Before paying a ransom, hacked companies should consider their ethics and values

August 18 2022, by Michael Parent

Credit: energepic.com from Pexels

The recent cyberattacks in August on Bombardier Recreational Products

and the Ontario Cannabis Store highlight the continuing scourge of cyber criminals and ransomware.

Ransomware is a piece of malware—malicious software—code that gets into an information system and blocks access to the computer or its files until the victim pays to obtain a key, or password. Ransomware was a term that did not enter the popular lexicon until about 10 years ago (and it was added to the Oxford English Dictionary in 2018).

It has now evolved, and in 2021, there were 3,729 ransomware complaints registered, with losses of US$49.2 million in designated critical infrastructures alone. The average ransomware payment climbed 82 percent to hit a record US$570,000 in the first half of 2021.

And it's only going to get worse. The FBI's Internet Crime Complaint Center reported 2,084 ransomware complaints from January to July 31, 2021—a 62% year-over-year increase.

For any organization, cyberattacks are not a matter of "if," but "when": A cyberattack is inevitable. This forces leaders to ask: Do we pay the ransom or not?

Roughly half of all organizations opt to pay ransom. But that also means that roughly half do not. What makes this an especially wicked problem is that there is no correct answer or clear structure. So the question becomes: Under what conditions should a ransom be paid? And what factors can help leaders make this decision?

Blocking access

There are four core actions that ransomware can execute, embodied in the acronym LEDS: Lock, Encrypt, Delete or Steal. Ransomware can lock, or prevent access to data or an information system, requiring a key

to unlock. Similarly, it can allow access, but the data are gibberish as they have been encrypted in place, again requiring a decryption key to make legible. Data can be deleted in place (erased) or sold to the highest bidder.

What makes today's ransomware attacks especially harmful and insidious is that they often deploy more than one of these effects.

Once malware is embedded in an organization's system, the criminals contact the victim, usually through an anonymous email, or through the malware itself (pop-up window) demanding immediate payment of a ransom in cryptocurrency, and typically threatening further harm.

Paying the ransom may lead to a decryption key being provided, which, when entered on the pop-up window immediately unlocks the system and anything that has been encrypted.

Considerations before payment

There are two dimensions to be considered when deciding to pay a ransom: the business decision and the ethical one.

Law enforcement authorities, including the FBI and the RCMP, adamantly advise against paying ransom, ever. They do so for two good reasons: first, it rewards and encourages criminal activity. Second, it may further endanger the organization when it becomes known in hacker circles that this is an organization willing to pay.

In other words, it may not make the crime go away and may make you even more of a target.

If the criminals are not a known terrorist organization, then payment of a ransom is not a crime. This might change, as some countries, notably the

United States, are proposing enactment of Sanctions Compliance Laws criminalizing all cyber-ransom payments. It might be difficult to attribute the attack, which is why the hackers often identify themselves to their victims.

An honest crime

There is a compelling business case to be made for paying a ransom demand. The crime works because, if you will, it is an honest one. That is, 70 percent of the time, paying a ransom will result in a valid decryption key being provided.

This makes sense. For criminals to profit from this endeavor, they must show good faith and deliver on their promise.

Criminals also know this. Targeted campaigns see attackers spending on average nearly six months inside a company's network before enacting ransom malware. They do so to ensure that their malware has infected as many systems as possible, including backups; to identify and extract the items of greatest value; to ensure they do not leave traces; and to garner any business intelligence (such as incident response plans or insurance policies). This allows them to determine the maximum amount of ransom to demand.

This is the essence of the business case decision. Suppose, for example, that the cost of a ransom event is estimated to be $500,000 (based on the size of the database, time to recover, data validation upon recovery and other expenses). A ransom demand of $250,000 is clearly a better alternative because it is not only cheaper, but faster than the alternative.

Organizations can calculate the cost of various incidents and determine, in principle, their willingness to pay for each possible ransom scenario. This leads to the development of what is referred to as a ransomware

payment matrix for the organization.

Moral dimensions

However, there is also a moral, or ethical dimension to this decision. Payments to criminals might not be consistent with the organization's core values, culture or code of ethics. Even if they are, this might not sit well with the company's employees, clients and other stakeholders.

There are many frameworks and theories dealing with ethics in the workplace, and leaders need to avail themselves of one or more. This will help them make a decision regarding paying a ransom because, while it may make great business sense to pay a ransom, it may not be the right thing to do for the organization.

Instead, the organization may choose to invest funds that would otherwise go to ransom payments into training, cyber-protection and upgrading and patching systems.

Whatever the decision, it is critical to explore all options well before any cyberattacks occur. This includes holding discussions with employees, customers and other stakeholders. It also includes insurers (who are increasingly loath to insure against ransomware events) and law enforcement authorities.

Accepting the inevitability of a cyberattack and thoroughly exploring different scenarios will have the dual effect of not only preparing for the attack, but allowing for a more effective response when it occurs.

Provided by The Conversation