

BDO CYBER THREAT INSIGHTS

Fall 2020 Report

SAFEGUARDING HIGHLY TARGETED
INDUSTRIES FROM CYBERATTACKS

In this issue

CYBER THREATS INCREASING IN NUMBER AND SOPHISTICATION **4**

FOCUS INDUSTRY: HEALTHCARE AND LIFE SCIENCES **6**

- 1. High-Value Data and Inadequate Security Spending **6**
 - 2. Common Cyber Threat Vectors **7**
-

FOCUS INDUSTRY: FINANCIAL SERVICES **8**

- 1. Increasing Vulnerabilities and Significant Consequences **8**
 - 2. Invest Now to Prevent Higher Costs Later **9**
 - 3. Cybersecurity in Financial Services Is a National Security Issue **9**
-

FOCUS INDUSTRY: TECHNOLOGY **10**

- 1. Greater Connectivity Brings New Risks **10**
 - 2. Changing the Conversation on Data Privacy **11**
 - 3. Regulatory Scrutiny and Expanding Privacy Legislation **11**
 - 4. Innovating With Intent **11**
-

SPOTLIGHT: INTERNET OF THINGS (IOT) DEVICES **12**

- 1. The Trouble With Connected Devices **12**
 - 2. Case Study: Prolonged Vulnerabilities in Medical Devices **12**
 - 3. Current Vulnerabilities and Severe Consequences **13**
-

CYBERSECURITY FOR ALL INDUSTRIES **14**

- Top Priorities for Cybersecurity in All Industries **14**
-

BDO CYBER THREAT INTELLIGENCE (CTI) SERVICES **16**

BDO CYBERSECURITY SERVICES **18**

CYBERSECURITY LEADERSHIP TEAM **19**



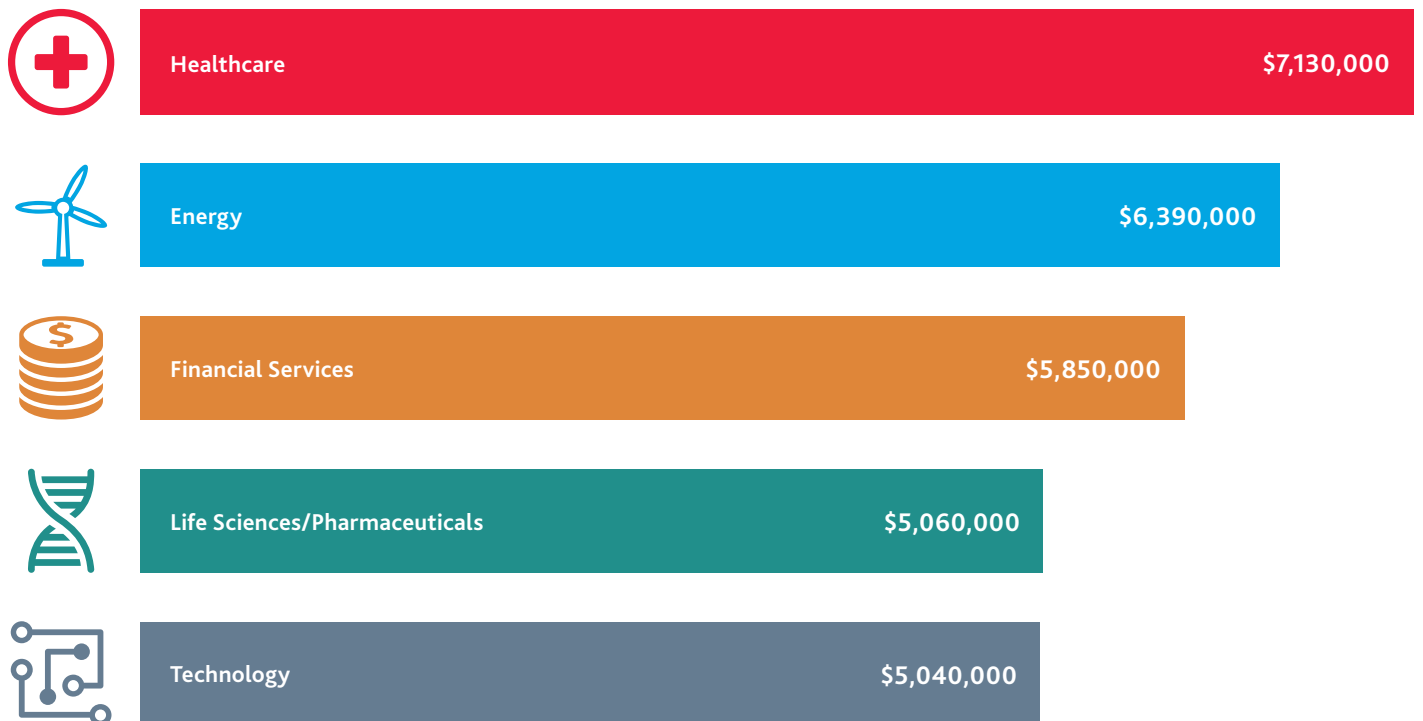
Cyber Threats Increasing in Number and Sophistication

Businesses have faced many acute challenges in 2020, and cyber threats rank high on that list. The COVID-19 pandemic brought abrupt business interruption and drastic revenue changes for many industries. Worse still, the sudden disruptions also opened new opportunities for cyberattackers, as many businesses rapidly adapted by leveraging technology solutions and shifting to a remote workforce where possible. As digital adoption accelerates concurrently with an increasing threat of cyberattacks and data breaches, businesses must take swift action to bolster their cybersecurity practices and build resilience.

