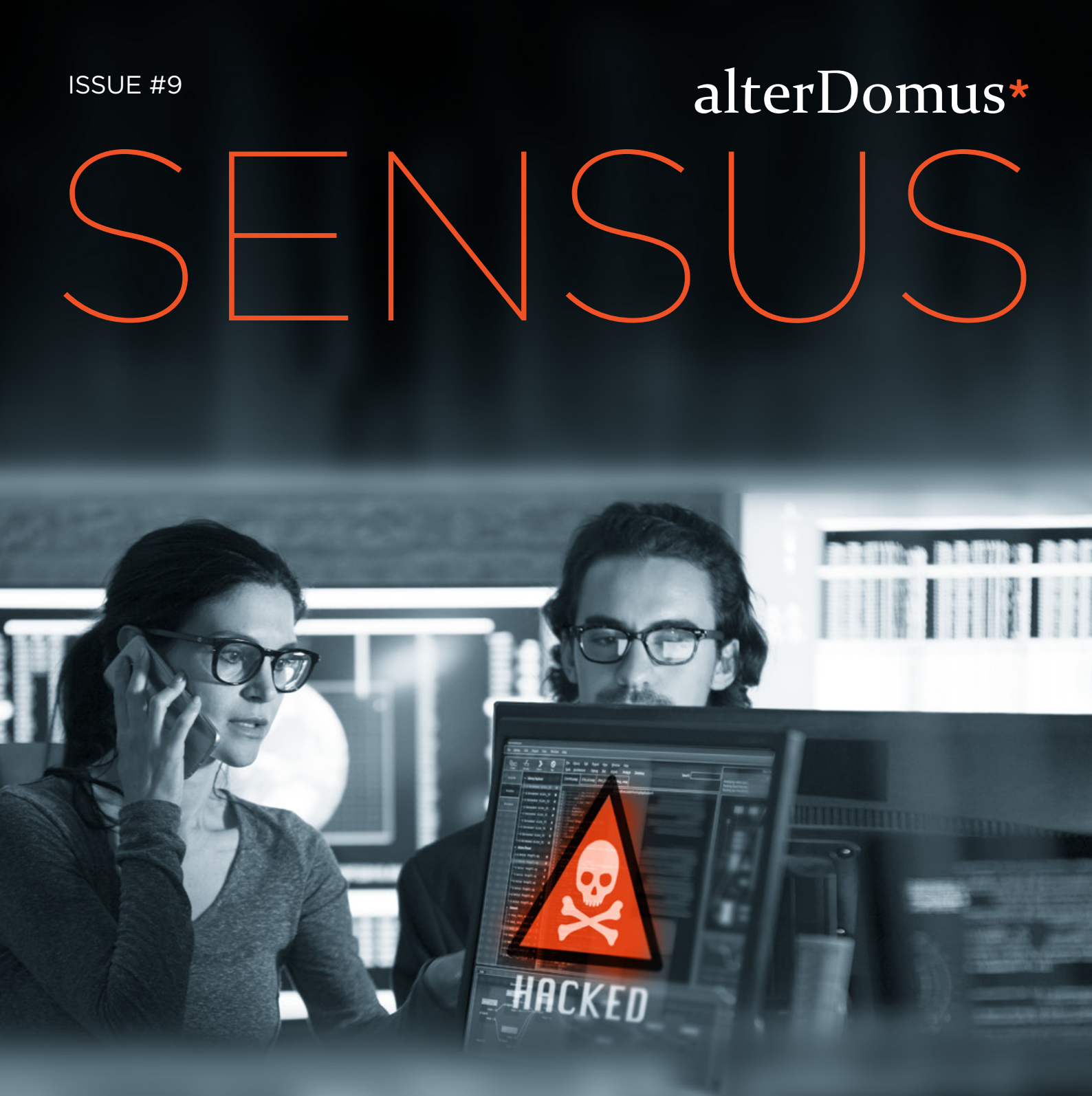
ISSUE #9

alterDomus*

SENSUS



CYBER RISK: WHY INVESTORS SHOULD CARE ABOUT CYBER SECURITY

Arno Robbertse, Chief Executive Officer, ITC Secure

CYBER RISK: WHY INVESTORS SHOULD CARE ABOUT CYBER SECURITY

Featuring Arno Robbertse from ITC Secure

A company's cyber preparedness is a crucial consideration in any investor's investment decision. It is a business risk that you cannot afford to ignore, says Arno Robbertse, Chief Executive Officer at ITC Secure.

As we have all witnessed, the pandemic pushed organisations over the technology tipping point, forcing companies to react quickly and accelerate adoption of new technologies and ways of working at record speed – transforming the business landscape forever.

