformation initiatives to prevent cybersecurity attacks while still providing streamlined access to authorized employees and partners. The company has worked with BlueCross BlueShield of Tennessee, Englewood, Colo.-based Catholic Health Initiatives and GlaxoSmithKline Vaccines in the healthcare space.

Carbon Black. Carbon Black leads a new era of endpoint security by enabling organizations to disrupt advanced attacks, deploy the best prevention strategies for their business, and leverage the expertise of 10,000 professionals to shift the balance of power back to security teams. Only Carbon Black continuously records and centrally retains all endpoint activity, making it easy to track an

attacker’s every action, instantly scope every incident, unravel entire attacks and determine root causes.

Centripetal (Herndon, Va.). Centripetal's core networking technologies are designed to simplify cyber intelligence collection and management to stop unwanted network traffic. The company's QuickThreat Gateway combines proprietary software and hardware to detect and enforce 5 million threat indicators.

Checkmarx. Checkmarx provides the best way for organizations to introduce security into their Software Development Lifecycle (SDLC), which systematically eliminates software risk. The product enables developers and auditors to easily scan un-compiled / un-built code in all major coding languages and identify its security vulnerabilities. Static Code Analysis (SCA) delivers security and the requirement of incorporating security into the software development lifecycle (SDLC). It is the only proven method to cover the entire code base and identify all the vulnerable areas in the software.

Checkpoint Software. Since 1993, Check Point has been dedicated to providing customers with uncompromised protection against all types of threats, reducing security complexity and lowering total cost of ownership. It is committed to staying focused on customer needs and developing solutions that redefine the security landscape today and in the future.

CipherCloud (San Jose, Calif.). CipherCloud's comprehensive multicloud security platform integrates advanced data protection, adaptive policy controls, monitoring and cloud risk analysis to secure organizations in financial services, insurance and healthcare industries, among others. CipherCloud works with healthcare organizations, pharmaceutical companies and insurance providers to safeguard private health information while maintaining HIPAA compliance. Cisco

CISCO (Mountainview, Calif,) Cisco has numerous options in its approach to cybersecurity as well, offering tools in access control and policy, firewalls, email security, next-generation intrusion prevention systems, malware protection, and more. Healthcare organizations looking to create a security strategy for risk and compliance, or control access to and segment their network may also benefit through Cisco. It also has specific services for connected healthcare organizations, so a digital platform can be created in a secure way. Cisco security innovations provide highly secure firewall, web, and email services while helping to enable mobility and teleworking.

Citrix (Fort Lauderdale, Fla.). Citrix provides a secure digital workspace to unify apps, data and services necessary for productive organizations while allowing IT personnel to manage complex cloud environments. The workspace as a service company developed a platform for enterprise file synchronization and sharing with users across all business segments. The Citrix Windows apps solution allows healthcare organizations to securely deliver apps to diverse mobile devices including tablets and smartphones. The company's Enterprise Mobility Management Technologies provides security for bring-your-own-device environments.

Clearwater Compliance (Nashville, Tenn.). The American Hospital Association endorsed Clearwater Compliance as a leading provider of hospital and health system compliance and cybersecurity management solutions. The company has implemented systems in hundreds of hospitals and health systems, Fortune 100 organizations and the federal government. Clearwater Compliance, LLC, focuses on helping health care organizations and their service providers improve patient safety and the quality of care by assisting them to establish, operationalize and mature their information risk management programs. Led by veteran, C-suite health care executives, Clearwater provides comprehensive, by-the-regs software and tools, educational events, and expert

professional/advisory services for health care organizations ranging from major health care systems, hospitals, health plans and Fortune 100 companies, to medical practices and health care startups.

Coalfire (Westminster, Colo.). Coalfire is the cybersecurity advisor that helps covered entities and business associates avert threats, close gaps, and effectively manage risk. By providing independent and tailored advice, compliance assessments, technical testing and cyber engineering services, the company secures health data throughout the care continuum. Coalfire is one of the original HITRUST CSF assessor firms with the experience required to efficiently manage successful certifications.

Code42 (Minneapolis). Code42 is a software as a service solution designed to back up distrusted end-user data on a secure platform. The company's software can protect files across Mac, Windows and Linux laptops and desktops automatically to limit risks and meet data privacy regulations.

CodeDX. Code Dx is a software vulnerability management system that brings together static and dynamic code analysis to quickly find and manage vulnerabilities in the code you write, in the languages you use, at a price you can afford. By correlating and consolidating the results of hybrid application testing techniques – static, dynamic and manual – Code Dx helps find the most severe and exploitable vulnerabilities first. Code Dx accelerates the vulnerability discovery and remediation process.

Comodo (Clifton, N.J.). Comodo has more than 100 million installations of its security product in healthcare as well as other industries. Comodo's technology authenticates, validates and secures networks and infrastructures around the world, designed to solve advanced malware threats, both known and unknown.

CORL Technologies (Atlanta). Founded in 2012, CORL Technologies provides vendor security risk management solutions as part of the vendor risk management program. The program allows healthcare organizations to monitor vendor risk, ease compliance audits and improve executive-level communications and risk analytics reporting.

Cryptzone (Waltham, Mass.). Cryptzone focuses on identity-centric security solutions to protect information from internal and external threats. The company uses a software-defined perimeter model to protect applications and content from threats, which can also streamline operations and lower costs. In the healthcare space, Cryptzone's network, application and content solutions are designed to encrypt data, restrict access to private information and share documents in a HIPAA-compliant way.

CSC (Washington, DC). Headquartered in Virginia, CSC offers end-to-end solutions that can adapt along with healthcare organizations as they evolve and as the current cybersecurity threats change. With a Business Continuity Management Program and strategic consulting services, CSC promises to keep organizations current on the latest technology deployment and any legal or regulatory mandates. Furthermore, CSC offers IT security assessments and assistance in securing cloud computing options, mobile, big data, and analytics.

Cyberark. CyberArk is the only security company laser-focused on striking down targeted cyber threats, those that make their way inside to attack the heart of the enterprise. Dedicated to stopping attacks before they stop business, CyberArk is trusted by the world’s leading companies — including more than 35 percent of the Fortune 100 companies — to protect their highest-value information assets, infrastructure and applications.

Cybereason (Boston). Cybereason's platform can identify a single component of an attack and connect it to other information in the system to shut down the attacker's entire campaign. The platform is designed to quickly build the complex attack story and simplify the resolution process.

Cylance (Irvine, Calif.). Cylance is an artificial intelligence-driven endpoint detection and response solution designed to predict and prevent cyberattacks. The company's products are designed to secure the entire healthcare infrastructure, working across Microsoft Windows and Mac OS X to integrate with existing security information and event management platforms.

Cymmetria (Palo Alto, Calif.). Cymmetria develops comprehensive cyber deception solutions based on breadcrumbs and decoys to lead attackers away from targets. Founded in 2014, the company aims to change the asymmetry of cybersecurity to reduce the odds hackers are left vulnerable information.

CynergisTek (Austin, Texas). CynergisTek is a cybersecurity and privacy consulting firm. The company helps organizations assess privacy and security risk programs with regulatory requirements as well as develop best practices for risk management. CynergisTek was named Best in KLAS for Cyber Security Advisory Services in 2017.

DarkOwl (Denver). DarkOwl is an information security company specializing in darknet (or "dark web") intelligence. Founded in 2009, DarkOwl has built the world's largest commercially available database of darknet content. Their database allows clients to search the darknet without accessing it directly, which is both difficult and dangerous. Their darknet platform also allows clients to passively monitor the darknet for their sensitive information, enabling near real-time awareness of any potentially breached information.