Cyber threats formed a chief concern for businesses even before the pandemic, with 39% of middle market executives saying cyberattacks and privacy breaches are their primary digital threat, according to BDO's [2020 Digital Transformation Survey](#). The widespread disruption caused by COVID-19 has further stoked those threats.

The [rush to enable remote work](#) and systems access for employees prized connectivity and operational continuity over network security. Many newly remote employees [use personal laptops](#) and devices for work but have not received additional cybersecurity training. Remote employees are also more likely to use unsecured or poorly secured Wi-Fi networks, which are an especially vulnerable entry point for threat actors. At the same time, cyberattacks [increased in number and sophistication](#), with malware and phishing attacks specifically [using COVID-19 uncertainty](#) to compromise their targets. These ongoing trends combine to create a cybersecurity crisis for many industries.

COST OF A DATA BREACH BY INDUSTRY



The proliferation of sophisticated cyber threats reflects the range of malicious actors targeting businesses, including criminal cyberattackers, hacktivists and nation-state-sponsored groups, as well as disgruntled insiders who pose an elevated risk to certain high-value industries. Cybersecurity concerns that preceded the COVID-19 outbreak have not subsided, and a report from [security advisory firm Crypsis Group](#) found that the healthcare and financial services industries were most likely to be targeted by insider threats during 2019, followed by information technology.

Businesses in healthcare, life sciences, financial services and technology store especially valuable, sensitive data, and they operate in complex cybersecurity and regulatory environments. So, it follows that they also face higher costs related to a data breach, as shown by a recent [IBM report](#).

Recovering from a cyberattack is often a months-long process that extends well beyond the cyber incident itself, causing a significant drain on internal resources. The total financial impact of business interruption can be much more significant than the costs related directly to the attack. Reputational harm from a cyber incident is also a key consideration, particularly for industries that rely on the trust of consumers, clients and partners.

The cumulative costs of a cyberattack or breach can vastly outweigh the costs of instituting robust cybersecurity practices, but achieving those practices also requires around-the-clock monitoring, comprehensive detection tools and rapid response measures, as well as routine testing and periodic improvements. Threat actors continually adapt their techniques as companies improve cybersecurity defenses, all too often staying several steps ahead of security professionals and mitigation measures. For example, distributed denial of service (DDoS) attacks can be used as a distraction technique to occupy IT resources while coordinating follow-up attacks through a back door in the system. Sophisticated attackers may also use anti-forensic tools and wiper malware to cover or erase evidence of the intrusion.

Because certain industries face more severe cybersecurity challenges than others, we've focused attention on key considerations and emerging threats for healthcare/life sciences, financial services and technology. Although the growing complexity of IT environments presents organizations with an uphill battle, there are clear best practices that can strengthen cybersecurity—particularly by using managed detection and response services—and increase resilience, which are more important to implement and maintain now than ever before.



Focus Industry: Healthcare and Life Sciences

HIGH-VALUE DATA AND INADEQUATE SECURITY SPENDING

Healthcare and life sciences organizations remain a popular target for cyberattackers in part because protected health information (PHI) is more valuable than most other types of data. A study from [Experian](#) found that medical records sold for up to \$1,000 each on the dark web, whereas credit card numbers sold for just \$100. Additionally, many life sciences companies have sensitive medical information related to clinical trials, as well as valuable intellectual property. In July, the Department of Justice announced that Chinese hackers had targeted COVID-19 vaccine research, highlighting the growing danger of cyber threats linked to state-sponsored espionage.

In the course of trying to offer better and more efficient care, healthcare and life sciences organizations are exposed to greater vulnerability. The growing use of telehealth, connected devices, data sharing and third-party partnerships all increase the number of access points for threat actors. Unfortunately, the expanded use of technology has not corresponded sufficiently to increased investment in cybersecurity. For example, [research by Gartner](#) found that healthcare providers only devote about 5% of the IT budget to cybersecurity, even though more than four in five hospitals had experienced a significant cyber incident in the past year.

Inadequate spending on security also increases the likelihood that human error could expose PHI to a breach, as misconfigured databases and cloud architecture can lead to poorly secured medical records. Healthcare organizations, particularly those in public systems, are also more likely to be underfunded, understaffed and undertrained for cybersecurity. Legacy systems running on outdated technology are much more susceptible to cyber threats, particularly if an organization relies on unpatched software that has known vulnerabilities. Unfortunately, deploying technology solutions without robust cybersecurity practices only invites new maladies.



