ESG Lab #2: cyber security

Paris, 15 January 2018

With cyber risk becoming ubiquitous, inescapable and potentially ruinous, PAI Partners brought investors, portfolio companies and specialists together to consider how best to upgrade the investment and corporate response.

The threat is growing. The costs can be enormous. And risk is lurking in every electronic device and every digital interaction with a customer, supplier or employee. Cyber security – the subject of PAI's ESG Lab in Paris in January 2018 – should be high on the agenda of every company and investor.

The statistics are stark. Introducing the event, PAI Partners' head of ESG Cornelia Gomez noted that 81% of French companies have been subject to cyber-attack. "If you're connected to a device, you're vulnerable," she said. For too long, however, the corporate response to cyber-attacks has been siloed within companies' IT departments. Cyber security is much more than a technology issue; it is about governance, human capital, and about companies' responsibility to their clients and shareholders to reduce risk.

It is also a growing regulatory challenge. The entry into force this year of the EU's General Data Protection Regulation (GDPR) – with steep fines for non-compliance, including failing to report cyber attacks – has focused minds. However, even here, in the face of a pressing regulatory deadline, many companies have yet to act: according to a survey conducted last year for Syntec Numérique, France's digital services trade association, 41% of companies questioned had not even begun considering their response to the regulation.

Cyber crime: a universal threat

If anyone in the room needed persuading of the universal nature of the threat, Chris Dilloway of consultancy Hakluyt Cyber, who chaired the seminar, was on hand: "Cyber security is about digital information, asset and systems – and there is no company that doesn't rely on them."

Cyber attacks can take many forms: stealing data, destroying information, installing ransomware, incapacitating systems through so-called distributed denial of service (DDoS) attacks,

> "Managing cyber risk will be the defining challenge for corporate leadership for the next five years"
>
> **Chris Dilloway, Hakluyt Cyber**

or even hijacking computer systems to surreptitiously generate crypto-currencies such as bitcoin. Some attacks can bring systems and even entire organisations to a grinding halt; others are not detected until long after the event.

And the losses can be enormous for individual firms: the NotPetya cyber attack in June 2017 cost shipping firm Moller-Maersk some $200-300 million in lost revenue, it told investors, while construction firm Saint Gobain estimated that the attack cost it $250 million in sales and $75 million in income.

Traditionally, there has been a hierarchy of attackers, with solo amateurs at the bottom, followed by hacker collectives and criminal gangs, with government agencies at the top. However, the distinctions between these groups are eroding, with some governments outsourcing cyber activities to criminals and amateurs, helping to disseminate advanced techniques. “Capability is migrating down the hierarchy,” Dilloway warned.

In terms of their effects on companies, cyber attacks can have profound direct financial impacts, operational impacts and, potentially most costly, reputational repercussions. These impacts mean that addressing the threat should be a high priority for company management – and will be a metric against which they will be judged by investors, customers and regulators. “Managing cyber risk will be the defining challenge for corporate leadership for the next five years, if not more,” said Dilloway.

Adam Black, head of ESG and sustainability at private equity firm Coller Capital noted that a survey carried out by his firm – the Coller Capital Global Private Equity Barometer – found that one in 20 institutional investors had suffered a “serious” cyber attack, with fully half expecting to do so within the next three years. Around half said they would expect their GPs and portfolio companies to introduce cyber policies within the next three years. Separately, the results of a Coller ESG questionnaire sent to its GPs found that half of GP respondents, and two-thirds of GP portfolio companies, were looking at cyber procedures and policies.

41%

The percentage of companies yet to begin planning for GDPR

From server farms to hydroelectric dams

Cyber risk can manifest itself in unexpected places. Stéphanie Lachance, head of responsible investment at Canadian pension fund manager PSP Investments, said that her organisation confronted the issue not only through investments in Silicon Valley companies, but also in hydroelectric dams: “How do you think those dams open and close? Those systems could be hacked.”

As well as threats to their portfolio companies, private equity firms can face direct exposures to cyber risk, noted Alexandra Pailhes, private equity manager at French insurer CNP Assurances. For example, if hackers are able to gain access to a firm’s investor lists and drawdown notices, they can amend bank account details to misdirect redemptions, potentially costing firms millions of euros.

Meanwhile, stakeholders – including customers, regulators and the media – expect more transparency regarding cyber security issues. Countries around the world are introducing laws mandating disclosure of attacks, such as the EU’s GDPR directive – or even suspected attacks, as is the case with Australia’s Privacy Act.