Dataguise (Fremont, Calif.). Dataguise provides a solution for global data governance, allowing organizations to detect, protect and monitor sensitive data in real time on the premises and in the cloud. Healthcare organizations can use the company's Hadoop product to streamline and analyze billing data to reduce costs and fraud incidents; digitize patient records; and incorporate sensor and internet of things health monitoring data.

DataMotion Health (Florham Park, N.J.). DataMotion Health enables providers to communicate more efficiently across the care continuum. DataMotion provides secure messaging and connectivity solutions to exchange protected health information for clinical use and to deliver improved care at reduced costs.

DB Networks (San Diego). DB Networks aims to protect databases from insider threats and cyberattacks. Founded in 2009, the company launched the first signatureless database cybersecurity product in 2013 and has received a patent for its approach to database protocol information extraction. Last year, the company launched its first artificial intelligence-based agentless database activity monitoring to protect against cyberattacks.

Deloitte (New York City, NY). Working hand-in-hand with member firm clients, Deloitte helps organizations plan and execute an integrated cyber approach to harness the power of information networks to enhance business operations, increase mission performance, and improve customer support, without compromising security or privacy.

DeviceLock (San Roman, Calif.). Established in 1996, DeviceLock provides endpoint device and portal control as well as data leak prevention software. The company has more than 70,000 licensed customers and a presence in the finance, medical, pharmaceutical and government markets.

DFLabs. DFLabs is a Technology and Services company, specializing in Cyber Security Incident and Data Breach Response. Its mission is eliminating the complexity of Cyber Security Incident and Data Breach, reducing reaction time and risk exposure. In other words Cyber Incidents under Control. IncMan NG is the cutting edge technology platform for managing and responding to cyber incidents and sharing intelligence. IncMan has been created for SOC and CSIRT orchestration, and it is currently being used by many Fortune 100/1000, and Financial Services Institutions worldwide.

Digital Defense (San Antonio). Digital Defense's Frontline Vulnerability Manager is a service platform designed to scan for vulnerabilities and provide penetration testing for organizations. The company's Frontline Social Testing promotes security-minded behaviors among employees. Overall, the company aims to safeguard data and ease burdens associated with maintaining information security. Founded in 1999, Digital Defense, Inc., is a premier provider of managed security risk assessment solutions protecting billions in assets for small businesses to Fortune companies in over 65 countries. A dedicated team of experts helps organizations establish an effective culture of security and embrace the best practices of information security. Through regular assessments, awareness education and rapid reaction to potential threats, clients become better prepared to reduce risk and keep their information, intellectual property and reputations secure.

DomainTools (Seattle). DomainTools examines network indicators and connects them with other active domains to develop risk assessments, identify attackers, assist in fraud investigations and map cybersecurity activity to attacker infrastructure. The company works with U.S. government agencies and contracts in addition to companies in the financial and healthcare space.

Duo Security (Ann Arbor, Mich.). Duo Security aims to secure organizations that operate in the cloud and manage a bring-your-own-device environment. Duo is a software as a service company that orchestrates two-factor authentication to help healthcare organizations maintain and share information in a HIPAA-compliant fashion.

eSentire (Cambridge, Ontario). eSentire is a pure-play managed detection and response service provider that protects organizations from the constantly evolving cyberattacks technology alone can't prevent. The company provides a 24-7 security operations center staffed by analysts to investigate and respond to threats in real time.

ESET (Bratislava, Slovakia). ESET was founded as an antivirus protection company and has expanded to include security solutions for customers in more than 200 countries. ESET's solution for healthcare companies protects against data breaches and can be deployed across multiple operating systems and endpoints.

EnSilo (San Francisco). EnSilo provides a comprehensive endpoint security platform to automatically respond to and eliminate complex security issues. The system also provides post-attack protection to avoid data theft or ransom. For healthcare organizations, the company's real-time endpoint security platform protects sensitive data in compliance with HIPAA standards.

Exabeam (San Mateo, Calif.). The Exabeam Security Intelligence Platform provides security intelligence and management solutions. Exabeam's platform can detect and respond to insider threats, track behavior analytics, protect against data loss, conduct breach investigations and report on data security compliance. The company earned SC Magazine's 2017 Best Emerging Technology award and was a finalist in the Cybersecurity Excellence Awards in 2017 for security analytics and threat hunting categories.

EY. (New York City, New York). EY has an integrated perspective on all aspects of organizational risk, and Cyber Security is a key area of focus, where EY is an acknowledged leader in the current landscape of mobile technology, social media and cloud computing. EY provides services in six core pillars with over 160 unique cyber offerings - including Cyber Digital & Analytics, Cyber Defense & Response, Cyber Strategy & Architecture, Cyber Operations (Cyber-as-a-Service), Cyber Governance & Compliance and Cyber Technology & Innovation.

Fireeye. FireEye has an approach to threat intelligence designed to combat advanced persistent threats (APTs). Whether a healthcare organization needs protection for mobile attacks, endpoint threats, network attacks, email threats, or even malware in data centers or file servers, FireEye might have an applicable option. Moreover, it offers analytic tools to help identify potential threats and improve an organization's response in real time. There is also a forensics aspect to further improve incident response. FireEye has invented a purpose-built, virtual machine-based security platform that provides real-time threat protection to enterprises and governments worldwide against the next generation of Cyber Attacks. These highly sophisticated Cyber Attacks easily circumvent traditional signature- based defenses, such as next-generation firewalls, IPS, anti-virus and gateways. The FireEye Threat Prevention Platform provides real-time, dynamic threat protection without the use of signatures to protect an organization across the primary threat vectors and across the different stages of an attack life cycle. The core of the FireEye platform is a virtual execution engine, complemented by dynamic threat intelligence, to identify and block Cyber Attacks in real time.

FireMon (Overland Park, Kan.). FireMon's Security Management Platform seeks to improve security while reducing operational costs through analytics, simulation and automation. The company focuses on protecting cloud-bound enterprises with next generation security intelligence.

Flexera Software (Itasca, Ill.). Flexera Software aims to help enterprises and application producers increase application usage and security. The company has more than 80,000 customers in a variety of industries. Flexera's FlexNet Producer Suite is designed for intelligent device manufacturers as an end-to-end solution for software licensing, entitlement management and device lifecycle management.

Forecepoint (Irving, Tex.) Forcepoint (previously Raytheon | Websense) was created to empower organizations to drive their business forward by safely embracing transformative technologies – cloud, mobility, Internet of Things (IoT), and others – through a unified, cloud-centric platform that safeguards users, networks and data while eliminating the inefficiencies involved in managing a collection of point security products.

ForeScout (Cupertino, Calif.). ForeScout's approach to security protects organizations against emerging threats with the ForeScout CounterACT. The company's technology assesses, remediates and monitors devices continuously and works with disparate security tools to accelerate incidence response. More than 2,400 customers in 60 countries use ForeScout technology for network security and compliance. Healthcare organizations use the technology to secure agentless medical devices and mobile computing against cyberattacks.

ForgeRock (San Francisco). ForgeRock is a digital identity management company that works with organizations to adopt the ForgeRock Identity Platform. The platform allows healthcare providers to create secure digital identities for patients that collects data from apps, wearables and digital health and wellness services.

Fortinet. Fortinet protects networks, users and data from continually evolving threats. As a global leader in high-performance network security, it enables businesses to consolidate and integrate

stand-alone technologies without suffering performance penalties. Fortinet solutions empower customers to embrace new technologies and opportunities while protecting essential systems and content.

Fox Technologies (Grand Rapids, Mich.). Fox Technologies aims to help companies protect corporate information assets with network security and access management software. The company also works with organizations to simplify compliance and streamline administration with its access management and account control solution. In May, the company launched Release 7.1 of its Privileged Access Management Solution to address new web-scale infrastructures used in global financial institutions, government, healthcare, telecommunication, energy and technology companies.

