Charity Times: Staying safe from the new cyber menace, Written by Antony Savvas, June/July 2017, Downloaed Thurs 11 April http://www.charitytimes.com/ct/junjul17-staying-safe-from-the-new-cyber-menace.php

Ransomware sees cyber criminals unleash malware onto users' computer systems that can lock anything from a single PC to hundreds or thousands of machines. Ransomware is often propagated by email and can be activated and spread across a network when a single user opens an attachment containing the rogue code. Once an operating system on a computer is infected the data on that machine is encrypted, and the user will be asked to pay a "ransom" in return for a code that can unlock and decrypt the data on the machine within a limited period of time.

If the organisation does not pay the ransom and does not have security systems in place that can counter the malicious software, they will lose their data, which can of course play havoc with their business operations. The charitable sector unfortunately is not immune to the threat of ransomware.

Widening threat: The increasing threat from ransomware has been charted by security software companies, putting the number of new ransomware malware families at around 200 in 2016. Last September, Comic Relief's internal systems were down for days after suffering a ransomware attack, after one of its server's was targeted by criminals. As a result, staff at Comic Relief were unable to access the internet or get their email, forcing a number to work at home instead. And before the Comic Relief attack, in March 2016, the headquarters of Catholic Charities of Santa Clara County in the US were targeted. A receptionist there opened an email attachment which was dressed up as an invoice. Instead, the file she opened connected her computer with a server in Ukraine.

It then downloaded ransomware code which began to rapidly encrypt files on her computer.
Duncan Hughes, systems engineering director for the EMEA region at A10 Networks, says of the threat: "Organisations in the charity sector should share simple safeguarding techniques amongst employees and volunteers and make sure that they are educated around the type of attacks to expect, but ultimately protection systems need to be put in place to keep hackers out.

> "IT decision makers need to think more strategically. The bad guys are looking for return on investment just like the good guys, and they don't want to work too hard to get it. Instead of focusing on doing everything right 100 per cent of the time, IT leaders can be more effective by doing a few things very strategically with the best technology available."
>
> Jonathan Orchard, a partner at Sayer Vincent which specialises in helping charities with risk management, says: "Charities are as vulnerable as businesses and are increasingly targets for cyber criminals because they hold a lot of data about stakeholders and donors. Organisations need to check their systems and ensure they have the most up-to-date firewalls and other security systems installed.
>
> "As the Charity Commission suggests, they should always install software updates as soon as they become available, as they will often include fixes for critical security vulnerabilities. They need to make regular data backups of important files, using an external hard drive, memory stick or online storage provider."

Orchard says any risk policy should include advice to employees and volunteers about not clicking on emails or links they are unsure about.

Prevention: In the case of the Catholic Charities of Santa Clara County attack, CCSCC director of IT, Will Bailey, had beforehand been looking to bolster the charity's cyber defence capabilities. He had already started a trial of Darktrace's Enterprise Immune System – a "self-learning" technology inspired by the human immune system and powered by machine learning and mathematics developed by specialists from the University of Cambridge.

One of a number of similar self-learning systems on the security market, Darktrace works by learning a network's "pattern of life" by modelling the behaviours of each user, device and the network as a whole. Based on this adaptive understanding, Darktrace is capable of real-time threat detection, automatically detecting any behaviour or activity that deviates from the norm.At the time of the attack, Darktrace's technology had been monitoring CCSCC's network for a few weeks and already had a well-established understanding of the company's normal behaviour and everyday activity.

Fortunately, once the attack on the receptionist's machine was detected, a member of the charity's IT security team was able to respond straight away, disconnect the targeted device from the network and prevent any further encryption or financial cost. The charity went on to permanently deploy Darktrace's Enterprise Immune System. Will Bailey says: "If Darktrace hadn't detected the ransomware attack who knows what could have happened. It delivers a core cyber defence that is specific to our network. As we use the Enterprise Immune System and drill down into the anomalies it presents to us, we can tighten parameters, modify the criteria for anomalous activity, verify behaviours which are actually legitimate and implement best practices."