COMMON CYBER THREAT VECTORS

According to [the U.S. Department of Health and Human Services](#), their Office for Civil Rights was investigating 306 healthcare provider breaches that were reported between January and October 1, 2020. More than two-thirds of breaches were related to hacking or IT incidents, exposing organizations to significant HIPAA violations. Hackers often use social engineering tactics to get compromised credentials by manipulating a company's employees to gain unauthorized access to sensitive data and systems.

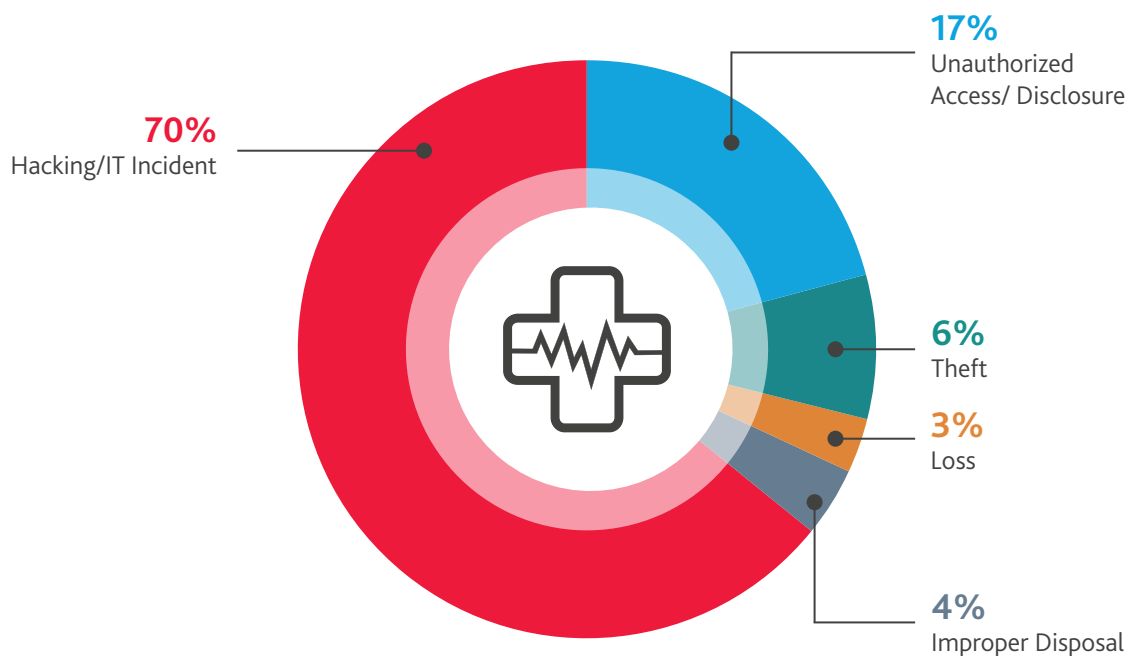
Healthcare providers are also a common target of ransomware attacks, which use malware to control key systems and databases and then demand payment to restore access. More than two dozen healthcare providers were [impacted by ransomware](#) just during the first five months of 2020, and the [American Hospital Association](#) noted that ransomware tactics have specifically adapted to exploit vulnerabilities during COVID-19. According to a [RiskIQ report](#), attackers deliberately target smaller organizations that are less likely to have strong cybersecurity practices. One small hospital in Colorado was struck by ransomware and subsequently found that five years of patient records were no longer accessible. Some hospitals affected by ransomware have even resorted to using paper records for tracking and treating patients, increasing the possibility of an error or delay that could directly impact patient safety.

Vishing is another type of cyberattack that has become more common during the COVID-19 pandemic. While phishing email scams have become common, and many organizations train employees to guard against them, vishing uses similar deception via phone calls that impersonate a trusted entity. The threat actor may try to get targets to disclose their login credentials or other sensitive information. The FBI and DHS issued a joint warning in August that remote workers in healthcare have been a [top target of vishing scams](#) during the coronavirus pandemic, seeking to exploit security gaps during the industry's rapid shift to telehealth.

Spoofed login pages are another popular hacking tactic. According to a study by the email security platform [IRONSCALES](#), more than 50,000 login pages and 200 brands were spoofed during the first half of 2020.

Healthcare and life sciences companies handle scores of sensitive data and rely on operational systems for care, but they may also have limited budgets for cybersecurity while facing an array of threats. That's why it's vital to focus resources on managed detection and response and increasing cyber resilience, which helps protect internal systems and secure the storage and transmission of high-value data.

