AN OFFERING FROM BDO'S CYBERSECURITY PRACTICE

BDO CYBER THREAT INSIGHTS

Fall 2019 Report

SPECIAL FOCUS:
HEALTHCARE INDUSTRY

In this issue

Cybersecurity Challenges & Best Practices in the Global Healthcare Industry

The global healthcare industry is increasingly dependent on interconnected devices and connection to the internet. Today there are billions of medical devices connected to the internet worldwide. Electronic Health Records (EHR) are a rapidly growing industry valued at over $30 billion globally. EHR and medical appointments are currently available to many patients from home, and the ever-growing integration of the "Internet of Things" (IoT) technologies are all aiming at improving the patient's medical experience, the patient's health, and related health communications. Yet, those same concepts and information technologies turn into a luring target for cyber-attackers of all sorts – from petty criminals to state-sponsored cyber-attack groups.

The global healthcare industry is different from many other industries and faces some unique challenges, because it directly affects human life. This gives the security of the healthcare industry special importance, knowing that a person entrusts his or her personal details, private life, sometimes their financial information, and ultimately their well-being with the companies in the sector.

The concept of cyber-attacks targeting organizations, healthcare included, for profit and espionage is not new. Private information, be it legal, medical, financial or intellectual, is always a target for cyber-attackers. During the past three years, we have seen the tremendous growth of cyber-attacks in the healthcare industry, especially cyber-attacks using ransomware, business email compromises (BEC), and distributed denial-of-service (DDoS) attacks. Many healthcare organizations have lost their data, money, and much more, without a means to recover the losses.

One of the biggest issues is cybersecurity for medical devices and medical instruments. Countries and healthcare organizations all over the world are conducting cyber-attack drills and simulations[1], and in those cyber-attack practice sessions the medical personnel must be prepared for the possibility that the medical devices themselves, which are often connected to the internet, will be attacked and their activity disrupted. It has been widely reported that the medical staff of many hospitals internationally are often completely oblivious to the information systems they are working with, the connections between the systems, and the flow of the data collected and stored on databases relying on these machines.

Government regulators and healthcare industry senior executives must ensure that appropriate information security and data privacy measures and regulations are both established and enforced to make sure cybersecurity protocols are aligned with current threats.

The global healthcare industry needs to implement proven cybersecurity best practices, including:

- Create a cybersecurity culture for everyone within the healthcare industry, including supply chain partners/vendors
- Provide periodic cybersecurity awareness, education, and training programs for everyone within the healthcare ecosystem
- Implement special standards for medical devices lifecycle data protection
- Ensure cyber-attack incident response plan protocols
- Deploy dynamic cyber-intrusion detection systems for email systems, networks, software applications, and endpoints
- Provide full end-to-end encryption of all data within the information system and a timely software patch management program
- Conduct 24/7/365 monitoring, detection, and response services
- Provide quality data backup routines and offline secure storage of information
- Understand the changing cyber threat landscape and tailor cybersecurity solutions for the healthcare industry

It is essential that each country ensure it is doing all it can to protect the health and safety of its citizens from cyber-attacks and significant cyber data breaches in their respective healthcare industries. Cyber data breaches in the healthcare industry can result in the theft of money, personal identifiable information (PII), protected health information (PHI), payment card information (PCI), and intellectual property (IP), and it can result in the disruption of patient services and medical treatments, and even the loss of human life. The focus of this issue of our BDO Cyber Threat Insights Report is to enhance your awareness of the real and significant cyber threats facing the global healthcare industry.

Respectfully,

GREGORY A. GARRETT, CISSP, CPCM, PMP

Head of U.S. & International Cybersecurity for BDO

1 https://www.theverge.com/2019/4/4/18293817/cybersecurity-hospitals-health-care-scan-simulation

Prominent Threats to the Sector

TREMENDOUS GROWTH OF RANSOMWARE CYBER-ATTACKS GLOBALLY – ESPECIALLY IN THE HEALTHCARE INDUSTRY

While ransomware attacks have been a prominent part of the cyber threat landscape for several years, it seems that 2019 has been a banner year with a 350%+ increase in ransomware attacks worldwide. Until recently, most of the attack campaigns utilizing ransomware were widely distributed, based on massive phishing or exploit kit techniques aiming to achieve the highest infection rate. Such campaigns often use generic phishing emails with content referring to an invoice, a transaction or a contract, for example. The ransomware distributed in these massive attack campaigns is rarely custom made – in most cases, it would be a ransomware file offered for sale in underground forums for several hundred dollars or for a share of the profit. These attacks could lead to full file encryption in many cases. However, efforts made by government agencies and cybersecurity initiatives have seemed to bear fruit, as in many cases researchers succeed in developing decryption tools[2].

Unfortunately, ransomware attacks targeting healthcare institutions, government facilities, and even commercial companies are mostly distinctively different. They are highly targeted and often involve extensive preparatory research – establishing access via phishing or hacking, gaining persistence and vital service mapping. Once the target network had been studied, the attackers execute the ransomware on the chosen network areas – those that hold sensitive patient data or, alternatively, those responsible for the operation of critical medical facilities. Statistics show that ransomware detection on consumer machines dropped in 2019, while business environment detection increased by 365% since mid-2018[3].

One of the first ransomware incidents in the medical field was the Hollywood Presbyterian Medical Center attack on February 18, 2016, which leveraged the Locky ransomware. The hospital paid a $17,000 ransom in bitcoin for the decryption key for patient data[4]. Healthcare institutions and state hospitals in particular are desirable targets for ransomware attacks for the following reasons:

- **Data Value:** Medical records are considered the most sensitive data records of all. Firstly, a person's medical history is private in its nature. Secondly, an accurate and up-to-date medical record is crucial to ensure continuity of care for a patient. Thirdly, information about sensitivities and current conditions is key to ensure suitable care and could lead to life-threatening situations if tampered with. Medical records are worth 10 times more than credit card information on dark web forums.
- **Data Utility:** Unfortunately, medical data can be used by cyber-attackers in a variety of malicious activities, including extortion in exchange for the information, identity theft, financial fraud, health insurance fraud, tailored spear-phishing, and even, in some cases, industrial espionage.
- **Public Sector Security:** Many governmental medical institutions face the difficulty of being a part of the public sector. Lack of financial resources lead to difficulties in recruiting and retaining quality IT and cybersecurity personnel; purchasing and maintaining top-of-the-line cybersecurity products tailored to the organization's need; and maintaining the systems so that they are patched and protected, as well as implementing new platforms and procedures.