The challenge is a serious one – but it’s not insurmountable, reassured Dilloway. “It’s a business risk, and it’s a complex technical problem – but it is manageable,” he said.

50%

of institutional investors expect a “serious” cyber attack within three years

He notes that technology is only one part of the solution: “The answer is not always about throwing technology at the problem. Sometimes it’s about the appropriate processes and putting the right controls in place.” Black at Coller Capital says that his firm’s head of cyber talks about the importance of “the human firewall”, and the need to properly train staff to understand the threat and how they should respond in a given situation.

$200-300 million

in lost sales for Moller-Maersk as a result of the NotPetya cyber attack

Detection and response

Zeina Zakhour, the global chief technology officer for cyber security at Atos, a European IT services company formerly owned by PAI, agreed there is no fail-safe technological answer. “Before, the answer was to build walls; now, it is about detection and response.” She notes that, on average, it takes 190 days for companies to detect that a cyber breach has occurred: in some cases, it has taken more than a year.

She adds that the idea that hackers are always one step ahead is a myth. She argues that the Wannacry attack – the May 2017 attack which inserted ransomware into more than 300,000 computers around the world – could have been prevented. The vulnerability the attack exploited was identified in 2016, and Microsoft issued a patch in March. “The problem is often a shortage of resources dedicated to cyber,” she argues.

Prevention of cyber risk will, however, only get companies so far, given that a successful attack, at some point, is a near certainty. A critical part of a company’s response to cyber security has to be its communication strategy. “The media is getting more aware of cyber security, and is asking more sophisticated questions,” notes Dilloway.

“I meet companies in two situations: either preparing for a cyber attack, or responding to one,” says Guy Fithen, a consultant who provides communications and crisis management advice. “I know which I prefer.”

His advice is for companies to ensure they have plans in place around how they will communicate in the event of an attack, with a team identified and scenarios rehearsed. “Most of the time, you need to have something to say.”

> “Before, the answer was to build walls; now, it is about detection and response.”
>
> **Zeina Zakhour, Atos**

Another important element is that the IT function is represented at board level, in the same way that communications and branding departments now typically are. “You can’t easily train CEOs to talk IT – it’s a lot easier to teach a technology specialist how to speak ‘management’,” he adds.

Taking out insurance

Insurance also plays a role, notes Jean Bayon de la Tour, cyber development leader for Continental Europe at insurance broker Marsh. Coverage against cyber attack has been available for many years, but interest in Europe, particularly, has been spurred by the introduction of the GDPR, he says. As with any insurance solution, the financial payout is only part of the offering. He describes "three pillars" of an insurance offering: financial compensation for the consequence of a cyber attack; support with crisis management to mitigate those consequences; and advice on preventing such attacks in the first place.

What about the role of investors? Lachance at PSP notes that, as direct investors often with board representation, PE firms have a responsibility to ensure that cyber security is addressed at the highest level of companies. She has prepared a "cheat sheet" for her deal teams to use during the due diligence process, which provides a series of questions that non-cyber experts can use to challenge management. "It's not about becoming experts, but it is about knowing when you need to turn to experts."

For private equity investors, the potential high frequency of cyber attacks poses a challenge for their oversight of the companies they own: what level of incident reporting should they require from their companies? "There should be a materiality test," argued Ivan Massonnat of PAI, reflecting the views of a breakout discussion. "It needs to be about financial impact." Of course, materiality is also a function of which sector is affected: the compromising of customer data from a healthcare company, for example, would be considerably more serious than a cyber attack on a manufacturer.

Service providers are stepping forward with products that can help investors and other stakeholders assess the readiness of companies. Gomez at PAI, noted that a GDPR label is being developed for B2C companies, to help their customers understand how safe their data is in these companies' hands.

> "You can't easily train CEOs to talk IT – it's a lot easier to teach a technology specialist how to speak 'management'."
>
> **Guy Fithen**

How private equity can help

Black at Coller notes that GPs are able help portfolio companies learn from each, noting that some of the GPs to which Coller has committed capital "have looked at their portfolio companies, and engaged with their IT people, and have brought them together to share best practices – it's like free consulting."

"One important message," concluded Dilloway, "is that investors, and private equity companies, are in a strong position to help set the tone. You are in a very strong position to help companies manage IT risks … You are in an excellent position to drive improvement."