



**BDO CYBERSECURITY  
SPOTLIGHT**

Summer 2020 Report

**SPECIAL FOCUS: FAMILY OFFICES**

# In this issue

---

<b>PREFACE</b>	<b>3</b>
<b>THE WORLD WE LIVE IN – AMID THE COVID-19 PANDEMIC</b>	<b>4</b>
<b>FAMILY OFFICES UNIQUE CYBERSECURITY ISSUES</b>	<b>5</b>
Case Study – High Net Worth Family Under Cyber-Attacks	5
<b>THE RISE OF CYBER THREAT ACTORS TARGETING FAMILY OFFICES</b>	<b>6</b>
Family Office – Cyber Data Breach – 7 Quick Tips	6
<b>GROWTH OF EMAIL BASED CYBER-ATTACKS ON FAMILY OFFICES</b>	<b>7</b>
<b>FAMILY OFFICES - TOP 12 CYBERSECURITY CHALLENGES</b>	<b>8</b>
<b>IMPLEMENTING THREAT-BASED CYBERSECURITY FOR FAMILY OFFICES</b>	<b>9</b>
<b>FAMILY OFFICES - TOP FIVE CYBERSECURITY RECOMMENDATIONS</b>	<b>10</b>
<b>SUMMARY</b>	<b>11</b>
<b>BDO CYBERSECURITY SERVICES</b>	<b>11</b>

---

# Preface

BDO Digital is proud to introduce our new quarterly publication entitled 'Cybersecurity Spotlight.' Each quarter BDO will research, write, and publish a new edition focused on a specific industry/business group. This first-edition is focused on cybersecurity services for a specialized business group, which are often referred to as Family Wealth Offices, Family Wealth Enterprises, or simply Family Offices.

At BDO we have a practice area called "Private Client Services," which is dedicated to serving the particular needs of high net worth families and individuals. Within that practice area is a boutique unit, our Family Office services team, who provide a comprehensive suite of services, tax, audit, and a vast array of BDO Digital advisory services, including: information technology, digital transformation, data analytics, data privacy, and cybersecurity.

BDO has over 2,500 information technology and cybersecurity professionals available to support clients in both the public and private sectors worldwide. BDO cybersecurity advisory services teams are currently located in 35 countries on six continents. Each BDO country cybersecurity advisory services team provides a comprehensive portfolio of advisory services and managed security services to all industries.

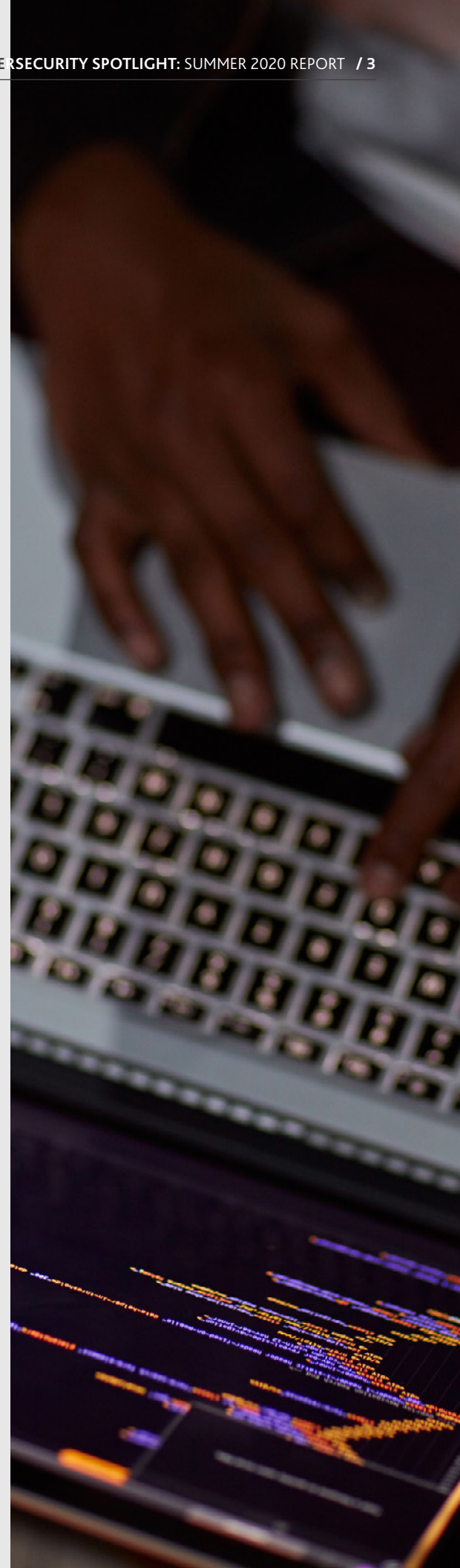
In this issue, we focus on understanding the unique aspects of Family Offices, potential cyber-threat actors, typical cyber-threat vectors, types of cyber-attacks, and specific cybersecurity challenges and best practices. Then we will discuss how to successfully implement a Threat-Based Cybersecurity program for Family Offices in order to create a customized cyber defense. Each Family Office has unique business risk issues, regulatory compliance matters, budget, and schedule requirements to support the evolving needs of the multi-generation family.