Not all of the ransomware attacks target the healthcare industry alone – many of the attacks, notably in 2019, targeted medical facilities as part of a campaign against the public sector. A key event is the notable "SamSam" ransomware attack – a malware which targeted public organizations, primarily in the healthcare field, mostly in the U.S. (Further information follows below.) The U.S. is the country most affected by ransomware, with some 50% of global detections originating from that country.

2 https://www.nomoreransom.org/en/decryption-tools.html

3 https://go.malwarebytes.com/q1-2019-ctnt-report-lp.html

4 https://www.latimes.com/business/technology/la-me-ln-hollywood-hospital-bitcoin-20160217-story.html

SIGNIFICANT DATABASE MISHANDLING AND MISCONFIGURATION – EXPOSING HEALTHCARE INFORMATION

It can almost be taken for granted that nowadays the majority of patient records and medical documents are uploaded to online servers, so they can be shared with patients, doctors, and anyone relevant to their care in real time. Collaboration between hospitals and medical institutions are leading to the integration of large-scale medical information via joint servers using top services such as Amazon Web Services (AWS) for research purposes. The potential is indeed enormous – data sharing and integration can lead to better preventive care, preparation for wider medical trends, and further study of new and known diseases.

Given the value and sensitivity of medical records, storing such sensitive data online while granting access to third-party professionals poses great danger and requires a tailored cybersecurity approach to these databases. However, in recent years, we have witnessed more and more cases in which medical records were poorly secured or even left utterly exposed to public view as a result of database mishandling. A survey conducted in February 2017 revealed that healthcare data breaches have affected 26% of U.S. consumers[5]. In 2018, researchers concluded that some 30% of online healthcare databases are left exposed online due to misconfiguration[6].

Such lack of attention can be found even among companies specializing in medical record management. Meditab, a medical records software maker for hospitals and pharmacies based in California, processes faxes for healthcare providers among its services. Unfortunately, the server storing the fax database was not properly secured, exposing six million records to attackers, including drug prescriptions, doctor's notes, medical data, and social security numbers[7]. In August 2019, security researchers found an exposed database with 14,000 documents that included sensitive personal and financial data from the medical billing vendor Medico[8]. The owners responded quickly to secure the database.

Medical information is sometimes handled by companies outside of the medical field. Such is the case of X Social Media, an ad company that recruits potential clients for law firms for harm and injury class actions[9]. The company left its database unprotected and open for anyone to access. The database included names, addresses, and info about the illness, accident, or injury. Such companies might not be aware of the sensitivity and value of the information they possess, or lack understanding of the risk.

None of the above incidents are equal in scale to the Hova Health data breach in Mexico, in which 2.4 million medical records were publicly available as a result of a misconfiguration of a MongoDB server[10]. Without a doubt, full recognition of the hosting service on which records are stored – as well as suitable security products assuring its protection against up-to-date threats – is key to maintaining a secured database.

5 https://newsroom.accenture.com/news/one-in-four-us-consumers-have-had-their-healthcare-data-breached-accenture-survey-reveals.htm

6 https://healthitsecurity.com/news/30-percent-of-online-health-databases-expose-patient-data

7 https://techcrunch.com/2019/03/17/medical-health-data-leak

8 https://healthitsecurity.com/news/2-misconfigured-databases-breach-sensitive-data-of-nearly-90k-patients

9 https://techcrunch.com/2019/06/14/medical-injury-claim-data-exposed

10 https://www.healthcareitnews.com/news/telemedicine-vendor-breaches-data-24-million-patients-mexico

LEGACY SYSTEMS AND UNPATCHED SOFTWARE PRESENT REAL & PRESENT DANGER TO GLOBAL HEALTHCARE

Up-to-date and fully patched operating systems and software are fundamental security measures, especially for data storage and collection environments. Running a legacy operating system, especially those that have been unsupported for five years or even longer, greatly increases the risk of a breach. Unfortunately, as many public healthcare institutions are poorly budgeted, so security procedures can fall behind in priority. Furthermore, the technical orientation level of many veteran healthcare employees is rather low, leading to them preferring to use older, simpler consumer machines during the day-to-day practice. This means that healthcare organizations can still be vulnerable to cyber-attacks that use known exploits. In such cases, an attacker may not even need to perform special preparations and study in order to access a medical database or a healthcare facility's network – one unpatched server in the network is all that's required.

In March 2017, Microsoft released a patch for an SMB vulnerability assigned CVE-2017-0144, previously exploited by the National Security Agency (NSA) for five years. The flaw, known as "EternalBlue," was used two months later in one of the biggest ransomware attacks ever observed – WannaCry. Among the affected organizations was the National Health Service (NHS) in the UK. More than 19,000 appointments had to be cancelled, and a full network cleanup was required, costing the NHS over £90 million in total. Proper patching mechanisms, or a solution which provides protection against known exploits, would have easily prevented the incident. A similar case had been observed recently, as Microsoft issued an urgent patch for a critical vulnerability dubbed "BlueKeep." (Further information can be found below.) While no exploits of the flaw have been reported yet, researchers estimate that more than 800,000 machines are still unpatched.

THE RISE OF PHISHING ATTACKS AND BUSINESS EMAIL COMPROMISE (BEC) ATTACKS IN THE HEALTHCARE SECTOR

While phishing is a dominant threat for almost all industries, it applies to the healthcare sector in particular. Phishing is the main method for attackers to initiate attacks for planting malware or stealing protected health information (PHI). A cybersecurity report published by the Healthcare Information and Management Systems Society (HIMSS) in 2019 lists phishing as the most commonly used method for initiating attacks in the health sector[11]. Moreover, a survey conducted by the Journal of the American Medical Association (JAMA) Network in March 2019 found that the click rate of phishing emails within the healthcare industry was 16.7%[12].

Healthcare systems are also uniquely vulnerable to phishing attacks. Employee turnover at hospitals is high, and there is a constant influx of new employees, including interns and students, who may have no prior cybersecurity training, which creates a continuous stream of newly susceptible employees. To train every employee who uses the hospital network would require a vast framework and a substantial budget. This risk is doubled when taking into account the large amount of IoT devices utilized in hospitals, as well as employee smartphones connected to the network.

11 https://www.himss.org/sites/himssorg/files/u132196/2019_HIMSS_Cybersecurity_Survey_Final_Report.pdf

12 https://jamanetwork.com/journals/jamanetworkopen/fullarticle/2727270

Spear-phishing techniques are becoming more and more sophisticated as well. Scammers will use hacked information to personalize emails for this type of social engineering scheme, which makes the recipient more likely to engage with the message, thinking it is a legitimate email. In the specific case of business email compromise (BEC), the scammer uses spear-phishing techniques to target a an employee and pretends to be a senior member of staff, such as a CEO, then requests sensitive information or an expedited fund transfer, claiming this is urgently needed for a vendor or known partner, but in fact the funds will go to the scammer. While scamming techniques are becoming more sophisticated, awareness of phishing attacks is growing too, but training employees in identifying phishing emails and carrying out routine testing cannot completely eliminate the risk.

