Introduction

According to the 2022 Cybersecurity Breaches Survey, 19% of UK charities identified a service-impacting cyber-attack with a negative outcome in 2022. The survey also reports only 5% of UK charities have a specific cybersecurity insurance policy. This report seeks to assess the security posture of PeopleCare, detail cyberthreats faced in the charity industry and give recommendations as to what PeopleCare may implement to combat these threats and mitigate the risk in the event of a breach. (Department for Digital, Media, Culture and Sport, 2022)

Scottish Action for Mental Health Charity breach in 2022

The attack vector

Scottish Action for Mental Health (SAMH) is a charity based in Scotland that works to provide mental health support to young people and adults. SAMH majorly does this by creating awareness about mental health challenges, supporting people facing mental health challenges through its various channels and services and its phone and email hotlines for suicide prevention run by their partner organization Samaritans. (SAMH, 2023) . On the 21st of March 2022, SAMH Chief Executive put out a statement on the charity's website informing the public that the charity had been victims of a targeted cyberattack. (SAMH, 2022). The attack was carried out with a malware payload infecting a node on the network.

What happened?

The news of the breach was broken when a Twitter post by cybersecurity researcher Soufiane Tahiri confirming reports of twelve gigabytes of data leaked on the dark web by hacking group RansomEXX surfaced. (Soufiane [@S0ufi4n3], 2022) The incident took down their email service as well as some of their national phone lines. They were able to restrict access from the infected machines to other environments within their network upon discovery of the attack.

What was compromised?

The information released within the 12GB dump included personal identifiable information about volunteers and beneficiaries of the charity's services such as passports, home addresses and driver's licenses. SAMH had to expend significant effort and financial resources to notify regulatory authorities as well as individuals impacted by the breach. (Soufiane [@S0ufi4n3], 2022)

How did the breach occur?

RansomEXX are a hacking group that has been in existence since 2018 and are responsible for the ransomware attack on Japanese printing company Konica Minolta. The attack on Konica Minolta was performed through a vulnerability in one of their Managed Service Providers, stealing administrator credentials and moving across the network to find file servers and clients to infect with their malware payload. The malware was able to successfully infect multiple systems as well as the operational Internet of Things networks controlling the industrial systems within Konica's production plants disrupting its core systems. (Benmalek, 2024). Cybersecurity company Cybereason says the RansomEXX malware "runs as a solely in-memory payload that is not dropped to disk, making it highly evasive." (Frank, 2022).

What was the impact of the breach?

According to the SAMH Annual Financial report for the year ended 31st March 2022, SAMH reported experiencing a 6-week delay in majority its strategy implementation activities due to the attack implying that valuable time and resources that would have otherwise been spent elsewhere were expended in dealing with the fallout of this attack. (Kingston, 2022)

Timeline of the attack

The attack began once the RansomEXX group infiltrated the target machine. It is still unclear exactly how they infiltrated the SAMH systems and for how long but it is likely they would have exploited a vulnerability present on the network as seen in the Konica Minolta breach. (Benmalek, 2024). The breach puzzled many cybersecurity industry experts because it seemed deviant from the RansomEXX group modus operandi to target entities that would be unable to afford the imposed ransom. (Trend Micro Research, 2022). See Fig. 1 below for a timeline of events.

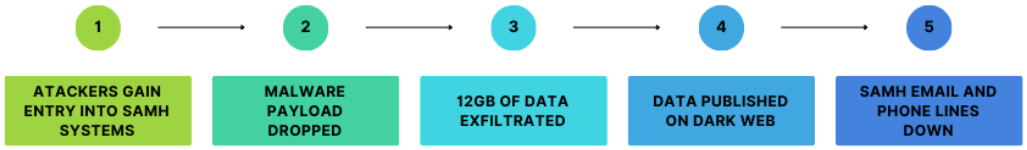

Fig. 1: Attack timeline of the SAMH ransomware attack

International Committee of the Red Cross data breach in 2022

The attack vector

The International Committee of the Red Cross (ICRC) is a global humanitarian organization that seeks to help people who are affected by armed conflict and natural disasters with a range of services such as first aid to people affected by armed conflict, support for asylum seekers and maintenance of water sources and habitat in conflict zones. (ICRC, 2014). On the 19th of January 2022, the ICRC issued a statement on their website confirming a breach of their servers through an unpatched vulnerability. (ICRC, 2022b)

What was compromised?