General Dynamics IT (Fairfax, Va.). General Dynamics IT's cybersecurity operations provide service support to select the best security systems, develop data protection policies and monitor their networks. The company provides cybersecurity for the Department of Defense, local and state governments and select commercial customers. The company provides its full security services in the General Dynamics Health Solutions package to secure hospitals' systems and protect information.

Gigamond. Gigamon provides an intelligent Visibility Fabric architecture for enterprises, data centers and service providers around the globe. Its technology empowers infrastructure architects, managers and operators with pervasive and dynamic intelligent visibility of traffic across both physical and virtual environments without affecting the performance or stability of the production network. Through patented technologies and centralized management, the Gigamon GigaVUE portfolio of high availability and high density products intelligently delivers the appropriate network traffic to management, analysis, compliance and security tools.

GigaTrust (Herndon, Va.). Founded in 2000, GigaTrust provides security software to protect emails and attachments, documents, administrative oversight and compliance tools. The company provides a software as a service secure document rendering experience inside and outside of an enterprise's network.

Globalscape (San Antonio). Globalscape was founded in 1996 and since then has grown to provide information exchange software and services to more than 13,000 customers in more than 150 countries. The company focuses on providing secure data transfer through its managed file transfer platform for on-premises, cloud or hybrid deployments. Globalscape also offers electronic funds transfer for healthcare organizations including secure and compliant data management, data integration, automation management, workflow management and real-time activity monitoring and tracking.

GreyCastle Security (Troy, N.Y.). GreyCastle Security is a risk management company with cybersecurity capabilities. The company provides a team of cybersecurity experts, a client portal to view cybersecurity efforts, custom security roadmaps, an incident response team and an account manager to maximize the cybersecurity program. The company also provides HIPAA risk assessments, 24/7 breach and incident response, HIPAA security training and policy development.

Guidance Software. Makers of EnCase, the gold standard in digital investigations and endpoint data security, Guidance provides a mission-critical foundation of applications that have been deployed on an estimated 25 million endpoints and work in concert with other leading enterprise technologies from companies such as Cisco, Intel, Box, Dropbox, Blue Coat Systems and LogRhythm.

GuardiCore (San Francisco). GuidiCore focuses on data center innovation and cloud security to deliver accurate and effective solutions to stop advanced threats. The company's real-time breach

detection and response software was developed by cybersecurity experts to fight attacks in an organization's data center.

Gurucul (Segundo, Calif.). Companies around the globe use Gurucul technology to detect insider threats, cyber fraud, internet protocol theft and external attacks. The company's technology includes user behavior analytics and identity access intelligence that includes machine learning anomaly detection and predictive risk-scoring algorithms to prevent unnecessary access and breaches.

Haystack Informatics (Philadelphia). Haystack Informatics was founded out of the Children's Hospital of Philadelphia to provide solutions for monitoring patient privacy. Haystack professionals analyze interactions between hospital staff and patients to identify privacy violations and security risks. The team uses multiple detection engines to identify inappropriate behavior and reinforces employee training in privacy matters.

Herjavec Group. Dynamic IT entrepreneur Robert Herjavec founded Herjavec Group in 2003 and it quickly became one of North America’s fastest-growing technology companies, delivering managed security services globally supported by state-of-the-art, PCI compliant Security Operations Centres (SOC), operated 24/7/365 by certified security professionals. This expertise is coupled with a leadership position across a wide range of functions including compliance, risk management, networking and incident response.

HID Global (Austin, Texas). HID Global provides identity security solutions to governments and hospitals as well as educational and financial institutions. The company provides information security solutions to hospitals, mobile device use, visitor management and HIPAA-compliant medical record security and also gives suppliers secure access to the appropriate data.

HITRUST Alliance (Frisco, Texas). HITRUST Alliance is a nonprofit organization leading advocacy efforts and educational support to safeguard healthcare information and manage risk. HITRUST was founded in 2007 to protect health information systems and exchanges, providing access to common risk and compliance management, de-identification frameworks and related assessment and assurance methodologies.

Hortonworks (Santa Clara, Calif.). Hortonworks creates and supports enterprise-ready open data platforms and modern data applications. Founded in 2011, the company provides services to Oracle, Microsoft and Red Hat, a multinational software company.

IBM (White Plains, NY). Headquartered in New York, IMB can assist healthcare organizations in crafting comprehensive and long lasting cybersecurity solutions to protect web applications, data, and processes. Along with stopping advanced threats, protecting critical assets, and safeguarding cloud and mobile solutions, IBM also offers facilities the ability to unite security silos. This can not only reduce complexity in the security program, but also help lower costs. IBM also offers threat sharing, so organizations can research the latest global security threats. IBM integrated security intelligence protects businesses around the world. New technological capabilities come with new vulnerabilities. How do you keep up with attacks when there is a shortage of IT security skills and rising costs to secure your data? How fast can you address an attack when your solutions aren’t integrated? IBM offers a deep enterprise security portfolio customized to a company’s needs.

Imperva. Imperva fills the gaps in endpoint and network security by directly protecting high-value applications and data assets in physical and virtual data centers. With an integrated security platform built specifically for modern threats, Imperva data center security provides the visibility and control needed to neutralize attacks from the inside and outside, to mitigate risk and streamline compliance.

Interset (Ottawa, Ontario). Interset's platform can correlate multiple data classes and link security events to users, machines, applications and files to identify threats and remove false positives. The technology is designed to stop sensitive data theft. Interset has partnered with Toledo, Ohio-based Promedica; Huntington, W.Va.-based Valley Health System; and San Francisco-based Dignity Health, among other healthcare providers.

Invincea (Fairfield, Va.). Invincea is an endpoint security software company focused on eliminating enterprise IT threats. More than 25,000 customers use its X by Invincea solution with Performance-Built-In to combine machine learning and behavioral monitoring that covers endpoint security blind spots. Healthcare organizations can use the technology to protect patient information and stop ransomware attacks.

i-Sprint. i-Sprint Innovations (i-Sprint) is a premier Identity, Credential and Access Management Solutions provider for global financial institutions and high security sensitive environments. i-Sprint maintains the highest value and reliability rankings among its clients, and is one of the most recognized names in the financial world.

Ixia (Calabasas, Calif.). Ixia was founded in May 1997 to provide testing, visibility and security solutions for governments, service providers and network equipment manufacturers. The company helps customers manage IT and protect against security threats with technologies for mobile devices, cloud security, internet of things management and improved network visibility.

Kaspersky Labs. Kaspersky offers an industrial cybersecurity solution for organizations, which includes flexibility options so it can be perfectly tailored to each enterprise's specific needs. This includes security options for desktops, laptops, and file servers. With file servers, there are also control tools, data encryption, and mobile security. Kaspersky also offers protections for mail servers, collaboration servers, virtual environments, and web gateway traffic. Kaspersky Lab is one of the fastest growing IT security vendors in the world. The company was founded in 1997 and today it is an international group operating in almost 200 countries and territories worldwide. It has 33 representative territory offices in 30 countries across five continents. Kaspersky Lab has a corporate client base of more than 250,000 companies located around the globe, ranging from small and medium-sized businesses all the way up to large governmental and commercial organizations.

KnowBe4 (Clearwater, Florida). KnowBe4 has become the world's most popular integrated Security Awareness Training and Simulated Phishing platform. Thousands of enterprise accounts are using it, 25 percent of which are banks and credit unions. Based on Kevin Mitnick's 30+ year unique first-hand hacking experience, you now have a tool to better manage the urgent IT security problems of social engineering, spear phishing and ransomware attacks. With this world-class, user-friendly and effective Internet Security Awareness Training, KnowBe4 provides self-service enrollment, and both pre-and post- training phishing security tests that show the percentage of end users that are Phish-prone.

