FINSBURY
COVID-19
INSIGHTS

Digitalisation, data, and the corporate landscape –

What does cyber risk mean in the new threat environment?

Charles O'Brien
Partner, London

Andrew France
Co-founder
of DarkTrace

Charles O'Brien, Partner in Finsbury's UK crisis practice and member of our cyber crisis task force, spoke with Andrew France, former Deputy Director for Cyber Defence Operations at GCHQ, subsequent co-founder of DarkTrace, – who shared his perspectives on the key issues that business and security professionals and leaders need to consider.

1. What do you understand by the term cyber risk?

I have a broad definition of cyber, so I am glad you framed the question in terms of cyber risk more specifically because I think that is a much more helpful approach. What I mean by that is cyber was once treated as a standalone technical issue – but not anymore. Cyber risk affects everyone from governments, to corporates to private citizens. It is more than a technological issue around protecting data, it is about recognising and protecting the ability to use data to better serve customers and generate value, but doing that safely and securely. Most companies are getting better in appreciating the true importance of their 'Crown Jewels' or the proprietary data which ultimately underscores the value of the business.

A company that is handling cyber risk well is probably doing other things well. Cyber risk management is a highly credible proxy for the effective running of an organisation. This fact is not lost on investors, shareholders or regulators.

2. How has the threat evolved in this new environment?

The risk has increased significantly as a consequence of the COVID-19 outbreak, primarily because of the rapid wholesale switch to home working.

Unfortunately, this virus will likely be with us for some time. For the foreseeable future, we may well be in a situation where 50% of staff have to work from home, with two metre social distancing having a real impact on the workplace. As companies evolve their approaches, we will likely see a portion of staff working from home and the remainder in the office – which could almost result in two different cultures. Attackers will feel more emboldened in this environment as the chances of success will potentially go up. Defenders will have to ensure that protections in the office environment apply equally when the workforce is at home. More importantly, they will need to make sure that when that workforce rotates from home back into the office that they aren't bringing anything 'nasty' into that environment.

3. Is this not simply about investing more in IT systems?

If you want to improve security in an organisation, you must address the culture in the business. Don't overcomplicate it. Security is first and foremost about mindset and about positively influencing people's behaviour, not just about better technology. A business could have a close to 100% secure network, but you wouldn't be able to use it to do anything meaningful (because it wouldn't be connected to anything, it wouldn't run any software, and would have no users). Therefore, given there will always be security challenges for any IT infrastructure, you have to have the right conversation with staff, employees and boards. Decisions made at board level and implemented without properly engaging staff will have a success rate of near zero.

The current environment is forcing companies to test the perceived limits of previous practice. For example, many boards that would never have operated remotely are now doing so consistently and effectively. Organisations that have a mature and positive conversation about digital risk are handling this better than those who are just saying 'it's an IT issue - let IT handle it.'

4. Who will the winners be?

Companies that put cyber risk management at the heart of their resilience preparation and continuity planning through COVID-19 and beyond will be the winners.

It's not uncommon to see organisations spending money on technical point solutions to cyber threats while not necessarily addressing or reducing the inherent risk. In this current period of great uncertainty, the companies that strike a more nuanced equilibrium between people, process and technology will fare much better. Those that have done well more recently in navigating the challenges around remote working are maintaining the right balance of robust culture, strong process, great IT support, and a Board acting as a strong and vocal advocate for the approach to risk management.

5. What new instruments are you seeing corporates employ to manage the heightened risk? Are they working?

- **Staff monitoring** can be a blunt instrument and quite intrusive if it is not focussed on where the risk is greatest. Conversations need to be had to avoid friction between staff and the Board, and the risk management team needs to have a strong sense of who in the business actually has access to the data that you are trying to protect.
- **Phishing tests** are not necessarily the right way to uncover security vulnerabilities. A company should be working on designing and building a network that is robust enough that if one person clicks on a phishing link, then it doesn't compromise the whole network. I worry that trying to catch staff out by clicking on a link is a massive distraction to the real issue at hand. Creating the right technical controls and establishing a constructive (and supportive) environment to foster a security culture where a phishing simulation is a carrot rather than a stick is far more effective in my view. In my experience helping staff to understand the risk and encouraging them to be safer online when they are in the home environment pays dividends in the working environment.
- **Data loss prevention software (DLP)** has its place as part of a layered security model, but in today's world it is never going to catch all the incidents of inappropriate data loss. Why? Because there will always be ways to circumvent a device that is looking for signature-based detection. Ubiquitous encryption (in a browser or stand-alone applications) means it is harder to monitor boundaries for data that shouldn't be leaving. Most DLPs aren't set up effectively anyway: there tends to be a large number of false positives. You do need to have other ways to ensure your sensitive data isn't leaving your organisation, for example through the encryption of your most sensitive data.

One needs to start looking at it from a security outcome position, instead of looking at a points solution to a specific problem. A company with DLPs in place doesn't stop someone leaving with data on a load of USB dongles at the end of the day (if you haven't addressed that issue!).

6. What does the current environment mean for the global trend towards digitalisation?

This trend will accelerate dramatically through COVID-19. Supply chains have become longer and more diffuse, which in the current environment could mean more risk exposure for global businesses. Organisations that have a good understanding of their own digital supply chain down to second and third order issues will fare better. The supply chain must be effective the whole way through. Understanding where the crunch points are – i.e. cyber risk – will be key.

Post COVID-19 I think there will be a much more nationalistic approach to managing suppliers which will create challenges. One of the consequences of the pandemic is that we have seen how vulnerable global supply chains are in the face of an international crisis. That is a problem for PPE, and it has also been a problem for digital supply chains including both hardware and software.

LONDON

The Adelphi | 1-11 John Adam Street | London | United Kingdom WC2N 6HT

+44 (0)20 7251 3801 | enquiries-uk@finsbury.com

www.finsbury.com