One notable healthcare phishing attack that occurred this year was an attack against the Oregon Department of Human Services (645,000 patients)[13]. The information stolen included protected health information that is due special protection under federal health privacy laws. The data breach resulted from a successful phishing attack via email, in which nine employees clicked on a phishing link, granting the sender access to their accounts and, thus, the entire network.

13 https://www.oregonlive.com/data/2019/05/stolen-wages-push-some-senior-care-workers-to-the-brink-investigation-finds.html

GARTNER SURVEY SHOWS UNDERINVESTMENT IN CYBERSECURITY BY HEALTHCARE INDUSTRY

When choosing between patient care and cybersecurity for where to spend limited resources, hospitals tend to choose the former. Public healthcare institutions are in constant need of additional medical equipment, patient rooms, and professional staff. These make it a lot harder to invest in threat monitoring, network management teams, and security solutions – especially since, in the cyber threat arena, a silent, threatless period could easily trick organizations into thinking they are fully protected.

A Gartner survey reveals that healthcare providers only invest approximately 5% of their information technology budget on cybersecurity[14]. This amount places the medical sector behind the banking and financial services sector, in which 7.3% of the budget is invested.

A healthcare institution's cybersecurity budget must be properly divided between prevention, detection, response, and emergency procedures[15]. Unfortunately, underfunded organizations are naturally understaffed as well. Thus, even when preventive security products are in place, they must be complemented by professionally trained teams capable of identifying and responding to threats detected by the products. The great value of patient records, combined with the common knowledge of the lack of budget and personnel in public medical institutions, makes hospitals a lucrative victim for cyber criminals.

However, many hospitals' cybersecurity budgets are growing in line with the growing number of attacks and security awareness. According to the HIMSS Cybersecurity Survey, some 38% of all healthcare providers increased their cybersecurity budget between 2017 to 2018[16]. It appears that cybersecurity is changing from an opaque concern to a real issue felt by many hospitals, and with good reason.

14 https://www.beckershospitalreview.com/cybersecurity/5-of-hospital-it-budgets-go-to-cybersecurity-despite-82-of-hospitals-reporting-breaches.html

15 https://healthitsecurity.com/news/how-to-build-a-balanced-healthcare-cybersecurity-budget

16 https://www.himss.org/sites/himssorg/files/u132196/2019_HIMSS_Cybersecurity_Survey_Final_Report.pdf

INTERNET OF THINGS (IOT) MEDICAL DEVICE SECURITY IS ESSENTIAL

IoT systems are considered one of the weakest network components[17]. Firstly, in many cases, IoT devices use a custom-developed software adapted to a specific OS version and updated in long time intervals, forcing them to often rely on outdated software and legacy operating systems that leave them vulnerable to attacks. IoT devices are also increasingly collecting and storing vast amounts of unique data, which make them an attractive target for cyber criminals. Lastly, IoT devices may serve as an easy entry point to a network.

Medical devices and industrial systems are typically not part of an organization's core IT infrastructure, making them a lower priority for an admin or security analyst. However, once they are on the network, they are exposed to a whole range of exploits. Symantec reports a 600% increase of attacks on IoT devices, and a 29% increase in attacks involving industrial control systems[18]. Additionally, many IoT devices, especially those maintained by home users, use an outdated software version or a default password, providing an easy access point to a network that can be exploited.

The healthcare industry has seen a particularly sharp increase in the use of IoT devices, driven partly by the rise in wearables and remote patient monitoring. Clinical uses of IoT have expanded as well, and the average hospital room now contains an estimated 15 to 20 connected medical devices. A large hospital could have as many as 85,000 connected devices, and that number will only continue to rise in coming years. While these IoT devices can have a role in improving efficiencies and the delivery of care, they also increase vulnerability to cyber-attacks[19].

Another difficulty lies in the remediation of an infected IoT device after an attack has been detected. To remove malware from a medical device, the device must often have all of its software reloaded by the manufacturer itself. If a vulnerability has been uncovered, the same goes for all of those devices in use around the world. The hospital security staff is not equipped or able to access the core of these devices that have been approved by the U.S. Food and Drug Administration (FDA), and a hospital admin cannot address security incidents in IoT devices on their own.

In 2017, malware such as WannaCry and NotPetya have effectively attacked medical and IoT devices as part of vast ransomware campaigns, shutting down operations in several medical facilities and in multiple major corporations for a few hours, simply because they are easy to infect. In 2016, the poor security of IoT devices gained public attention as a massive botnet called Mirai enslaved insecure Linux-based IoT devices and leveraged them to perform DDoS attacks to knock websites offline[20]. While the Mirai botnet mainly took over devices such as security cameras, digital video recorders (DVRs), and routers, the growing use of IoT devices in the healthcare industry leads many to believe that medical devices could be the next targets if a similar attack were to take place. And since the Mirai source code was leaked and has since been utilized in similar attacks, it is not unlikely.

The interest of cyber-attackers in medical devices, as a means of gaining easy access to medical data and patient records, surfaced back in 2015. The attack vector, which has grown since then, was given the name MEDJACK – for medical device hijacking[21]. In one of the first persistent attacks published online, the attackers compromised three blood gas analyzers of a hospital. They used these devices to establish a backdoor to the hospital network for lateral movement. After the attackers infected machines in the network with malware, they stole medical data records.

As some of the devices are strictly on-premises and others are carried by the patient home and elsewhere, quality internet connectivity must be achieved at all times. Correspondingly, dynamic security against hacking attempts must be achieved at all times too. Firewalls and access rules, based on each IoT device's protocols, functions, and home network, could also protect against attack attempts by filtering out unknown connections or data transmission attempts.

