Ransomware in 2022: what you need to know and do about it

Ransomware should be a major concern for charities, but there are steps you can take to help protect your organisation, says Simon Bulleyment

"MANY CHARITIES WILL BE ALARMED AT THE THOUGHT OF SENSITIVE DATA RELATING TO STAKEHOLDERS BEING LEAKED ON THE INTERNET"

Simon Bulleyment
is director of Sibrossa

ASK ANYBODY in charge of IT security at most organisations the question "what is your biggest concern?" and either at the top of their list, or very close to it, will be ransomware. It has been around for many years and gained prominence in 2017 with the WannaCry outbreak – a global attack that exploited a vulnerability in the Microsoft Windows operating system. It resulted in significant impact to countless organisations and according to NHS England, affected 80 of its 236 trusts (due either to ransomware infection or proactively switching off devices).

Charities are just as at risk from ransomware as other organisations, with attacks in recent years on the Salvation Army, St John Ambulance, and the Scottish Association for Mental Health (SAMH). Many charities hold thousands of sensitive records relating to members, donors, volunteers etc, so there is much to lose if attackers gain access to these or render them unusable.

If you have ever been a victim of a ransomware attack, you will be only too aware of the following timeline summary:

- A piece of malware gets a foothold within the IT network.
- The attack is launched, it travels around the network and begins to encrypt data, rendering files, servers, and applications inoperable.
- A ransom note gets dropped somewhere onto the network.
- Either data/systems are recovered from backup or the ransom is paid.

So how does ransomware usually get into a network? By far the most common approach is for attackers to use social engineering techniques and dupe staff into opening infected email attachments or links. I suspect there are very few charities not regularly receiving suspicious emails. However, attackers will also try other means, such as guessing/cracking passwords and logging in via remote access systems or exploiting vulnerabilities in externally facing servers.

> "Ransomware as a Service is a relatively new concept"

Once a ransomware attack has launched and files have become encrypted, ransom payments tend to be in cryptocurrencies, such as Bitcoin, as they are much harder for authorities to trace back to individuals.

HOW RANSOMWARE IS EVOLVING

While there is yet to be a follow-up on the same scale as WannaCry, ransomware and the attackers behind it are constantly evolving. When ransomware first became an issue, it generally required expert knowledge and sophisticated techniques to launch an attack. Shortly after the WannaCry outbreak, the UK's cyber security advisory body, National Cyber Security Centre (NCSC), attributed it as the work of "state actors".

Ransomware as a Service (RaaS) is a relatively new concept, where developers of ransomware tools hire them out to less sophisticated attackers, with both parties taking a share of ransom payments. Some of these organisations have a surprising amount of structure to them, with HR, recruitment and comms teams, and even provide technical support services to those hiring their tools.

However, the most worrying change to ransomware has been the use of double and multi extortion techniques. Previously, if an organisation became a victim of an attack, as long as there was an effective back-up strategy in place, the ransom note could be ignored, data restored, and operations continued. However, many attacks now incorporate an initial phase of copying the victim's data to an external location (referred to as "data exfiltration") prior to it being encrypted. The ransom note will then demand payment not only to recover data but also to ensure exfiltrated data is not released to the public. Many charities will be alarmed at the thought of sensitive data relating to stakeholders being leaked on the internet – the reputational, financial and regulatory risks being significant. A further extortion tactic can result in attackers threatening to disrupt the operation of websites by bombarding them with traffic, rendering them inoperable (known as "denial of service"). While this might not be a major issue for charities hosting "magazine" type websites, those with systems in place to interact with members, donors, volunteers, or

payments for services/goods will feel very different about such threats.

EFFECTS OF RANSOMWARE

The effects of ransomware can vary greatly depending on how successful an attacker has been at invading a network. In most circumstances, at a minimum there will be significant disruption to the charity while the IT/incident response teams analyse the extent of the attack, work out how to contain it, eradicate malicious software from any infected devices and finally move to recovery and the restoration of IT services. This can be particularly challenging for charities who rely on external IT providers due to the lack of in-house skills.

While some activities during an attack will seem obvious, such as the internal/external IT team working around the clock to restore services, it is easy to overlook the impact in other areas, such as time spent with insurers and legal teams to determine the appropriate courses of action for notification to the police (via Action Fraud), Charity Commission (reporting a serious incident), other relevant regulators and possibly the Information Commissioner's Office (ICO). The UK General Data Protection Regulation (GDPR), states that loss of access to personal data, for example due to encryption by ransomware, is a breach and therefore such an event could require notification to the ICO (within 72 hours of being made aware of any attack). There might also be time and stress involved in having to write to stakeholders to inform them of interruption to operations or loss/breach of their data.

> "The default position must be never to pay"

In the event of an attack, senior management may have to contend with the notion of paying the ransom. While the default position must be never to pay, for organisations who have been attacked, are unable to restore data (eg due to IT failures) or are concerned about exfiltrated data being released to the public, ransom payment might become a consideration. Veeam, a company specialising in backup/disaster recovery products, stated in its 2022 Ransomware Trends Report (based on feedback from 1,000 organisations), that 52% of those with encrypted data paid the ransom and that on average it took 18 days to recover from an incident.

