Latest Cybersecurity Threats and Best Practices for Alternative Investment Funds

AKRAM
Assurance, Advisory & Tax

EFSI

{B(W)} CYBER LLC
COMPLEXITY SIMPLIFIED

OUR FEATURED PANELISTS

Muhammad Akram

MODERATOR

Akram | Assurance, Advisory & Tax Firm

Steve Rosen

SPEAKER

Akram | Assurance, Advisory & Tax Firm

Anthony D. Mascia

GUEST SPEAKER

EFSI

Micheal Brice

GUEST SPEAKER

BW Cyber Services

OFFICIALLY REGISTERED

AKRAM & ASSOCIATES is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing professional education on the National Registry of CPE Sponsors. State boards of accountancy have final authority on the acceptance of individual courses for CPE credit. Complaints regarding registered sponsors may be submitted to the National Registry of CPE Sponsors through its web site: www.nasbaregistry.org

Program level : Basic

No prerequisites are required

No advance preparation is required

AKRAM
Assurance, Advisory & Tax

EFSI

{B(W)} CYBER LLC
COMPLEXITY SIMPLIFIED

For more information please contact:

Muhammad A. Akram - CPA and Founding Member Toll-Free: 844-386-3829 | makram@aifundservices.com

ABOUT

AKRAM
Assurance, Advisory & Tax

AKRAM & ASSOCIATES IS A FULL-SERVICE ACCOUNTING FIRM PROVIDING ASSURANCE, ADVISORY, AND TAX SERVICES FOR THE FINANCIALLY SAVVY, ESPECIALLY HEDGE FUNDS & CRYPTOCURRENCY FUNDS.

EFSI

ESSENTIAL FUND SERVICES INTERNATIONAL, LLC ("EFSI") IS AN INDEPENDENTLY OWNED, SOC 1 COMPLIANT, FULL-SERVICE FUND ADMINISTRATION FIRM BASED IN NEW YORK. WE PROVIDE INVESTMENT MANAGEMENT FIRMS WITH A COMPREHENSIVE SUITE OF FUND ADMINISTRATION SERVICES IN A COST-EFFECTIVE STRUCTURE.

{B(W)} CYBER LLC
COMPLEXITY SIMPLIFIED

BW CYBER PROVIDES TAILORED CYBER SECURITY SOLUTIONS FOR NFA MEMBERS, HEDGE FUND ADVISERS, BOARD OF DIRECTORS AND FAMILY OFFICES. OUR APPROACH TO THIS DEMANDING NEW WORLD OF CYBER SECURITY COMPLIANCE: "COMPLEXITY SIMPLIFIED".

INTRODUCTION

The alternative investment industry, which includes investments outside of traditional assets like stocks and bonds (e.g., private equity, hedge funds, real estate, venture capital), is not immune to cybersecurity threats. In fact, the sensitive nature of the financial data and the potentially high returns associated with these investments can make the industry an attractive target for cybercriminals. Here are some cybersecurity threats that the alternative investment industry may face.

DATA BREACHES:

Cybercriminals may attempt to infiltrate investment firms' networks to gain unauthorized access to sensitive financial and personal data of investors, employees, and partners. This information could be used for identity theft, fraud, or other malicious activities.

RANSOMWARE ATTACKS:

Ransomware attacks involve malicious software that encrypts a firm's data, making it inaccessible until a ransom is paid. Alternative investment firms often store sensitive financial information, and losing access to this data could have significant operational and financial consequences.

PHISHING AND SOCIAL ENGINEERING:

Cybercriminals may use phishing emails and social engineering tactics to trick employees into revealing confidential information or performing actions that compromise security. For example, fraudulent emails that appear to be from legitimate partners could lead to fund transfers or divulging login credentials.

POLLING QUESTION

IN THE CONTEXT OF THE ALTERNATIVE INVESTMENT INDUSTRY, WHAT IS A POTENTIAL CONSEQUENCE OF RANSOMWARE ATTACKS?

a) Increased operational efficiency.

b) Unauthorized access to sensitive data.

c) Enhanced financial returns.

INSIDER THREATS:

Insiders with access to sensitive information can pose a significant threat. Malicious insiders might steal data for personal gain or sabotage systems. Even unintentional actions by employees, such as accidentally sharing confidential information, can lead to security breaches.

THIRD-PARTY RISK:

Alternative investment firms often collaborate with various third-party vendors and service providers. If these vendors have weak security measures, they can become entry points for cyberattacks that target the investment firm's network.

SUPPLY CHAIN ATTACKS:

Cybercriminals might target the supply chain to compromise software or hardware components used by investment firms. This can lead to breaches, data theft, or the insertion of backdoors into systems.

REGULATORY COMPLIANCE & LEGAL CONCERNS:

The alternative investment industry is subject to various regulations (e.g., GDPR, SEC regulations) that require safeguarding sensitive financial and personal data. Failing to meet these requirements can lead to legal consequences and reputational damage.

POLLING QUESTION

CONSIDER CYBERSECURITY THREATS IN THE ALTERNATIVE INVESTMENT INDUSTRY, WHAT IS A CONCERN RELATED TO THIRD-PARTY VENDORS?

a) Increased operational efficiency.

b) Strengthened internal security measures.

c) Potential entry points for cyberattacks.

LACK OF AWARENESS AND TRAINING:

Employees and stakeholders within the alternative investment industry may not be adequately trained to identify and respond to cybersecurity threats. This lack of awareness can lead to unintentional security breaches.

WEAK AUTHENTICATION AND ACCESS CONTROL:

Poor access controls and frail authentication methods create opportunities for unauthorized entry into crucial systems, leading to potential data breaches. Strengthening authentication mechanisms and refining access controls is vital to prevent unauthorized access and safeguard sensitive information.

POLLING QUESTION

WHICH OF THE FOLLOWING IS A POTENTIAL CYBERSECURITY RISK FACED BY ALTERNATIVE INVESTMENT FIRMS?

a) Overwhelming supply chain resources

b) Excessive regulatory compliance

c) Weak authentication and access control

POLLING QUESTION

CHOOSE A KEY OBJECTIVE OF THE NEWLY ADOPTED SEC RULES REGARDING CYBERSECURITY DISCLOSURES?

a) Encouraging companies to keep cybersecurity incidents undisclosed.

b) Ensuring consistent and comparable cybersecurity disclosures for investors.

c) Reducing the reporting requirements for foreign private issuers.

RECOMMENDED CYBESRECURITY STRATEGY TIPS:

- Regular employee training on cybersecurity best practices and awareness.
- Robust firewalls, intrusion detection systems, and antivirus software.
- Multi-factor authentication to enhance access security.
- Regular security assessments and penetration testing.
- Strong data encryption for sensitive information.
- Incident response plans to effectively manage and recover from cyber incidents.
- Vendor risk assessments and due diligence.
- Compliance with relevant regulations and standards.
- Continuous monitoring and updating of security measures to adapt to evolving threats.

THANKS FOR LISTENING

AKRAM Assurance, Advisory & Tax | EFSI | {B(W)} CYBER LLC COMPLEXITY SIMPLIFIED

For more information please contact:

Muhammad A. Akram - CPA and Founding Member Toll-Free: 844-386-3829 | makram@aifundservices.com