Liberty Investigation Forensic and Response Services (New York City). LIFARS is a global digital forensics and cybersecurity intelligence firm that provides cybersecurity solutions. The company conducts digital forensic investigations, incidence response services, web application security testing, digital risk assessments and academic research to optimize an organization's digital infrastructure.

LightCyber (Ramat Gan, Israel). Cyberwarfare experts founded LightCyber in 2011 to help security analysts identify attacks on their networks. The LightCyber Magna behavioral attack detection

platform provides security visibility into advanced or targeted attacks as well as insider threats and malware that circumvent traditional security controls.

Lockheed Martin (Washington, DC). Lockheed Martin underlines the importance of ensuring that an organization's technology, employees, and business processes are properly aligned in order to create a proactive approach to cybersecurity issues. Lockheed's services include options for threat protection, threat monitoring, and managed IT support. Furthermore, there are tools for insider threat detection, industrial control systems management, and direction on how to turn incident response into incident prevention. At Lockheed Martin, cyber security begins with the customer's mission and requirements and ends with a security solution that is integrated, proactive and resilient.

LookingGlass Cyber Solutions (Reston, Va.). LookingGlass Cyber Solutions protects global enterprises and government agencies against cyberattacks. The company provides healthcare organizations with a team of analysts through its Threat Intelligence Analysis and Management system to identify potential security threats, analyze multiple threat factors and indicators and develop a plan to mitigate threats in real time.

McAfee. Part of Intel Security, MacAfee highlights why organizations should focus on cybersecurity awareness in their network assets, data, and activity. It's necessary to index sensitive data stored on networks, and then be able mine the data. This helps organizations understand how it is used, who owns it, and where it has proliferated. Database security, network security, risk and compliance monitoring, and security information and event management also all fall under the MacAfee cybersecurity umbrella.

MedCrypt (Encinitas, Calif.). MedCrypt provides application programming interfaces to encrypt data sent from devices and allows customers to assign unique keys to every actor in the system and monitor what devices are doing remotely in real time. After installation in the device, MedCrypt Nodes communicates with the company's centralized transaction monitoring service to look for anomalous behavior.

Meditology Services (Atlanta). Meditology Services provides consulting and management advisory to large hospitals and healthcare organizations across the country. Meditology's experts in IT risk management and healthcare IT consulting focus on assessing and developing security and compliance programs.

Menlo Security (Palo Alto, Calif.). Menlo Security's Isolation Platform contains and eliminates malware while giving a completely native experience. The company's platform uses the isolation model to ensure malware doesn't reach the endpoint to access patient data at hospitals, allowing administrators to expand internet capabilities without risking data security issues.

Microsoft (Redmond, Wash.). Microsoft invests more than $1 billion in security research and development each year and created the Microsoft Enterprise Cyber Security Group to develop solutions for Microsoft customers. The company opened its Cyber Defense Operations Center in 2015 and works with healthcare organizations' C-suites to support a culture of cybersecurity.

MicroStrategy (Washington, D.C.). MicroStrategy provides enterprise analytics and mobility software to clients worldwide. Healthcare organizations use MicroStrategy's enterprise solution to boost operational efficiency, expand businesses and improve the quality of care and patient experience. The company's healthcare solutions focus on supply chain management, revenue cycle optimization, hospital operations, population health management and claims analysis.

Mimecast (Watertown, MA). Mimecast makes business email and data safer for customers worldwide. Founded in 2003, the company's next-generation cloud-based security, archiving and continuity services protect email and deliver comprehensive email risk management. With Mimecast healthcare organizations can respond to industry risks by safeguarding protected health information, preventing advanced attacks like ransomware, archiving email and keeping employees connected during a mail server outage. Mimecast also meets healthcare privacy regulations having completed the HIPAA security compliance assessment. Mimecast delivers cloud-based email management for Microsoft Exchange, including archiving, continuity and security. By unifying disparate and fragmented email environments into one holistic solution that is always available from the cloud, Mimecast minimizes risk and reduces cost and complexity, while providing total end-to-end control of email.

NCC Group (Manchester, United Kingdom). Formed in 1999, NCC Group provides expertise in cybersecurity and risk mitigation. The company has more than 35 offices and 15,000 clients worldwide, providing a variety of services including internet of things consultancy.

NetScout (Westford, Mass.). NetScout's Adaptive Service Intelligence optimizes a hospital's analytics platforms to identify signs of outages in the hospital's network before they happen to diagnose and repair the issues quickly. The technology could prevent issues with a surgical robot powering down in the middle of surgery or video screens going dark during a procedure.

Netskope (Los Altos, Calif.). Netskope has a patented cloud-scale security platform designed to provide governance of all cloud usage while allowing real-time access to updates from the corporate network, remotely or from mobile apps. The company works with Oakland, Calif.-based Kaiser Permanente among other healthcare clients to protect against threats in the cloud and detect unusual data movement or activity.

Netwrix (Irvine, Calif.). Netwrix Auditor, a visibility platform for data security and risk management, provides clients with security analytics to detect anomalies in user behavior and investigate threat patterns. The Netwrix Auditor's solutions are HIPAA compliant.

Nexusguard. As a longtime leader in DDoS defense, Nexusguard is at the forefront of the fight against malicious internet attacks, protecting organizations worldwide from threats to their websites, services and reputations. Continually evolving to face new threats as they emerge, it has the tools, insight and know-how to protect clients' vital business systems no matter what comes their way. The overriding objective is to prevent attacks that disrupt online businesses and enable the use of the internet as intended.

Nexthink (Switzerland). Nexthink's Nexthinker is designed to help organizations reduce health information breach incidents and improve security and compliance. In the healthcare space, Nethink helps institutions secure protected health information, ensures HIPAA compliance, reduces risk for HITECH penalties and facilitates bring-your-own-device adoption for physicians and clinicians.

Northrop Grumman (Washington, DC). With corporate offices in Virginia, Northrop Grumman specializes in creating cybersecurity measures for identity management, situational awareness, modeling and simulation, cloud security, and supply chain. An active cybersecurity defense includes the necessary tools to disrupt, mitigate and neutralize cyberattacks and vulnerabilities. Northrop Grumman also offers guidance in creating situational awareness, creating contingency plans, and working through targeted networks unimpeded. This can help prepare the operational environment. Northrop Grumman is a leading global security company providing innovative systems, products and

solutions in unmanned systems, cyber, C4ISR, and logistics and modernization to government and commercial customers worldwide.

NTT Security (Ismaning, Germany). NTT Security offers security, risk and compliance services to help organizations meet immediate challenges in data security. The company's technology solutions team works alongside consulting services to give advice on the appropriate solutions for risk management.

Okta (San Francisco). Okta's IT products use identity information to grant access to applications on any device at any time while enforcing strong security protections. The platform connects companies to customers and partners securely. Okta works with CMS, New York City-based Mount Sinai Health System and Nashville, Tenn.-based Envision Healthcare, among other healthcare customers, to provide adaptive multifactor authentication and HIPAA-compliant cloud identity solutions.

OPSWAT (San Francisco). OPSWAT focuses on technologies to protect clients against cyberattacks. The company's solutions secure and manage IT infrastructure by scanning for known threats with anti-malware engines and sanitizing documents to prevent unknown threats.

Osirium (Theale, United Kingdom). Osirium's software development team aims to fill the virtual air gap for privileged account access. The company was founded in 2008 and focuses on cybersecurity and hybrid-cloud automation technology as well as privileged protection and task-automated solutions.

Ostendio (Arlington, Va.). Ostendio serves primarily healthcare clients, including WellDoc, the American College of Cariology and Higi. The company's MyVCM Cybersecurity and Information Management platform uses behavioral analytics to drive employee and vendor engagement. Ostendio's solution manages all aspects of security and allows organizations to report their security profile to internal and external stakeholders.