According to an investigation by the ICRC into the incident, 515,000 records may have compromised through the breach of servers hosting personal information relating to beneficiaries of its Restoring Family Links program, an initiative to reunite families separated by violent conflict. There was no indication the compromised personal data contained in the servers has been published or sold at the conclusion of the ICRC investigation in June 2022. (ICRC 2022a)

How did the breach occur?

The attack was deemed to have been targeted directly at the ICRC servers due to the discovery of the Media Access Control address contained in the malicious code executed on the servers. The attackers also utilized special tools not available to many threat actors to disguise their activities as legitimate users thereby evading detection for about 70 days from when the breach first occurred. (International Committee of the Red Cross, 2022a). The attackers utilized an unpatched Common Vulnerability and Exploit 2021-40539 (CVE-2021-40539) in the Zoho ManageEngine

ADSelfService Plus software which allowed them to bypass the access control measures present on the targets. (MITRE, 2021).They were then able to import malicious code with the access gained and execute it, compromising the servers.

What was the impact on ICRC?

The ICRC expended significant effort notifying all individuals affected by the breach because of how remote the residences of some of the impacted individuals are. ICRC stated it was evaluating the risk profile of each data subject breached and utilized various means such as announcements, hotlines, letters and sending a volunteer to physically inform the impacted individuals. (ICRC, 2022a). The ICRC also had to make changes to its endpoint monitoring and intrusion detection system due to their failure to detect the vulnerability in a timely manner.

Timeline of the attack

The attack began on 9th November 2021 when the attackers were able to gain entry into the target server via the unpatched vulnerability CVE-2021-40539. The attackers were then able to perform their attack with advanced tools and conceal their activities with obfuscation. During a security enhancement program activity on 18th January 2022, one of ICRC's security vendors detects an anomaly on the affected servers and immediately took them offline to investigate it. A statement was issued on 19th January 2022 confirming the attack and informing the public of the next steps to be taken. A further statement was issued on 24th June 2022 confirming the affected servers had been restored to service and significant measures toward addressing what went wrong. See Fig. 2 below for a timeline of events.

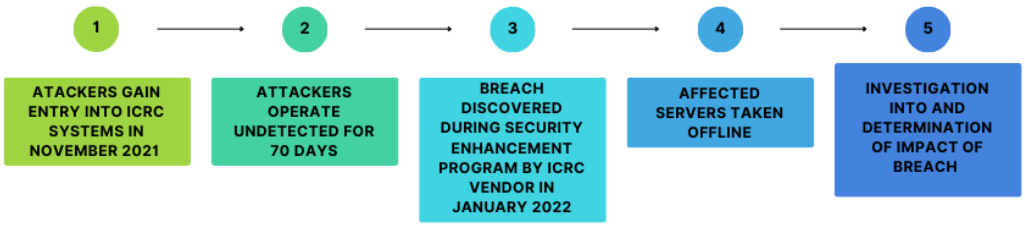

Fig. 2 Attack timeline of the ICRC attack

As seen in the 2 cyberattacks reported on above, for most charitable organizations, confidentiality and availability of information is paramount due to the sensitive nature of the work they do as seen in the Red Cross breach and the consequences of this information falling into the wrong hands as shown in the Scottish Action for Mental Health case. For PeopleCare, an implementation of the Committee of National Security Systems (CNSS) security model should address all potential information security concerns. The CNSS security model is an industry standard information security model represented by a 3 by 3 by 3 cube representing:

- the key goals of information security which are **Confidentiality, Integrity and Availability**,
- the potential states of any data within an information system (**Storage, Processing and Transmission**),
- the security controls for achieving the above-mentioned key goals (**Policy, Education and Technology**) (McCumber, 1991).

