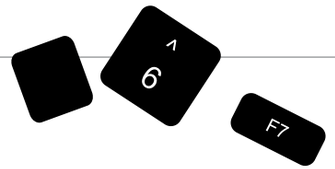
Into the breach

High-profile hacks have promoted cybersecurity from a backroom IT issue to a boardroom headache. But what opportunities does it represent for investors, asks Joy Dunbar

On New Year's Eve 2015, the BBC's website, which includes iPlayer, one of the UK's most popular on-demand entertainment streams, went down for several hours following a cyber attack. The website experienced a distributed denial of service, or DDoS, by a US-based hacking group testing its "capabilities" against terrorists.

The incident is the latest in a growing number of hacks against government defences and large corporates, including the White House, Sony and TalkTalk. Many of these attacks have taken place across multiple jurisdictions and due to the constantly evolving nature of hacking, the response of authorities across the world has been hindered.

"Cybersecurity has gone from being perceived as an IT issue or scaremongering to an important boardroom challenge in the last five years," says Nick Bray, CFO of IT security firm Sophos, which is part-owned by ▶



private equity firm Apax. "With cyber criminals, there is a constant adversary," he adds, citing figures* that value the IT security market at about US$35 billion globally and growing at 7% per annum.

Company owners, CEOs, boards and governments are growing increasingly aware of this threat and the damage a breach can inflict on the reputation of their business and its bottom line. And rightly so, when you look at the increasing number of cybersecurity breaches in recent years: the UK Government dealt with 100 cyber national security incidents per month over summer 2014 – a year later that figure had doubled.

Breaches have also become more expensive for companies, according to research conducted by PwC for the Department for Business, with the average cost of the most severe online security breaches for big business now starting at £1.46 million – up from £600,000 in 2014.

The age of 'everyware'

The internet has integrated into everyday life with the growth of the Internet of Things and cloud-based services, resulting in even greater cybersecurity challenges for businesses and prompting more investor interest in their solutions. The EU's General Data Protection Regulation – new legislation governing the security and management of personal data, both of customers and employees – is also raising the bar for companies in terms of cybersecurity compliance.

According to US-focused venture capital database *CB Insights*, venture capitalists are betting on cybersecurity companies in mobile and cloud-based defence and identity management.

Among the top 20 firms *CB Insights* surveyed in 2015, 13 have made 10 or more investments in cybersecurity during the last five years and all have made at least one deal. These firms participated in deals that invested US$222 million in cybersecurity in the first quarter of 2015 – significantly more funding than in all of 2010. The deals included tech venture capital firm Andreessen Horowitz investing US$52 million in cybersecurity firm Tanium. There was also a US$40 million Series C round of funding to Ionic Security from Google Ventures and Kleiner Perkins Caufield & Byers.

In the UK, cybersecurity firm Darktrace raised £12.27 million from a number of venture capital and private equity investors last year, including Hoxton Ventures, Talis Capital and Invoke Capital.

Meanwhile, Paladin Capital, the Washington DC-based private equity firm, expanded into Europe last year with the launch of its dedicated Cyber Fund. It forecasts that cyber investing "will grow substantially, driven by high spending by governments and the private sector on 'technologies of need' to protect proprietary information and critical infrastructure." Sir David Omand, a former director of UK intelligence agency GCHQ, and Sally Tennant, former CEO of Kleinwort Benson Bank, have both been appointed as directors.

Alex van Someren, managing partner of the Early Stage Funds at Amadeus Capital Partners and founder of Cyber London (CyLon), Europe's first cybersecurity accelerator programme, points to significant demand for better cybersecurity solutions and says UK innovation in this space is thriving.

"The UK has a lot of expertise in the cybersecurity domain," he says. "We've got a large number of universities working on innovation in this space, government agencies that are spinning out projects, and large corporates who are interested in spin-out projects or allowing teams to set up new businesses."

Hacked nation: 2015's high-profile breaches

BBC
The BBC's website and iPlayer service went down on New Year's Eve following a cyber attack.

Ashley Madison
The adulterer's dating website had the personal information of 33 million of its 'discreet' customers around the world posted online.

Carphone Warehouse
Up to 2.4 million people had their personal information compromised, including the encrypted credit card data of 90,000 customers.

TalkTalk
The UK phone and broadband provider had unencrypted information stolen, including the bank details of 4 million customers.

BBC iPlayer fell victim to a cyber attack on New Year's Eve

**Source: IDC WW IT Security Products 2014–2018 Forecast and 2013 Vendor Shares: Comprehensive Security Product Review*

Extramarital affair website Ashley Madison had its database compromised

Hot topic

Ten years ago, cybersecurity companies were acquired or raised capital via an initial public offering (IPO), says Colin Tankard, managing director at data security specialist Digital Pathways. "Often, when bought, the technology from these small companies was lost or deliberately buried. Also, it was almost impossible to get a chance to pitch a cybersecurity firm to a venture capitalist. But that has changed."

Venture capitalists and, in particular, crowdfunders are interested in cybersecurity because it's a hot topic and the investment opportunity is clear, Tankard explains. He adds: "Now there is interest from other investment routes, smaller companies can hold out longer, not take the IPO or acquire route and allow their technology to grow, become known and forge some market share. Ultimately this increases the market value and hence makes the return on investment better."

The market is complex, however, and investors should exercise caution, he says. "Encryption, for example, is often in the press, so to an investor anything that says 'encryption' must be good. Not all encryption is the same or as secure as others, so investors need to be careful."

Cybersecurity lecturer, Dr Daniel Dresner, from the University of Manchester, echoes this view and says companies that release their technology first are often rewarded most, in terms of being remembered. But those that do are not necessarily the most secure. He adds: "Investors should look for technology firms with staff who can build security products and have the capacity to communicate and articulate the benefits."

There can be significant challenges when validating these benefits and claims should not be taken at face value, stresses van Someren. "One of the things we try to do to get products validated is to get a customer – for example, a big financial institution, a government department or another security expert – to help a start-up prove their claims are valid," he explains. "This helps us to make the investment case a lot more robust and less risky."

In November 2015, Chancellor George Osborne announced the Treasury is to make available £165 million for buying or investing in cybersecurity start-ups. While this is undoubtedly a coup for the industry, accessing the capital may prove more difficult for market-tested solutions that need a little more financial help to grow, says Tankard.

"Funding ideas is great but often these ideas, once developed, are sold to larger companies and so the government grant is lost," he says. "Companies that are developing solutions and have market presence are, generally, in it for the long haul. They are building products, market share and revenue for the country." ■