2020 HEALTHCARE PROVIDER BREACHES BY TYPE



Focus Industry: Financial Services

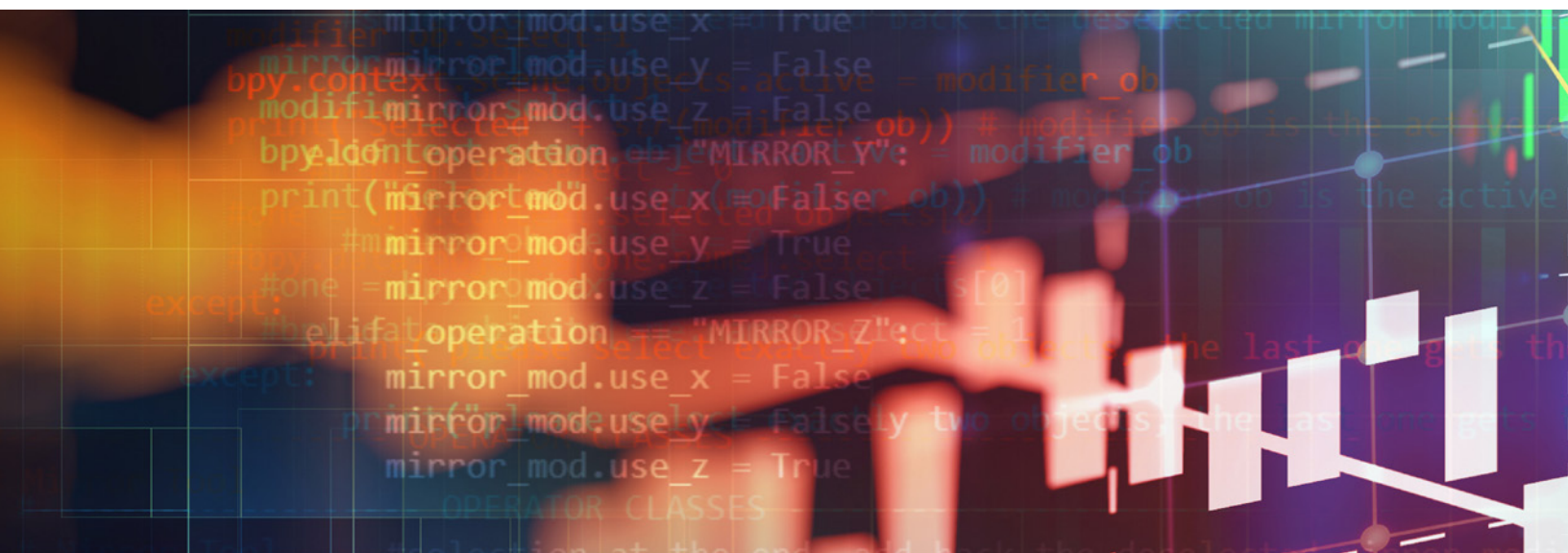
INCREASING VULNERABILITIES AND SIGNIFICANT CONSEQUENCES

Cyberattackers target financial services organizations to compromise sensitive data for fraud or theft, and the industry also operates under the watchful eye of multiple regulatory bodies. Simply put, it's where the money is, so the consequences of lax security can be especially dire. The interconnected nature of banking also means that an attack on one part of the financial system could potentially disrupt activity on a much more widespread level, such as affecting banks' abilities to service their creditors, as the [Federal Reserve Bank of New York noted](#) in their "pre-mortem analysis" released earlier this year. These factors make robust security practices an operational necessity, but digital adoption also opens the door to new risks.

As financial services organizations seek to improve the customer experience and offer multichannel support for a seamless interaction across platforms, that also increases entry points to the network. In the course of providing customers with ease of access to their account information and assets, financial services organizations have more vulnerabilities than ever, including payment cards, ATMs, mobile apps, point-of-sale systems, SWIFT transfer systems, cryptocurrency platforms and more, in addition to companies' own internal systems. The use of these digital tools has increased even further as a result of COVID-19. Threat actors can use numerous attack vectors to exploit these systems, such as malware, business email compromise, spear-phishing and botnets.

According to BDO's [2020 Financial Services Digital Transformation Survey](#), 45% of middle market executives say cyberattacks and privacy breaches represent their most significant digital threat. And approximately two-thirds (65%) say bolstering cybersecurity is among the top business objectives for their digital strategy over the next 12-18 months. However, security system complexity can lead to gaps in detection and response capabilities, so it's important to have measures in place that enable coordinated management of multiple security tools, such as advanced security information event management (SIEM) software and security automation.

Because financial services is a highly regulated industry—subject to review by the SEC, OCIE, FFIEC, CFPB and NYDFS, to name a few—it faces higher costs related to a data breach and greater scrutiny over cybersecurity practices. U.S. and international regulators have recently increased pressure on the industry to build cyber resiliency as well. Applicable compliance regulations include the Sarbanes–Oxley Act and Gramm–Leach–Bliley Act, as well as international standards for data security, such as the Payment Card Industry DSS, SWIFT CSP and ISO/IEC 27001. Ensuring robust security and ongoing compliance with this raft of regulations sets up a daunting but necessary task.