In this section of the report, four intersections of this model with one implementable security control for each one will be discussed below:

1. **Integrity, Storage and Technology:** McCallister *et al.* (2010) suggests an implementation of the principle of least privilege by restricting users to the least amount of read, write or execute privileges on information systems as required to perform a task. This security control ensures that each user does not have unlimited privileges to manipulate the PeopleCare systems. This control protects the integrity of the information systems in the event a legitimate user's credentials are stolen from exploitation as the activity will be flagged as anomalous.
2. **Availability, Processing and Policy**: The PeopleCare information systems need to be highly available to be able to properly serve its global beneficiaries and donors. Downtimes on PeopleCare systems may leave already vulnerable people who rely on PeopleCare services much more vulnerable. Malware and ransomware attacks can impact availability of information systems due to the downtime that will be experienced as seen in the SAMH cyberattack. A security control that can be implemented is the management of removable media to reduce the probability of malware entering the PeopleCare corporate network. This control is in line with the ISO/IEC 27001 A.8.3.1 guideline (Kenyon, 2019).
3. **Availability, Transmission and Technology:** The PeopleCare information systems are networked to ensure global access to PeopleCare's services for beneficiaries. A recommendation by ISO 27001 is segregation in networks (Kenyon, 2019). Due to the global nature of PeopleCare's operations, it is paramount that all the information within its network remains protected even if parts of it are compromised by natural disaster, human error, or attack from malicious entities. PeopleCare may implement this through networking technology that segregates users by their authorization level within the network, servers and information systems that are segregated by the level of confidentiality of the information on them. For example, file and authentication servers should be on separate networks from each other.
4. **Integrity, Transmission**: To ensure the integrity of all information accessed over the charity's corporate network, it is recommended that the information is encrypted and passed through secure channels if it is to be transmitted outside the bounds of the corporate network. This can be achieved through encryption and virtual private networks (VPNs). Suppose an employee in Dublin, Ireland wants to send a file to an employee in Tokyo, Japan the file may be sent over the internet due to its ubiquitous nature, but the ease of access may come at a trade-off with security due to the number of malicious actors that may be present on the public internet.

In line with the Cybersecurity Framework proposed by NIST, it is recommended that PeopleCare have the following roles within their organization dedicated to cybersecurity. Mahn *et al.* (2021) identified 5 key functions of the framework and the recommendation to PeopleCare is to have one role to cater for each function:
Chief Information Security Officer: This role will be responsible for the overarching security strategy and will be the advocate at management level for cybersecurity awareness. Due to the nature of the limited financial capacity of charities as a result of the humanitarian nature of the work they do, it is recommended PeopleCare considers outsourcing this service to ensure they have the best value for the investment due to the limited number of individuals with the right skills and experience to fill this role.

Security Engineer: This role will be responsible for fulfilling the **Identify** function of the NIST framework by designing and implementing security hardware and software solutions. This ensures PeopleCare keeps up with the newest threats in the threat landscape of the charity industry.
Cybersecurity Awareness Coordinator: This role will be responsible for fulfilling the **Protect** function of the NIST framework by ensuring users are consistently trained on all possible incidents and simulation of possible scenarios to ensure readiness in the event of an incident.
Security Operations Analyst: This role will be responsible for fulfilling the **Detect** function of the NIST framework by detecting and responding when appropriate to cybersecurity events. This ensures PeopleCare is in the know of the strength of their security measures, what kinds of threats they may face and how to address any existing gaps they have identified.
Incident Response Manager: This role will be responsible for fulfilling the **Respond** and **Recover** functions of the NIST framework by managing cybersecurity incidents that occur by coordinating with internal stakeholders, affected parties and ensuring the incident is contained.
Security Compliance Manager: This role will be responsible for ensuring the charity is compliant with industry standard guidelines and conducting internal audits as specified in relevant guidelines.
System and Network Administrators: These roles are crucial to the ensure that all other core security functions can perform their functions by ensuring all recovery functions such as backups and access control mechanisms pertaining to information technology hardware and software are working properly.
In conclusion, PeopleCare will benefit immensely from the implementation of the recommendations of this report to improve its security posture and ensure adequate protection of its assets and organizational reputation.

