ford+scott
Financial Planning Pty Ltd
'Relationship Driven Strategic Advice'
ABN: 67 009 566 161

Data Breaches & Cryptoworms: The World Held to Ransomware

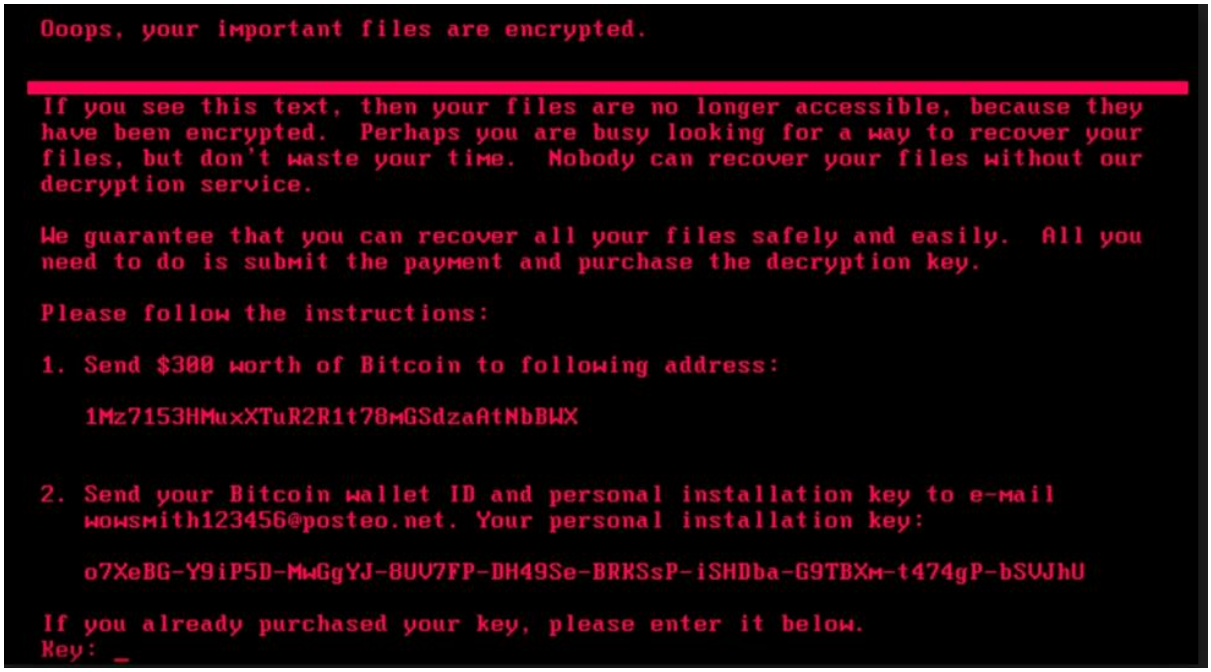
Technology stocks shuddered Monday, following the New York Times expose of a politically aligned insights group harvesting the data of 50 million Facebook users. While raising fears of regulatory intervention in big tech, this demonstrates how data security and cyber risk need to be front of mind for companies, governments and investors. Over the past few years, an escalating and increasingly concerning spate of data breaches and hackings has come to light, providing genuine cause for concern.

In June of 2017, reports of companies falling ill to new hijacking software began filtering through news agencies. Cyber Security firm, Kaspersky, was reporting wide ranging infections of a new malware variant causing material damage to organisations. The severity of this wave of "ransomware" became more apparent as it spread from little known Ukrainian banks to large Western corporations. This malicious software, dubbed NotPetya, followed hot on the heels of the less damaging, but highly pervasive, WannaCry outbreak. The gravity and economic impact of this event only became quantified as global listed companies began reporting the quarterly earnings impact of losing access to their data and systems for several days. Maersk, hit so severely that internal communication devolved to WhatsApp messaging, announced a financial impact of US$300m on its third quarter earnings. FMCG behemoth Reckitt Benckiser, the U.K based manufacturer of household brands like Dettol, acknowledged the incident would reduce like-for-like sales from 3% to 2%, or around £100m, owing to supply chain disruptions and manufacturing down time. Many other listed corporations including FedEx, Merc and WPP joined the chorus of downgrades, and these were just the businesses that were required to under statutory reporting laws. Countless companies were spared the reputational damage of confessing their security breach.