INVEST NOW TO PREVENT HIGHER COSTS LATER

Ransomware and other malware have become more prevalent in recent years, particularly against financial services organizations. A report from VMware found that 45% of financial services executives say custom malware was the most frequently experienced type of attack, compared to an average of just 18% for respondents across all industries. And 31% of financial services companies say attacks have become significantly more sophisticated.

Ultimately, the failure to prevent a cyberattack can represent an existential threat for businesses. For example, Travelex, the world's leading foreign exchange company used by financial institutions, was attacked by the REvil/Sodinokibi ransomware in late December 2019—the same ransomware that had targeted hundreds of dentist offices in the U.S. earlier that year. The company reportedly paid out a \$2.3 million ransom to recover their networks. Despite this, all systems—including Samsung's digital wallet—were affected for several days, and some systems remained out of operation for weeks. In August, the company entered bankruptcy proceedings.

Financial services companies rely on the trust of their customers, who need to feel confident that their assets and information are being handled securely at all times. Consequently, this industry is particularly vulnerable to reputational harm from a breach, and more than one-third of financial services executives report severe reputational damage from a cyberattack, significantly higher than other industries surveyed by VMware. IBM also found that the average length of time for financial services organizations to identify and contain a data breach was 233 days, which stretches the costs of lost business, mitigation and restoration across many months.

In light of the potential financial and reputational damage, regulatory scrutiny and ever-evolving nature of cyber threat actors, it's critical for financial services organizations to leverage managed detection and response services and build robust cyber resilience to address their unique threat profile.

Cybersecurity in Financial Services Is a National Security Issue

Nation-state cyber threat actors—whether those directly sponsored by a government or linked to a country's intelligence services—have also increased their activity in recent years to disrupt adversaries and gain funding for other activities. These attackers include advanced persistent threat (APT) groups in China, Russia, Iran, North Korea and elsewhere, posing a threat to U.S. national security.

A group of U.S. agencies, including the FBI and Treasury Department, recently [released a substantial activity report](#) warning that a North Korean group, known as the BeagleBoyz, had renewed efforts to conduct ATM cash-out schemes that have netted millions of dollars. The group had also used social engineering to target banking employees on LinkedIn with fake job postings, and then sent them a file containing malware. And in August, [the Justice Department filed](#) a civil forfeiture complaint and moved to seize hundreds of cryptocurrency accounts, which they claim have been used by North Korea to steal and launder more than \$250 million.



Focus Industry: Technology

GREATER CONNECTIVITY BRINGS NEW RISKS

When the world shut down, the tech industry turned on. Technology has powered business growth for decades, but the global pandemic made innovation an imperative like never before. As more work, services, education and transactions went online, the tech industry enabled resilience and continuity, but it also opened new areas of risk for security and data privacy.

Technology companies are prime targets for cybercriminals seeking valuable information, such as critical business and consumer data or intellectual property and trade secrets, whether it's stored in the cloud, on internal systems, on personal devices or elsewhere. According to BDO's [2020 Technology Digital Transformation Survey](#), a plurality of tech executives (44%) reported cyberattacks and privacy breaches as their top digital threat. Even prior to the pandemic, 61% of tech executives said bolstering cybersecurity was a top short-term business objective.





Now, Zoom is the new conference room and classroom. Consumers have increased their online purchases, and telehealth is surging. Contracts, invoices and proprietary information could be exchanged via email or on collaboration and messaging platforms, and those may be accessed via personal devices and home networks that lack robust security protections. Security protocols—including data encryption, virtual private network (VPN) access and multi-factor authentication—and proper configuration of these systems is paramount.

Many tech companies have expanded their permanent work-from-home options, and other industries are following suit with the aid of software-as-a-service (SaaS) and other cloud solutions. According to an IBM survey, 76% of respondents said remote work would increase the time to identify and contain a breach. Undoubtedly, ensuring the security of remote work will continue to be a major priority in the months and years ahead.

The tech industry not only must ensure its own security, but it has to enable robust security practices for the many industries that it serves. The stakes are high, so tech companies are investing in security and data privacy with purpose. Compliance with regulatory and industry standards is the bare minimum, and tech companies should seek to go above and beyond when it comes to cybersecurity.

As threat actors adapt their methods and probe for any vulnerability to exploit, the technology industry must work continuously to keep pace and evolve the tools, systems and controls to monitor and guard against cyber threats. Security analytics, data encryption and continuous threat monitoring are just a few of the tools that the industry deploys in the battle against cyber threats.