This report is based upon BDO's extensive experience providing cybersecurity advisory services and managed security services to both high wealth individuals and Family Offices worldwide. We hope you will find this report both interesting and valuable.

Respectfully,



**GREGORY A. GARRETT, CISSP, CPCM, PMP**  
Head of U.S. & International Cybersecurity  
Advisory Service



# The World We Live In – Amid the COVID-19 Pandemic

Globally there has been a sharp rise in cyber-attacks since the Chinese government disclosed the spread of the coronavirus (COVID-19) within China and internationally. Especially, cyber-attacks focused on healthcare providers using spear-phishing and ransomware, cyber-attacks on ATMs and Point of Sales (POS) systems, impersonation attacks combined with business email compromise (BEC) targeting financial systems, supply-chain cyber-attacks focused on manufacturing operations and food distribution, and distributed denial of service (DDoS) cyber-attacks on the energy, hospitality, and travel industries.

With the spread of COVID-19 worldwide, every country has seen unprecedented demands for increased internet services, cloud-based services, and information technology (IT) support services occurring across nearly all industries. Globally employees, students, university faculty, and others are being asked or required to work or study remotely from their homes to reduce the spread of the virus. As a result, nation-state cyber-attack groups and criminal cyber-attack groups are taking maximum advantage to target cyber vulnerabilities in selected industries, especially those most impacted by the current crisis.

Realizing that 40% or more of cyber vulnerabilities are directly linked to employee behavior, per the Gartner Group's latest studies, it is vital that organization's focus more on their employees via cybersecurity awareness, education, training, and use of simulations to create a stronger human firewall to protect their vital digital assets.

According to the Gartner Group's December 2018 study of cybersecurity investments, the manufacturing, retail, hospitality, and healthcare industries were amongst the lowest in their respective investments in cybersecurity averaging 5% or less of their respective information technology (IT) annual budget. According to IBM Security's latest findings the average cost of a cyber data breach is now \$8.2 million.



# Family Offices Unique Cybersecurity Issues

It is important to know that Family Offices come in all shapes, sizes, and level of services depending upon the unique requirements of the multi-generational family they support. Family Offices are essentially professional services businesses which are built to serve the professional and personal needs of the family members. There is no typical family office, as they can range from essentially a single family member with administrative support to a multi-faceted organization with dozens and sometimes over 100 employees. Most Family Offices have just a few employees and outsource many functions. There typically is a CEO or president who leads a team of business professionals, including: accountants, attorneys, investment managers, tax managers, charitable foundation managers, event and travel planners, physical security specialists, and others as needed.

However, most Family Offices outsource their information technology (IT) services to either local small IT firms or large professional services companies. As a result, the level of cybersecurity expertise available to most Family Offices tends to vary from very little and cheap to a lot but very expensive. Increasingly, cyber criminals have turned their focus on Family Offices, as they see a significant opportunity to steal a great deal of valuable information and money and face a minimal amount of cybersecurity measures to overcome.

---

## CASE STUDY – HIGH NET WORTH FAMILY UNDER CYBER-ATTACKS

**Situation:** A family based in New York, three generations with about 25 family members, with assets of over \$10 billion encounter a sudden rash of cyber-attacks, including:

- ▶ Spear-phishing attacks on the family members, personal mobile phones and home computers via emails and text messages – leading to a data breach on one of the family members, mobile phone
- ▶ Business email compromise (BEC) and impersonation attacks on their Family Office employees' computers and mobile devices
- ▶ Spear-phishing attacks combined with ransomware attacks and wiper viruses on their private equity firm and portfolio of 15+ companies in the U.S. and Europe

**Solution:** BDO Family Office services recommended the BDO cybersecurity advisory services practice, which worked with the family members, Family Office, private equity firm, and portfolio of companies to design a comprehensive threat-based cybersecurity program for each entity and the whole enterprise, including:

- ▶ Implemented a customized cybersecurity education and training program
- ▶ Conducted spear-phishing campaigns
- ▶ Provided advanced mobile phone security services for family members and key personnel
- ▶ Installed advanced email/network/endpoint cyber-attack monitoring and detection services enterprise-wide
- ▶ Provided incident response (IR) planning, testing, and support services

# The Rise of Cyber Threat Actors Targeting Family Offices

Unfortunately, Family Offices are increasingly becoming victims of cyber-attacks from three distinct groups of cyber threat actors:








- ▶ **Nation-State Cyber-Attack Groups:** Most cyber-attacks originate from four (4) nations: China, Russia, Iran, and North Korea. The extent of cyber-attacks on Family Offices from nation-states often depends upon the amount of wealth and profile of the family members, including their political, industry, economic, and social influence and connections. Cyber-attacks are often focused on blackmail, espionage, or theft of valuable and/or sensitive information, contacts/connections, and financial assets. Often nation-states fund or sponsor criminal cyber-attack groups, by providing the criminals with resources, facilities, and/or sharing hacking technologies and tools to perform the targeted cyber-attacks for an agreed fee.
- ▶ **Organized-Criminal Cyber-Attack Groups:** Typically, criminal cyber-attack groups are seeking to steal family member personal and sensitive information and then monetize the stolen information via transactions on the Dark Web, including:
  - Personal Identifiable Information (PII)
  - Protected Health Information (PHI)
  - Payment Card Information (PCI)
  - Intellectual Property (IP)
- ▶ **Hacktavists Cyber-Attacks Groups:** Groups of hackers are formed based upon a shared political, economic, religious, or social agenda. Often these cyber-attack groups seek to negatively impact influential and wealthy family members seeking money or promotion of their issues/agenda on social media or national press coverage to advance their messages.

According to recent FBI reports, the three above stated cyber-attack groups are often working in a coordinated, sponsored, or integrated manner to facilitate larger and more complex national or multi-national cyber-attacks. Since, many Family Offices manage property and other financial assets in numerous countries they are increasingly targeted by a combination of these cyber-attack groups.

---

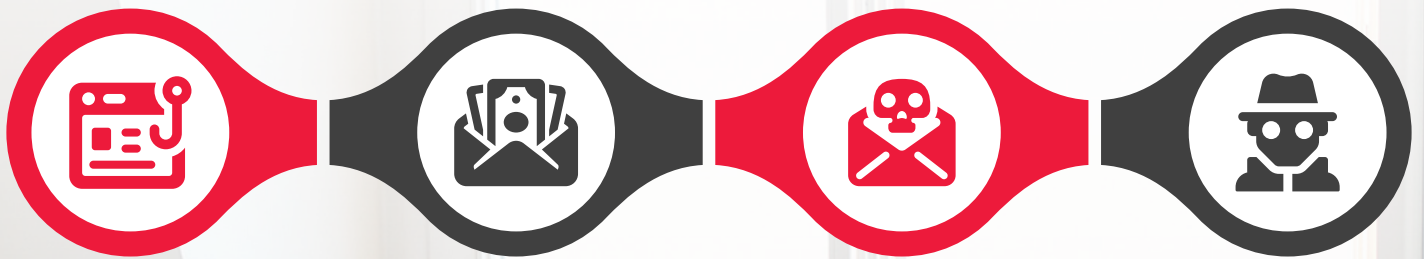
## FAMILY OFFICE – CYBER DATA BREACH – 7 QUICK TIPS:

### Immediate Actions:

-  Assess the situation and gather information
-  Implement the incident response plan with senior executives and IT
-  Contain the breach
-  Eradicate the malware
-  Communicate with all necessary parties
-  Notify authorities and law enforcement as needed
-  Recover data and Restore operations

# Growth of Email Based Cyber-Attacks on Family Offices

Based upon BDO research and extensive field-experience most successful cyber-attacks on Family Offices have used email as the preferred threat vector, including:



## **Socially-Engineered Spear-Phishing Cyber-Attacks**

Designed to gather personal information, gain computer access, and control of sensitive Family information

## **Business Email Compromise (BEC) and Impersonation Attacks**

Redirect financial payments, charitable contributions, or investments

## **Emails Containing Malicious Web Links or Attachments**

Intended to launch malware or spyware on your computer or other devices to steal valuable information

## **Ransomware Cyber-Attacks**

Designed to encrypt information and extort payment via a demand for crypto-currency such as Bitcoin



# Family Offices - Top 12 Cybersecurity Challenges

Family Offices typically experience numerous cybersecurity challenges, including:

1. Minimal cybersecurity education and training of employees
2. Lack of information technology (IT), data privacy, and cybersecurity strategic plan
3. No dedicated Chief Information Security Officer (CISO) to lead cybersecurity strategic planning
4. Lack of a cyber incident response (IR) program, IR communications plan, and periodic IR testing
5. Inadequate cyber intrusion monitoring and detection system for the email, network, and all endpoints
6. Insufficient computer vulnerability scanning to identify malware
7. Lack of regular independent penetration testing of firewalls, anti-virus, and anti-malware software
8. Inadequate or non-existent business continuity plan (BCP) or back-up plan for the information systems
9. Failure to meet state or industry-specific data privacy and cybersecurity regulatory compliance requirements
10. Insufficient identity, credentials, and access management information security controls
11. Inadequate mobile phone communications security, especially for Family members traveling internationally on either business or pleasure
12. Under investment in information technology, automation, and cybersecurity to enable business growth, ensure data integrity, and protect data privacy

**Key Question to Consider:** If a \$500 million global operating company on average spends \$1.25 million on cybersecurity hardware, software, and professional services – should a \$500 million family wealth enterprise do the same?





# Implementing Threat-Based Cybersecurity for Family Offices

In the face of ever-expanding cyber threats and increasingly sophisticated cyber-attackers, Family Offices should protect themselves by implementing a Threat-Based Cybersecurity program. Developing a Threat-Based Cybersecurity program begins by conducting specific cyber diagnostic tests/assessments to gain an understanding of the actual cyber threats the organization is currently encountering. It is vital for the Family Office to know:

- ▶ Who are the cyber-threat actors attacking the Family Office and/or family members?
- ▶ Which cyber-threat vectors are most commonly used?
- ▶ What types of cyber-attacks should the Family Office be prepared to defend against: including: tactics, techniques, and procedures (TTPs)?
- ▶ What are the Family Office information system vulnerabilities to cyber-attacks?
- ▶ What are the Family Office email system and network endpoints vulnerabilities to cyber-attacks?
- ▶ How susceptible are Family Office employees to potential cyber-attacks?

Once the Family Office gains a clear understanding of the answers to the above stated questions, then it can begin to design a customized cyber defense program to protect the organization's data. With increased investment and adoption of new technologies (cloud computing, advanced data analytics, artificial intelligence [AI] powered devices, and more) Threat-Based Cybersecurity can serve as an essential element of success for Family Offices by providing real data privacy and information security.



# Family Offices - Top Five Cybersecurity Recommendations

To reduce both the probability of a cyber-attacks or a significant data breach and mitigate the negative financial and reputational impacts, we offer the following cybersecurity recommendations:

- 1. Create an organizational culture of cybersecurity:** Ensure the CEO or president of the Family Office on down consistently promotes and supports all employees practicing effective cybersecurity policies, processes, and procedures via a comprehensive cybersecurity awareness, education, and training program including spear-phishing campaigns and cyber data breach table-top exercises.
- 2. Conduct advanced cyber diagnostic assessments, on a regular basis, including:**
  - ▶ Email Cyber-Attack Assessments
  - ▶ Network & Endpoint Cyber-Attack Assessments
  - ▶ Vulnerability Scanning Assessments
  - ▶ Penetration Testing
  - ▶ Spear-Phishing Campaigns
- 3. Establish a Rapid Cyber-Attack Incident Response Plan:** Develop and periodically test an enterprise-wide well-coordinated information system incident response plan to quickly identify, contain, eradicate, and recover from cyber-attacks.
- 4. Implement 24 x 7 x 365 Monitoring, Detection, & Response (MDR):** It is essential to continually monitor, detect, and respond to all cyber incidents including: email system, network, software applications, and all information system endpoints using advanced security information event management (SIEM) software, data visualization tools, automation, and artificial intelligence (AI) capabilities.
- 5. Ensure information system resilience:** Implement and periodically test an enterprise-wide business continuity plan (BCP) and disaster recovery plan (DRP).