17 https://blog.checkpoint.com/2019/05/29/ultrasound-iot-hack-security-risks-healthcare-medical-device-michigan-ransomware/

18 https://www.symantec.com/content/dam/symantec/docs/other-resources/2018-istr-executive-summary-for-healthcare-professionals-en.pdf

19 https://www.businessnewsdaily.com/15031-connected-medical-devices-healthcare-cybersecurity.html

20 https://krebsonsecurity.com/tag/mirai-botnet

21 https://www.securityweek.com/medical-devices-used-pivot-point-hospital-attacks-report

CYBER ESPIONAGE AND INTELLECTUAL PROPERTY THEFT INCREASE IN THE MEDICAL SECTOR

Cyber espionage activity occurs less frequently than data theft or ransomware campaigns in the medical sector. However, a recently released report suggests that this threat is on the rise, targeting organizations such as research institutions, hospital R&D units, and pharmaceutical companies[22]. The damages caused by the theft of medical compounds, clinical research findings, or sensitive test results can amount to hundreds of millions of dollars, but worst of all, it can damage the release of a drug or a new treatment, endangering patients worldwide.

Another key factor to consider when examining the threat of espionage campaigns is the nature of the attackers – competitor data and intellectual property tend to attract more nation-state actors. APT10 is an advanced espionage group affiliated with the Chinese government. Its activities are primarily aimed at intellectual property theft in accordance with China's economic development plans. The group's most notable operation is the supply chain attack 'Cloud Hopper' against managed service providers (MSPs) to collect sensitive data from their customer networks. Among their targets are healthcare organizations, and APT10 had previously used healthcare-themed phishing documents to target medical companies[23].

Chinese APT (advanced persistent threat) groups stand out in the medical cyber espionage field with another group – APT41. The group establishes and maintains strategic access to organizations in the healthcare industry, among others, using custom-designed tools[24]. According to a report, between 2014 and 2016, APT41 carried out a campaign targeting a medical device manufacturer. The targeted machines and spoofed addresses reveal that the group attempted to reach the company's IT staff and the software in use.

It appears that Chinese APT groups pose the greatest threat in this field, probably due to China's universal healthcare by 2020 initiative, which motivates it to improve its medical and pharmaceutical research. Healthcare cyber espionage may also open the door to financial gain, as it could enable Chinese companies to distribute new drugs faster than their Western competitors.

22 https://www.fireeye.com/blog/threat-research/2019/08/healthcare-research-data-pii-continuously-targeted-by-multiple-threat-actors.html

23 https://www.alienvault.com/blogs/labs-research/apt10-group-targets-multiple-sectors-but-seems-to-really-love-mssps

24 https://www.fireeye.com/blog/threat-research/2019/08/apt41-dual-espionage-and-cyber-crime-operation.html

Healthcare Sector - Notable Attacks

UNITYPOINT PHISHING ATTACK AFFECTED 1.4 MILLION PATIENTS

UnityPoint, a network of hospitals and clinics located in Iowa, Illinois, and Wisconsin, discovered a widespread breach in May 2018[25]. The attackers used phishing emails to get credentials that provided access to the company's email system. While the breach did not include other internal systems, UnityPoint notified 1.4 million customers that sensitive personal information and PHI could have been exposed by the breach of the email system[26]. This was in addition to a separate phishing attack discovered by UnityPoint in February 2018, which impacted 16,400 patients[27]. A class action lawsuit was filed over the breaches.

RANSOMWARE ATTACK DISRUPTED EMERGENCY SERVICES AT OHIO HOSPITAL

On November 25, 2018, there were reports[28] of an unnamed ransomware attacking two hospitals in Ohio. The hospitals – East Ohio Regional Hospital and Ohio Valley Medical Center – suffered numerous disruptions, including emergency squads being diverted, several systems taken offline, and having to use paper charting. However, the hospitals' security was able to stop the attack at an early stage, preventing it from causing further damage. No information breach has been reported.

ATRIUM HEALTH BILLING VENDOR BREACH EXPOSED 2.65 MILLION PATIENT RECORDS

For a week in late September 2018, an unauthorized third party accessed databases that held payment records for approximately 2.65 million Atrium Health patients, ZDNet reported[29]. This large-scale breach occurred through Atrium Health's billing vendor, AccuDoc Solutions. The records included patients' names, addresses, birthdates, insurance information, and other account details. Worse still, the breach also exposed approximately 700,000 Social Security numbers, although credit card information was not affected. Atrium Health stated that the unauthorized access did not allow for download or removal of the records. The organizations reported the breach to the FBI, and no misuse of data was found.

25 https://eu.desmoinesregister.com/story/news/health/2018/07/30/unitypoint-data-breach-million-patients-email-hack-hacked-phishing-e-mail-health-care-iowa/866760002/

26 https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

27 https://madison.com/wsj/news/local/courts/class-action-lawsuit-filed-against-unitypoint-over-data-breach-disclosed/article_68c2c679-3dbf-5d92-9280-697efe81868f.html; https://madison.com/wsj/news/local/health-med-fit/lawsuit-mulled-in-second-unitypoint-health-data-breach-this-year/article_0dbc2774-2b2a-5624-be97-9c2029ccf9eb.html

28 https://www.forbes.com/sites/leemathews/2018/11/28/ransomware-attack-disrupts-emergency-services-at-ohio-hospital/; http://www.timesleaderonline.com/news/local-news/2018/11/hospitals-patient-information-safe-in-eorh-ovmc-computer-attack

29 https://www.forbes.com/sites/leemathews/2018/11/28/ransomware-attack-disrupts-emergency-services-at-ohio-hospital/; http://www.timesleaderonline.com/news/local-news/2018/11/hospitals-patient-information-safe-in-eorh-ovmc-computer-attack

SAMSAM RANSOMWARE ATTACKS CONTINUE

On October 30, 2018, the cybersecurity company Symantec presented a report[30] on the activity of "SamSam" (aka "samas" and "MSIL.B") ransomware. The report stated that the ransomware was behind several notable attacks and primarily targeted healthcare organizations. It had been active throughout 2018, mostly in the United States, and used vulnerabilities in remote desktop protocols (RDP), Java-based web servers, and file transfer protocol (FTP) servers to gain access to the victims' networks, or used "brute force" attacks against weak passwords to obtain initial access.

One of the attacks targeted networks for the city of Atlanta on March 22. The considerable scope of the attack made it one of the worst cyber incidents to hit a U.S. city. As Reuters reported in June that year: "More than a third of the 424 software programs used by the city have been thrown offline or partially disabled. … Nearly 30 percent of the affected applications are considered 'mission critical,' affecting core city services, including police and courts."[31] The attackers demanded $51,000 worth of bitcoin, which the city reportedly declined to pay, while the recovery process was estimated to cost millions of dollars.

On November 28, the U.S. Department of Justice (DOJ) announced an indictment[32] against Faramarz Shahi Savandi and Mohammad Mehdi Shah Mansouri, accusing the two Iranians of developing the "SamSam" ransomware. The indictment alleged that the two men acted from Iran to deploy the ransomware beginning in December 2015. Per the DOJ, their "more than 200 victims included hospitals, municipalities, and public institutions," and the two men "collected over $6 million in ransom payments to date, and caused over $30 million in losses to victims."