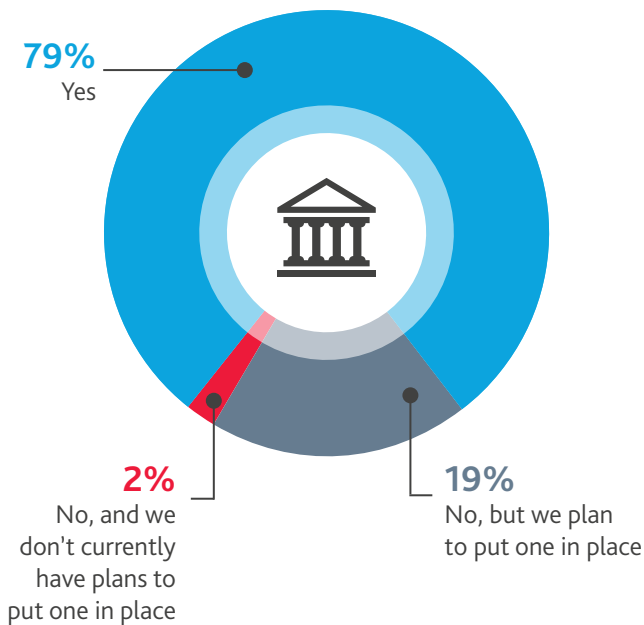
DOES YOUR ORGANIZATION USE THE FOLLOWING SECURITY MEASURES?

		All Respondents
	Security Analytics	82%
	Data Encryption	78%
	Continuous Threat Monitoring	77%
	Managed Security Services	72%
	Industrial Controls Systems Security	60%

CHANGING THE CONVERSATION ON DATA PRIVACY

Tech companies are increasingly touting privacy as a benefit and differentiator. In a new ad campaign launched in September, Apple notes that “some things shouldn’t be shared” and promises more control over information. Indeed, a new privacy sector is rising to meet growing needs for data services, ranging from personal data scrubbers to software to help businesses comply with the California Consumer Privacy Act (CCPA) and other rules. [The International Association of Privacy Professionals](#) reported 259 privacy start-ups as of October 2019, up from just 44 in 2017. The demand is there, and it’s growing: Atlanta-based OneTrust, one of the global leaders in privacy-law compliance technology, earned the top spot on the Inc. 5000 list of fastest-growing companies for 2020, reporting 48,337% growth over three years.

DO YOU HAVE A DATA ETHICS POLICY IN PLACE?



Source: 2020 Technology Digital Transformation Survey

Regulatory Scrutiny and Expanding Privacy Legislation

Data breaches have significant implications relative to expanding data privacy legislation, which often specifies penalties for breaches of consumer information.

For example, the CCPA provides consumers with a private right of action, which allows those affected to file class actions seeking class-wide statutory damages. These actions also have a lesser burden of proof than other types of litigation. The required fine is a minimum of \$100, and a maximum of \$750, per consumer per violation. The total pool of money is also uncapped, so the total fine can be substantial depending on the size of the class, meaning that the monetary impact of remediating a data breach can significantly impact a business' bottom line.

Several high-profile class actions have been filed against major technology companies, including the Amazon-owned smart device maker Ring, cloud-based software service Salesforce, video communication platform Zoom, social game developer Zynga and facial recognition provider Clearview AI.

INNOVATING WITH INTENT

Tech companies' clear focus on privacy and security is paying off both in results and reputation. In the beginning of 2020, 56% of tech companies reported that customers' level of trust in their company had increased in the past year. Looking ahead, the new marketplace will bring new opportunities for every sector of the tech industry, and companies seem poised to build products and services with security and privacy as a baseline.

Spotlight: Internet of Things (IoT) Devices

THE TROUBLE WITH CONNECTED DEVICES

Over the last decade, Internet of Things (IoT) devices have become increasingly common for consumers and businesses alike. There are billions and billions of IoT devices in use, and that total will only continue to grow. These interfaces help companies gather and analyze greater amounts of business intelligence, which can improve the customer experience and power growth, but poor security for connected devices poses a significant threat.

IoT devices are used in a variety of functions across industries. In healthcare, remote patient monitoring tools and wearables were already widespread, and since COVID-19, their use has risen further with the increased use of telehealth. In the manufacturing and energy industries, IoT tools are used to monitor machinery and other infrastructure to detect maintenance needs, which helps prevent costly breakdowns that disrupt operations. IoT can also take the form of sensors used to measure machine performance and can be deployed to track the movement of goods throughout supply chains. Real-time data collection can allow companies to detect disruptions and respond quickly.

However, since IoT tools collect and share large amounts of sensitive data, and they also tend to have insufficient security protections, they are a prime target for cybercriminals. IoT devices can serve as an entry point to other business systems, so the consequences of a single breach can be catastrophic. And the more IoT devices a business has throughout its operations, the more potential access points there are for bad actors.

Case Study: Prolonged Vulnerabilities in Medical Devices

In September 2019, a vulnerability was identified in wireless IoT modules made by Thales. These components are used by more than 30,000 companies and installed on millions of IoT devices, including many medical devices. By exploiting this vulnerability, hackers could generate false alerts, hide changes in patients' vitals or even administer overdoses via drug pumps.

In February 2020, a patch was released to resolve this vulnerability, but the patching process is not a quick fix, especially in industries that are highly regulated like healthcare. Medical devices need to be recertified after a patch has been applied, which can be a lengthy process, and many devices remain vulnerable months after the patch was released.

