Cybersecurity for Asset Management Firms

Asset Management Firms are at risk

One of the biggest business risks to the financial service industry is cybercrime. A typical organization faces an average of 85 attacks every year, and an estimated one third will succeed.[1] Asset management firms are not exempt from this statistic. A new report reveals that cybersecurity improvements are a key business priority for 33% of asset managers.[2]

> "There is no shortage of criminal networks continuing to attempt to compromise the corporate networks of our financial institutions. We have seen a rise in the risk of targeted network attacks being carried out against [asset management] firms."[3]

Cybercriminals are targeting asset management firms for banking and financial credentials, trading and investor information or strategies, consumer data, business and tax filing, fraudulent redemptions and more.

The potential effects of a breach include:

- Financial loss
- Disruption of operation
- Compromised confidential information
- Reputational damage
- Investigations and/or fines from regulatory bodies

Threats targeting firms

Much like the rest of the finance industry, asset management firms are being bombarded by cyber-attacks, from DDoS and APT to ransomware and zero-day attacks. Asset management firms also need to consider the threats posed by their clients. If a client's email is hacked, it can be used to send emails to the firm requesting money, appearing legitimate.[4]

According to eSentire Threat Intelligence[5], the common attack methods used against the finance industry include:

Phishing: Which could indicate a lack of security among all employees.

Coin Miners: Which could indicate a lack of acceptable use policies and technical controls.

Tech Support Scams and Fake AV Social Engineering: Which could indicate a lack of employee awareness and the use of appropriate technical controls.

These threats can cause serious business challenges if not detected and responded to quickly. Recent data on asset management firms from Accenture shows that 59% of firms take months to detect a breach and 15% of breaches aren't discovered for a year or more.[6]

Unfortunately, the majority of asset managers are inadequately prepared to guard against cyberattacks. This is largely due to the fact that many asset managers assume their firms don't present an appealing target for cyber criminals, unlike big retail banks. Cyber criminals are capitalizing on this complacency. Many asset managers are being targeted as they are not only unprepared, but they also lack the cyber cleverness and security measures to ward off cyberattacks.[7]

Cybersecurity compliance requirements

Regulators are no longer accepting negligent cybersecurity defenses.

Depending on your region and business activities, your firm will need to adhere to a number of different regulations, including (but not limited to) the following:

US	FINRA, SEC, State-Level, CFTC
CANADA	OFSI, IIROC, Provincial Securities Commission
UK	FCA, GDPR, PRA

The faster the firm catches the threat, the lower the impact

Fortunately, the next victim doesn't have to be you. According to Aberdeen's Monte Carlo analysis, being twice as fast at threat detection and incident response lowers the business impact of a cyber-attack by approximately 70%.[8]

It's time to step up your cybersecurity game. 65% of the senior asset management professionals surveyed believe that the threat posed to their organization from cybercrime this year is greater than in 2017. As a result, investments to improve cybersecurity measures by the asset management industry are anticipated to rise, with 50% of respondents saying their organization plans to increase expenditure in this area in 2018.[9]

The only way to avoid an incident and react quickly is to have a certified Security Operations Center (SOC) with human analysts hunting and responding to threats on your network 24x7x365.

We defend against the threats facing asset management firms

eSentire Managed Detection and Response™ (MDR) keeps asset management firms safe from cyber-attacks that other technologies miss. Our 24x7 Security Operations Centers (SOC) are staffed by elite security analysts who hunt, investigate and respond to known and unknown threats in real time.

With **MDR**, you'll experience:

- **24x7x365** continuous hunting and monitoring
- **Detection of unknown attacks** leveraging patterns and behavioral analytics
- **Human-led investigation** utilising always on full packet capture, logs and event data
- **Full forensic analysis** to confirm threats and eliminate false positives
- **Isolation and communication disruption** of the threat on your behalf, with no retainer fee
- **Full remediation support** until the threat is eliminated, not just alerting and guidance

We prepare asset management firms for complex compliance and regulatory requirements

Beyond MDR, our dedicated security experts help firms assess risks, address known gaps and build a comprehensive cybersecurity program that meets stringent regulatory requirements.

With **eSentire Advisory Services**, you'll have access to:

- Security Program Maturity Assessments
- Security Policy Guidance
- Security Incident Response Planning
- Security Architecture Review
- Health Checks
- Executive Briefings
- Penetration Testing & Vulnerability Assessments
- Risk Assessments
- Phishing Campaigns

[1] https://www.accenture.com/us-en/insight-cyber-security-asset-managers
[2] https://financialit.net/news/security/asset-managers-beef-cyber-defences-priority-new-industry-survey-reveals
[3] https://www.institutionalinvestor.com/article/b1505p7bbg9cx7/cyber-gangs-threaten-asset-managers-watchdog-warns
[4] https://18assetmanagement.com/thought-leadership/cybersecurity-risk-management-from-an-asset-manager%E2%80%99s-perspective
[5] 2017 Threat Report
[6] https://www.accenture.com/t20170418T210238Z__w__/us-en/_acnmedia/PDF-49/Accenture-InsideOps-Cybersecurity-Asset-Management.pdf#zoom=50
[7] https://18assetmanagement.com/thought-leadership/cybersecurity-risk-management-from-an-asset-manager%E2%80%99s-perspective
[8] https://www.mcafee.com/in/resources/reports/rp-aberdeen-cybersecurity-2017-summary.pdf
[9] https://financialit.net/news/security/asset-managers-beef-cyber-defences-priority-new-industry-survey-reveals

About eSentire

eSentire is the largest pure-play Managed Detection and Response (MDR) service provider, keeping organizations safe from constantly evolving cyber-attacks that technology alone cannot prevent. Its 24x7 Security Operations Center (SOC), staffed by elite security analysts, hunts, investigates, and responds in real-time to known and unknown threats before they become business-disrupting events. Protecting more than $6 trillion in corporate assets, eSentire absorbs the complexity of cybersecurity, delivering enterprise grade protection and the ability to comply with growing regulatory requirements. For more information, visit www.eSentire.com and follow @eSentire.

esentire®