MISCONFIGURED UW MEDICINE DATABASE CAUSED MAJOR HEALTH DATA BREACH

The Seattle-based medical system UW Medicine was reported[33] to have suffered a major breach on December 4, 2018. The breach affected 974,000 patients for approximately three weeks and exposed patient names, medical record numbers, and lab tests, but not Social Security numbers, financial information, or medical records. The compromised information may have contained private and sensitive details, such as test results for HIV and dementia. It was reported[34] that contacting all the affected patients would cost around $1 million, but the estimated cost of the full response was not published.

The unidentified attacker exploited an error that occurred when the sensitive information was moved to a new server, resulting in a database misconfiguration. This misconfiguration left the database open to search engines such as Google.

1.5 MILLION PATIENTS IMPACTED BY INMEDIATA CYBER DATA BREACH

On May 21, 2019, it was reported[35] that a misconfigured website of the Inmediata Health Group left more than 1.5 million patients' personal information open to access. The company, which provides clearinghouse services, as well as software and business process outsourcing tools for the health industry, had discovered in January that some health information of its patients was allowed to be indexed by search engines.

Upon discovery, the issue was fixed and there was no reported evidence of copying or saving the exposed information, yet the company did not promptly notify its clients about the potential exposure. The information included patients' names, addresses, dates of birth, and gender, as well as medical claims data like dates of service, diagnosis codes, procedure codes, and treating physicians. Some patients' Social Security numbers were also exposed. The Michigan Attorney General became aware after Inmediata was reported[36] to have sent multiple letters to the same people, with some of the letters misaddressed to other names.

30 https://www.symantec.com/blogs/threat-intelligence/samsam-targeted-ransomware-attacks

31 https://www.reuters.com/article/us-usa-cyber-atlanta-budget/atlanta-officials-reveal-worsening-effects-of-cyber-attack-idUSKCN1J231M

32 https://www.justice.gov/opa/pr/two-iranian-men-indicted-deploying-ransomware-extort-hospitals-municipalities-and-public

33 https://www.bankinfosecurity.com/misconfiguration-leads-to-major-health-data-breach-a-12042

34 https://www.seattletimes.com/seattle-news/health/uw-medicine-mistakenly-exposed-information-on-nearly-1-million-patients

35 https://healthitsecurity.com/news/mailing-error-for-inmediata-while-reporting-health-data-breach

36 https://www.michigan.gov/ag/0,4534,7-359-92297_47203-496435--,00.html

IMPERIAL HEALTH RANSOMWARE ATTACK IMPACTED MORE THAN 116,000 PATIENTS

Imperial Health, a Louisiana-based physicians' network, reported in August 2019 about an unnamed ransomware attack detected in May of that year that compromised files and a database for its Center for Orthopedics. That database contained PHI for more than 116,000 patients. While there was no evidence that patient information was accessed or stolen in the attack, Imperial Health notified the affected patients about the breach[37].

AMERICAN MEDICAL COLLECTION AGENCY (AMCA) DATA BREACH COMPROMISED 20 MILLION CLIENT RECORDS

The American Medical Collection Agency (AMCA) suffered a long-term data breach between August 1, 2008, and March 30, 2019. The information stolen included first and last names, dates of birth, addresses, phone numbers, dates of service, providers, and balance information.

AMCA acts as a third-party billing collections firm for medical testing corporations such as LabCorp and Quest Diagnostics. These companies use AMCA's payment portal to bill their medical consumers. Therefore, despite being a small firm, AMCA holds information of a vast number of clients. In the breach, over 20 million clients' information from various medical testing firms was compromised[38].

In the case of LabCorp, some 7.7 million customer records were exposed. This followed AMCA's notification of Quest Diagnostics – LabCorp's competitor – that attackers were able to obtain personal, financial, and medical data of nearly 12 million of its patients.

AMCA eventually filed for bankruptcy due to the disastrous costs of the data breach, which included IT support costs, legal fees, and loss of business[39]. Many lawsuits were filed against AMCA because of their delayed disclosure of the information about the incident. Not much is known about how the breach occurred and who was responsible for it; it is also unclear how the breach took place for so long without being detected.

37 https://www.hipaajournal.com/imperial-health-ransomware-attack-impacts-more-than-111000-patients

38 https://techcrunch.com/2019/07/17/millions-patients-amca-breach

39 https://techcrunch.com/2019/07/17/millions-patients-amca-breach

Notable Global Events – Q3 2019

MICROSOFT URGES USERS TO INSTALL "BLUEKEEP" PATCH

Following a May 2019 report, Microsoft issued a statement urging companies to install the "BlueKeep" vulnerability patch. In an irregular move, the company released the patch for older platforms like Server 2003 and Windows XP, which are no longer updated or supported. In June, the NSA[40] and several other cyber authorities[41] published a statement as well, prompting the users to block the TCP port 3389 on their firewall, disable unneeded remote desktop services, and enable network level authentication.

The vulnerability, labeled CVE-2019-0708, makes use of the remote desktop protocol (RDP) and allows remote code execution (RCE) on the target system. This allows the potential attacker to install programs, view, change, or delete data, and create new accounts with full user rights[42]. The vulnerability does not require authentication or any user interaction, only a specially crafted request to the target systems' remote desktop service via RDP. Because of this ability to create accounts and generally act before any check happens, Microsoft called this vulnerability "wormable,"[43] in the sense that a malware using it will be able to spread from one infected system to another. Although there is no reported exploit of the vulnerability "in the wild," more than 800,000 systems[44] were estimated to be unpatched and vulnerable.

"ROBBINHOOD" RANSOMWARE SHUT DOWN COMPUTER SYSTEMS IN BALTIMORE

As of May 7, 2019, computer systems for the city of Baltimore were attacked[45] by ransomware from an actor calling itself "RobbinHood," which affected thousands of computers and public systems. City officials decided not to pay the ransom and attempted to recover the systems independently. The ransom request amounted to $76,000, but the damage caused due to the shutdown was estimated at more than $18 million. The identity of the person or persons behind "RobbinHood" are not clear. Until its shutdown on June 3rd, they had operated a Twitter account @Robihjbn, where they published documents allegedly from the compromised systems, and sent tweets mocking the mayor and members of the city council.

The ransomware reportedly used the "EternalBlue" exploit – a tool leaked by the "ShadowBrokers" group in April 2017 and used in large-scale ransomware attacks like WannaCry (May 2017), NotPetya (June 2017), and others – and leverages a vulnerability which allows a remote attacker to perform RCE on several, mostly older, Windows systems[46]. However, some researchers doubt this, claiming the ransomware's code is fairly standard, without special additions in the vein of "EternalBlue[47]."

