Cyber for Asset Management Firms

Does Cybersecurity Matters for Asset Management Business?

kpmg.mc | cyber

In a Nutshell

KPMG Monaco supports Monegasque companies on a wide range of management, financial and regulatory issues, and is now strengthening its local presence in Cybersecurity.

This document is intended for portfolio management companies, their business issues and the technological challenges they face.

Many sources agree that the main cyber threats faced by asset management companies are:

- **Exfiltration of customer or personal information (CID)** by disgruntled, vengeful or resigned employees,
- **Infiltration of order processing systems** or mailboxes for fraudulent transactions by cybercriminals,
- **Ransomware attacks by cybercriminals,** leading to **information leaks**, system restoration costs and sometimes loss of backups, **and loss of reputation**.

To face up to these internal and external threats and avoid the additional costs of remediation and regulatory sanctions, you need support form people who know your business. KPMG Monaco has local cyber experts to provide you with relevant answers, thanks to our business and technical knowledge derived from our various expertise and auditing activities.

Evaluating the basic security of your information system (general security audit or penetration test) often costs less than €10,000.

You'll find our suggestions and approach on the following pages.

To contact us, just contact our Cybersecurity BU Manager at cmaillioux@kpmg.mc.

Content

Business Challenges

Portfolio management companies face a number of business challenges.

The portfolio management industry is **highly competitive**: you need to find ways to differentiate yourself and generate optimal returns for your clients..

The current trend suggests that **customers' expectations are changing**, as they seek more personalized portfolio management solutions, and more socially responsible investment options, for example. **At the same time, the pressure to cut costs while maintaining consistent service quality is ever-present**.

Added to these business challenges are external factors: financial regulations are strict and constantly evolving; you need to comply with precise regulatory standards and requirements, such as investment risk management. This is crucial to protecting your customers' interests but requires significant resources for compliance..

Given these conditions, the integration of technology for operations automation, data analysis and investment management is becoming essential. And with it, data security and protection against cyber threats are major concerns.

In short, you need to remain agile, adapt to change, invest in technology, offer innovative services to your customers and, last but not least, ensure compliance with the many regulations in force, while maintaining business continuity in the face of new IT security threats.

Impacts of Cyber Risks

Cybersecurity is becoming a crucial issue for asset management companies.

Some of the most significant cyber risks you may face include:

Data breach: Sensitive customer information, such as personal information, accounts and financial data, could be stolen.

Phishing attacks: Employees could be the target of phishing e-mails aimed at obtaining confidential information. In this case, cybercriminals send out fraudulent e-mails or messages that entice employees to divulge sensitive information, such as passwords or identification data.

Ransomwares : Ransomware infections have become infamous in recent years, which could result in data loss or the payment of a ransom. If you pay the ransom, there's no guarantee that your data will be restored, and criminals will still have access to your information.

Exploitation of software vulnerabilities: Security flaws in the software you use could be exploited by malicious attackers.

Malicious parties or disgruntled employees: Employees or subcontractors with access to your systems could cause deliberate problems to harm you directly or take advantage of their access to data to steal, disclose or sell it.

DDoS attacks: Distributed denial-of-service attacks could disrupt your online operations, or IT links with your group, crippling your day-to-day management.

To reduce these risks, it's important to implement robust security controls, provide cybersecurity awareness training for staff, keep a close eye on suspicious activity, and have strict security policies in place to protect your data. Constant monitoring is essential to detect potential threats at an early stage.

Several asset management companies have publicly reported on incidents they have experienced, including :

Azimut Group (2023) : The company has publicly disclosed that it received a ransom note from a cybercriminal group and will not cooperate under any circumstances. Fortunately, the institution did not suffer any compromise of customer or advisor positions, no fraudulent orders were placed, and no business continuity problems were noted.

BlackRock (2020) : BlackRock, one of the world's largest asset management companies, suffered a data breach in 2020. The incident was caused by human error, which resulted in data being sent to the wrong recipients, rather than a security issue.

JP Morgan (2014) : JP Morgan is said to have suffered an attack focused on servers hosting sensitive customer information, with access to the chase.com or jpmorgan.com websites. The data stolen seems to be contact data (name, email, etc.) but not sensitive data (account numbers, passwords, for example).

ETRADE Financial (2013) : ETRADE faced a cyber attack in 2013 that compromised the personal data of some of its customers (name, email, etc.), with sensitive data seemingly unaffected.

