



INVENIRE RISK

WHITE PAPER / OCTOBER 2025

Cyber risk trends in Europe

Amid geopolitical
instability

Building resilience for NGOs, SMEs and public sector
organisations

TECHNICAL RESILIENCE

ORGANISATIONAL STRATEGY / GOVERNANCE & POLICY

Risk expertise. Connected.

Inside this paper

A practical guide for organisations protecting essential services, sensitive information and public trust.

Introduction	3
Geopolitical drivers of cyber threats in Europe	4
Impact on NGOs, SMEs and the public sector	7
Strengthening technical resilience	10
Adapting organisational strategy	13
Enhancing governance and policy	18
Conclusion	21
Sources and further reading	23

THREE CONNECTED PRIORITIES

- | | |
|----|---|
| 01 | Technical resilience
Strengthen access control, patching, backups, phishing protection and incident response. |
| 02 | Organisational strategy
Sequence urgent actions, medium-term capability building and long-term adaptation. |
| 03 | Governance and policy
Sustain oversight, clear responsibilities, effective policies and assurance. |

About this edition

This edition retains the analysis and historical examples of the October 2025 manuscript. The publication treatment updates presentation and UK spelling; it is not a new threat assessment. The original document is dated 15 October 2025. General information and risk commentary, not legal advice. Implementation and regulatory applicability require an organisation-specific assessment.

Introduction

Europe's cyber threat landscape has been profoundly shaped by recent geopolitical instability. The war in Ukraine, intensifying great-power rivalries, and conflicts in the Middle East have all contributed to a surge in cyber attacks – from state-sponsored espionage to hacktivist disruption – that reach far beyond the conflict zones. In the wake of Russia's invasion of Ukraine in 2022, for example, the volume and variety of cyberattacks escalated significantly, with the ongoing war “continu[ing] to influence the landscape” and fuelling a rise in hacktivist activity. Likewise, hacktivism expanded through new groups aligning with geopolitical causes, and ransomware incidents spiked amid the chaos.

Simultaneously, nation-state actors have become more active and aggressive: one recent global report noted a 150% surge in cyber espionage attacks linked to China in 2024. In late 2023, the eruption of war between Israel and Hamas triggered waves of cyber aggression as well – multiple aid and humanitarian organisations had their websites knocked offline by coordinated attacks within days. These examples underscore that geopolitical strife does not stay confined to the battlefield; it spills into cyberspace and directly impacts organisations across Europe, including non-profits, small businesses, and public sector agencies.

At the same time, these sectors often have limited resources to defend against sophisticated threats, making them attractive targets for both cybercriminals and state-backed hackers. Not-for-profit organisations and charities, for instance, handle sensitive personal data yet typically operate on tight budgets and minimal IT staffing – a combination that can leave them disproportionately vulnerable to cyberattacks^[1]. Public sector bodies and small businesses face similar challenges in balancing mission delivery with cybersecurity investment. The consequences of a successful attack on these organisations are severe: disruption of critical services, financial losses, exposure of sensitive data, and erosion of public trust. In one UK study, 32% of charities reported experiencing a cyber incident in the past year, and among those affected almost all (94%) were targeted with phishing attempts – a reminder that even basic social engineering attacks can seriously impact operations.

Clearly, rising cyber risks driven by geopolitical instability demand a proactive and resilient response from organisations of all sizes.

This whitepaper provides an in-depth look at the major cyber risk trends in Europe amid current geopolitical tensions and offers guidance for NGOs, SMEs, non-profits, and public sector organisations on how to bolster their resilience. It examines how the conflict in Ukraine, evolving U.S.–China dynamics, and Middle Eastern tensions are shaping the threat landscape, and analyses the impacts on key sectors where charitable and public interest organisations operate. Finally, it presents comprehensive guidance in three critical areas – Technical Resilience, Organisational Strategy, and Governance/Policy – to help organisations strengthen their defences and continuity in the face of these challenges. By understanding the threats and adopting best-practice safeguards, even resource-constrained organisations can significantly reduce risk and ensure they can continue their vital work securely despite turbulent market conditions.