40 https://www.nsa.gov/News-Features/News-Stories/Article-View/Article/1865726/nsa-cybersecurity-advisory-patch-remote-desktop-services-on-legacy-versions-of

41 https://www.us-cert.gov/ncas/alerts/AA19-168A; hxxps://www.cyber.gov.au/news/protect-against-BlueKeep

42 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708

43 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708

44 https://www.bitsight.com/blog/industry-response-to-bluekeep-vulnerability?utm_campaign=public-relations&utm_source=public-relations&utm_medium=referral; hxxps://www.wired.com/story/microsoft-bluekeep-patched-too-slow/?verso=true

45 https://www.news18.com/news/tech/hackers-take-down-an-entire-citys-cyber-infrastructure-using-nsa-made-tool-2160317.html

46 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0144

47 https://krebsonsecurity.com/2019/06/report-no-eternal-blue-exploit-found-in-baltimore-city-ransomware/;
https://www.darkreading.com/threat-intelligence/robbinhood-inside-the-ransomware-that-slammed-baltimore/d/d-id/1334874

GOLDBRUTE BOTNET ATTACKED 1.5 MILLION SERVERS BY EXPLOITING "BLUEKEEP" RDP VULNERABILITY

According to research[48] published by the SANS Technology Institute in June 2019, a botnet called "GoldBrute" was discovered; it attempts to leverage the aforementioned "BlueKeep" vulnerability by conducting a "brute force" attack against potentially vulnerable servers. It is estimated that the botnet targets around 1.5 million servers, and the number is expected to grow as the scanning continues. The botnet harvests credentials to remote servers with open and/or vulnerable RDP connections. Generally, the botnet is controlled by a single C&C server, and exchanges data with the network via encrypted connections to collect valid username and password combinations.

SODINOKIBI RANSOMWARE DISTRIBUTED VIA HACKED CLOUD AND SECURITY SERVICE PROVIDERS

One of the more notable ransomware events of 2019, and specifically since April 2019, was the worldwide and alarmingly fast-paced spread of the "Sodinokibi" ransomware. Different estimations point at hundreds of organizations across the U.S. alone which have been infected with the ransomware. In the case of Sodinokibi, the attackers gained access to several types of service providers, according to the targeted organizations. More specifically, attacked service providers include Webroot Antivirus, Kaseya IT software, and a cloud backup service. The incidents, in which the attack was carried out via an external cloud backup software, make the attacked organization extremely vulnerable for ransomware attacks, since in this case the organization is deprived of the possibility to restore the compromised systems to their former status and retrieve the encrypted files. It seems that in these cases, the only option available at this stage is paying the ransom and hoping that it would indeed result in receiving the files back.

Upon gaining access to the service provider, the attackers release a bat script to download an additional payload – the Sodinokibi ransomware – and execute it in memory. Once the ransomware is executed, it deletes shadow copies and executes the ransomware functions – file encryption and ransom note display. Sodinokibi does not feature worm or auto-spread capabilities. It relies on manual execution via a compromised third-party control console or other tools such as PsExec.

The Sodinokibi ransomware is utilized by multiple threat actors in a Ransomware-as-a-Service (RaaS) model. The business model of RaaS is based on the fact that many actors would like to enter the ransomware business, which is deemed highly profitable, but lack the technological skills required to write a ransomware and a control panel. When offered as a service as part of an affiliates program, the buyer is granted a functioning ransomware and a comprehensive management panel, which allows them to monitor infections, profits, and decryption keys. The operation's revenue is then split between the attacker and the ransomware author, based on an agreed commission (usually around 40%).

As Sodinokibi is a RaaS, it is harder to attribute it to a specific actor. In most cases, actors who use RaaS are unskilled hackers wishing to easily enter the threat landscape without actually writing a code of their own. Such attackers often hire distribution services as well. Yet, the aforementioned campaign is different, in the sense that there is a reason to suspect an advanced actor behind the ransomware wave. The use of supply-chain attacks and the carefully chosen service providers suggest that an advanced threat actor has used the rented service, probably to cover their tracks.

48 https://isc.sans.edu/forums/diary/GoldBrute+Botnet+Brute+Forcing+15+Million+RDP+Servers/25002

DATA BREACH IN BIOSTAR 2 BIOMETRIC SECURITY PLATFORM AFFECTED MILLIONS OF USERS

The cybersecurity company vpnMentor reported[49] in August about a large data leak from a biometric security platform used in over 5,700 companies. Some of them are "large multinational businesses, governments, and banks," per the report. The platform, named BioStar 2 and integrated into the AEOS access-control system by the Suprema company, is a centralized application which allows admins to control access to secure areas of facilities, manage user permissions, integrate with third-party security apps, and record activity logs.
The researchers were able to access, among other sensitive information, over 27.8 million records containing plaintext usernames and passwords, and over one million fingerprint and face-recognition entries. The vulnerability that allowed access to the database, as well as attack attempts by threat actors, were not disclosed.

The leaked information, which also included mobile device information and employee clearances, could be leveraged by threat actors to hack into secured facilities and possibly even manipulate security protocols. Affected businesses include the U.S.-based companies Phoenix Medical, Lits Link, and Union Member House. Additional affected companies include Britain's Farla Medical, Germany's Identbase, and India's Power World Gyms franchise.

49 https://www.vpnmentor.com/blog/report-biostar2-leak

SPOTLIGHT

Protecting the Healthcare Industry Through Threat-Based Cybersecurity

When it comes to cybersecurity, you're only as strong as your weakest link. Three healthcare organizations learned that the hard way after they fell victim to one of the largest medical data hacks in history.

The incident, reported in June, arose from an eight-month breach of the debt collector American Medical Collection Agency (AMCA), which exposed the information of more than 20 million patients of Optum360, LabCorp and BioReference. The widespread hack and ensuing expenses led directly to bankruptcy filing for Retrieval Masters Creditors Bureau, AMCA's parent company. The incident also underlined how healthcare organizations face additional vulnerability from working with multiple partners and vendors that operate with varying levels of cybersecurity.

Healthcare organizations hold a trove of valuable data that makes an attractive target for cyberattackers, with the electronic health records (EHR) industry valued at more than $30 billion globally. These records can include a patient's name, address, phone number, date of birth, insurance information, payment card information (PCI), protected health information (PHI) and more, which could facilitate a wide range of criminal activity.

