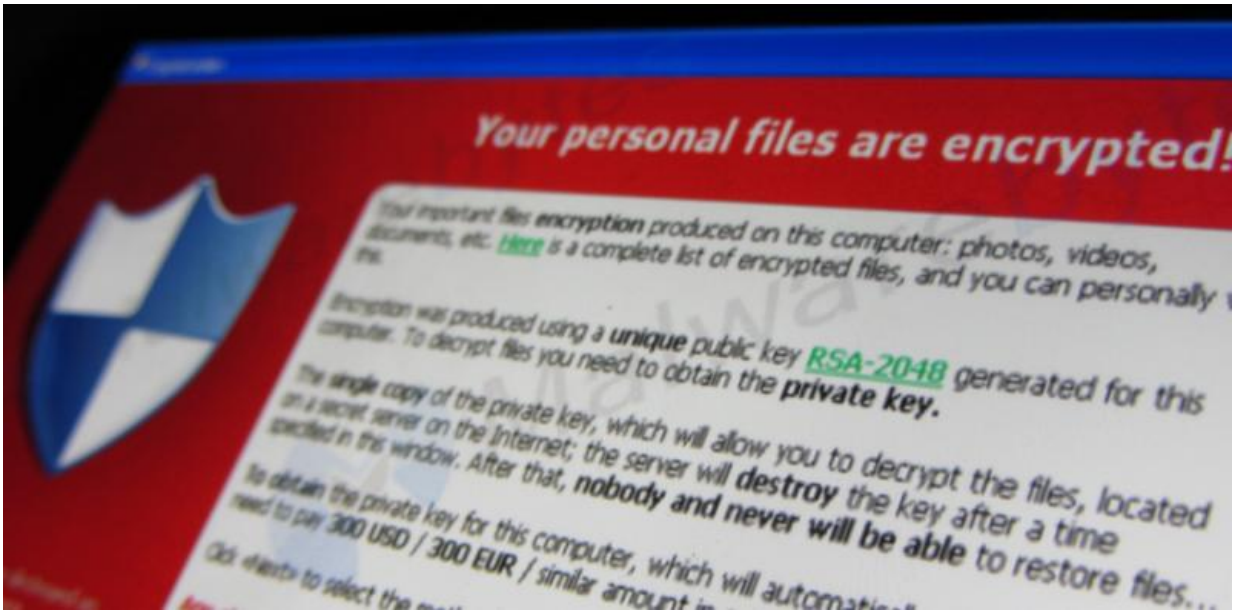
When it comes to ransomware, it's sometimes best to pay up

May 30 2017, by Micheal Axelsen



Businesses struck by ransomware have to make some hard decisions. Credit: Christiaan Colen/Flickr, CC BY-SA

Companies hit by ransomware are faced with an ethical dilemma: pay up to save their now-encrypted data, or hold the moral high ground and lose it all.

This is a question many companies may have to face. The recent WannaCry cyber-attack, which targeted the data of organisations

including UK hospitals, is part of a growing and lucrative "industry".

In most cases, the perpetrators attempt to encrypt a business's data and then refuse to share the decryption key unless a ransom is paid. WannaCry reportedly demanded that companies pay upwards of US$300 in Bitcoin.

Of course, there are ways to protect yourself. Up-to-date software and effective backups are good controls for ransomware, but many people fail to keep up. For examples, an estimated 7% of computers globally still use Windows XP software, despite Microsoft having ended support for the platform. In the case of WannaCry, this was an important vulnerability.

Paying up may be the rational choice for an individual business, but given that cybercriminals go where the money is, the repercussions for others could be significant.

The case for paying up

Pop-culture morality tells us a ransom should not be paid; movies tell us that paying the ransom means the bad guys win.

In the real world, however, businesses faces a serious dilemma. Paying the ransom could save the business and keep staff employed, but the cybercriminal will probably feel encouraged to continue their attacks.

Ultimately, businesses held to ransom have at least four choices:

- Refuse to pay the ransom and risk the possibility that the criminals will carry out their threats
- Call authorities to launch a criminal investigation, although whether the data will be decrypted is uncertain

- Attempt to use decryption tools to access the data. One such method is "brute force" – a trial and error computational method to guess all possible variants of the decryption key – but some mathematicans estimate that's beyond the processing power of most computers.
- Pay the ransom and hope you get your data back.

Several factors may affect the decision, including whether the victim expects that the encrypted data will be returned once payment is made, or how embarrassing it will be to inform clients about the incident.

The value of the data is also important. If the data held hostage is not integral, then the business is obviously less likely to pay.

Thinking about others

The victim's consideration of the consequences of their choice for others is also important.

Economically, rather like the decision of an individual trawler to over-fish the seas or a factory to pollute the air, paying the ransom creates a "negative externality".

That is, paying the ransom may benefit the cybercriminal as well as the business and its survival, but it's a sub-optimal choice from the perspective of the wider community. The business that pays the ransom obtains all the benefits of their choice, but much of the cost is borne by others, who may become the victim of emboldened cybercriminals.

The moral dilemma is difficult: paying the ransom saves the business but hurts others. However, not paying the ransom is to feel morally superior while waiting in the unemployment line.

How to fight ransomware

Avoiding such a dilemma entirely requires businesses to prepare for ransomware attacks.

There are several key actions and responses a company can take to blunt the impact of a cyber-attack. Chani Simms, co-founder of Meta Defence Labs, has suggested, among other things:

- Implementing preventive controls to make attacks less successful, such as regularly "patching" software and training staff in good information security practices.
- Ensuring data is backed up offline and business continuity plans are in place.
- If an attack is still successful, quickly isolating infected computers to limit losses.

Such simple strategies are estimated to mitigate most cyber intrusions as well as ransomware. Yet the risk remains that ransomware creators will find a vulnerability, encrypt important data and leave the business with a sticky choice.

Until someone creates a ransomware-proof software system, some might decide that paying up is the rational choice.

This article was originally published on The Conversation. Read the original article.

Provided by The Conversation