Cybersecurity

Risk

The risk of cyber attack presents an ever-increasing threat to commercial results, through lost business, fines, ransom and fraudulent payments as well as resulting reputational damage. We wanted to demystify this threat and so we conducted a 'Maturity Assessment', across each business, to determine their cybersecurity readiness and the risk it poses to them.

The recent (Not)Petya outbreak – which occurred soon after the similar WannaCry attack - resulted, according to press reports, in a significant operational and cost impact on British consumer products company Reckitt Benckiser. According to widely released reports, they suffered an estimated £110m ($135m) in lost revenue as a result of production disruption. Chocolate maker Mondelez was also affected. They put the damage at a three percentage point loss, from their second-quarter sale growth. Other household names, reportedly affected by (Not)Petya included advertising group WPP, FedEx, shipping giant Maersk and Nuance Communications.

Hg's research

In the world of private equity, cybersecurity presents a direct threat to enterprise value. However, it is possible to 'protect' this value and, in doing so, demonstrate a well-managed business. In short, being able to demonstrate that you manage cyber risk well can create additional value.

It was important to us, at Hg, to demystify the risk and threat of cybersecurity. We wanted to support our portfolio businesses in helping them to understand the threat, where they stood in terms of preparedness and what they needed to do next.

We created a standardised 'end to end' cybersecurity assessment, employing industry best-practice frameworks and standards across fourteen non-technical (for example, governance and risk management) and technical (for example, malware protection) control areas. We applied this to thirty four companies within the HgCapital portfolio.

This research was based around an interactive and facilitated self-assessment. To ensure we got the most useful information from this, a qualified member of our Operational Innovation team worked through the assessment questionnaire with a Senior Technology Leader (typically the CIO, CTO or CISO) from each portfolio company.

Each response was constructively challenged, scored and relevant observations or recommendations discussed and noted.

For every assessment conducted we produced a standardised report. This contained:

1. 'Cybersecurity maturity and posture' ratings – The two ratings provided were:
    a. Overall Cybersecurity Maturity (Scale of 0 (very bad) to 10 (very good))
    b. Cybersecurity Maturity scores within the five primary categories and fourteen subcategories assessed (same scale as 1.a)
2. 'Industry and portfolio' Financial benchmark data (for example, % of IT budget consumed on Cybersecurity)
3. Each company's' Cybersecurity maturity 'position' in relation to the other portfolio companies assessed
4. Observations and recommendations arising from the assessment specifically to each company.

Action on Cybersecurity

But we didn't want to limit it to a report. Action is important to us. That's why, importantly, every report was discussed with the relevant portfolio business executives, and with the members of the Hg team, that hold places on each Board of Directors. We focused on the key 'messages' from the assessment process, and made sure to identify and agree the specific actions required for improvement.

Once we had collated this information we drew it together to generate a 'portfolio level' view of cybersecurity risk. With this we can provide a more direct level of support, across our Hg community. We have used it to set out a priority order for improvement activities and as a 'baseline' from which to measure success.

But it doesn't stop there. Every business involved took part in an open, honest and constructive way. As a group we're firmly committed to managing cybersecurity risks in a proactive and robust way. However, cybersecurity is a rapidly changing world, requiring constant attention. That's why every assessed business has already had an informal three month 'progress review' and will be formally reassessed and rescored after a one-off six month period and then, as standard, every twelve months.

Being prepared

Most importantly, this has been an exercise in preparation and support. Not only have we been able to identify areas for improvement but we've been able to develop tools, as a community, for tackling them. We've formed a cybersecurity community, of CTOs, CIOs and CISOs, from within our portfolio and we've developed a Minimum Standard, as well as 'Jump-Start' materials such as our Risk Register. Understanding and preparedness are improved across the Hg community and we continue to work to reduce the threat and risk level.

'Hg's approach to Cybersecurity has been supportive, informed, challenging and collaborative; a valuable sense-check to help protect investor assets'

Alex Cutler, Chief Information Officer, IRIS