Palo Alto Networks (Palo Alto, Calif.) With a healthcare-specific platform for next-generation cybersecurity needs, Palo Alto offers protections for network perimeters, data centers, endpoints – including medical devices, mobile devices, and cloud computing options. Furthermore, Palo Alto has a security platform designed to keep patient data security, prioritize patient safety, and to help organizations maintain regulatory compliance. Palo Alto also offers options in threat detection, firewall, anti-malware, and sandboxing. Cybersecurity protections are available for physical platforms and virtual machines. Palo Alto Networks, Inc. has pioneered the next generation of network security with an innovative platform that allows you to secure your network and safely enable an increasingly complex and rapidly growing number of applications. At the core of this platform is a next-generation firewall, which delivers visibility and control over applications, users and content within the firewall using a highly optimized hardware and software architecture.

PhishLabs (Charleston, S.C.). PhishLabs is a 24/7 service that protect organizations against cyberattacks targeting employees or customers. Founded in 2008, the company provides a full range of services to detect attacks, identify attack operations and mitigate underlying infrastructure to stop the threat. The company also provides services and training specific to protecting patient and healthcare provider information.

Praetorian (Austin, Texas). Praetorian's solutions aim to identify and solve cybersecurity problems enterprisewide. The company's technical engineers and developers offer security expertise to minimize risk across digital assets. Praetorian offers corporate and product security solutions unified

through its software platform. In the healthcare space, the company works with medical device manufacturers to identify and address vulnerabilities.

Prevalent Networks (Warren, N.J.). Prevalent Networks focuses on risk management through a product suite focused on automated vendor risk assessment, continuous vendor threat monitoring and vertical vendor networks. Healthcare organizations can use Prevalent Vendor Risk Management to better manage and monitor third- and fourth-party business associate risks.

PriorityOne Group (Rutherford, N.J.). PriorityOne Group manages, implements and provides integrated IT services to healthcare organizations in and around Bergen County, N.J. The company focuses on guiding providers, including ASCs, through HIPAA compliance, product integration and technology acquisition.

Proficio (Carlsbad, Calif.). Proficio provides always-on cybersecurity protection and services to help customers detect and respond to or prevent security breaches. For healthcare industry clients, the company provides round-the-clock managed security services to protect confidential patient information and maintain HIPAA compliance.

Promisec (Boston). Promisec is an endpoint system, software asset management and compliance company that aims to help organizations avoid cyberthreats and attacks that lead to data breaches. The company's technology provides secure endpoints and clean audits to meet regulatory compliance standards.

Proofpoint. Proofpoint, Inc. helps the most successful companies in the world protect and govern their most sensitive business data. Proofpoint is an innovative security-as-a-service vendor that delivers data protection solutions that help organizations protect their data from attack and enable them to effectively meet the complex and evolving regulatory compliance and data governance mandates that have been spawned from highly publicized data breaches.

Protegrity (Stamford, Conn.). Protegrity aims to develop solutions to protect data throughout its lifecycle without disrupting workflow. The company can provide security across big data clusters, cloud environments, databases and mainframes. The Protegrity data security platform can protect sensitive healthcare data through tokenization and encryption technologies.

Prot-On (Spain). Prot-On provides a solution to protect files, decide who has access to files and track file activity. Healthcare organizations use Prot-On to securely store and communicate patient and prescription information as well as share health records with patients.

Protenus (Baltimore). Protenus' platform proactively monitors and protects patient privacy in EHRs. The company's technology uses artificial intelligence to understand how the workforce accessed patient records in the EHR.

Pulse Secure (San Jose, Calif.). Pulse Secure provides secure access solutions to enterprises and service providers. The company's virtual private network, network access control and mobile security products are designed for data security. In the healthcare space, Pulse Secure provides medical-grade network visibility and control solutions to support a bring-your-own-device environment and can ensure security for the internet of things.

PWC. Cyber security is more than an IT challenge, it’s a business imperative. New technologies, well-funded and determined adversaries, and interconnected business ecosystems have combined to increase your exposure to cyber attacks. Your critical digital assets are being targeted at an unprecedented rate and the potential impact to your business has never been greater. What’s at risk?

The theft of research and development information, monetization of credit card data or financial records, rapid replication of product or process, access to strategic or customer information, and the disruption of operational stability. To sufficiently protect your competitive advantage and shareholder value, your approach to Cyber Security must adapt to keep pace.

Rapid7. Rapid7's IT security solutions deliver visibility and insight that help to make informed decisions, create credible action plans, monitor progress, and simplify compliance and risk management. Over 2,500 enterprises use Rapid7's simple, innovative solutions and its free products are downloaded over one million times per year and enhanced by more than 200,000 open source security community members.

Risk Based Security (Richmond, Va.). Risk Based Security focuses on risk identification and security management tools to protect a variety of clients, including drug companies and healthcare providers. Founded in 2011, the company offers a full set of analytics and dashboards designed to identify security risks by industry. The company provides several HIPAA- and HITECH-compliant solutions for protecting patient data.

RiskIQ (San Francisco). RiskIQ focuses on digital threat management, offering the RiskIQ Community Edition giving security analysts free access to the company's solutions within a collaborative online environment. RiskIQ provides a comprehensive digital threat management platform for healthcare providers to audit, discover, monitor, investigate and mitigate threats.

RiskSense (Albuquerque, N.M.). RiskSense focuses on reducing cyberattacks and security risks. Cybersecurity practitioners founded the company as a spin-off of New Mexico Institute of Mining and Technology in Socorro, which originally conducted research as a service projects. Since then, the company has developed to advise the Department of Defense and intelligence community and create the RiskSense platform. The company also partners with healthcare organizations that have limited resources to protect against cyberattacks.

Rogue Wave Software (Boulder, Colo.). Founded in 1989, Rogue Wave has grown into a global company focused on cross-platform software development tools and embedded components. The company provides life science and medical companies with necessary tools and consulting expertise to accelerate the time it takes to bring their devices to market as well as achieve accurate and reliable results.

root9B. root9B is a dynamic provider of cyber security and advanced technology training capabilities, operational support and consulting services. root9B’s personnel are internationally recognized and trusted providers of advanced cyber solutions, satisfying requirements for missions and enterprises globally, dedicated to the delivery of solutions and services based on technical innovation and professional excellence

RSA. RSA provides more than 30,000 customers around the world with the essential security capabilities to protect their most valuable assets from cyber threats. With RSA’s award-winning products, organizations effectively detect, investigate, and respond to advanced attacks; confirm and manage identities; and ultimately, reduce IP theft, fraud and cybercrime.

Rsam (Secaucus, N.J.). Rsam sets the foundation for enterprise risk management and includes intuitive templates to deploy in complex situations. The company offers audit management, compliance, risk management, security incident response and vendor risk management, among other services. In the healthcare space, Rsam delivers a comprehensive risk assessment tool and

establishes repeatable and consistent processes to support compliance and an enterprisewide incident management program.

Rubicon Labs (San Francisco). Founded in 2012, Rubicon Labs' Zero-Knowledge Platform provides abstract key management services. The company's authorization capabilities, device security services and software can secure physicians' devices as well as medical devices to prevent hacking.

SAS Institute. SAS Cyber Security security analytics software uncovers abnormal network behavior to keep you ahead of potential threats. The software's accurate and continuous security insights help you better manage security risk and improve profitability. Real-time processing of network traffic and business data generates intelligent data. When combined with top-ranked advanced and predictive capabilities and automatic prioritization of suspicious activity, SAS Cyber Security's actionable results reduce your mean time to detect an incident.

Seclore (Sunnyvale, Calif.). Seclore focuses on document protection to allow organizations to collaborate securely. Pharmaceutical companies can use Seclore's offerings to secure and govern their internet protocol and other confidential assets. The company's electronic digital reference model provides patient protection from product dossiers, unauthorized access and issues related to file sharing.

