cowbell

Cyber Threats Targeting Charities and Non-Profits

Notable incidents, threat actors, and mitigations for the non-profit sector

Executive Summary

Charities, non-governmental organizations (NGOs), think tanks, and professional associations play a crucial role in supporting global communities and civil society. However, their reliance on digital systems to manage sensitive donor data, beneficiary information, and financial transactions has made them a highly attractive target for cybercriminals.

In 2024, the average ransom payment for a compromised organization reached $1.2 million, with 51% of victims paying the demand. Alarmingly, of those who paid, 40% reported that their data was still leaked.

Our intelligence reveals that the non-profit sector is facing a dual-threat landscape: financially motivated ransomware and business email compromise (BEC) attacks, alongside highly sophisticated nation-state espionage and hacktivism aimed at disrupting advocacy efforts. This white paper outlines the current threat landscape affecting the US and UK non-profit sectors, details notable incidents, and provides a sound approach to digital resilience.

Matthieu Chan Tsin
SVP & General Manager, Cowbell Resiliency Services

The Threat Landscape: Why Non-Profits are Vulnerable

The non-profit sector has historically been slower to adopt digital transformation compared to private enterprises, resulting in significant gaps in cybersecurity posture.

- **Limited Resources & Budget Constraints:** Approximately 88% of US non-profits spend less than $500,000 annually on operating costs. According to recent surveys, 56% of NGOs report that their allocated IT resources do not fulfill their cybersecurity needs, and many lack basic protections like Multi-Factor Authentication (MFA).
- **High-Value Data:** Charities store massive amounts of personally identifiable information (PII), financial records, and medical data of vulnerable populations.
- **Reliance on Volunteers:** The sector's heavy reliance on volunteers and part-time staff, who often lack formal cybersecurity training, increases the success rate of social engineering and phishing campaigns.
- **Geopolitical and Social Advocacy:** Non-profits engaged in human rights, environmental, or political advocacy face unique threats from state-sponsored actors and hacktivists seeking to gather intelligence or deploy Distributed Denial of Service (DDoS) attacks to silence their operations.

Notable Cyber Incidents: United States

Brokers know firsthand the immense pressure US non-profits face. They are tasked with solving our communities' most complex problems, often while operating on razor-thin margins.

Unfortunately, cybercriminals do not see these financial constraints as a reason for mercy; they see them as vulnerabilities to exploit. Intelligence highlights a disturbing trend of double-extortion ransomware and highly targeted Business Email Compromise (BEC) fraud aimed at American charities. By understanding the mechanics of these specific attacks, we can better advise our non-profit policyholders on how to structure their Cyber and Directors & Officers (D&O) coverage, ensuring they have the financial backing to weather a crisis and continue their vital missions.

Easter Seals

In April 2024, the Rhysida ransomware group attacked this disability services non-profit, stealing the personal information of 14,855 individuals, including Social Security numbers, passports, and medical details. The group demanded a ransom of 20 Bitcoin (approximately $1.3 million).

Water For People

In January 2024, the Medusa ransomware group targeted this clean water non-profit, demanding a $300,000 ransom to prevent the publication of stolen historical data.

The Internet Archive

In October 2024, hacktivist group SN_BLACKMETA conducted a massive DDoS attack against the Internet Archive (operator of the WayBack Machine), resulting in a week-long operational shutdown and the exposure of 31 million users' encrypted passwords and emails.

Roots of Peace (BEC Fraud)

A sophisticated Business Email Compromise (BEC) attack impersonated the CEO of this California-based non-profit, resulting in a fraudulent $500,000 wire transfer to a bank account in Hong Kong.

Notable Cyber Incidents: United Kingdom

The third sector provides indispensable support to our most vulnerable populations. Yet, as the intelligence below demonstrates, charities and social enterprises are squarely in the crosshairs of sophisticated, financially motivated ransomware syndicates. For UK brokers, these incidents underscore the critical need to move beyond standard cyber hygiene conversations. Our non-profit clients need our guidance to understand that an attack is no longer a remote possibility - it is an active threat with severe regulatory and reputational consequences. By reviewing these regional case studies, we can help charities proactively build the resilience required to protect their donor data, their operations, and their beneficiaries.