References

Benmalek, M. (2024) 'Ransomware on cyber-physical systems: Taxonomies, case studies, security gaps, and open challenges', *Internet of Things and Cyber-Physical Systems*, 4, pp. 186–202. Available at: https://doi.org/10.1016/j.iotcps.2023.12.001

Department for Digital, Media, Culture and Sport (2022) *Cyber Security Breaches Survey 2022*, *GOV.UK*. Available at: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2022/cyber-security-breaches-survey-2022 (Accessed: 21 February 2024).

Frank, D. (2022) *Cybereason vs. RansomEXX ransomware*. Available at: https://www.cybereason.com/blog/research/cybereason-vs.-ransomexx-ransomware [Accessed 21 February 2024].

ICRC (2014) *What we do*. Available at: https://www.icrc.org/en/what-we-do [Accessed 22 February 2024].

ICRC Cross (2022a) *Cyber-attack on ICRC: What we know | ICRC*. Available at: https://www.icrc.org/en/document/cyber-attack-icrc-what-we-know (Accessed: 16 February 2024).

ICRC (2022b) *Sophisticated cyber-attack targets Red Cross Red Crescent data on 500,000 people*. Available at: https://www.icrc.org/en/document/sophisticated-cyber-

attack-targets-red-cross-red-crescent-data-500000-people [Accessed 22 February 2024].

Kenyon, B. (2019). *ISO 27001 controls–A guide to implementing and auditing.* IT Governance Ltd.

Mahn, A., Marron, J., Quinn, S. and Topper, D. (2021) *Getting started with the NIST cybersecurity framework: a quick start guide*. Available at: https://doi.org/10.6028/NIST.SP.1271

McCallister, E., Grance, T. and Scarfone, K.A. (2010) *Guide to protecting the confidentiality of Personally Identifiable Information (PII)*. Available at: https://doi.org/10.6028/NIST.SP.800-122

McCumber, C. J. R. (1991) 'Information systems security: A comprehensive model', in *The 14th National Computer Security Conference.* Washington DC, 1-4 October 1991, pp. 328-337. Available at: http://csrc.nist.gov/publications/history/nissc/1991-14th-NCSC-proceedings-vol-1.pdf [Accessed 23 February 2024].

MITRE (2021) *NVD - cve-2021-40539*. Available at: https://nvd.nist.gov/vuln/detail/cve-2021-40539 [Accessed 22 February 2024].

SAMH (2022) *SAMH announcement: Cybersecurity attack*. Available at: https://www.samh.org.uk/about-us/news-and-blogs/samh-annoucenment-cybersecurity-attack [Accessed 16 February 2024].

SAMH (2023) *100 years of SAMH.* Available at: https://www.samh.org.uk/about-us/centenary/centenary-100-yrs [Accessed 18 February 2024].

Soufiane [@S0ufi4n3] (2022) *Dirty work from #RansomEXX #ransomware group who just added SAMH (Scottish Association for Mental Health) to their victim's list. +12Gb of data leaked* [Twitter]. Available at: https://twitter.com/S0ufi4n3/status/1505856171089006594 [Accessed 22 February 2024].

Trend Micro Research (2022) *Ransomware spotlight: RansomEXX*. Available at: https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-ransomexx [Accessed 18 February 2024].