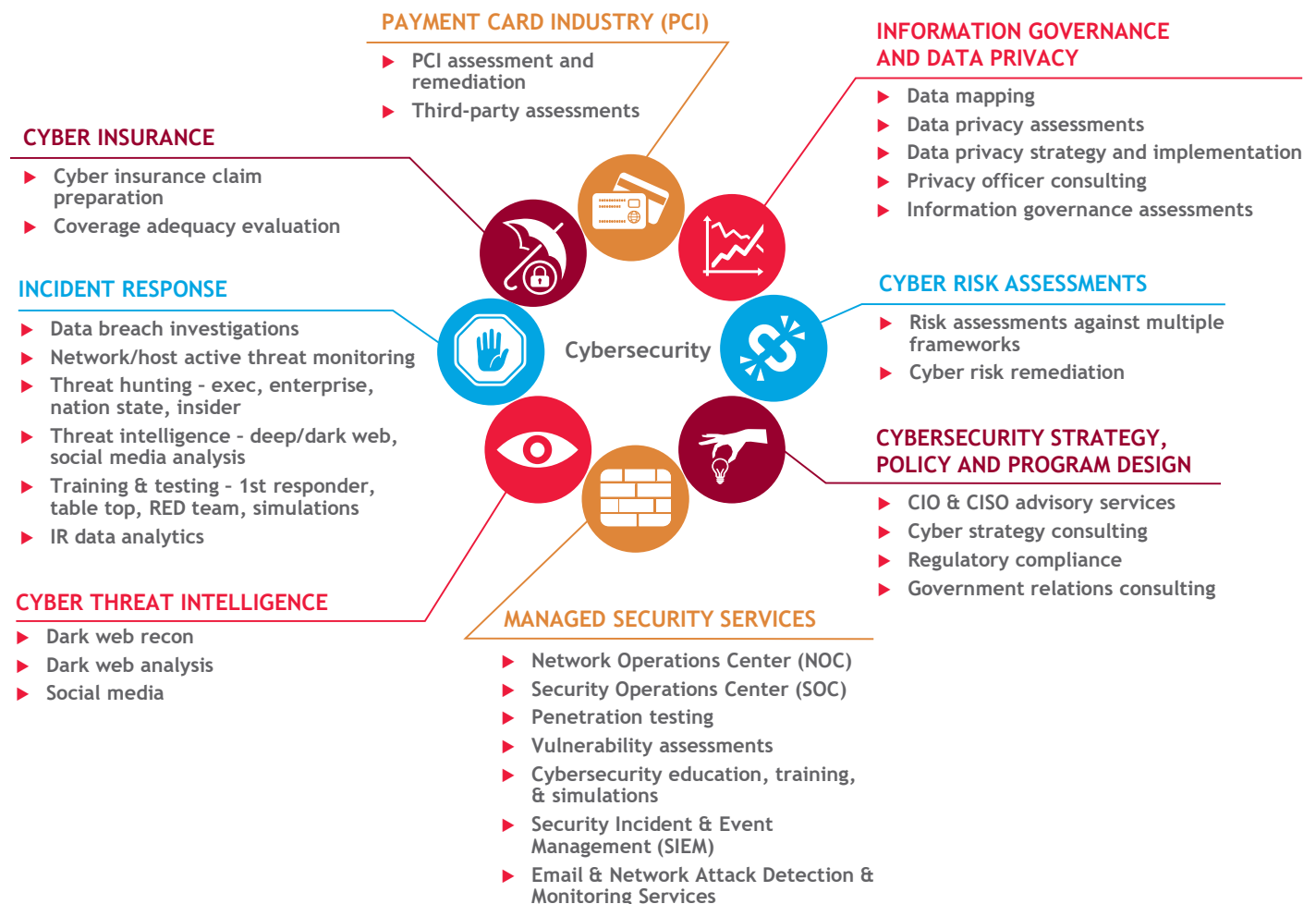
# Summary

Family Offices have a unique mission to provide a wide-range of expert personal and professional services to support the ever-evolving needs of multi-generation families with vast and diverse financial investments and assets often worldwide.

The one area which many Family Offices need additional expertise is cybersecurity. Increasingly, cyber-threat actors including: Nation-state cyber-attack groups, organized-criminal cyber-attacks groups, and hactivists are targeting Family Offices which are considered by cyber-attackers as a “target-rich-zone.”

Family Offices are rapidly realizing they can no longer fly-under the radar of hackers. Instead, Family Offices need to enhance their digital transformation and data privacy via implementing a Threat-Based Cybersecurity program.

## BDO Cybersecurity Services



# Cybersecurity Leadership Team



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



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



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



**JEFFREY KANE**  
National Managing Partner  
Private Client Services  
616-389-8619 / jkane@bdo.com



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



**CRAIG WITCHER**  
National Managing Director  
Family Office Services  
616-389-8679 / cwitcher@bdo.com



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



**AMY PIENTA**  
Managing Director  
Family Offices Services  
312-730-1414 / apienta@bdo.com



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



**LORI MYERS**  
Managing Principal, Private Client Services  
Southeast Region Co-Leader  
561-207-3214 / lmyers@bdo.com



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



**MARTY CASS**  
Managing Director, Private Client Services  
Southeast Region Co-Leader  
561-207-2810 / mcass@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.

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