# *Ransomware Attack on Bright Future Charity*

- Fundamentals of Cyber Security
- Threat actors associated with ransomware attacks
- Attack vectors used in ransomware attacks
- Impacts of an attack
- Mitigation methods & how they can be used by the charity
- Recommendations of proactive security measures

# *Background on the Bright Future Charity*

- The Bright Future Charity is a non-profit aiding underprivileged children's education
- A ransomware attack encrypted financial records and donor information
- Vulnerabilities exploited include:
  - **Weak password policies**
  - **Lack of multi-factor authentication**
  - **Outdated software**
  - **No Intrusion Detection and Prevention System (IDPS)**

# *Fundamental Concepts of Cyber Security: CIA Triad*

- **Confidentiality:** The assurance that data and information is only accessible by authorised parties (Centre of Internet Security, 2018).
- **Integrity:** Data must be accurate, and should not in any way be altered, unless required by an authorised party (Centre of Internet Security, 2018).
- **Availability:** The ability for an organisation to obtain and access data when required (Centre of Internet Security, 2018).

- **Non-repudiation:** Ensuring that someone is unable to deny their actions and when a system can verify the authenticity of an event or transaction occurring within it (Kidd, 2023).

# *Threat Actors: Cybercriminals*

- Attacks can be committed by groups or individuals (IBM, 2023)
- Largely committed for financial gain. **95%** of all cyber-attacks **were financially motivated** (Verizon, 2024).

- Cybercriminals employ a variety of techniques to achieve their goals which can include:
  - **Malware**
  - **Phishing**
  - **Social Engineering**

# *Threat Actors: Hacktivists*

- Attacks commonly committed by a group and motivated by a **specific cause** (Fortinet, 2023)

- Example: **Anonymous**

- Techniques used by hacktivists can include:
  - **Denial of Service Attacks**
  - **Malware**
  - **Website Defacement**

# *Threat Actors: Insider Threats*

- Insider threats come from users who are **authorised to access data**, such as employees and volunteers (IBM, 2023).
- This can be done either **intentionally or unintentionally** (IBM, 2023).

- Techniques used by insider threats include:
  - **Data theft / leaks**
  - **Sabotage**
  - **Malware**

# *Attack Vectors: Social Engineering*

- **Social Engineering**: A user-based vulnerability that **manipulates** individuals to reveal information they should keep confidential (IBM, 2024).

- Examples of social engineering include:
  - **Baiting**
  - **Watering Hole Scams**
  - **Scareware**

  - Example: Minneapolis Star Tribune ads scareware

# *Attack Vectors: Phishing*

- **Phishing**: A user-based vulnerability that involves sending **deceptive communications** that seem to originate from a trusted source (Cisco, 2017).

- How could this be exploited:
  - Attacker sends an email that seems to come from a trusted source
  - The email has an attached file or link that also seems trustworthy
  - The user interacts with the content, as they haven't had effective employee training. The ransomware is executed, and the data is encrypted

- A study from GOV.UK (2024) shows that **83%** of cyber-attacks against charities **are phishing attacks**.

# *Attack Vectors: Software Vulnerabilities*

- **Software Vulnerability**: A security flaw or bug in software that could be exploited by an attacker (Foster, 2020)

- Example of a software vulnerability:
  - **The EternalBlue vulnerability; exploits vulnerabilities in the Server Message Block version 1 (SMBv1) protocol on unpatched Windows versions** (Burdova, 2020)

- How could this be exploited:
  - The charity uses an outdated Windows version with unpatched SMBv1 vulnerabilities
  - An attacker exploits this by sending malicious data packets to the charity's network which allows them to run their own code onto the system
  - The malicious code deploys ransomware onto the charity's network, encrypting sensitive data

# *Potential impacts of the attack*

- Financial loss: The ransomware attack would deplete the charity's funds, reducing the resources available to aid the children's education (Pyle, 2024).
- Reputational damage: A cyber-attack can significantly damage public trust in a charity, reducing the likelihood of donors supporting the charity (Pyle, 2024).
- Operational disruption: The charity requires technology for operations. The ransomware attack would disrupt or stop these processes preventing them from carrying out the aim (Pyle, 2024).

- Example: **Edinburgh Festival Fringe Society**; lost £70k after a ransomware attack

# *Mitigation Methods: Intrusion Detection and Prevention Systems (IDPS)*

- **IDS**: An application designed to monitor network traffic, identifying threats as well as detecting suspicious or malicious activity (Fortinet, 2023). IDPS builds upon IDS by actively preventing threats (Fortinet, 2022).

- Benefits of IDPS can include:
  - **Detection of threats in real-time**
  - **Automated response to threats**

- Possible limitation of IDPS can include:
  - **False positives**

- Could have been used by the charity to **identify the ransomware** early and **provide immediate protection** to data.