CURRENT VULNERABILITIES AND SEVERE CONSEQUENCES

IoT's proliferation has led to an entirely new set of security risks throughout business operations. For example, botnets (a network of devices infected with the same malware) can attack websites and services on a mass scale by spamming them with traffic. As IoT devices often rely on a single layer of security to access their interfaces (typically just password protection), they are highly susceptible to breaches. For instance, many users fail to change the device password from the known default.

A report by ESET found that seven out of the 10 most frequent IoT vulnerabilities in Q2 2020 were related to unauthorized access via password, information leakage or directory traversal. The report also found that the top 10 vulnerabilities for Q2 2020 originated before 2016, demonstrating that many vendors aren't patching or replacing their devices to protect against the latest threats.

The shift to remote work during COVID-19 has led to an even greater reliance on IoT devices, and there has been an uptick in cyberattacks targeting IoT. A survey of CTOs, CIOs and CISOs conducted by VMware found 89% of respondents reported threat increases in IoT exposure, second only to COVID-19-related malware.

The integration of cyber-physical systems also means that digital attacks can have real-world consequences. In the energy sector, a breach could give a cybercriminal access to industrial control systems, potentially allowing an intruder to shut down portions of the power grid, for example. Widespread outages could also interrupt health and other emergency services. Even if a breach didn't get that far, the information obtained could enable hackers to launch a more coordinated and harmful attack in the future. According to the security trade group ASIS International, just 19% of companies unite their operations for cybersecurity, physical security and business continuity within the same department. Such siloed security operations can raise additional challenges in guarding against overlapping risks.

However, legislative action could prompt IoT device makers to introduce new security standards. In September, the House of Representatives passed the IoT Cybersecurity Improvement Act, which specifies security requirements for IoT devices used by government agencies and directs the National Institute of Standards and Technology to create IoT security guidelines for the federal government. This and similar efforts could lead to sweeping changes for connected devices.

There are several steps that organizations should consider for bolstering their IoT cybersecurity, including:



Encrypt stored data and only transfer information over secure channels.



Institute enterprise-wide standards for all IoT tools, and patch or replace IoT devices more frequently, as appropriate.



Consider using endpoint detection and response (EDR) cybersecurity, or more robust unified endpoint management (UEM) tools, which can be paired with identity and access management (IAM) tools.

Cybersecurity for All Industries

Digital tools and increased connectivity offer many benefits, especially as businesses mitigate the impacts of a global pandemic, but security should be top of mind as technology adoption accelerates. This is especially important for the healthcare, life sciences, financial services and technology industries, because the highly sensitive data that they collect, store and process is a high-value target for determined threat actors.

Continuous threat monitoring and coordinated management of security tools help to guard against vulnerabilities, but there are always new risks emerging, and this has been especially true during the COVID-19 pandemic. Many organizations have also tightened budgets during the economic downturn, although it's foolish to skimp on cybersecurity. That's why prioritizing specific areas for security resources is so crucial.

As businesses confront cyber threats that are increasing in both number and sophistication, it's critical to prioritize spending on managed detection and rapid response, as well as overall cyber resilience. These are the cybersecurity must-haves in 2020. When supported by routine assessment of the technical infrastructure, alongside firm-wide security training for all employees, even businesses in the most frequently targeted industries can protect against the persistent barrage of cyber threats.

Top Priorities for Cybersecurity in All Industries

- 1. Use managed detection and response services:** Ensure you have security measures in place to continuously monitor, detect and respond to threats to the email system, network, software applications and all information system endpoints. Use advanced security information event management (SIEM) software, data visualization tools, artificial intelligence tools and security automation as needed to achieve 24/7/365 monitoring and instantaneous response.
- 2. Confirm information system resilience on a continual basis:** Establish and periodically test the comprehensive incident response plan, business continuity plan and disaster recovery plan to minimize the potential damage from cyberattacks and protect operations.
- 3. Conduct diagnostic assessments of technical architecture:** Regularly conduct penetration testing, network and endpoint assessments, vulnerability scanning assessments, email cyberattack assessments and more.





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 apply 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 of 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.