02 / THE CONTEXT

Geopolitical drivers of cyber threats in Europe

Fallout from the War in Ukraine

Russia's war on Ukraine has had far-reaching cyber repercussions across Europe. From the outset of the conflict in 2022, Russian state-sponsored hackers and affiliated groups have engaged in campaigns targeting not only Ukraine but also NATO allies and organisations providing aid or support. This war introduced a new era of hybrid warfare where cyber operations accompany kinetic military actions. European governments and critical service providers have been on high alert for spillover attacks – and indeed, a number of incidents have occurred. For example, in the early days of the war, a disruptive attack on a satellite internet provider (Viasat) impacted connectivity in multiple European countries, illustrating how cyber offensives against Ukraine can unintentionally cascade into Europe.

More deliberately, pro-Russian hacktivist collectives have singled out European institutions perceived as supporting Ukraine. In early 2023, the pro-Russia group KillNet called for DDoS attacks on hospitals in Europe (including the Netherlands) as retaliation for Western aid to Ukraine^[2]. Following these calls, hospital websites in the Netherlands and other EU nations were hit with denial-of-service attacks, forcing some offline and disrupting services^[2]. Similarly, the European Parliament's website was temporarily taken down by a KillNet DDoS attack in late 2022 amid votes condemning the invasion. While many of these hacktivist attacks have been relatively unsophisticated (DDoS barrages that cause outages but no lasting damage), they demonstrate how public sector and civil society organisations in Europe have been dragged into the cyber crossfire of the Ukraine war.

Beyond hacktivism, advanced persistent threat (APT) groups tied to Russia continue to conduct espionage and sabotage operations. Ukrainian government and energy networks have been frequent targets, but Russian cyber units have also probed NATO countries' systems – from attempts to phish EU government officials to malware campaigns aimed at critical infrastructure in Poland and Germany. European energy companies and government agencies have had to bolster their monitoring after detecting intrusions linked to suspected Russian actors (for instance, Sandworm and APT28 have long histories of attacking European targets). Notably, information manipulation and influence operations have been a key element of Russia's cyber strategy.

According to EU cybersecurity analyses, propaganda and disinformation campaigns accompanying the kinetic war have “become prominent” components of Russia's aggression. These operations seek to spread false narratives, erode European public support for Ukraine, and sow discord within EU societies. For NGOs and public-sector entities, such influence campaigns can translate into harassment, defacement of websites with propaganda messages, or misinformation that confuses the public (for example, fake social media posts impersonating aid organisations). In short, the Ukraine conflict has elevated the baseline threat level – Europe has seen more frequent cyber attacks of various kinds, and organisations must be prepared for hostile activity ranging from disruptive hacks to subtle information warfare.

At the same time, it is worth noting that the most catastrophic cyber scenarios (e.g. a crippling attack on European critical infrastructure in retaliation for sanctions) have so far been largely avoided or thwarted. Western governments' defensive posture and coordination – such as improved intelligence sharing and

public-private collaboration on cyber threats – have helped contain the worst-case outcomes. Nonetheless, the conflict is ongoing, and Russian attackers (or sympathisers) remain active. The European Union's cyber agency reported in late 2023 that geopolitics continues to have a “strong impact” on cyber operations, with threat actors often driven by political motivations. For the foreseeable future, any spike in East-West tensions related to the Ukraine war could trigger a corresponding spike in cyber incidents targeting European networks, especially in government, defence, energy, and organisations seen as influential on public opinion.

U.S.–China Rivalry and Global Cyber Tensions

The geopolitical friction between the United States and its rivals (notably China, as well as countries like Iran and North Korea) also reverberates in cyberspace, affecting European organisations. China in particular has dramatically expanded its cyber espionage campaigns, aiming at governments and industries worldwide – including in Europe – to gather intelligence and competitive advantage. According to CrowdStrike's intelligence report, China-nexus cyber activity surged by 150% in 2024. This means Chinese state-backed hacker groups ramped up intrusion attempts at a startling rate, often stealing sensitive data or intellectual property. European firms in sectors such as finance, media, manufacturing, aerospace, and industrial technology have been among the targets, with CrowdStrike observing up to a 300% increase in targeted attacks on those industries.