The healthcare industry has seen a sharp rise in cyberattacks over the last three years, especially those using ransomware, business email compromise (BEC) and distributed denial-of-service (DDoS). The insurer Beazley found that healthcare led all other industries in attacks and breaches during 2018, with more than double the second-highest industry. Organizations face an uphill battle in protecting against an increasingly sophisticated array of threats from cybercriminals, hacking groups, nation-state actors and even their own staff.

Ransomware attacks pose a relatively new problem, usually seeking to take over and encrypt an organization's files and offering the decryption key in exchange for a ransom, typically to be paid in cryptocurrency. These types of attacks have risen significantly in 2019, with a Malwarebytes report showing business detection of ransomware increased 365% between June 2018 and June 2019. While some organizations have opted not to pay the ransom in such attacks—instead choosing the painstaking and costly work of trying to restore systems from backups, if available—the healthcare industry has limited options. Prompt access to accurate medical records and patient information is vital to effective medical care, so a ransomware attack can pose a life-or-death situation.

Complicating data security even further, the proliferation of internet-connected devices has created more points of access and vulnerability than ever before. The quest for faster, more convenient medical care has led to a rise in telemedicine and remote patient monitoring, accompanied by wearables and clinical devices that transmit health data. The market for so-called Internet of Medical Things is expected to exceed $150 billion by 2022, more than a three-fold increase from 2017. Unfortunately, many of these devices use outdated software with minimal security that can't be easily patched or updated against newfound threats.

Worse still, many healthcare organizations—especially those in the public sector—tend to be relatively underfunded, understaffed and undertrained for cybersecurity, often relying on outdated legacy systems that increase the likelihood of breaches and database mismanagement. Faced by evolving threats, increased points of vulnerability and lagging security measures, the healthcare industry must respond with a strategic approach to cybersecurity.

THREAT-BASED CYBERSECURITY

To protect this wealth of important data across sprawling channels of operation, healthcare entities should foster an organization-wide focus on cybersecurity, so that all personnel understand the risks and best practices. Threat-based cybersecurity takes a proactive approach to identify high-value data, assess data storage and transmission for vulnerabilities, and mitigate the most likely risks and attack vectors. This maximizes the efficacy of cybersecurity resources by focusing on an organization's unique threat profile. Achieving this comes as part of a continuous process that responds to emerging cyber threats.

The U.S. Department of Health and Human Services (HHS) lists more than 300 instances where a reported breach of PHI affected at least 500 individuals—and those are just from the first nine months of 2019. These occurred in at least 45 different states and impacted more than 37 million people in total. Among these, 62% were attributed to a hacking or IT incident, and a staggering 79% targeted healthcare providers.

As the AMCA incident underlined, healthcare organizations face increasing vulnerability from third-party vendors and proliferating points of access. That vulnerability is only going to grow as silos on the healthcare supply chain blur. By examining large-scale data breaches and assessing the methods of cyberattackers, each healthcare organization can better craft a threat-based approach to cybersecurity centered around their unique profile.

2019 ENTITY TYPES

Covered Entity Type	Entity Type Amount	Entity Type %
Business Associate	33	10%
Health Plan	34	10%
Healthcare Clearing House	2	1%
Healthcare Provider	261	79%
Total	**330**	

2019 BREACH TYPES

Breach Type	Breach Type Amount	Breach Type %
Hacking/IT Incident	203	62%
Improper Disposal	4	1%
Loss	9	3%
Theft	27	8%
Unauthorized Access/ Disclosure	87	26%
Total	**330**	

Healthcare organizations can take several concrete steps to detect and respond to risks more effectively, including:

- **Bolster their access controls** – technical policies and procedures to ensure only authorized employees have access to protected health information (PHI) via Electronic Health Records (EHR), and personal identifiable information (PII)—and be more stringent about who they grant access.
- **Implement stronger audit controls** – to track and identify internal and external access to and exploration of information systems that contain PHI and PII.
- **Strengthen intrusion detection systems (IDS)** – to more accurately monitor traffic moving throughout their email, network, and information system endpoints to identify suspicious activity and clear threats in real time.
- **Make top-down personnel education a priority for everyone** – from the Board of Directors, to the C-Suite, managers, and employees, ensure all individuals with access to an organization's networks, medical devices and data understand their roles and responsibilities in defending against cyber threats.
- **Create an internal and external crisis communications plan** – to align with existing enterprise risk management frameworks (i.e., HIPAA, HITRUST, NIST, etc.).
- **Implement cyber insurance claims preparedness and adequate coverage** – to identify and quantify incurred event response costs for inclusion in an insurance claim.
- **Create an incident response plan** – to include the participation of organization leadership and key personnel from all technology, business, administration and clinical functions.
- **Develop and test a Business Continuity Plan (BCP)** – in order to have real information resilience it is vital to have an effective information back-up capability which can quickly replace any data loss.

With increased adoption of technologies (i.e., cloud computing, data analytics, automation, artificial intelligence, IoT and blockchain) across the healthcare industry, threat-based cybersecurity can form an integral part of digital transformation efforts that will help carry the business forward through the next decade.

Learn more here about how BDO can help you throughout your organization's unique lifecycle.

BDO Cyber Threat Intelligence (CTI) Services

THREAT INTELLIGENCE – "PROACTIVE DETECTION OF A BREACH"

Situational awareness is "the perception of environmental elements and events with respect to time or space, the comprehension of their meaning and the projection of their future status," while intelligence is "the ability to acquire and applied knowledge and skills."

BDO Cyber Threat Intelligence (CTI) is a combination of both: the objective of acquiring knowledge and skills to support better organizational ability and anticipate cyber events that could impact the future status of the business environment.

The BDO CTI Reports are based on research performed by the BDO Cybersecurity Centers. Our Cyber Threat Intelligence Centers in the U.S. and Israel work as an integrated team to transform reactive organizational situational awareness into proactive situational awareness to Cyber Threats. This enables an organization to better understand the likelihood and characteristics of a breach and enables an additional layer of proactivity in the detection of unidentified breaches that might be happening.

HOW DOES IT WORK?

Cybersecurity Research

Our Cyber Research teams reverse-engineer cyberattack techniques, malicious code and lateral movement to identify actual targets and methods used by different perpetrators with different malicious agendas.

Online Fictitious Identities

Our Cyber Intelligence team maintains online fictitious identities to enable their activity within threat communities, to infiltrate an online forum or create a connection with suspected threat actors or hackers, and establish online 'chatter' platforms, to establish 'trusted' conversation environments.

Monitoring Cybercrime Forums

Our Cyber Intelligence team monitors various cybercrime forums to identify premeditated attacks on organizational networks or personnel by monitoring any type of hostile chatter regarding these 'targets.'