Backing up: With the Comic Relief attack, the backing up of data was key to preventing any serious data loss.

The files held on the targeted server were only copies of information which was also held elsewhere. This gave the charity time to work with an external security company to investigate and alleviate the effects of the ransomware and get systems back to normal with the use of the backed up data.

First Capital Cashflow helps charities process donations in a safe and secure way using its cyber-security software. Jo Gibson, operations director at First Capital Cashflow, says: "A lot of UK charities currently use telephone or paper-based donation systems and keep data on local computers that are very vulnerable to hacks. Charities need to ensure that sensitive information is properly secured by using cloud-based technology systems that provide comprehensive security benefits that are far superior to paper-based or in-house software solutions.

> "One of the biggest safety advantages for charities is that sensitive information can be stored in an outsourced, off-site data centre with experts on hand to tackle any unwanted incidents. In the event of a cyber security breach, data needs to be accessed instantaneously to alleviate the problem as quickly as possible and the cloud supports this."

With the increasing use of the cloud in mind, security vendor Acronis recently launched the latest version of its data backup product bundled with automated anti-ransomware protection. Acronis competes with the likes of Veeam, Veritas, Commvault and Dell EMC in the data backup space, but by bundling automated anti-ransomware protection for data stored both on-premise and in the cloud, it feels it has an edge in today's growing ransomware climate. So there are clear security technologies and policies out there to protect charities against the emerging threats, including the growing threat of ransomware. Here's a check-list:

Perform regular backups: Regular full image backups are the ultimate way to mitigate ransomware attacks. Critical files should be protected by regular backups within minimal intervals – preferably to a secure cloud storage space that is itself protected against ransomware. Choose backup software that has in-built real-time protection against ransomware. Such a solution will use behavioural heuristics analysis to detect and stop ransomware even when your anti-malware programme is not able to do it.

Use anti-malware protection: Anti-malware software, or what is commonly known as "anti-virus" software can help form a defence against ransomware, but choose your software carefully. Remember, many free anti-virus programmes don't offer any protection against ransomware.

Keep up to date with software updates: Do not ignore software update messages – they are there for a reason. Software updates are designed to introduce new features or patch up security holes abused by cyber criminals. The sooner you patch up, the less likely your system will be exploited by ransomware.

Make all your file extensions visible: Your operating system may hide file extensions by default in order to try and keep things simple. It is highly recommended to make them visible. You do not expect people to send you a JavaScript file unless you're a software developer, for instance. Enable file extensions to spot the file types you don't usually receive in your mailbox, contributing to the efforts of spotting potential ransomware.

Be careful with email attachments: If you receive something from a person you don't know, or something you don't expect – don't open it! Run it through your anti-virus programme. You may need to do the same thing even for emails received from people you know. Don't open suspicious email attachments and don't click the links, especially the ones asking you to download software "to read this attachment". Be careful and where appropriate don't be afraid to ask the email sender for confirmation of what has been sent.

Don't give your computers more rights than they need: If a computer has administrator privileges, it could spell disaster to all computers and devices on that network. As an extra layer of security do not switch on UAC (user account control) in Windows either.

Don't enable macros in document attachments received via email: When you receive a Word document or an Excel spreadsheet by email and it asks you to "enable macros" — don't do it! A lot of harmful malware is spread this way, including ransomware. If the file is infected and you turn the macros on, you give the hackers permission to install ransomware and start encrypting your data.

Use new security features in your business applications: Essential business software applications, such as Microsoft Office 2016, now include an option to "Block macros from running in Office files from the internet". This is handy. Make sure it is enabled on your computer.

Disable remote desktop connection: Ransomware often accesses target machines using Remote Desktop Protocol (RDP), a Windows utility that allows others to access your desktop remotely. If you do not need to access your computer remotely, you can safely disable RDP to protect your machine.

END