SecureAuth (Irvine, Calif.). Founded in 2005, SecureAuth focuses on authentication to ensure all entities attempting to access data are known and verified. The company's technology offers flexible identity access control solutions to protect virtual private network, on-premises, cloud, mobile and homegrown applications. For healthcare organizations, SecureAuth protects electronic prescriptions and protected health information in a HIPAA-compliant way.

SecureMy Social (New York City). SecureMy Social technology scans social media use and warns organizations about activities that expose them to risk in real time. The platform prevents information breaches and data leaks on social media.

SecureWorks. Dell SecureWorks uses cyber threat intelligence to provide predictive, continuous and responsive protection for thousands of organizations worldwide. Enriched by intelligence from the Counter Threat Unit research team, Dell SecureWorks' Information Security Services help organizations predict threats, proactively fortify defenses, continuously detect and stop Cyber Attacks, and recover faster from security breaches.

Sedara (Buffalo, N.Y.). Sedara is a managed security service provider with clients across the U.S. The company manages network security for clients and ensures regulatory compliance, including HIPAA compliance, for organizations across the spectrum. The company provides continual data monitoring and alert systems to identify and defeat hack attempts.

SentinelOne (Palo Alto, Calif.). A group of international defense and intelligence experts founded SentinelOne to tackle cybersecurity issues with a new endpoint protection approach. The company's platform is certified as an antivirus preplacement. The SentinelOne Endpoint Protection Platform can monitor all endpoints accessing HIPAA-sensitive information and protect health information and can also predict advanced attacks and automate the threat response process.

Sera-Brynn. Sera-Brynn is a globally recognized Cyber Security audit and advisory firm dedicated to helping its clients secure their computing environments and meet applicable mandatory industry and government compliance requirements in the most economic and efficient manner possible. In addition to PCI, FFIEC, HIPAA, NERC, GDPR and other standards, security professionals are global leaders in developing, documenting and implementing FISMA, NIST, and DoD compliance requirements

across a broad range of civilian and Department of Defense federal agencies and DoD support organizations.

Shape Security (Mountain View, Calif.). Shape provides protection against web and mobile cyberattacks to corporations around the world. The company is focused on protecting against high traffic and mobile application attacks. In the healthcare space, Shape Security can protect against distributed denial-of-service attacks and keep the organization's website running.

Skybox Security (San Jose, Calif.). Skybox is a privately held cybersecurity management company established in 2002. Skybox's security platform uses firewall and network device data to detect vulnerabilities, and its powerful attack vector analytics can reduce response times for greater network control. The company covers more than 2,000 enterprises globally, including Delta Dental, Neptune, N.J.-based Meridian Health System and eHealthInsurance in the healthcare sector.

Skycure (Palo Alto, Calif.). Skycure Mobile Threat Defense is a layered solution leveraging on-device, in-could and crowd-based intelligence to defend against mobile malware, network-based threats, device vulnerabilities and physical attacks. The company's platform provides secure mobile access to EMR and patient data and meets regulatory compliance.

Skyhigh Networks (Campbell, Calif.). Skyhigh is a cloud access security broker that deals with shadow IT and sanctioned IT could data security. Skyhigh has worked with Long Beach, Calif.-based Molina Healthcare, AtraZeneca and Altamonte Springs, Fla.-based Adventist Health System in the healthcare space, providing a risk rating for the organizations and ensuring protected health information isn't stored or shared in the cloud or other non-secure space.

Sophos. Sophos helps organizations keep their data safe and stop the growing number of complex threats. It provides a full range of endpoint, encryption, email, web and NAC products, helping customers protect their businesses and meet compliance needs.

Spirion (Irvine, Calif.). Spirion provides enterprise data management software to minimize risks, costs and reputation damage associated with cyberattacks. The company's platform is designed to identify, classify and monitor personal information, medical records, credit card numbers and other intellectual property.

Stratiform (El Segundo, Calif.). PCM acquired Stratiform in January 2017. Stratiform is a cloud IT solutions provider with consulting, professional and managed services. The company specializes in Microsoft cloud technology and post-acquisition Stratiform plans to grow in the U.S. and Canada.

Swimlane (Louisville, Colo.). Swimlane is a security and operations management platform with the capability to centralize security alerts and automate attack response. The company provides security automation and orchestration to unify, analyze and resolve alerts from the organization's existing security tools and provide analysts with threat intelligence. The company's solution can also gather security metrics and generate reports on cybersecurity efforts.

Swivel Secure (West Yorkshire, United Kingdom). Founded in 2001, Swivel Secure's AuthControl Sentry authentication platform allows organizations to tailor authentication requirements according to individualized security policies. Earlier this year, the company expanded their global partner program concentrating efforts on the United States.

Sword & Shield (Knoxville, Tenn.). Sword & Shield is a holistic information security provider with solutions to evaluate, remediate and monitor data security. The company also provides consultants to assist in all aspects of the security and compliance lifecycle, including HIPAA compliance. The

company's team of experts make recommendations to increase HIPAA compliance with the HIPAA Security and Privacy kit.

Symantec (Menlo Park, Calif). Symantec offers organizations tools in advanced threat monitoring, cyber readiness, and incident response. Moreover, enterprises can receive advanced analysis of attacks, as well as the motivations and techniques of threat actors. Employees must also be ready in cybersecurity measures, and Symantec has tools to create a roles-based approach to security education and simulation exercises. CISOs can also learn how cyber insurance could potentially benefit their organization. Founded in 1982, Symantec has evolved to become the global leader in cyber security, with more than 11,000 employees in more than 35 countries. Operating one of the world's largest cyber intelligence networks, it sees more threats, and protects more customers from the next generation of attacks. Symantec helps companies, governments and individuals secure their most important data wherever it lives.

Synopsys (Mountainview, Calif.). Synopsys is a software partner for companies around the world, focused on electronic design automation and semiconductor internet protocol. The company works with healthcare organizations to address cybersecurity risks for personal patient information and medical device hacking.

Tanium (Emeryville, Calif.). Tanium's solution for hospitals and health systems provides complete visibility across managed and unmanaged endpoints to improve security hygiene. The tool allows users to ask a simple or complex question of any or all endpoints and receive a response directly from all endpoints within 15 seconds. Tanium can also collect data from third party endpoint agents to bring multiple security and IT operations under one platform, which can help streamline operations and reduce costs.

Tenable Network Security. Tenable Network Security is relied upon by more than 20,000 organizations, including the entire U.S. Department of Defense and many of the world's largest companies and governments, to stay ahead of emerging vulnerabilities, threats and compliance-related risks. Its Nessus and Security Center solutions continue to set the standard for identifying vulnerabilities, preventing attacks and complying with a multitude of regulatory requirements.

ThreatMetrix (San Jose, Calif.). The ThreatMetrix Digital Identity Network is designed to inspect digital transactions across applications, devices and locations in real time. The company also provides online fraud prevention and can pinpoint suspect behavior and fraud attempts before damage is done. The company also provides authentication for patients, payers and physicians logging into the system.

ThreatStack. Threat Stack helps you protect your cloud from intrusions and data loss by continuously monitoring and providing insights into your system activity. Securing your cloud shouldn't prevent your business from running fast. The lightweight, cloud-native design takes the hassle out of staying protected. Threat Stack's team of security and operations experts set out to create a product that's simple to deploy, keeps you protected, and gets security out of your way so you can focus on growing your business.

Thycotic (Washington, DC). Thycotic deploys smart, reliable IT security solutions that empower companies to control and monitor privileged account credentials and identity access for administrators and end users. An Inc. 5000 company, Thycotic is recognized as the fastest growing privileged management vendor in IT security and one of the top 30 fastest growing companies.