# *Mitigation Methods: Unified Threat Management (UTM)*

- **UTM**: A combination of multiple security features and services into a single package within a network (Fortinet, 2024).
- Features can include:
  - **Anti-malware & Antivirus**
  - **Firewall**
  - **Website filtering**
  - **Centralised management**
  - **IDPS**

- Could have been used by the charity **to prevent the lack of an IDPS from being exploited**, as well as **to prevent the ransomware** from being able to harm data and spread across the network through anti-malware and firewall features.

# *Mitigation Methods: Regular Software Updates and Patching*

- **Patches**: Updates for software and operating systems designed to **fix security vulnerabilities** in a program or product (CISA, 2023).
- Benefits of regular updating and patching of software:
  - **Closing software-based security vulnerabilities before they could be exploited**
  - **Enhanced security features**

- Possible complication of regular updating and patching of software:
  - **Non-compliance from users;** 32% of ransomware attacks exploit unpatched vulnerabilities (Sophos, 2024)

  - Could have been used by the charity **as part of a UTM** to **prevent outdated software from being exploited.**

# *Mitigation Methods: Employee Training*

- Employee training can include:
  - **Making staff aware of human-based vulnerabilities with continuous support**
  - **Running real-time training scenarios**

- Benefits of employee training can include:
- **Cost-benefits**
- **Improved human-based practices**

- Possible limitation of employee training can include:
- **Outdated training that doesn't cover emerging threats**

- Could have been used by the charity to **prevent user-based vulnerabilities** from being exploited

# *Proactive Defenses*

- Security audits: **Reviews** an organisation's **security systems**, **assesses effectiveness** and **recommends improvements** (Palatty, 2023).
- Multi-factor authentication (MFA): **Securer** login process that requires the user to **provide more proof of identity** than just a password (AWS, 2023).
- Network Segmentation: **Splitting a network** into smaller parts to improve security (Cisco, 2019).

- Recommendations:
  - **Commit regular security audits**
  - **Enforce multi-factor authentication;** biometrics
  - **Implement network segmentation**

# References

## Reference list


Abacus (2021) *Why Is It Important to Update Security Patches? - Abacus*, *GoAbacus*. Available at: https://goabacus.com/why-is-it-important-to-update-security-patches/ (Accessed: 14 December 2024).

AWS (2023) *What is Multi-Factor Authentication (MFA)? - Cloud Security Beginner's Guide - AWS*, *Amazon Web Services, Inc.* Available at: https://aws.amazon.com/what-is/mfa/ (Accessed: 16 December 2024).

Burdova, C. (2020) *What Is EternalBlue and Why Is the MS17-010 Exploit Still Relevant?*, *Avast*. Available at: https://www.avast.com/c-eternalblue (Accessed: 12 December 2024).

Center for Internet Security (2018) *Election Security Spotlight – CIA Triad*, *CIS*. Available at: https://www.cisecurity.org/insights/spotlight/ei-isac-cybersecurity-spotlight-cia-triad (Accessed: 7 December 2024).

Centre for Internet Security (2020) *Cybersecurity Spotlight - Website Defacements*, *CIS*. Available at: https://www.cisecurity.org/insights/spotlight/cybersecurity-spotlight-website-defacements (Accessed: 10 December 2024).

CISA (2023) *Understanding Patches and Software Updates | CISA*, *www.cisa.gov*. Available at: https://www.cisa.gov/news-events/news/understanding-patches-and-software-updates (Accessed: 14 December 2024).

Cisco (2017) *What Is Phishing? Phishing Attack Examples and Definition*, *Cisco*. Available at: https://www.cisco.com/c/en_uk/products/security/email-security/what-is-phishing.html#~free-trials (Accessed: 13 December 2024).

Cisco (2019) *What Is Network Segmentation?*, *Cisco*. Available at: https://www.cisco.com/c/en/us/products/security/what-is-network-segmentation.html (Accessed: 16 December 2024).

Cisco (2024) *What Is a Social Engineering Attack in Cybersecurity?*, *Cisco*. Available at: https://www.cisco.com/c/en_uk/products/security/what-is-social-engineering.html#~types-of-attacks (Accessed: 12 December 2024).

CybSafe (2023) *Security awareness: 7 Reasons Why Security Awareness Training Is Important in 2023*, *CybSafe*. Available at: https://www.cybsafe.com/blog/7-reasons-why-security-awareness-training-is-important/ (Accessed: 15 December 2024).

Fortinet (2022) *What Is an IPS (Intrusion Prevention System)?*, *Fortinet*. Available at: https://www.fortinet.com/resources/cyberglossary/what-is-an-ips (Accessed: 14 December 2024).