The NotPetya catastrophe was an example of a Cryptoworm, designed to encrypt data and storage devices, then demand Bitcoin payments to unlock them. Malicious software is a continuously evolving beast, driven by a cat and mouse game between hackers, security firms and governments. A fortuitous development for this illicit craft was the onset of cryptocurrencies, allowing anonymous transfers of digital ransom. Even paying the ransom may not save your data, as the intent of the malware is often to merely inflict damage. NotPetya's ability to harvest ransom was also limited as the email address used to receive decryption keys was quickly shutdown by its ISP. The likely resolution in most cases was for I.T staff to simply restore systems to backup images and attempt to resurrect systems to an operating state.

1/31 Davey Street
Hobart TAS 7000
Tel: (03) 6224 4011
Fax: (03) 6224 0809

GPO Box 2250
Hobart TAS 7001
Email: info@fordscott.com.au
Web: www.fordscott.com.au



Viruses have plagued organisations for as long as computers have enabled data to be transferred. Corporate history is littered with incidents of enterprises crippled by nefarious code targeting key systems. Perhaps the most prolific worldwide infection was the Slammer worm in 2003, which managed to exploit Microsoft SQL databases all over the world. The result was to crash servers, drain network resources and in the process slow the entire World Wide Web. While frustrating and time consuming to eradicate, this generation of viruses lacked the audacious economic and often political motives featured in contemporary ransomware.

As devastating and operationally disruptive ransomware attacks can be, they often pale in comparison to the reputational damage inflicted when customer data is stolen, rather than destroyed. This form of attack has become a favourite of the hacker community, where network vulnerabilities are exploited, and sensitive customer data held for ransom. A well-publicised case occurred October 2016 when Uber's databases were breached and the records of 60 million riders and 7 million drivers lifted. While the company paid a US$100,000 ransom to maintain discretion, it later moved to disclose the event.

In 2017, U.S credit bureau Equifax suffered what was likely the most damaging hack in U.S corporate history. More than 140 million citizens had their most sensitive of personal data, including demographic and credit card numbers, stolen from the company's servers. The hacker's demand for a US$2.6m ransom was not forthcoming but related costs, fines and class actions are likely to be several hundred million.

Simultaneously terrifying and hilarious was the case of dating site Ashley Madison. After gigabytes of user data was copied from their servers, the hackers made public the names and email addresses of subscribers. Good Samaritan internet vigilantes quickly made the information easily searchable online, resulting in much consternation for philanderers worldwide. The websites owner, Avid Life Media, ended up settling a user class action for $11.2m.

A more complex development was the discovery of two vulnerabilities in common microprocessors, dubbed Meltdown and Spectre, earlier this year. Academics discovered it was theoretically possible for data to "leak" from one computer process to another whilst running on the same machine. While concerning for personal devices, the real danger is to cloud computing services, including AWS and

Google Cloud, where multiple organisations run independently on the same hardware platform. Under this cost effective and efficient form of socialised computing, customers have processes separated into virtual "instances" but the shared physical processing may open up potential vulnerabilities. Chip makers and software providers quickly released patches for the susceptibilities, yet decades worth of PC's and servers manufactured with the bug left millions of machines potentially still exploitable.

In Australia, digital intrusions have been less high profile but still concerning. Car sharing network GoGet admitted to having consumer data accessed by a hacker who used the information to steal vehicle access. A 2011 incident involved daily deals website Catch of the Day, where stolen personal information and credit card numbers were not reported to customers nor the police for over three years. Since then, Australia's laws governing the theft of consumer data have come up to date with most western economies. As of February 2018, the Privacy Amendment (Notifiable Data Breaches) Act 2017, requires the prompt notification of data breaches, and applies to companies with annual revenue in excess of $3 million a year. All of these incidents have become a lightning rod for corporations to assess their information security regimes. A spate of class actions now sees cyber security firmly entrenched in the ESG (Environment, Social Governance) lexicon, requiring boards to clearly formulate strategies to protect their data and the privacy of their customers.

The array of threats to individuals and organisations from data destruction and theft has evolved alongside a burgeoning digital security industry. Today's technology industry relies on companies offering hardware and software solutions to protect us from the digital barbarians threatening our security and privacy. Aside from exorbitant fees extracted by I.T security consultants, a number of investment themes take advantage of this necessary obsession with data fidelity. One such company, F5 Networks, is included in our Global Growth portfolio.

F5 specialises in communications equipment, targeted at the Application Delivery Controller (ADC) market. Based in Seattle in the U.S, the company's products help secure the applications and websites of service providers, corporate and government customers around the world. The group benefits from the exponential growth in data flow, driven by trends including cloud computing, streaming video and online retail. Whilst the firm was only incorporated in 1996, the company has grown into a USD2bn revenue business with a strong growth and profitability profile.