PREVENTING AND PREPARING FOR RANSOMWARE

Within the cyber security world, there is a well-known statement along the lines of "it's not if you will be attacked, but when" and unfortunately there is a good degree of truth to it. Sophos, a company specialising in security software, recently published its State of Ransomware in 2022 report. It interviewed 5,600 mid-sized organisations across 31 countries and found that 66% had been the victim of ransomware in the previous year.

While being attacked might seem like an inevitability, there are still ways of minimising the risk. From my own experience, where attacks are successful, it is generally due to multiple processes, human or technical control failures, and it is rare for only one thing to have gone wrong.

At the top of the list should be ensuring that appropriate controls have been put in place, that they are working effectively and are tested on a regular basis. While an exhaustive list is beyond the remit of this article, four key technical controls to discuss with your internal/external IT teams are as follows:

- Given that a majority of ransomware originates by email (as infected attachments or links to malicious sites), an obvious first line of defence is the email gateway. Many charities are using the Microsoft 365 cloud platform to host email in conjunction with a third-party anti-spam/anti-malware/email archive system. However, some of these products are no longer capable of detecting sophisticated email attacks, despite what their vendors might claim. Charities should review their effectiveness and consider alternative systems from Microsoft and third parties, designed to protect against advanced and sophisticated email threats/ransomware attempts.
- Once malware gets as far as an end user's PC/laptop, anti-malware software can be a last line of defence. In recent years there has been a shift from "next generation" antivirus software to "endpoint detection and response" (EDR) products. The latter is capable of detecting sophisticated ransomware, determining how it operates and

providing analysis tools and functionality to halt infections/techniques used by attackers.
- Ransomware attacks will often attempt to exploit security vulnerabilities within operating systems and applications. Microsoft and third-party software providers regularly produce fixes (known as patches) to resolve them and it is vital that IT teams implement these as soon as possible (ideally two weeks from them being made available). Microsoft has been providing tools to patch their products for many years; however, it is equally important to ensure all third-party applications are kept updated.

Another approach used by attackers to get ransomware into a network is to exploit any weak passwords in use. Charities need to ensure the following are in place:
- Secure passwords for logging on to networks (NCSC provides further guidance on this).
- Systems to detect/impede "brute force" attacks (where an attacker will keep guessing passwords repeatedly).
- An additional layer of authentication control is used for all remote access to data or data held on cloud-based systems. This is known as multi-factor authentication and generally takes the form of codes generated by a smartphone app or sent via text message.
- Unique and secure passwords are in use for all applications/cloud-based systems that do not rely on network logons (known as single sign-on). The only practical way to achieve this is to provide employees with a password manager application.

It is also imperative that systems are in place to detect, provide early warning of and investigate breaches. While many solutions are available on the market, the downside is they usually require skilled IT personnel to operate them. Larger organisations will establish a security operations centre (SOC) to monitor and manage security. A SOC is complex to setup, run and beyond the financial means of smaller charities; however, third parties can provide similar services on an affordable annual cost basis.

Charities must also ensure that relevant human and process controls have been put in place. As previously stated, ransomware often finds its way into a network due to staff unwittingly clicking on attachments or opening links. Regular security awareness training can be an effective way to educate staff about latest threats and techniques being used by attackers.

> "Risk assessments should be updated to deal with ransomware"

In the event of a ransomware attack, there will be a great deal of reliance on the IT and operations teams. Having worked with several clients during or following an attack, it quickly becomes an emotional situation. Panic can set in and that often leads to poor decision-making. Charities should therefore plan for a cyber/ransomware attack by creating an incident response plan (IRP) – a set of procedures and tools to guide teams through an event. Once the IRP has been written, it needs to be tested and refined on a regular basis, using table-top exercises, or working with a specialist provider to plan and launch a simulated but realistic attack (known as red team testing).

In addition to the IRP, charities should ensure they have effective disaster recovery and business continuity plans in place, detailing how IT services are recovered and how day-to-day operations continue during an attack.

NCSC has created some very useful (and free) content relating to the above:
- NCSC cyber security training for staff: https://bit.ly/305OlD8
- Exercise in a Box – table-top exercises covering ransomware and other scenarios: https://bit.ly/2VoscBx

Charities may also wish to consider implementing a security framework, such as the government-backed Cyber Essentials (CE) and Cyber Essential Plus certification – a prescriptive set of controls designed to protect any size of organisation from the most common form of cyber attacks. CE is also a great way to demonstrate to stakeholders that your charity takes cyber security seriously. NCSC provides the following guidance:
- Cyber Essentials – https://bit.ly/3QfmhaE
- Cyber Security: Small Charity Guide – https://bit.ly/3d3VxeS
- For larger charities, the cyber security Board Toolkit - https://bit.ly/2CsYwbO
- For medium and larger charities (can be used in tandem with the Board Toolkit), 10 Steps to Cyber Security - https://bit.ly/3Sqw931

Cyber insurance policies with ransomware cover can be very useful in the event of an attack and in the past, insurers have generally paid out when required. However, with the ongoing rise in the number of attacks, premiums are increasing, restrictions on cover are being applied and insurers are demanding that organisations have effective security controls in place.

Cyber security improvement should be an embedded process within all charities. Risk assessments should be updated to adequately deal with ransomware and other types of cyber threats. Following that, a plan can be devised to prioritise actions around implementing/improving controls and associated spend. If you are struggling to work out an approach or simply do not know where to start, perhaps consider engaging with a consultancy firm to perform a security review/gap analysis and assist in formulating a plan. ●