HOLDING DATA TO RANSOM

With organisations across the world still reeling from the impact of the WannaCry ransomware attack, Michael Rohrs highlights the factors that influence the severity of a cyber extortion incident

Our firm was founded in 1975 as a kidnap for ransom response company, helping organisations around the world protect against and respond to extortion of all kinds. That experience has taught us that even as the techniques for extortion change, many of the fundamentals for handling them endure.

In recent years, cyber-enabled extortion has become a highly prolific and public technique. It is vital for all organisations to have a well-structured and properly resourced plan for technical incident response to such an event. That plan should include the capability to detect, evaluate, escalate, contain, remediate and recover from attacks against the information assets most valuable to your business.

However, technical incident response must also be executed inside of a broader approach to responding to a cyber extortion incident – an approach that must be driven by managing the entire business' risk, not just resolving the immediate technical problem.

The severity of a cyber extortion incident is determined by three things: capability plus intent; cost versus benefit; and crisis management. Each of these is ultimately about assessing risk to the business and weighing up the resulting implications to the entire enterprise – which should govern and encompass the organisation's technical response.

Capability plus intent

One of the first essential questions to answer when you are alerted to a cyber extortion incident is, "Is the attacker capable of what they claim?" To answer this question, it is important to verify the claims with evidence, if possible. Many scams, hoaxes, and scareware campaigns seek to make their victims anxious and take advantage of our natural human tendency to act rashly when we are uncomfortable. Keeping this in mind goes a long way to ensuring you can focus on making a measured assessment of the situation.

Depending on the case, reviewing system logs to verify the attacker's access or analysing sample data to see whether it is authentic are useful methods for triaging the attacker's capability to follow through on their threat. Consulting threat intelligence from government organisations and the private sector cyber security community on known attack groups and campaigns is another valuable way to quickly gauge how capable and how credible an attack could be.

Without these indicators, it is important to use any information you have available to do a sense-making test – given what you know, does it make sense that the extortion threat is legitimate? Further, based on their demands, what do they really want and why was my organisation the target?

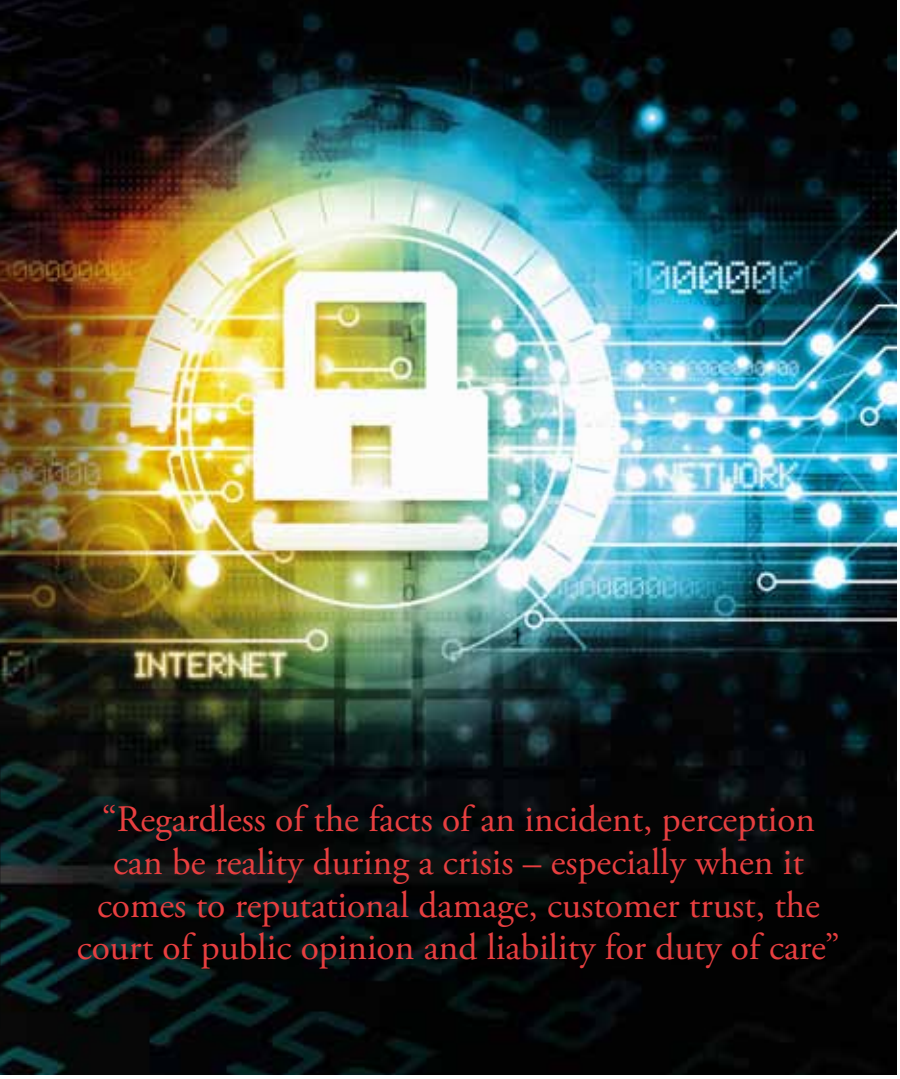
The majority of cyber extortionists are motivated by one or more of four things: money, ego, revenge and politics.

