Extortion, infidelities, and cybersecurity

August 2015

Speed read

Online extortion of businesses is emerging as another bet-the-bank reason to have strong cybersecurity. Hacking a business to get credit card and other details is not especially profitable. It can be more effective to take sensitive data and hold the business to ransom, including because the hacker has a point to make, rather than to make money. "It's more profitable to extort someone than it is to use their stolen credit card information to get money".[1]

Following on the heels of the Sony heist along those lines, (see our article) comes the adult infidelity site, Ashley Madison, where participants can seek illicit hook ups. Its slogan is "Life is short. Have an affair."

Hackers have seized names, addresses, sexual fantasies and credit card information for 50 million people on the service. Credit card details may be worrying those people a lot less than being outed to their spouses and others.

But spare a thought for Ashley Madison even if you don't like their morality. The hackers – calling themselves The Impact Team (or, um, mumble, for short) - said that unless Ashley Madison[2] shuts down, they will dribble out more personal details of the users of the service. And that's what's happening.

Even if Ashley Madison doesn't kill itself by shutting down, can it survive this breach? Would your average adulterer want to take that risk?

Yet another example of why cybersecurity is bet-the-bank for businesses large and small; after all, SMEs can be held to cyber-ransom too.

In a very good article, Ashley Madison and the Rise of Data Kidnapping,[3] Time magazine notes:

> *"[R]ight now, every executive at every firm in the country should be hard at work doing an honest assessment about what their valuable data really is. Then, they need to invest wisely in protecting data that might seem inconsequential if stolen in one context, but a disaster of stolen in another. Because every company will have to plan for ransom and extortion requests now."*

We also touch on some insurance aspects below, and we have some practical tips from Graeme Neilson, Chief Information Security Officer at cyber security specialists, Aura Information Security.

The Detail

This extortion only became public late last month, so the full story is yet to play out. However, there are signs that this is the tip of an iceberg, whereby some companies both large and small, are being data kidnapped, in the words of the Time article, and simply paying out or meeting the demands.

As one insurance commentator referred to by Time notes:[4]

> *"Although some criminals eventually back down and do not follow through with their extortion threats, some threats do get carried out and these incidents can often be expensive. The tools available to criminals are vast and they have the power of the Internet behind them."*

He goes on to point out that many insurance policies won't have cover for cyber extortion – the sort of cover, extended to data, which applies to kidnapping and ransom of executives.

Says Graeme Neilson, Chief Information Security Officer at cyber security specialists, Aura Information Security,

> *"This Ashley Madison attack highlights that most companies have weak information security measures on their internal networks and systems. Once an attacker is in, they are able to steal everything as in the Ashley Madison case where they have got the customer database and the CEO's email. Companies need to plan for a breach (for example from an employee being phished) and implement internal security measures that limit the potential damage from an attacker. Not every employee in the company should have access to all the data."*

We'll be covering this and other insurance aspects of cyber-security in forthcoming articles.

1. http://time.com/money/3973377/ashley-madison-data-kidnapping/

2. And another site owned by the same company.

3. http://time.com/money/3973377/ashley-madison-data-kidnapping/

4. C Aberhart, Cyber Extortion Poses Threat to Small & Large Business (http://time.com/money/3973377/ashley-madison-data-kidnapping/)

Wigley+Company
PO Box 10842
Level6/23 Waring Taylor Street, Wellington
T +64(4) 472 3023 E info@wigleylaw.com
and in Auckland
T +64(9) 307 5957
www.wigleylaw.com