TraceSecurity (Baton Rouge, La.). TraceSecurity is a leading provider of cybersecurity and compliance solutions that help organizations of all sizes reduce the risk of cyber breaches and demonstrate compliance. With a combination of software and services, TraceSecurity can help organizations manage their information security program and supplement it with third-party validation.

TrapX Security (San Mateo, Calif.). TrapX Security's TrapX DeceptionGrid allows customers to send "traps" that impersonate systems and devices, responding like attackers in the real world, to fool and entrap attackers. Sending out multiple traps alongside real systems and devices ensures the system can identify and contain attackers before any damage is done. The technology can detect sophisticated attackers and provide real-time forensics and analysis for the hospital's security operations team to take immediate action.

Trend Micro (Irving, Texas). Trend Micro is a global cybersecurity company providing solutions for consumers, businesses and governments. The company's XGen solution was developed to help healthcare organizations improve security before, during and after attacks. Trend Micro has tools to help organizations learn how to detect, analyze, and prevent breaches and targeted attacks. Specifically, Trend Micro offers an intrusion prevention system, detection of network anomalies, custom sandboxed analysis, network threat sharing, and identification of and protection against network centric vulnerabilities. Trend Micro also utilizes ATP measures, security management tools, and weekly updates to help address known vulnerabilities.

TrustPoint Solutions (Suwanee, Ga.). TrustPoint Solutions provides IT transformation, disaster recovery and security services to healthcare organizations. The TrustPoint team provides strategic advisory, planning and implementation services to help clients leverage their IT investment.

Trustwave (Chicago). Trustwave currently works with more than 3 million businesses to protect data and reduce security risks. The company provides a flexible portfolio of services to healthcare organizations designed to protect their specific infrastructure, networks and data while remaining HIPAA and HITECH compliant.

Tufin (London, U.K.). Tuftin's security policy orchestration solutions streamline security policy management across complex, heterogeneous organizations. The company's technology alliance program partners with industry leaders to integrate the Tufin Orchestration Suite with their existing solutions.

Untangle (Sunnyvale, Calif.). The Untangle NG Firewall is designed as a single, modular platform that clients can run on their own hardware or as a virtual machine. Untangle helps the healthcare industry comply with HIPAA and HITECH through granular controls over who has access to the data.

Varonis (New York City). Varonis' platform collects, stores and analyzes metadata in real time to protect data from cyberattacks. Organizations can monitor their unstructured data using the company's platform. Varonis specializes in protecting file and email systems storing spreadsheets, word processing documents, presentations and audio and video files that contain sensitive information. The company also offers a HIPAA compliance crash course.

VASCO Data Security (Oakbrook Terrace, Ill.). With more than 10,000 customers in 100 countries, VASCO provides security access to online information with two-factor authentication, transaction data signing, e-signature and identity management solutions. In the healthcare space, the company can secure protected health information in EHRs, protect electronic prescriptions and safeguard against unauthorized manipulation of mHealth apps.

Venafi (Salt Lake City). Venafi's platform pinpoints machine identity weaknesses and automatically makes updates to lower security risks. The company's platform is designed to help healthcare organizations better secure keys and certificates against privacy breaches by strengthening the cryptology.

Vera (Palo Alto, Calif.). Vera aims to protect data with strong encryption on any device without changing the existing workflow. The company's data-centric security solution is designed for collaboration while ensuring a high level of security, visibility and control. Vera includes HIPAA-compliant verticals for healthcare providers as well as pharmaceutical companies to secure intellectual property and trial data.

Virtru (Washington, D.C.). Virtru's products allow businesses and individuals to control access to emails, documents and dataregardless of where the files are shared. In the healthcare space, the company's technology allows providers to share HIPAA-compliant emails and attachments, automatically identifying and encrypted personal health information. The company focuses on business privacy and data protection for more than 5,000 organizations worldwide.

WinMagic (Mississauga, Ontario). WinMagic is a data security solutions company that secures data where it's stored and provides enterprise-grade data encryption and key management policies across an organization's operation systems. In the healthcare space, the company's platform encrypts patient data and takes steps to ensure there won't be a compliance breach.

WhiteHat Security (Santa Clara, Calif.). WhiteHat Security focuses on securing web applications and delivering solutions to reduce the risk of cyberattacks. Healthcare providers use the company's technology as well as expertise to deploy secure applications and websites, as well as third-party apps.

Wombat Security Technology (Pittsburgh). Founded in 2008, Wombat Security Technologies received funding from the National Science Foundation and Department of Defense to develop a suite of cybersecurity software training and filtering technologies. The company evolved its provider awareness and training software to support clients' efforts to teach secure behavior. In February 2017, the company expanded its healthcare security awareness training program to include ransomware training.

Zenedge (Aventura, Fla.). Zenedge offers security for web applications and networks. The company's platform stops malicious bot traffic and distributed denial-of-service attacks and offers ongoing monitoring and security updates. The company's cybersecurity platform includes an artificial intelligence engine and advanced bot mitigation and management. Zenedge's cybersecurity solution can protect medical records and health information.

Ziften. Ziften's groundbreaking solution provides continuous real-time visibility and intelligence, enabling incident prevention, detection and response. Ziften continuously assesses user and device behaviors and highlights anomalies in real time, allowing security analysts to hone in on advanced threats faster and minimize Time To Resolution (TTR). Ziften's Endpoint Detection and Response solution allows organizations to more rapidly determine the root cause of a breach and decide on the necessary corrective actions.

Zimperium (San Francisco). Zimperium is a mobile threat management platform designed to deliver continuous cyberthreat protection for mobile devices and applications. This on-device solution can detect threats in real time. As healthcare organizations rely on mobile devices to communicate and

provide better care in the hospital and home care settings, Zimperium's zIPS app provides continuous self-service mobile threat detection and remediation.

Zix (Dallas). Zix protects business communications through email encryption. The company's solutions support around 15,000 businesses and 1,200 U.S. hospitals with email encryption, data loss prevention and bring-your-own-device security.

AUTHORIZATION & AUTHENTICATION SOLUTIONS	
1	FIREEYE
2	SAILPOINT
3	AVATIER
4	SECUREAUTH
5	AUTH0
6	OPTIMAL IDM
7	CROSSMATCH
8	IMPRIVATA
9	BETA SYSTEMS
10	CENTRIFY
11	OKTA
12	ONELOGIN
13	HEALTHCAST
14	PING IDENTITY
15	EXPERIAN
16	JANRAIN
17	ONE IDENTITY
18	ZEBRA
19	JUMPCLOUD
20	IDM WORKS

BLOCKCHAIN SOLUTIONS	
1	HASHED HEALTH
2	POKITDOK
3	IBM BLOCKCHAIN
4	HEALTHCOMBIX
5	MEDICAL CHAIN
6	HEALTH LINKAGES
7	BLOCK MD
8	BLOCKCHAIN HEALTH
9	GEM
10	TIERION
11	YOUBASE
12	HEALTHBOX
13	CORAL HEALTH
14	GUARDTIME
15	BURST IQ
16	FACTOM
17	BLOQ
18	BRONTECH
19	STRATUM
20	SCALAMED

COMPLIANCE & RISK MANAGEMENT SOLUTIONS	
1	CLEARWATER COMPLIANCE
2	EY
3	DELOITTE
4	SERA-BRYNN
5	KPMG
6	COALFIRE
7	CYNERGISTEK
8	BAE SYSTEMS
9	TELOS CORPORATION
10	DIGITAL DEFENSE
11	ACCENTURE
12	CIMCOR
13	CONTINUUM GRC
14	LOCKPATH
15	PWC
16	RISK SENSE
17	BWISE
18	NNT
19	BT GLOBAL
20	SAINT CORP

