Board of Management

Date of Meeting	**Wednesday 21 June 2017**
Paper No.	**BoM6-Y**
Agenda Item	**14.4.5**
Subject of Paper	**Global Cyber Attack**
FOISA Status	**Disclosable**
Primary Contact	**F Samara, VP Infrastructure**
Date of production	**13 June 2017**
Action	**For Noting**

1. Recommendations

The Board is asked to note the report following the Global WannaCry Ransomware Cyber Attack.

The WannaCry Ransomware Attack

Update Produced - 13 June 2017

Background

This malware targets computers running Microsoft Windows operating system[1] and was first detected on Friday 12 May 2017. On infected computers the virus encrypts local and network data files disables the machine and displays a message demanding payment of a Bitcoin ransom varying between $300 and $600 ostensibly to provide the decryption key for releasing the locked files. (It is understood that the release mechanism does not in fact work and that no files have been decrypted after paying the ransom.)

Ransom message by unknown criminal.
Image in Public Domain, https://en.wikipedia.org/w/index.php?curid=54032765

By the afternoon of Friday 12 May the BBC web site (amongst others) was reporting multiple attacks on NHS computers throughout the UK and on various large organisations worldwide. The virus spread easily amongst networked computers and throughout the Internet due to the propagation method which exploits a flaw in the way Windows technically *shares files*. It is not even necessary users to take any action (such as clicking an email link) to trigger the infection since the 'worm'[2] spreads automatically. Within one day the ransomware quickly spread worldwide infecting more than 230,000 computers in over 150 countries.

The *file sharing* flaw was only revealed when tools developed by the United States' NSA for their own work came to light after being stolen by a group called *The Shadow Brokers*. Microsoft released a patch (MS17-010) for the flaw in March 2017 (prior to the WannaCry outbreak) however this only provided protection if applied to supported versions of the operating system. No security patch was released for unsupported versions of Windows like XP and Server 2003. The continued prevalence of many legacy XP/2003 systems[3] coupled with a high probability that the released patch had not yet been applied to supported systems probably accounts for the high number of affected NHS systems.[4] Microsoft subsequently (on 13 May) released a security patch for the unsupported XP and Server 2003 systems.

---

[1] The majority of College desktop computers run the Microsoft Windows operating system. Although in some instances the virtual desktop architecture used provides protection from certain malware, this is not the case with WannaCry since data files are the main target. The other major operating system used, Apple macOS, is not at risk from WannaCry.

[2] A computer worm is a malware variant that replicates itself in order to spread via a network to other computers. The payload carried by the worm is generally harmful and may corrupt files or disrupt the network.

[3] There are a very small number of legacy versions of Windows in use within the College. They are all necessarily retained for specialised purposes.

[4] It is worth pointing out that no College systems have been affected by the WannaCry malware.

Apart from the application of MS17-010 one important factor in slowing the spread of the virus was the discovery of a 'kill switch' by a security researcher while analysing the code. The switch prevents the virus encrypting files and propagating itself if a particular Internet domain address exists; by registering the address the researcher was able to immediately slow down the malware's spread and provide time for unpatched (and unaffected) systems to be patched.

The only effective way of restoring encrypted files on an infected computer is by reverting to a previous backup taken before the ransomware attack however this only works if an up to date backup exists. Prevention is always better than cure and this ransomware incident has been viewed by many as a wake-up call which demonstrates the importance of allocating sufficient resources to the establishment of proportionate security measures designed to prevent malicious damage to ICT infrastructure.[5]

Initial College Reaction

During the course of Friday 12 May and into that evening College IT staff became aware of the extent of the malware issue and started investigating the risk to College computers. Various web sources provided useful technical details although at this stage there was much uncertainty and speculation regarding the nature of the threat and its means of propagation.

The timing of the attack, just before the weekend, provided a fortuitous break in College business when the vast majority of computers would be switched off and therefore (temporarily at least) protected from the spreading virus. Physical access to the building would also be limited.

On Saturday 13 May morning numerous phone calls, texts and emails between groups of IT staff took place to further assess the risk in the light of an increasing body of technical information. By this time Sophos (the College's anti-virus provider) had released WannaCry detection patches for the relevant platforms and these were automatically installed in any (uninfected) client computers that happened to be switched on. A considerable advantage of the VDI (thin client) architecture in this situation is the ease with which software patches can be and were centrally and remotely deployed.

We quickly estimated that approximately 9% of the total College computer compliment could potentially be vulnerable since they hadn't yet received the Microsoft MS17-010 patch (or its XP equivalent). A large number of these would be Windows laptops that weren't included in the imaging[6] work (fortunately) undertaken over the Easter 2017 period. Of these laptops, a considerable number would not be contactable over the wired or wireless networks as they would be powered off or located off-site.

Various other measures were taken on Saturday and Sunday to harden the College's ICT infrastructure against the virus, such as observing the (positive) reaction when MS17-010 was selectively applied to powered up computers, restricting access to networked drives, modifying the behaviour of thin client USB drives, preventing the creation of certain file types and limiting remote access from home.

[5] A comprehensive technical description of the story behind the WannaCry ransomware attack appears at https://en.wikipedia.org/wiki/WannaCry_ransomware_attack

[6] Imaging is the process of updating a number of (physical as opposed to virtual) computers with a disk image of software consisting of the operating system (containing the latest security patches) and all relevant application software. Each computer is imaged over the network from a master image held centrally.

The discovery of the ransomware 'kill switch' and the availability of Microsoft and Sophos patches provided further reassurance and enabled IT staff to agree to keep in touch over the remainder of the weekend while monitoring the changing situation. A 'Cobra' meeting was also scheduled for 7:00am on Monday 15 prior to the arrival of staff and students.

Follow-up Actions

The Monday 15 May morning meeting discussed:

- the general background and overnight developments,
- the confidence level in the automatic patching mechanism,
- how best to communicate with staff and students,
- a plan for tracking down and patching all Windows laptops and any remaining unpatched Windows desktop computers.

Manual patching of identified servers started and continued throughout the week. If a server had become infected it would at least have been possible to rebuild it from College data backups.

Throughout the period of maximum WannaCry activity the College had no reported incidents of infection and because of the confidence in the measures undertaken over the preceding 48 hours it was possible to remove restrictions such as network drive access by 9am. To date, there still have been no reported cases of infected College computers.

Lessons Learned

As a result of this incident the following procedures have either been initiated or strengthened:

- Continue to monitor traditional information sources but also pick up reports from new sources such as trusted sources on social media.
- Increase the total number of IT staff with responsibility for monitoring anti-virus software effectiveness.
- Continue with plans to evaluate alternative anti-virus products.
- Review approach to taking backups of PC desktop local drives.
- Review the role of desktop technicians when using the SCCM deployment tool.
- Increase the monitoring of the firewall's Intrusion Prevention System (IPS).
- Incorporate lessons learned into the draft ICT Business Continuity Plan. One possibility is to designate a member of IT staff to be available out of hours to co-ordinate efforts in the case of a major ICT incident.
- Re-instate staff education sessions similar to those undertaken for New Campus but with an additional security focus.
- Review the student handbook induction material to promote best practice when accessing computers. This may result in an update to the College ICT Acceptable Use Policy.
- Engage with College partners such as FES, Transas, etc with a view to establishing more effective protocols for maintaining and protecting software (BMS, Simulator, etc) under their control.
- Review desktop and server security patch deployment mechanism.