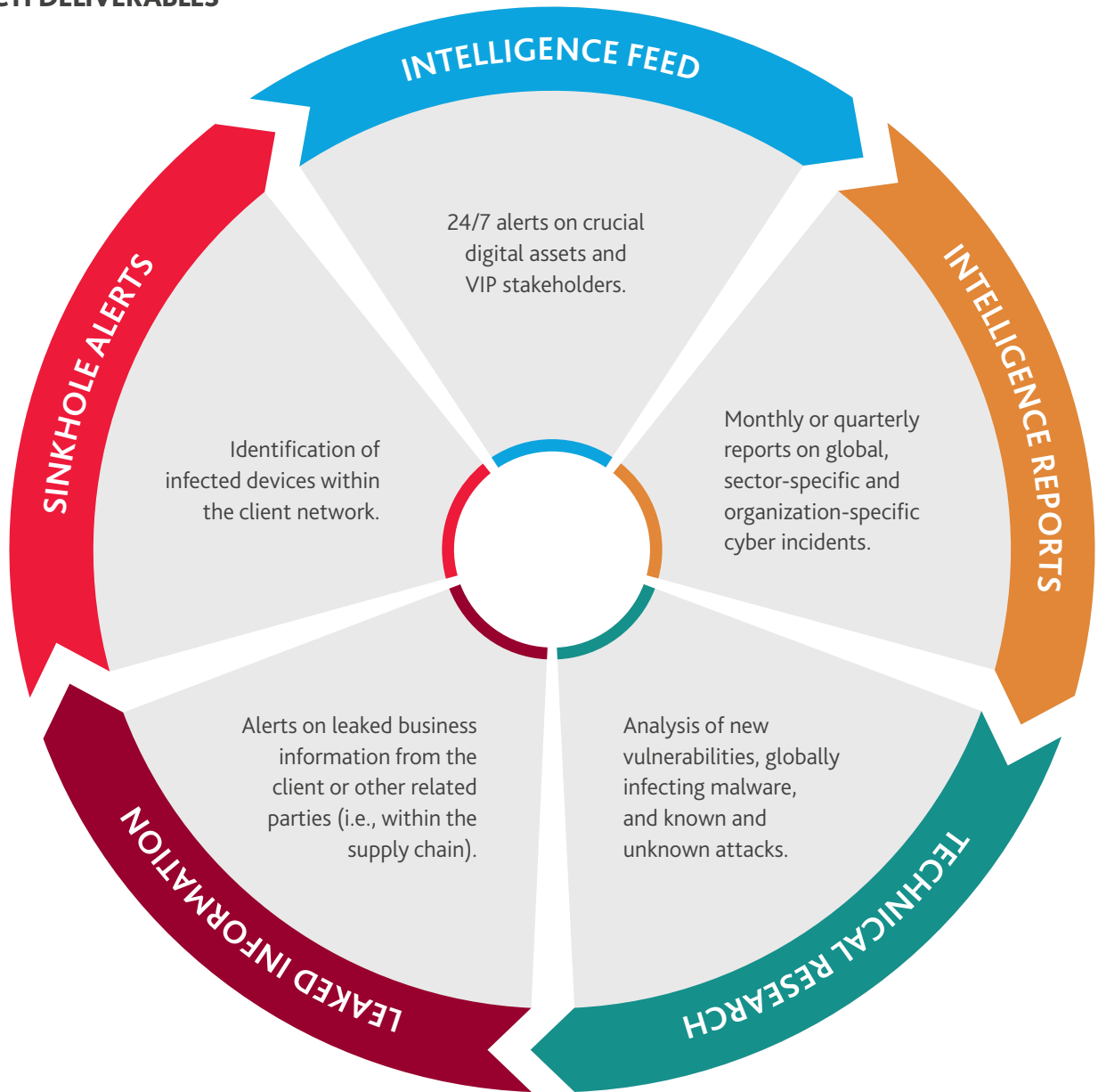


CONTACT:



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

BDO CTI DELIVERABLES





Cybersecurity Leadership Team



RIC OPAL
Principal, Cybersecurity
630-686-4302 / ropal@bdo.com



DOUG HART
Assurance Partner,
Technology Industry Co-Leader
415-490-3314 / dhart@bdo.com



MICHAEL DOMBROWSKI
Managing Director, Infrastructure and
Cyber Solutions Group Co-Leader
302-468-3774 / mdombrowski@bdo.com



MICHAEL LEE
Principal, Senior Client Executive
630-286-8126 / milee@bdo.com



MARK HOUSTON
Managing Director, Financial Institutions &
Specialty Finance National Practice Leader
212-885-8098 / mhouston@bdo.com



MALCOLM "CHIP" COHRON
National Digital Transformation
Services Leader
404-979-7109 / ccohron@bdo.com



PATRICK PILCH
Senior Managing Director, Healthcare
Advisory National Practice Leader
212-885-8006 / ppilch@bdo.com



MAURICE LIDDELL
Principal, Senior Client Executive
713-407-3265 / mliddell@bdo.com



AFTAB JAMIL
Assurance Partner,
Technology Industry Co-Leader
408-352-1999 / ajamil@bdo.com

People who know Cybersecurity, know BDO Digital.

BDO Digital, LLC is a Delaware limited liability company, and a wholly-owned subsidiary of BDO USA, LLP.

BDO USA, LLP, a Delaware limited liability partnership, is the U.S. member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. BDO is the brand name for the BDO network and for each of the BDO Member Firms. For more information on BDO Digital, LLC please visit: www.bdo.com/digital.

Material discussed is meant to provide general information and should not be acted on without professional advice tailored to your needs.

© 2020 BDO USA, LLP. All rights reserved. www.bdo.com