# If your enterprise is held to ransom, what should you do?

October 2016

**Speed read**

With potentially fatal reputational factors at play, what is a company to do when their information is held to ransom?

Despite Police advice that recommends not to give in and pay ransoms, in the real world sometimes the best option is to pay up. Even the FBI says "To be honest, we often advise people just to pay the ransom."


Overall, having a comprehensive cybersecurity plan is essential in being prepared to best deal with these attacks.

This article was originally featured in CIO.

**The Detail**

What does a company do when ransomware locks up its system and the company information, and it can't quickly rescue the situation such as by backup restores? In other words, what if best practice protections fail and the company is caught out?

A Police website says "*Do not pay any money*". An internet safety NGO's advice is *"Do NOT pay the ransom"*.

Really?

Is it realistic for a company, brought to its knees with its systems not working, to not try and sort this out by paying the bitcoin ransom?

This is the real world. Most likely, those doing the ransoming are well outside the reach of your local police force, as they are based overseas and often in jurisdictions that make enforcement tricky.

Even if the local police get Interpol on the job – where does that take us and how long does it take?

In the meantime, the impact on the business is huge and sometimes fatal. There's reputational impact (for example, the world now thinks the company did not have best practice protections).

There are lost revenues as the business slows or stops. And there are legal concerns, with possible legal obligations breached by issues around contracted service supply, protection and retention of customer information, and so on.

We're told that ransomers are known to release the system after the payment is made. Not always though.

After all, they want repeat business. So these typically well organised criminals will have incentives to have a reputation of honouring the ransom requirement.

Yes, paying out encourages future ransoming. But, really, in the balance of things, for a typical company in this kind of situation that will understandably be a small factor in all this.

If your enterprise is held to ransom, what should you do?

The FBI might have it right. As Joseph Bonavolonta said (he's an FBI Assistant Special Agent in the Cyber and Counterintelligence Program):

> *"The ransomware is that good…To be honest, we often advise people just to pay the ransom."*

Protecting against ransomware in the first place, and having good systems to be able to restore if ransomware gets in, is of course best practice.

The law in many countries would put an obligation on companies to have such best practice (for example, to protect the data of the company's customers).

Some contracts impose an even higher standard and require 100 per cent protection, not just what is reasonable.

For example, a supplier might make a promise of continuous service. This is so that there is no getting out of legal responsibility due to a cybersecurity attack, even if best practice protections are in place.

Generally, companies should try to avoid those types of commitments. Also, each situation, enterprise and country is different, with different laws potentially applying to each industry sector (for example, banking, health and so on).

But, mostly, having best practice protections greatly reduces legal risk.

What to do after a ransomware attack has been resolved and the systems and data are restored and operational?

The obvious point is do a review as to how it could happen and to remedy both the level of protection, including from a social engineering perspective, and to have robust restoration arrangements in place.

Being successfully attacked is like having a target on the company's back; it's an invitation for the hacker to have another crack at it.

That is also a great time to do what is essential to do anyway, but what many companies fail to do.

They need to have a contingency plan, up and ready to go for the next cybersecurity attack.

That plan needs to cover much more than the technology issues.

It must include a PR plan for the media to handle fallout among external stakeholders; legal review/approach; and having the board ready to move quickly and with a good grasp of the issues.

This is not the time to be struggling with these issues due to a lack of preparation, as this likely plays out rapidly.

This is part of a special report on the New Zealand edition of the 2017 Global Information Security Survey conducted by PwC, CIO and CSO.

**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