Case study

Backup breakdown

Engineering firm's files wiped out by ransomware

Unlike healthcare and financial services organizations who regularly handle personal information, some professional services providers like engineers have been slower to adopt cyber insurance policies, assuming their risk is fairly limited.

But, any business that relies on computer systems to generate or store business-critical information can have a very real exposure to cyber risks if they lose or are unable to access their digital files, and should have a cyber insurance policy in place that provides appropriate cover.

WannaCry descends

In May 2017, there was a global outbreak of ransomware known as **WannaCry.** Ransomware is a type of malware that works by encrypting data files on a particular computer or network, and then demands that ransom be paid in order for the data to be decrypted. Ransomware is usually delivered via emails that look like they're from legitimate sources, but which actually contain links or attachments that, when opened, allow the ransomware to run on the computer and encrypt the files. WannaCry was unique in that it didn't require a significant number of people to click on links in order to spread. Instead, it utilised a vulnerability in the Windows operating system known as Eternal Blue, which allowed the ransomware to spread through structures that share files, like drop boxes and shared drives for documents or databases.

> Within just 24 hours, over 230,000 computers had been infected in more than 150 countries

WannaCry spread rapidly from computer to computer. Within just 24 hours, over 230,000 computers had been infected in more than 150 countries. There were many high-profile casualties, including the National Health Service in the UK and the Spanish telecommunications giant Telefonica. But there were many smaller organisations and businesses that were victims of this attack, too, including a small, four person engineering firm based in London.

Where's our data?

On 12 May 2017, the firm was hit by the WannaCry ransomware which encrypted all of the data files on their server as well as data they had backed up on a local hard drive. This included a catalogue of technical drawings, prints and complex design specifications for the various projects and bids that they had worked on over the years. Not only was this valuable intellectual property and the very foundation of their business, but they also often used modified versions of these previous drawings and specifications to help with marketing, preparing for bids and undertaking new projects. Not being able to access this information would therefore have a detrimental long-term impact on the business.

At first glance, the impact of the incident didn't appear too serious as the company had a contingency ▶

plan in place for data recovery in the form of a remote cloud back-up. The solution was fairly straightforward: the business could simply recover their data from the cloud.

Unfortunately, when the business attempted to restore their data, it was discovered that **their cloud backup had been failing since 2014.** This meant that every document, design specification, drawing or print for each of the projects and proposals they'd undertaken over the past three years was now **unrecoverable.**

Estimating the loss

Up to this point the cost of IT services to deal with the initial cyber event, purchasing a new server, and attempting to recover the data had amounted to nearly $20,000 (USD)*. With data recovery no longer possible, the only remaining option was to **re-create the data from scratch,** which would amount to significantly more.

To determine the cost of re-creating their data, the company considered two approaches. The first was simply to assign a percentage to the overall value of each project that would represent the cost to re-create the data. But given that the data was highly sensitive intellectual property and required technical skills to reproduce, this method proved too basic a measure as it discounted the specific requirements of each project.

> The second approach was to determine how much time, in hours, it would take to re-create each project, and assign a cost to that time.

*All figures mentioned have been converted from GBP to USD at a rate of £1 to $1.32 as of 29/06/2018.

Projects 2016/17	Director hours	Senior engineer hours	Engineer hours	Assistant engineer hours	Total re-creation hours	Total re-creation cost
Project A	20	91	62	31	204	$16,610
Project B	74	686	921	760	2,441	$141,860
Project C	8	21	129	45	203	$11,360
Project D	30	170	315	123	638	$40,775

Projects 2015/16	Director hours	Senior engineer hours	Engineer hours	Assistant engineer hours	Total re-creation hours	Total re-creation cost
Project A	6	8	22	5	41	$3,405
Project B	32	12	380	536	960	$41,420

Projects 2014/15	Director hours	Senior engineer hours	Engineer hours	Assistant engineer hours	Total re-creation hours	Total re-creation cost
Project A	6	16	4	25	51	$3,685
Project B	20	25	85	120	250	$14,375

The second approach was to determine how much time, in hours, it would take to re-create each project, and assign a cost to that time. Because the task of recreation would involve engineers working under the guidance of the company itself, the hours estimated for each project were allocated according to the level of expertise needed (i.e. director, senior engineer, engineer and assistant engineer) with each role incurring a different hourly rate. In this case, a director's work cost **$250 per hour,** a senior engineer's work cost **$85 per hour,** an engineer's work cost **$50 per hour** and an assistant engineer's work cost **$25 per hour.**

Re-creation time

Together, the total amount payable for data re-creation alone came to over **$270,000.** This data was effectively the lifeblood of the insured's business and without having a cyber policy in place, the cost of re-creating it would have been **totally uninsured.**

Top tips

- Always backup your data
- Put a backup testing plan in place, and test regularly
- Keep your backup app up-to-date and test when using a new version or operating system.

Understanding data recovery versus data re-creation

Every company relies on data, whether customer data, financial data, or simply its own intellectual property. And while many companies follow best practice for both data security and data storage, the impact of a cyber incident can often be greater than expected. Many cyber policies only provide cover for the cost to recover or restore data from backups, but not the costs to re-create lost data from scratch. This engineering firm had purchased a comprehensive cyber policy from CFC that provided cover not only for recovering data but also for re-creating it, ensuring that they weren't left with the full financial burden of the ransomware attack.