Information Security Now – 42

Your Money or Your Data?
The Ransomware Payment Dilemma

John Mitchell

Once your files are encrypted and the ransomware demand has been received, there are three choices: re-install your complete system from scratch, restore from a recent backup, or pay-up. However, as a member of the Chartered Institute of IT you are bound to a code of conduct and ethics which means that there are a number of associated areas which also need to be considered.

Reputation (Theirs Not Yours)
Ransomware criminals tend to keep their word and unlock the data after payment because they want future victims to believe they will get their files back. If that faith is diminished, then their game is over since victims will be less likely to pay if they hear reports of data not being restored. *Gartner* reports that ransomware is expected to collect £1.4 billion this year from people, or companies, who pay-up, so it is in the blackmailers' interest to keep this cash river flowing. The other thing to remember is that it is in the criminals' interest to leave you with sufficient functionality to conduct email and internet transactions so that you can pay-up if you so decide. They therefore, tend to leave you with your software functionality.

Legal & Ethical Aspects
Blackmail is an act involving threats to make a gain or cause loss to another unless a demand is met. Essentially, it is coercion. It is a statutory offence in many countries, but does paying-up make you a criminal too? Not in most countries and certainly not the UK. Experts in the USA advise that you should never agree to ransomware's demands to pay. Instead, the United States Computer Emergency Readiness Team (US-CERT) advises to report the incident to the FBI's Internet Crime Complaint Centre. While this may cause more pain in the short term, it is supposedly better than supporting malicious attempts to hold your data hostage. However, although the authorities may not like you paying, they cannot stop you so it is sensible to have a policy on what you intend to do if you are hit.

The Need For A Policy
The differential between the demand price and the cost of sorting out the mess that you are now in is a standard business investment dilemma. Which is the cheaper? If you run a business, then you must maximise the return to your investors within the law. As paying is not breaking the law, then if that is cheaper than alternative scenarios it can be argued that you are obliged to do so, unless you already have a policy of non-payment. Indeed, you could even ease your own conscience by rationalising that you are simply paying for a business service which is saving you the greater cost of restoring your system. Having a policy and associated action plan resolves this dilemma, so it is advisable to get your plans in place in advance of the risk being crystalized.

This not only leads to clearer thinking; it also avoids mistakes being made in the panic of the aftermath from an actual attack. Having already made the decision as to whether to pay, or not, as the case may be, brings a degree of calm to the proceedings. You may well develop a policy with some inbuilt granularity: if their demand is below this value we will pay, if above we will not. Where the cut-off figure is will be based on a standard cost-benefit analysis.

Potential ransom demands should be on your risk register, as they impact on your ability to deliver a service. Your risk register should be kept confidential as you do not want potential attackers to know what your planned response will be.

Operational Considerations

Re-installing your system from scratch implies the write-off your app and data investment, but ethically you are on the high ground. You have not given-in to blackmail, even though the cost to you in starting from scratch may be higher than the ransom demand. However, this choice is really only an option for low-level data users who have not backed-up their data because they only use their devices for occasional email, or internet browsing and whose data is of no great value to them. However, most businesses will not have this luxury. The investment in data over many years is huge and although not shown as a tangible asset on the balance sheet may well exceed the capitalisation value of the business. The Apple's of this world do not purchase bricks and mortar when they buy a company, they purchase the data.

Without fail, experts recommend the best way to recover files after you've been infected by ransomware is to restore from prior backups. That is after you've removed the virus, cleaned your system and made sure your backups aren't also encrypted. Your backup and recovery plan will be a subset of a larger disaster recovery plan. A viable backup plan ensures you have the right backup data sets available, in the right place, at the right time so that you can minimize potential losses to productivity, profits or reputation. As the criminals have effectively corrupted your data the recovery is no different from having suffered (say) a disk failure.

Restoring from a pre-ransom back-up implies that you regularly back-up your files and have a recent one available which the criminals have not been able to get at. Even so, you will lose any data which has been changed between the last back-up and your files being encrypted. You also need to be quite certain that you have removed the ransomware software from your system.

Malware Evasion

You may well be curious as to how the ransomware evaded your malware detection mechanism in the first place? Well, the malware defenders are always running behind the perpetrators, as you can't defend against something you don't know about; the so called zero-day attack. However, it is also likely that the ransomware has been processed through a "crypting" service. Put simply, a crypting service takes a piece of malware and scans it against the available antivirus tools to see how many of them detect the code as malicious. The service then runs its own encryption routines to obscure the malware so that it no longer resembles the piece of code that was detected by the antivirus tools. It iteratively repeats this process until the malware is completely undetectable by the tools on the market.

What this means is that it is just a matter of time before you are hit. All the more reason to iron out your policy and procedures in the cold light of day, rather than during the nightmare of a ransomware attack.

John is Managing Director of LHS Business Control, a corporate governance consultancy. He is a member of BCS Council, it's Audit & Risk Committee and Chair of the Information Risk Management and Assurance (IRMA) specialist group. He can be contacted at: john@lhscontrol.com, www.lhscontrol.com, or on +44 (0)7774 145638