Cybersecurity for Asset Managers

Linedata

Protect your business before it's too late.

Cybercrime is one of the most serious threats to business and the world's economy.

Experts predict the global cost of cybercrime damages will climb to $6 trillion a year by 2021 – more than the GDP of Japan.

Cyber attacks are 300 times more likely to target financial institutions than other businesses, with an average annual cost of $18 million per institution.

No one less than Warren Buffet has termed cyberthreats 'the number one problem with mankind'.

Because of cyber threats' massive potential for causing societal harm, funding criminal activity and destabilizing the global economy, many governments have introduced regulation aimed at forcing companies to take appropriate data and cyber-protection measures.

This means that you can be penalized for non-compliance, even if your security isn't breached. And, senior executives will almost certainly be held accountable if breaches occur as a result of inadequate precautions.

Cybercrime Damages:
$6 Trillion
a year by
2021

Sources
2019 Cybersecurity Almanac
Business Insider
Forbes
SEC Public Statement

Fortunately, all is not doom and gloom. Cybersecurity threats – while serious and constantly evolving – can be tackled like other forms of risk.

The path to success starts with analyzing potential threats, understanding the associated risk and potential damage if that risk was realized, and understanding how much you can afford to spend on mitigating that risk.

This allows you to implement appropriate controls based on established best practices, and with the help of expert partners who can complement your in-house knowledge and resources.

The CIS Controls Framework

To help organizations like yours address cyber risks, the Center for Internet Security (CIS) has developed the CIS Controls™, a set of best practices informed by the experience of senior cyber experts from a broad range of industries.

Importantly, the CIS Controls don't just focus on prevention. They can also help you detect compromised machines and prevent attackers from inflicting additional damage on your organization.

Taken as a whole, the Controls provide a strategic yet highly actionable framework for building – and sustaining – your organization's cyber defenses.

Linedata is referencing the CIS Controls™ framework under a Creative Commons Attribution-Non Commercial-No Derivatives 4.0 International Public License: https://creativecommons.org/licenses/by-nc-nd/4.0/legalcode.
You can access the most up-to-date CIS Controls™ framework at https://www.cisecurity.org/controls.

Implementing controls - 5 areas of focus

Taking Ownership

This includes everything from maintaining a full and accurate inventory of your software, hardware and data assets, to ensuring that all software, hardware, network and mobile devices are securely configured and kept up to date.

Protecting Assets

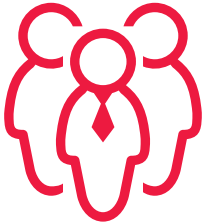
A huge percentage of attacks aim to steal data or other digital assets or hold them for ransom ('ransomware attacks'). Asset protection starts with securing your network from email and web-based threats and storing all data securely.

Keeping Watch

Cyber protection can't afford to take a day off. Continuous scanning and monitoring, automation and audit log review is critical to preventing cyberattacks – and to responding appropriately when incidents occur to limit the damage.

Reducing Exposure

The threat landscape is constantly evolving, in part due to software updates which introduce potential vulnerabilities. Your security program must manage these changes, and staff need to understand the risks and know how to respond.



Managing Behavior

Humans are always the weakest link in any cybersecurity program. Controlling access to information, services and administrative privileges is critical, as is securing Wi-Fi to prevent unauthorized access and improper or risky usage.

Cybersecurity regulations and guidelines

Data and cybersecurity are the subject of regulation and legal guidelines worldwide. Here are some key examples:

- The EU General Data Protection Regulation (GDPR) and related national legislation
- California Consumer Privacy Act (CCPA)
- New York State Department of Financial Services 23 NYCRR Part 500
- SEC Guidance
- The Monetary Authority of Singapore (MAS) Technology Risk Management Guidelines
- The Hong Kong Monetary Authority (HKMA) Cybersecurity Fortification Initiative (CFI)

of small companies that suffer a cyberattack go out of business within six months, according to the U.S. National Cyber Security Alliance.

Source: Inc.com

High-profile data breaches

have led to eye-watering fines and court settlements. In a two-day period in July 2019, the UK Information Commissioner's Office (ICO) fined British Airways and the Marriott Group a total of **over $350 million** for GDPR breaches. Days later in the US, Equifax agreed to spend **up to $425 million** to settle a 2017 data breach.

Source: ico.co.uk; ftc.gov

Linedata Cybersecurity Services

At Linedata, we know asset management – and we know cybersecurity. Our service gives you an ongoing view of internal, external and vendor risk based on the very techniques used by the intelligence community.

Unlike Due Diligence Questionnaires – which are potentially out of date the moment after they're submitted – our reporting gives you the dynamic, real-time threat intelligence you need to act quickly and decisively to protect your business, and your clients.

Security Risk Assessment
We review, identify and help you prioritize "at risk" areas.

Layered Defense
Full stack and layered defense strategies incorporating EDR (Endpoint Detection and Response) and threat isolation.

Vulnerability and Penetration Testing
Our threat experts identify both technical and non-technical areas of possible exploitation in your environment.

Threat Intelligence
Ongoing monitoring, alerting and actioning on new and emerging threats.

Phishing and Awareness Training
Engaging in-person or online training that educates and prepares staff for cyber events.

Policy and Controls Review
We develop and keep current regulatory compliance policies, procedures and controls.

360-degree Risk Analysis
'Beyond DDQ' monitoring of real-time vendor risk. Machine learning anti-virus technology plugs security holes while adapting to new traffic and providing customized alerts.

Linedata Asset Management provides a robust, configurable platform of software, data and services that enable our wealth, institutional and alternative clients to grow, operate efficiently, manage change and provide excellent service to their own clients and stakeholders.

Boston: +1 617 912 4774
New York: +1 212 607 8214
Luxembourg: +352 29 56 651
Northern Europe: +44 20 7469 8600
France: +33 1 46 11 70 00
Asia: +852 3583 7900

getinfo@linedata.com or visit: **www.linedata.com**

Linedata