Portfolio management companies are not safe from cyber threats. They must then react to restore their reputations, and i**nvest heavily in post-incident security**, in addition to **risking fines** linked to data leakage and **the cost of remediating the attack**.

Proactively staying vigilant and **investing to prevent such incidents and protect both customer data and corporate reputation** is essential.

Preventing Cyber Risk

To protect your company from cyber risks, experts recommend, among other things, implementing the following basic actions:

Cybersecurity training and awareness: Offer regular training to your employees to raise awareness of cyber threats and help them recognize phishing attacks or other attempts to steal data.

Software updates and patches: Ensure that all software and systems used in your company are regularly updated with the latest security patches to reduce exploitable technical vulnerabilities.

Firewalls and Antivirus : Install high-quality firewalls and antivirus software to protect your network against attacks and malware.

Identity and Access Management : Implement strict access controls to ensure that only authorized people have access to the data they need..

Crisis Management and Incident Response Plan: Prepare an incident response plan so you know how to react in the event of a data breach, including notification of the relevant authorities and customers if necessary. Exercise your cyber crisis management skills.

Data Backups: Make frequent backups of all your critical data, and make sure they're stored securely.

Data Encryption: Use encryption to protect sensitive data, especially when in transit (email, transfer platforms).

Evaluation and management of third-party: If you work closely with suppliers or partners, make sure they meet high security standards. They may fall victim to incidents, impacting your data in their systems.

Periodic cybersecurity assessments: KPMG experts can assess your organization's cybersecurity. We can identify your company's specific vulnerabilities and weaknesses through audits or penetration testing and offer tailored recommendations. It's important to work with trusted cybersecurity experts to customize an appropriate approach to your company's specific needs, business imperatives and regulatory requirements.

Why KPMG Monaco ?

KPMG Monaco has a local cyber team of passionate, certified people with the expertise to meet your needs.

Our local team provides you with the proximity and knowledge of Monegasque regulations to serve you at best. We can also call on KPMG's international network to address specialized expertise or international issues. Here is an example of an assignment carried out in the industry:

Monegasque Asset Management Company

Internal Pentesting

Our experts carried out attacks on the company's internal network (LAN) using a computer with the limitations associated with an intern (trainee) profile.

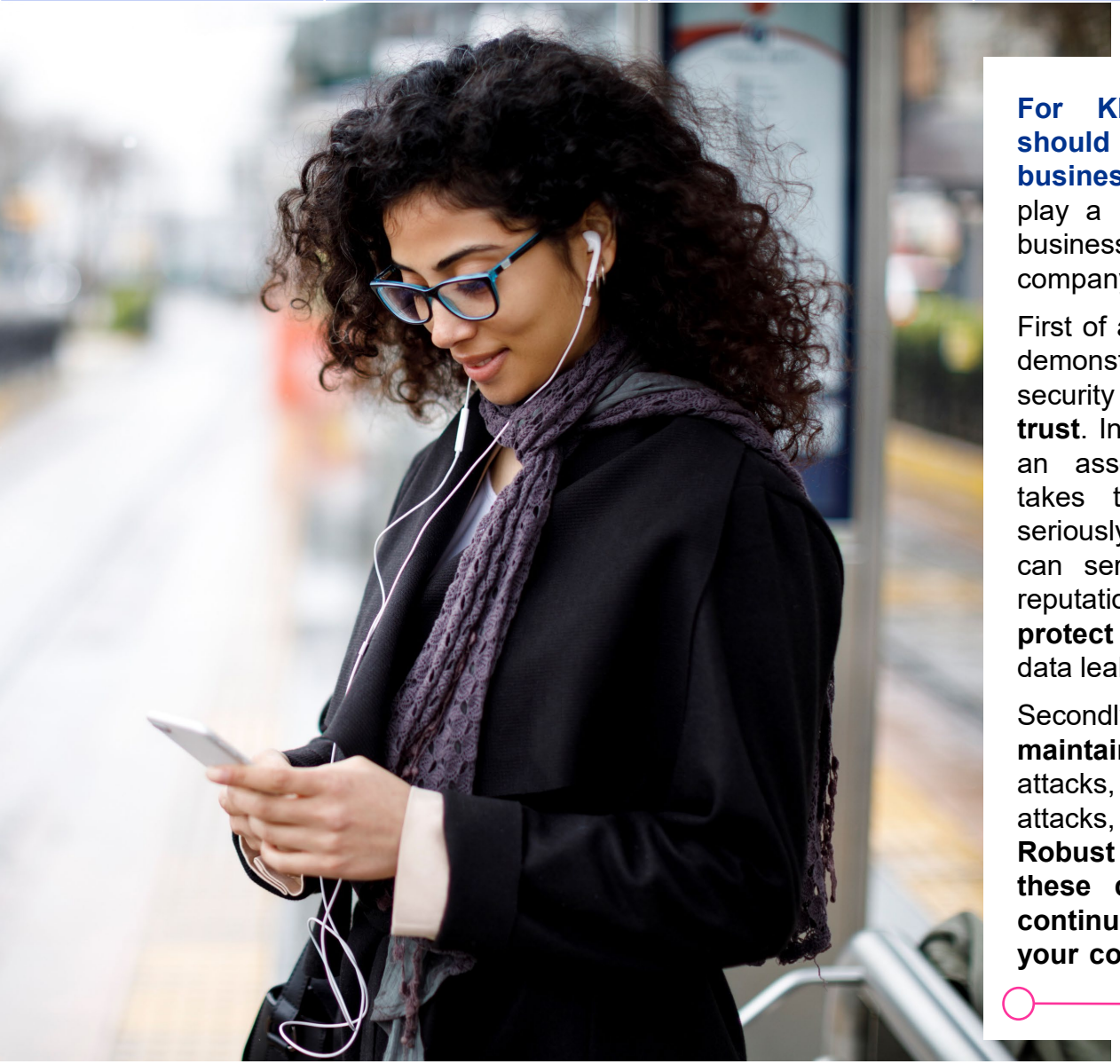
As a result, the confidentiality of customer data has been strengthened, not only by improving the security of workstations and network services, but also by restricting certain user rights. IT investment will be directed towards real gains in security, in particular through the choice of more effective anti-virus software and the application of hardened configurations for information system users.