The tactics of Chinese APTs are evolving as well – at least seven new distinct Chinese APT groups were identified in 2024, some with highly specialised techniques. Their operations are shifting from noisy “smash-and-grab” hacks to stealthier, more focused intrusions aimed at long-term espionage goals. For example, suspected Chinese hackers have infiltrated European government agencies to collect diplomatic communications, targeted tech companies to steal research on advanced semiconductors, and breached cloud service providers to exploit trusted access into client networks. This rise in state-sponsored spying is linked to geopolitical moves – as the U.S. and Europe restrict technology exports to China and deepen strategic alliances, Chinese intelligence units are redoubling efforts to acquire strategic information by cyber means.

European organisations, even small NGOs or public bodies, may inadvertently hold data of interest (think of an NGO working on human rights in China, or a university research project on AI). Thus, being in Europe is not immunity from cyber espionage – global politics can put a target on one's back if the organisation's information or partners intersect with great-power interests.

Meanwhile, other adversarial states also contribute to the threat landscape. Iranian cyber units have conducted aggressive campaigns ranging from espionage against European governments and NGOs (especially those involved in Middle East policy or Iranian human rights issues) to destructive attacks on Israeli or Gulf-related targets that can have wider fallout. North Korea's cyber operations – often financially motivated due to sanctions – have hit global NGOs, cryptocurrency firms, and even healthcare organisations to steal funds or data, which sometimes impacts European entities. Additionally, the United States' own cyber posture and actions (such as indicting foreign hackers, or its cyber operations against adversaries) can lead to retaliation against US allies.

For instance, when Western law enforcement took down major cybercriminal infrastructure (like the Hive ransomware network in early 2023), there were concerns of retaliation hacks broadly against Western targets. European networks must therefore brace for blowback from global cybercrime crackdowns and geopolitical confrontations that they may have little direct role in. In summary, “American geopolitics” – encompassing great-power tech competition, sanctions, and military alliances – manifests as increased cyber threat activity in Europe. Organisations need to be aware that sophisticated attackers from China,

Iran, North Korea and other states are actively probing for weaknesses, and their motivations can extend beyond immediate financial gain to long-term strategic objectives.

Middle East Conflict and Hactivist Spillover

The flare-up of conflict between Israel and Hamas in October 2023 quickly spilled into the digital realm, unleashing a wave of hacktivism and cyber attacks that reached Europe and beyond. Within minutes of the initial Hamas attacks, pro-Palestinian hacktivist groups began flooding Israeli websites with DDoS (Distributed Denial of Service) attacks, aiming to knock critical services offline. In the days and weeks that followed, cybersecurity observers tracked an explosion of cyber activity associated with the war: at least 90 pro-Palestinian hacking groups and 23 pro-Israeli groups became active, defacing websites, conducting DDoS assaults, and attempting data breaches as forms of protest or retaliation.

Notably, European organisations became collateral targets in this frenzy. Some pro-Palestinian threat actors broadened their attacks to any entities perceived as supporting Israel – for example, they hit websites of global companies and media outlets reporting favourably on Israel, some of which were European. On the other side, a few pro-Israel hackers sought to deface sites they associated with Palestinian advocacy in Europe. This chaotic environment illustrated how a regional conflict can ignite cyber operations across continents, driven by loosely affiliated actors rallying to a cause.

Humanitarian organisations and NGOs were directly caught in the crossfire. Reuters reported that the websites of two relief groups providing aid in the Israel-Gaza crisis – United Hatzalah (an Israeli emergency medical charity) and Medical Aid for Palestinians (a British charity assisting Gazans) – were both disrupted by DDoS attacks in mid-October 2023. These attacks, apparently by opposing hacktivist factions, temporarily impeded the charities' ability to collect donations and communicate their mission. "It is beyond disappointing that anyone should wish to disrupt the work of a humanitarian relief organisation, particularly during [an] unprecedented humanitarian crisis," lamented a director at Medical Aid for Palestinians when their site was forced offline.

The tactic of DDoS-ing humanitarian sites – while unsophisticated – shows that even NGOs providing neutral relief may be targeted for symbolic impact. Cybersecurity analysts noted a general pattern of hacktivists focusing on services that people urgently seek during crises: "rescue services, telecom, government services, media – anything that people need at this time" was at risk of DDoS or defacement, according to experts monitoring the Israel-Gaza cyber fallout. European civil society organisations, especially those with any involvement or stance in contentious international issues, must therefore prepare for sudden surges in malicious traffic or hacking attempts when global events spark online mobilisation.