2018 Awarded Cybersecurity Vendors

ranked by Key Performance Indicators

CYBERSECURITY ADVISORY & CONSULTANTS	
1	LEIDOS
2	KPMG
3	EY
4	SECURE DIGITAL SOLUTIONS
5	CYNERGISTEK
6	IBM
7	ATOS
8	IMPACT ADVISORS
9	PONDURANCE
10	DELOITTE
11	ACCENTURE
12	NAVIGANT
13	BOOZ ALLEN HAMILTON
14	MANDIANT FIREEYE
15	CLEARWATER COMPLIANCE
16	ADVISORY BOARD
17	THE HCI GROUP
18	CHAN HEALTHARE/CROWE HORWATH
19	HPE
20	SANTA ROSA CONSULTING (FORTIFIED)

CYBERSECURITY TRAINING & EDUCATION	
1	KNOWBE4
2	INSPIRED ELEARNING
3	DIGITAL DEFENSE
4	THE SANS INSTITUTE
5	(ISC)2
6	OPTIV
7	VANGUARD
8	CIRCADENCE
9	ATAATA
10	WOMBAT
11	INFOSIGHT
12	FIREEYE
13	SECURE NINJA
14	INFOSEC INSTITUTE
15	CYBER ACES
16	ESET TRAINING
17	CYBER TRAINING 365
18	SILVERSKIN
19	KAPERSKY
20	CYBRARY

DDOS ATTACK PROTECTION	
1	IMPERVA
2	CLOUDFLARE
3	F5 NETWORKS
4	FORTINET
5	ARBOR NETWORKS
6	NEXUSGUARD
7	AKAMAI TECHNOLOGIES
8	ROOT 9B
9	CODE DX
10	A10 NETWORKS
11	RADWARE
12	CORERO
13	LINK11
14	VERISIGN
15	NEUSTAR
16	CENTURY LINK
17	LEVEL3 COMMUNICATIONS
18	KAPERSKY
19	MCAFEE
20	VIPRE

END POINT SECURITY SOLUTIONS	
1	CARBON BLACK
2	SYMANTEC
3	FORTINET
4	CHECK POINT SOFTWARE
5	DUO BEYOND
6	ABSOLUTE SOFTWARE
7	COUNTER TACK
8	TREND MICRO
9	TANIUM
10	SENTINEL ONE
11	MICROSOFT
12	MCAFEE
13	MALWAREBYTES
14	DELL SECURITY
15	CYLANCE
16	CYBERBIT
17	CYBEREASON
18	WEBROOT
19	CROWDSTRIKE
20	KAPERSKY LABS

2018 Awarded Cybersecurity Vendors

ranked by Key Performance Indicators

END-TO-END/ENTERPRISE CYBERSECURITY SOLUTIONS	
1	SYMANTEC
2	PALO ALTO NETWORKS
3	TREND MICRO
4	FIREEYE
5	NORTHOP GRUMMAN
6	CSC
7	IBM
8	CISCO
9	JUNIPER NETWORKS
10	BOOZ ALLEN HAMILTON
11	BT
12	FORTINET
13	AT&T
14	LEVEL 3
15	MCAFEE
16	NETSCOUT
17	VMWARE
18	BLACK DUCK
19	SECUREWORKS
20	KASPERSKY

ENTERPRISE ACCESS MANAGEMENT	
1	BOMGAR
2	IMPRIVATA
3	TREND MICRO
4	MICROSOFT
5	CISCO
6	SAILPOINT
7	RSA SECURITY
8	MICRO FOCUS
9	CORE SECURITY
10	IMPERVA
11	DELL
12	CA TECHNOLOGIES
13	ORACLE
14	IBM
15	SAP

ENTERPRISE FIREWALL NETWORKS	
1	FORTINET
2	SONICWALL
3	ZSCALER
4	CHECKPOINT SOFTWARE
5	PALO ALTO NETWORKS
6	CISCO
7	HUAWEI
8	FORCEPOINT
9	SOPHOS
10	JUNIPER NETWORKS
11	WATCHGUARD
12	BARRACUDA NETWORKS
13	H3C
14	STORMSHIELD
15	VMWARE
16	F5 NETWORKS
17	SECUCLOUD
18	SKYBOX SECURITY
19	WATERFALL SECURITY
20	IT SOLUTION

HEALTHCARE DATA ENCRYPTION	
1	ONPAGE
2	SENETAS
3	THALES
4	DATA LOCKER
5	SYMANTEC
6	SOPHOS
7	CHECK POINT
8	TREND MICRO
9	FLEXENTIAL
10	VIRTRU
11	APRICORN
12	BLUE FIN
13	GEMALTO
14	INTEL SECURITY
15	KAPERSKY
16	PANDA SECURITY
17	CYLANCE
18	IBM
19	SENTINEL ONE
20	NETGAIN

INTRUSION PROTECTION SOLUTIONS	
1	IMPERVA
2	CISCO
3	INTEL SECURITY (MCAFEE)
4	TREND MICRO TIPPINGPOINT
5	IBM
6	PALO ALTO NETWORKS
7	ALERT LOGIC
8	HP
9	HUAWEI
10	EXTREME NETWORKS
11	STONESOFT
12	NSFOCUS

PATIENT PRIVACY MONITORING	
1	FAIRWARNING
2	CONVERGEPOINT
3	HAYSTACK
4	IATRIC
5	CYNERGISTEK
6	MAIZE ANALYTICS
7	JERICHO SYSTEMS
8	TRUE VAULT
9	UNIVERSAL PATIENT KEY
10	SEDARA SECURITY

RANSOMWARE PROTECTION	
1	ZIX CORPORATION
2	IBOSS
3	ZSCALER
4	DIGITAL GUARDIAN
5	WEBSENSE
6	CISCO
7	SYMANTEC
8	BARKLY
9	INTEL SECURITY (MCAFEE)
10	THYCOTIC
11	BLUE COAT SYSTEMS
12	BARRACUDA NETWORKS

SECURE COMMUNICATIONS PLATFORMS	
1	DOC HALO
2	PERFECTSERVE
3	PATIENT SAFE SOLUTIONS
4	VOCERA
5	IMPRIVATA
6	SPOK
7	ONPAGE
8	TIGER TEXT
9	TELEMEDIQ
10	VOALTE
11	ON MD
12	LUA
13	QLIQ SOFT
14	UNIPHY
15	DRFIRST
16	DEVERO
17	DIAMOND HEALTH COMMUNICATIONS
18	MEDX
19	AT&T
20	MEDTUNNEL

SECURITY INFORMATION & EVENT MANAGEMENT SOLUTIONS (SIEM)	
1	SPLUNK
2	LOGRHYTHM
3	FORTINET
4	FIREEYE
5	TRUSTWAVE
6	LOGPOINT
7	NETSURION
8	IBM
9	MCAFEE
10	RAPID7
11	MICRO FOCUS
12	DELL RSA
13	BLACK STATUS
14	MANAGE ENGINE
15	SECURONIX
16	ALIEN VAULT
17	EVENT TRACKER
18	ACCEL OPS
19	FORTIFIED
20	HEWLETT PACKARD

2018 Awarded Cybersecurity Vendors

ranked by Key Performance Indicators

THREAT DETECTION & CYBER ATTACK PREVENTION	
1	DIGITAL GUARDIAN
2	SYMANTEC
3	FORCEPOINT
4	CROWDSTRIKE FALCON
5	CARBON BLACK
6	CISCO
7	TRAPX SECURITY
8	MCAFEE
9	FIREEYE
10	IBM
11	FORTINET
12	IMPERVA
13	CYLANCE
14	JASK
15	MICROSOFT
16	PHISHLABS
17	DARKTRACE
18	VERIZON
19	BT
20	ZIFTEN