We reviewed the recommendations with our customer during a feedback meeting **to propose solutions suited to his context.** Applying our recommendations will bring **direct benefits** in terms of **increased protection** against **threats** such as **ransomware,** denial of service, the widespread impact of a successful **phishing attack** and the **exploitation of technical vulnerabilities** by malicious individuals.

It also enables our client to **communicate how seriously it takes the protection of its customers' data, to avoid accusations of negligence from regulators** such as the CCIN in the event of a data breach, and to **invest wisely in its IT security.**

We offer a range of other services dedicated to the financial sector, such as **cyber maturity assessments**, **ransomware readiness assessments**, advice on **best practices and cyber crisis management simulations** to help you prepare your company for such incidents.

Business & Cybersecurity



For KPMG Monaco, cybersecurity should not be a constraint, but a business enabler. Cybersecurity can play a key role in how you meet your business challenges as a management company.

First of all, in terms of communication, by demonstrating a commitment to data security **you reinforce your clients' trust**. Investors are more likely to choose an asset management company that takes the protection of their assets seriously. Moreover, since a data breach can seriously damage your company's reputation, **cybersecurity can help you protect your brand image** by preventing data leaks.

Secondly, cybersecurity helps you **maintain operational efficiency**. Cyber attacks, such as ransomware or DDoS attacks, can disrupt your operations. **Robust cybersecurity can minimize these disruptions and maintain the continuity of your services**. You'll **save your company from additional costs** in the event of incidents, linked to incident remediation, loss of reputation, and investments that were not planned to strengthen security in subsequent years.

Going one step further, **new usage opportunities can be opened up to your customers** thanks to new technologies, and these solutions are **increasingly driven by cybersecurity to protect** financial transactions and customers' data in this new context. **Innovative services must be secure to ensure customer buy-in** and enable companies to stand out from the competition.

We believe that cybersecurity can be a business advantage, by creating new revenue streams, strengthening your brand image and enabling you to take advantage of the continued growth of the cybersecurity sector. This can help you diversify your business and remain competitive in the portfolio management market.

Contacts

KPMG GLD et Associés S.A.M.
Athos Palace
2, rue de la Lüjerneta
98000 Monaco

www.kpmg.mc

Sabina Debussy
Partner
Head of Advisory

sdebussy@kpmg.mc

Clément Maillioux
Senior Manager
Advisory IT | Cyber

cmaillioux@kpmg.mc