Fortinet (2023a) *What Is an Intrusion Detection System (IDS)?*, *Fortinet*. Available at: https://www.fortinet.com/resources/cyberglossary/intrusion-detection-system (Accessed: 14 December 2024).

Fortinet (2023b) *What Is Hacktivism and Anonymous Hacktivism*, *Fortinet*. Available at: https://www.fortinet.com/resources/cyberglossary/what-is-hacktivism (Accessed: 10 December 2024).

Fortinet (2023c) *What Is Scareware? Defined and Explained | Fortinet*, *Fortinet*. Available at: https://www.fortinet.com/uk/resources/cyberglossary/scareware (Accessed: 12 December 2024).

Fortinet (2024) *What Is Unified Threat Management (UTM)?*, *Fortinet*. Available at: https://www.fortinet.com/resources/cyberglossary/unified-threat-management (Accessed: 13 December 2024).

# References Continued


Foster, S. (2020) *Top 10 Software Vulnerabilities + Vulnerabilities Definition*, *Perforce Software*. Available at: https://www.perforce.com/blog/kw/common-software-vulnerabilities (Accessed: 12 December 2024).

GOV.UK (2024) *Cyber Security Breaches Survey 2024*, *GOV.UK*. Available at: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2024/cyber-security-breaches-survey-2024 (Accessed: 13 December 2024).

IBM (2023) *What Is a Threat actor? | IBM*, *www.ibm.com*. Available at: https://www.ibm.com/topics/threat-actor (Accessed: 9 December 2024).

IBM (2024) *What is Social Engineering?*, *www.ibm.com*. Available at: https://www.ibm.com/topics/social-engineering (Accessed: 12 December 2024).

Microsoft (2022) *What Is Insider Threat? Unraveling Insider Risks | Microsoft Security*, *Microsoft.com*. Available at: https://www.microsoft.com/en-gb/security/business/security-101/what-is-insider-threat?ef_id=_k_EAIaIQobChMIypfMt6qqigMVmZNQBh2pqw_9EAAYASAAEgJGEPD_BwE_k_&OCID=AIDcmmao55x8o7_SEM__k_EAIaIQobChMIypfMt6qqigMVmZNQBh2pqw_9EAAYASAAEgJGEPD_BwE_k_&gad_source=1#heading-ocu8ow12 (Accessed: 11 December 2024).

National Cyber Security Centre (2016) *Denial of Service (DoS) Guidance*, *National Cyber Security Centre*. Available at: https://www.ncsc.gov.uk/collection/denial-service-dos-guidance-collection (Accessed: 10 December 2024).

National Cyber Security Centre (2023) *Cyber threat report: UK charity sector*. Available at: https://www.ncsc.gov.uk/files/Cyber_threat_report-UK-charity-sector.pdf (Accessed: 9 December 2024).

Nivedita James Palatty (2023) *What Are Security Audits? - Types, Process & Checklist*, *Astra Security*. Available at: https://www.getastra.com/blog/security-audit/security-audits/#Security_Audit_Checklist (Accessed: 16 December 2024).

Oleg Shomonko (2021) *Insider Threat Techniques & Best Methods to Detect Them | Syteca*, *Syteca*. Available at: https://www.syteca.com/en/blog/insider-threat-techniques (Accessed: 11 December 2024).

Pathlock (2023) *16 Ways To Prevent Insider Threats and Detect When They Occur*, *Pathlock*. Available at: https://pathlock.com/learn/16-ways-to-prevent-insider-threats-and-detect-when-they-occur/ (Accessed: 11 December 2024).

Raza, M. (2023) *The Principle of Least Privilege Explained (with Best Practices)*, *Splunk-Blogs*. Available at: https://www.splunk.com/en_us/blog/learn/least-privilege-principle.html (Accessed: 7 December 2024).

Sharif, A. (2023) *What are Audit Logs? Use Cases and Challenges | CrowdStrike*, *Crowdstrike.com*. Available at: https://www.crowdstrike.com/en-us/cybersecurity-101/next-gen-siem/audit-logs/ (Accessed: 7 December 2024).

Sophos (2024) *Ransomware Report: Sophos State of Ransomware Report 2021*, *SOPHOS*. Available at: https://www.sophos.com/en-us/content/state-of-ransomware (Accessed: 14 December 2024).

Verizon (2024) *2024 Data Breach Investigations Report*, *Verizon Business*. Available at: https://www.verizon.com/business/resources/reports/dbir/ (Accessed: 15 December 2024).

Woodstock IT (2024) *Effectiveness Of Cybersecurity Training | Woodstock IT*, *Woodstock IT*. Available at: https://www.woodstockit.co.uk/blog/annual-cybersecurity-training-isnt-effective/ (Accessed: 15 December 2024).