Claud Bilbao
VP, Underwriting & Distribution UK & Australia

Save the Children

In September 2023, the BianLian ransomware group exfiltrated 6.8 terabytes of sensitive data from this global charity, including 800GB of financial records, medical data, and international HR files.

The Big Issue

In March 2024, the Qilin ransomware group attacked this social enterprise, stealing 530GB of sensitive personnel data, financial records, and contracts, which were subsequently leaked on the dark web.

Richmond Fellowship Scotland

In January 2024, the Medusa ransomware group encrypted sensitive data belonging to this mental health charity, causing severe infrastructure disruption and demanding a $300,000 ransom.

Threat Actor Profiles

The non-profit sector is targeted by a mix of financially motivated Ransomware-as-a-Service (RaaS) operators and politically motivated advanced persistent threats (APTs).

- **Star Blizzard:** A Russia-based, state-sponsored threat group linked to the FSB. Star Blizzard conducts highly targeted spear-phishing campaigns against NGOs, think tanks, and human rights defenders to gather geopolitical intelligence.
- **Medusa:** A RaaS group that aggressively targets unpatched systems and poorly segmented networks within the non-profit and healthcare sectors. Medusa frequently uses public Telegram channels and dark web countdown clocks to pressure charities into paying ransoms.
- **Rhysida:** Operating since May 2023, this group exploits weak credentials and VPN vulnerabilities to deploy double-extortion ransomware, demonstrating a willingness to leverage highly sensitive medical and disability data for extortion.
- **Qilin:** A ransomware group utilizing custom Rust-based malware that evades traditional endpoint detection. They are known for aggressive double-extortion tactics and targeting critical infrastructure and social enterprises.

The Sound Approach to Risk: Recommendations

Digital risks are real, but they are manageable with sound protection. Non-profits must prioritise foundational security measures that offer high impact for minimal cost.

1. **Implement Basic Cybersecurity Training:** Human error remains a primary attack vector. Conduct mandatory training for all staff and volunteers on identifying BEC fraud and phishing. Leverage free resources from organizations like the CyberPeace Institute and the NetHope Digital Leadership Institute.
2. **Enforce Email Security & MFA:** Deploy domain-based message authentication (DMARC, SPF, DKIM) to prevent email spoofing. Require phishing-resistant Multi-Factor Authentication (MFA), such as FIDO tokens, for all administrative access and financial portals.
3. **Establish DFIR Playbooks:** Develop clear Incident Response playbooks tailored to the non-profit's specific critical systems. Knowing exactly who to call, how to contain a breach, and how to communicate with donors minimizes downtime and preserves organizational trust.
4. **Conduct Regular Risk Assessments:** Utilize free, official frameworks like the NIST Cybersecurity Framework or the Nationwide Cybersecurity Review to identify vulnerabilities before threat actors do.

Intelligence Sharing & Resources

Charities do not have to navigate the cyber threat landscape alone. Several global organizations provide free tools and intelligence to the non-profit sector:

- **CyberPeace Institute:** Delivers free cybersecurity assistance, self-assessment tools, and awareness training specifically tailored to NGOs.
- **Preventing Charity Fraud:** Offers helpsheets, webinars, and templates to strengthen charity defenses against financial fraud and BEC scams.
- **CISA Cyber Hygiene Services:** The US Cybersecurity and Infrastructure Security Agency provides free vulnerability scanning and testing services to help organizations reduce their exposure to ransomware.
- **NCSC:** The UK National Cyber Security Centre provides practical incident management and cybersecurity guidelines for small-to-medium enterprises and charities.

Cowbell: The Sound Approach to Risk

Cowbell delivers insurance that cuts through complexity and adapts as risks evolve. With streamlined quoting, expert guidance, and protection designed for the realities of today's threats, we make coverage easier to understand and more reliable when it matters most. Behind it all is the Hum—our constant, quiet vigilance—building stronger businesses, trusted partnerships, and the quiet confidence to keep moving forward.

cowbell®

US0068 0626