Making money is by far the most prevalent intent in cyber extortion cases. Cyber-crime is an economy. Mirroring legal economies, markets exist to purchase malware, hacking tools, and stolen data; to rent anonymous infrastructure; and to hire criminal services. There is market competition between crime groups and some campaigns offer discounts or instalment payment plans.

For those simply out to make money, the same principles of business economics apply when trying to make it in the market – they are motivated to concentrate their efforts on what makes the most money for the least work. In cases like this, it is fairly straightforward to assess the implications for each of your courses of action in response.

Although less frequent, in cases where the attacker is driven by ego, revenge or politics, the situation can be more complicated. These attackers tend to be more persistent and more malicious. As such, the victim often has less power to influence a timely resolution and to manage the impact – for which we recommend seeking the support of outside resources, including for crisis management and legal counsel.

> "These attackers tend to be more persistent and more malicious. As such, the victim often has less power to influence a timely resolution and to manage the impact"



"Regardless of the facts of an incident, perception can be reality during a crisis – especially when it comes to reputational damage, customer trust, the court of public opinion and liability for duty of care"

Cost versus benefit

Being extorted can be emotional. Regardless of the circumstances, it can feel invasive, infuriating and embarrassing – particularly if you've been targeted more than once. But not all extortion attempts have the same level of severity or implications. In each instance, what you are as a business, what your risk tolerance is, and the details of the circumstances matter significantly. For every case, it is important to list your response options and take a critical look at the cost versus benefit of each.

For example, in widespread commodity extortion campaigns, the demand is often the same regardless of the target – but that same payment may be insignificant for a multi-national corporation and a small fortune for a family-owned business.

For another example, consider the worldwide WannaCry campaign in May 2017. Although the relatively low bitcoin ransom demand – the equivalent of approximately US$300 – would be an inconvenient price to pay for most, the impact on the UK's National Health Services (NHS) was significant and in some cases life-threatening. The possible corruption of hospital computers, MRI scanners, blood-storage refrigerators and other essential medical equipment forced some NHS services to turn away non-critical emergencies. Several large hospital chains in the US have found themselves in the same straits in the past year.

Even in dire cases like this, however, only after you have determined that complying with the extortion demand will likely alleviate your problem, that you cannot afford the potential impact otherwise, that you can accept the reputation damage, and that you can treat the risk of becoming a repeat target, should you consider complying with the extortion demand. In that case, we recommend taking expert advice to begin a structured negotiation with the attacker.

On the other hand, depending on the circumstances well-prepared companies are frequently in a position to restore encrypted systems from backup, limit the damage from potential data release, stand on principle not to pay ransom, or otherwise ignore the extortion threat and absorb a minor setback.

Take for example Netflix in December 2016. Netflix is certainly a potentially lucrative target. An attacker reportedly gained access to pre-release copies of a popular series when they compromised a post-production company Netflix works with. They attempted to extort money from Netflix, threatening to release the content where people could pirate it for free unless Netflix paid by their deadline. Except they misjudged Netflix's cost/benefit calculus and tolerance for risk. Netflix called their bluff and refused to pay. The attacker leaked their content, but walked away empty handed after expending resources for the operation, exposing their name and infrastructure to the security community, and proving to their criminal competitors and other potential victims that they may not be worthy of being taken seriously.

Crisis management

Regardless of the facts of an incident, perception can be reality during a crisis – especially when it comes to reputational damage, customer trust, the court of public opinion and liability for duty of care. Sometimes how you manage the other aspects of the incident – business continuity, internal communications, legal obligation, customer management and media interaction to name but a few – matters more than your technical response. A company's ability to respond at the business level when things go wrong can be the difference between an isolated incident and an enduring crisis.

As part of your preparation to handle an extortive event, we highly recommend that you establish a structured crisis management programme. This programme should include senior representatives from across the business, with clear lines of communication, executive decision-making authority, and a common understanding of the business' priorities and standing policies during an extortion event. It also requires regular practice. Incident response and crisis management exercises are the best way to ensure your team and its plans can in fact withstand the pressure and complications of an extortion incident.

Preparing for the expected

Extortion is a well-established and evolving technique for amassing illicit income and exercising influence. Unfortunately, cyber extortion is now a common occurrence across sectors around the world. It will likely continue to happen as long as it works. The best way to secure your enterprise and reduce your risk is to prepare the entire business ahead of time to manage the incident, and to remember these sober principles when the situation seems emotional and chaotic.

We offer the advice in this article from experience to chief information, risk and security officers who must prepare for the possibility that they will one day have to handle a case of cyber extortion, to help guide their focus and govern their decision making.

MICHAEL ROHRS

Michael Rohrs is a Washington-based senior consultant in the cyber security practice of Control Risks, the global business risk consultancy

www.controlrisks.com