The implementation of remote working and collaboration capabilities was accelerated by 43 times, compared to estimates before the crisis according to a global survey of executives conducted by McKinsey. Similarly, digitisation of customer and supply chain interactions, and of internal operations, accelerated by three to four years in a matter of months.

While this enabled organisations to rapidly introduce new business models and reach customers in new ways, this shift also widened the threat landscape further, leaving businesses exposed to the growing complexity in cyber security. The new security perimeter and the ever expanding cyber-attack surfaces have led to a surge of sophisticated cyber attacks, with top concerns including cyberterrorism, internal threats, and industrial espionage.

CYBER CRIME CAN HAVE A CONSIDERABLE IMPACT ON FINANCIAL COMPANIES

Prominent data breaches have served to shine a light on the scale of potential impact on a company. According to a recent global study, the average cost of a data breach has now reached $4.24 million in comparison to $3.86 million in the previous year.

We must also not forget that there is reputational damage associated with cyber security attacks. According to research by HSBC, it can take an average of two years for a business's reputation to recover after a data breach is uncovered. Furthermore, share prices of companies affected have been shown to underperform by 15.6% in the three years following an attack.

Additionally, regulation, including legislation such as the EU General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), is increasingly making cyber security mandatory. Approximately 60 countries have data and privacy rules on the books and 14 additional states in the US are considering similar measures – further establishing cyber security health as a global business priority.

As a result, there is a growing trend that sees investors place increased priority on cyber security within their investment decisions and portfolio companies as part of how they are evaluated – a requirement that is as vital as ensuring the correct foundations are in place for accounting, supply chains or customer services.

ADOPTING A HOLISTIC APPROACH

The growing impact of cyber attacks – coupled with the increased public and regulatory scrutiny of a company's cyber security practices further asserts the need to systematically integrate cyber due diligence in the investment lifecycle.

By holistically assessing the cyber health associated with every investment – from pre-acquisition decision-making to post-acquisition portfolio management through to post-breach investigative and risk management support – investors will be able to stay ahead of the curve and protect both the value and the brand of their companies.

Whilst undergoing due diligence, it is also important to think seriously about how changes to working and operational models prompted by the pandemic have affected the cyber security of the company. With the rapid shift to new ways of working, the security perimeter is no longer confined to a company's network. In a cloud native world, identity is the new perimeter, which brings about a new way of thinking and measures to manage risk.

Finally, investors need to be mindful not just in terms of their investment decisions and the cyber health of portfolio companies – but also themselves. Considering the regular involvement with third parties and large quantities of capital involved, investment firms themselves can be prime targets for sophisticated cyber attacks such as targeted phishing, spoofing and digital impersonation, where large amounts of funds could be funnelled off during the course of a complex deal. This makes your own cyber security an area that cannot be ignored. *

> "Investment firms themselves can be prime targets for sophisticated cyber attacks such as targeted phishing, spoofing and digital impersonation."
>
> **Arno Robbertse**
> Chief Executive Officer
> at ITC Secure

14 KEY INDICATORS FOR A CYBER DUE DILIGENCE ASSESSMENT

SENIOR MANAGEMENT AND BOARD ACCOUNTABILITY

1 Does the company identify a named person at senior management or executive committee level with overall responsibility for cyber security?

2 Is the board or board committee responsible for cyber security issues?

BOARD COMMUNICATION

3 Does the company communicate cyber risks to the board (and how, by whom and how often)?

4 Does the board receive detailed information about the company's cyber security strategy, including what information it receives and how it assesses this information?

LEGAL COMPLIANCE

5 Does the company publicly commit to compliance with all relevant laws, including those related to cyber and data protection?

POLICY

6 Does the company publicly disclose a data protection and/or privacy policy?

7 Does the policy explicitly cover its entire operations, including third parties?

SKILLS AND RESOURCES

8 Does the company disclose that it has a cyber security team and/or dedicated budget?

9 Does the company state that the board engages with relevant industry initiatives on cyber security and/or has access to internal or external expertise on cyber security?

10 Does the company actively seek such skills when appointing directors?

TRAINING

11 Does the company provide training on cyber security requirements to all employees?

ASSESSMENT

12 Does the company conduct audits of cyber security policies and systems?

GOVERNANCE

13 Has the company established an incident management plan, including disaster recovery and business continuity?

14 Has the company disclosed cyber security as a key part of its risk assessment/business continuity plan?

HEAD OFFICE

Alter Domus Luxembourg S.à r.l.
15 Boulevard F. W. Raiffeisen - L-2411
Luxembourg
BP 2501, L-1025 Luxembourg
Grand Duchy of Luxembourg
+352 48 18 28 1

www.alterDomus.com

alterDomus*