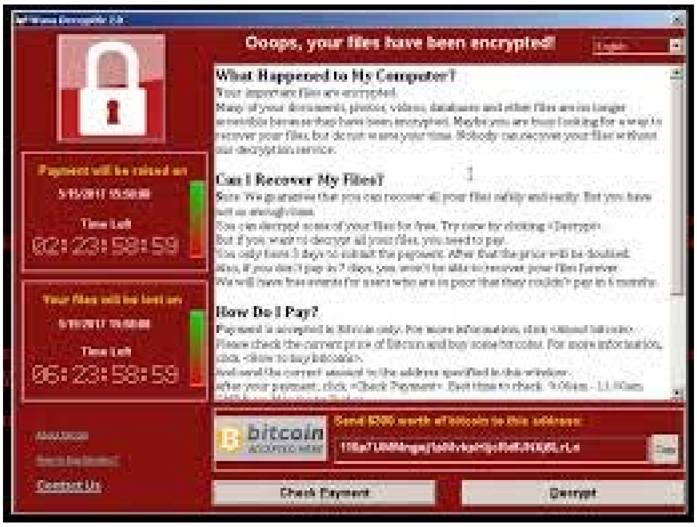
Uniac Update - May 2017

Major Cyber Security Attack

On 12th May 2017 computers in 150 countries were affected by the ‘WannaCry’ major malware attack. The attack is thought to have affected over 200,000 computers globally in both the public and private sectors. In the UK, this included around 61 NHS organisations which led to systems going down, patient appointments being cancelled and sensitive data being potentially put at risk. Other victims included Germany's rail network Deutsche Bahn, Spanish telecommunications operator Telefonica, US logistics company FedEx and Chinese energy giant PetroChina.

The ‘WannaCry’ Attack

The WannaCry Ransomware attack targeted Microsoft Windows computers encrypting data files and sending a message to users demanding a ransom payment (see below).



Ooops, your files have been encrypted!

What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Payment will be raised on
5/15/2017 [illegible]
Time Left
02:23:58:59

Your files will be lost on
5/19/2017 [illegible]
Time Left
06:23:58:59

Send $300 worth of bitcoin to this address:
[illegible]

It seems to have originated via ‘phishing’ emails which contain infected code in an attachment or link. Phishing attacks are increasing greatly because they exploit a lack of user knowledge and require only one user to respond to potentially infect a whole network. Once a user clicks on the attachment or link, the malware is launched and infects any vulnerabilities in the system - for example applications or operating systems which have not been security patched to protect against the latest attacks. Older operating systems are particularly vulnerable because they may no longer be supported by vendors.

A 2016 survey by Cybersecurity firm SentinelOne found that 23 HEIs (of 58 responding to a survey) had been subject to a ransomware attack in the previous year. One University (Bournemouth) had been hit 21 times in 12 months (source: BBC News http://www.bbc.co.uk/news/technology-37166545).

ISOQAR REGISTERED
UKAS MANAGEMENT SYSTEMS 0026
Certificate Number 13024
ISO 9001, OHSAS 18001, ISO 14001

finalist
Cyber Security Awards

What do Universities need to do?

There have been instances of older legacy systems being in use within universities and there will continue to be an emphasis on ensuring that investments are brought up to date. However, from our experience, secure practices are not just a question of investing in technology. It needs to be accompanied by robust system management and administration which ensures that updates are applied promptly and systematically.

The National Cyber Security Centre (NCSC - an arm of the government's GCHQ) outlines three essential steps which organisations need to take

- Keep your organisation's security software patches up to date
- Use proper antivirus software services
- Most importantly for ransomware, back up the data that matters to you, because you can't be held to ransom for data you hold somewhere else.

To the above, we would add that ongoing user education and training are absolutely essential to guard against these types of attacks succeeding. The upside of these high profile stories is that it emphasises this is a real threat, happening now. Many Universities are introducing specific phishing training courses and 'fake phishing' campaigns which ascertain how many users will open or click a suspect email. In many cases the offending users will be sent for 're-training' and we envisage this approach growing - inevitably accompanied by disciplinary action - given the scale of the problem and the implications.

In addition, institutions need to ensure that adequate insurance and legal cover is in place to mitigate the threats of any losses.

Get in Touch

Uniac undertake cyber security audits at Universities across the UK which include assessing the levels of vulnerability to phishing and ransomware attacks. If you would like to discuss how Uniac could help provide assurance over cyber security risks and controls, please contact:

Ian Musgrave - Head of IT Risk and Assurance

☎ 0161 247 4697

imusgrave@uniac.co.uk

ISOQAR REGISTERED UKAS MANAGEMENT SYSTEMS 0026

Certificate Number 13024
ISO 9001, OHSAS 18001, ISO 14001

finalist Cyber Security Awards