FINANCIAL TIMES
SUNDAY 11 AUGUST 2019

Cyber Security

Companies must start taking cyber risk seriously

The introduction of 5G and the spread of artificial intelligence will see threats multiply

HENRY CRUMPTON

More than three decades ago, I attended the CIA's first ever "computer operations course". I learnt there that people, not technology, are the weak points in the realm of cyber risk.

This is a lesson I was reminded of recently with the revelation of a significant data breach at Capital One Financial. However, many executives continue to ignore the fundamental principle of peoplecentric digital risk. As technology evolves, the adversary is not a virus or a bot-net, but a person or group of people who use digital technology in alternative, often illegal, ways. Yet so many leaders default to simple technical solutions, and fail to understand the multi-dimensional nature of digital risk.

The introduction of 5G and the advent of artificial intelligence will turbocharge the internet of things, amplifying the cyber threat. With corporations and governments continuing to cut costs by shifting to the cloud, the exposure of even the most diligent organisation rises exponentially.

There are valuable lessons to be learnt from executives who have embraced the challenge of learning about the threat and taking decisive action. First, they accept that digital risk may be the most salient threat their enterprise will face. As one of the US's top CEOs told me: "I fully understand how serious this is. It's a . . . war. I devote my best people, with plenty of incentive, and a robust budget to fight our cyber adversaries every second of the day and night. I understand my duty and accept that responsibility. My brand reputation demands that."

The second lesson concerns the intelligence-driven process required to determine the best strategy for the company. Producing this intelligence requires constant assessment of a company's vulnerabilities and capabilities matched to the ever-changing threat environment. Moreover, as and when companies change direction, they grow organically and through mergers to match market needs. Their digital risk plans must, therefore, also change. Intelligence can measure complex change and provide an advantage in decisions, both tactical and strategic.

Third, invest in employees who understand and manage digital risk. Some firms employ an external, unbiased expert auditor who complements the company's digital risk team, much like outside counsel or an accounting firm that scrubs the books every quarter and reports to the board.

An innovative Fortune 100 CEO outlined this audit concept to me a few years ago: "This is a responsibility bigger than the C-suite. I need help, and the board needs to understand and contribute. The risk will grow. We need to be ahead of the threat." Such companies must also grasp the opportunities afforded by digital technology.

Fourth, work with elected officials and regulators to improve risk-management. The bipartisan introduction of the US Cybersecurity Disclosure Act this year may help business leaders focus on cyber crime. The act requires publicly traded companies to include in their filings to the Securities and Exchange Commission information on whether any member of their board is a cyber-security expert. If none is, they have to explain why having this expertise on the board is not necessary.

Compliance is currently just a check-the-box procedure, not a specific strategy. This legislation may help boost the level of attention to and responsibility for an important element of digital risk management.

The final lesson is to inculcate a culture of digital responsibility, discipline and flexibility throughout the company. As that same Fortune 100 CEO told me, "Digital risk management is a journey, not a destination". He's right: it is a journey that demands the best intelligence to inform the best decisions.

The writer is chief executive of Crumpton Group, a business intelligence firm, and a former US coordinator of counterterrorism