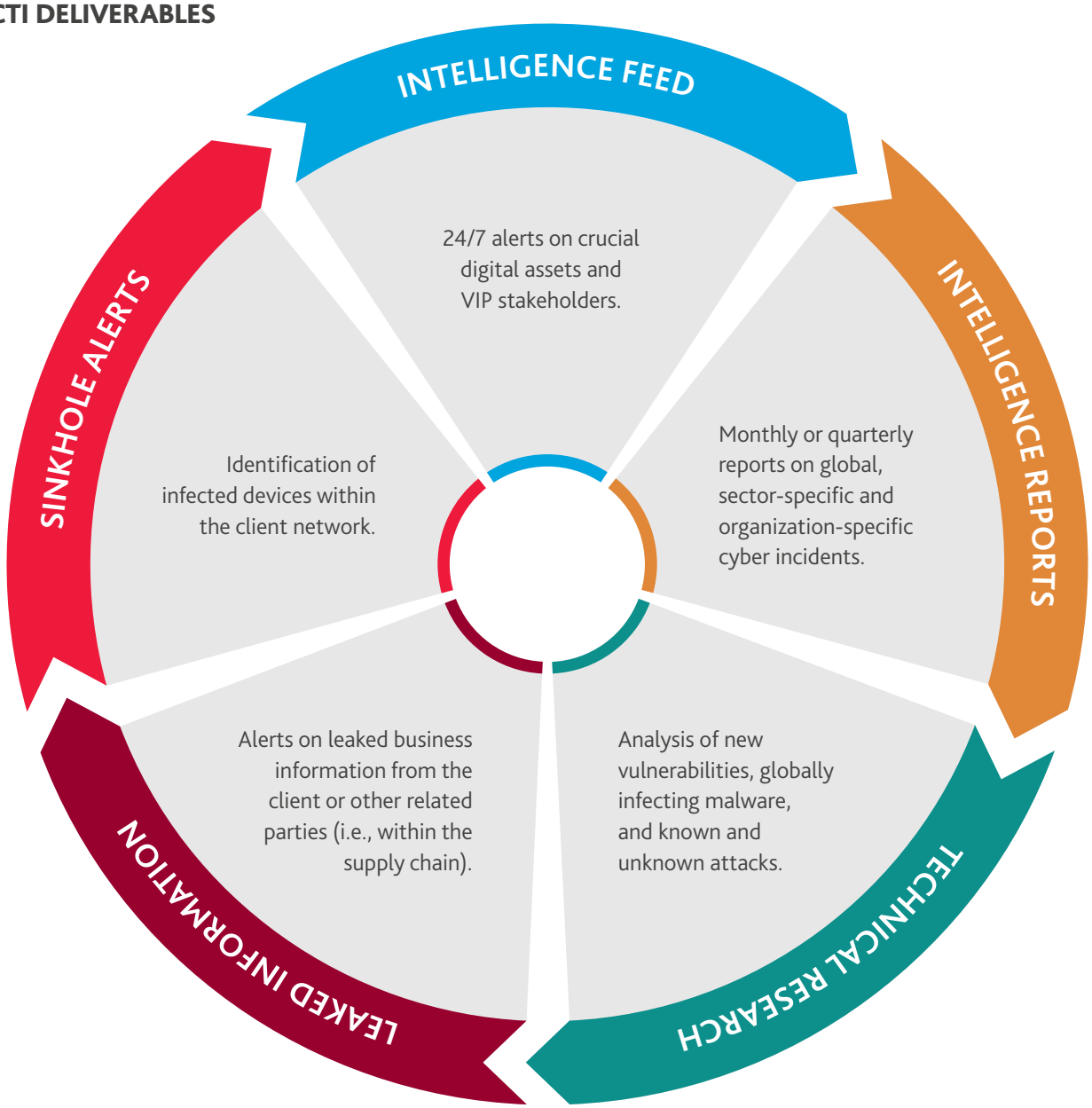
Monitoring Data Leakage Platforms

Our team can trawl hacker-oriented data leakage platforms to identify specific data leakage that might lead to a potential attack against an organization.

CONTACT:

ERIC CHUANG
Managing Director,
Cybersecurity Advisory Services
echuang@bdo.com

BDO CTI DELIVERABLES



BDO Cybersecurity Services

PAYMENT CARD INDUSTRY (PCI)

- PCI assessment and remediation
- Third-party assessments

INFORMATION GOVERNANCE AND DATA PRIVACY

- Data mapping
- Data privacy assessments
- Data privacy strategy and implementation
- Privacy officer consulting
- Information governance assessments

CYBER INSURANCE

- Cyber insurance claim preparation
- Coverage adequacy evaluation

INCIDENT RESPONSE

- Data breach investigations
- Network/host active threat monitoring
- Threat hunting - exec, enterprise, nation state, insider
- Threat intelligence - deep/dark web, social media analysis
- Training & testing - 1st responder, table top, RED team, simulations
- IR data analytics

CYBER RISK ASSESSMENTS

- Risk assessments against multiple frameworks
- Cyber risk remediation

CYBERSECURITY STRATEGY, POLICY AND PROGRAM DESIGN

- CIO & CISO advisory services
- Cyber strategy consulting
- Regulatory compliance
- Government relations consulting

CYBER THREAT INTELLIGENCE

- Dark web recon
- Dark web analysis
- Social media

MANAGED SECURITY SERVICES

- Network Operations Center (NOC)
- Security Operations Center (SOC)
- Penetration testing
- Vulnerability assessments
- Cybersecurity education, training, & simulations
- Security Incident & Event Management (SIEM)
- Email & Network Attack Detection & Monitoring Services

Cybersecurity Leadership Team

GREGORY GARRETT
Head of U.S. & International Cybersecurity
703-770-1019 / ggarrett@bdo.com

GREG SCHU
Partner
612-367-3045 / gschu@bdo.com

MICHAEL STIGLIANESE
Managing Director
212-817-1782 / mstiglianese@bdo.com

JEFF WARD
National Managing Partner,
Third Party Attestation Services
314-889-1220 / jward@bdo.com

STEVEN SHILL
Practice Leader Healthcare
Excellence & Innovation
714-668-7370 / sshill@bdo.com

JESSICA ALLEN
Director
513-592-2375 / jessica.allen@bdo.com

ERIC CHUANG
Managing Director
202-644-5435 / echuang@bdo.com

FRED BRANTNER
Director
206-403-4036 / fbrantner@bdo.com

People who know Cybersecurity, know BDO.