Another striking aspect of the Israel-Gaza cyber conflict was the convergence of hacktivist communities. Some groups that initially formed around the Russia-Ukraine war (like the pro-Russian KillNet collective and its affiliates) turned their attention to the Middle East turmoil, launching attacks against Israeli targets. Also, hacktivists from disparate countries (Morocco, Indonesia, Malaysia, etc.) joined in operations related to the conflict. This blending of hacktivist campaigns means that European organisations could find themselves targeted by an unpredictable mix of actors united by ideology rather than geography. For instance, a European NGO advocating for Middle East peace or a government agency making statements on the conflict might incur the wrath of far-flung hacktivists.

The scale and speed of hacktivist attacks have clearly increased, enabled by readily available tools and global messaging platforms to coordinate actions. Even if these attacks are mostly website defacements or transient outages, they can cause real disruption, stress public sector IT teams, and deflect resources during critical moments.

In summary, the ongoing Middle Eastern tensions reinforce a broader lesson: any major geopolitical event can trigger cyber ripple effects worldwide. Organisations in Europe should monitor international developments and be ready to heighten their cyber defences during periods of heightened conflict. The Israel-Gaza case underlines the importance of having protections (like content delivery networks or DDoS mitigation services) for websites, as well as incident response plans to quickly restore online services. It also emphasises the need for cross-sector information sharing – e.g., governments alerting NGOs about emerging cyber threat campaigns related to global crises.

03 / THE CONTEXT

Impact on NGOs, SMEs and the public sector

Geopolitically driven cyber threats have tangible impacts across multiple sectors, especially those where non-profits, charities, small-to-medium enterprises (SMEs), and public institutions operate. These organisations often provide essential services – from humanitarian aid and healthcare to education and local governance – yet they tend to have constrained budgets and less mature cyber defences, making the consequences of attacks particularly acute.

Non-Governmental Organisations (NGOs) and Charities

NGOs and charitable organisations have become prime targets for certain cyber adversaries. They typically hold sensitive personal data (e.g. on donors, beneficiaries, refugees, or vulnerable populations) and often work in conflict or crisis zones, which can attract espionage or retaliatory attacks. The International Committee of the Red Cross (ICRC) hack in late 2021 was a wake-up call: attackers (later deemed likely state-sponsored) infiltrated a Red Cross subcontractor's servers and stole data on over 500,000 highly vulnerable people – a breach so sophisticated that the ICRC described it as a “highly sophisticated and targeted operation” fitting a nation-state profile. The hackers deliberately targeted databases used for reuniting families separated by conflict.

Such an attack has dire humanitarian implications: it “severely harm[s] the trust relationship” that NGOs like ICRC rely on, and it jeopardises the safety of individuals whose confidential information (e.g. identities of refugees or prisoners of war) could be misused. This example illustrates the high stakes for NGOs – a data breach can literally put lives at risk or derail relief operations. Apart from espionage, NGOs face hacktivism (as seen with Gaza-related DDoS attacks on aid groups) and cybercrime. Criminal ransomware gangs have in some cases hit nonprofits or small charities, either by accident or under the assumption that these organisations might pay to restore critical data.

Unfortunately, many NGOs lack the technical safeguards or incident response plans to recover quickly, meaning an attack can halt their services for days or weeks and cost enormous effort to remediate.

Public Sector Organisations

Government agencies, local authorities, and public service providers in Europe have been consistently in the crosshairs of both state-aligned hackers and cybercriminals. In fact, public administration was the single most targeted sector in Europe in recent threat analyses, accounting for about 19% of reported incidents – the highest of any sector. This is not surprising: public sector entities manage critical infrastructure and citizen data, and disruptions to their systems can have wide impact. We have seen ransomware attacks paralyse city administrations (for example, the city services of Antwerp, Belgium were knocked offline in December 2022 due to a ransomware attack on its IT provider).

Hospitals and public health agencies – which often straddle the line between government and non-profit – have also been frequent targets. In one spate of attacks in 2023, multiple European hospitals' websites were hit by pro-Russian hackers, prompting warnings from national cyber authorities^[2]. Even when these were “just” DDoS attacks that didn't steal data, they interrupted patient services and caused anxiety about system integrity. More nefarious are ransomware or wiper malware attacks against healthcare: such incidents can force hospitals to divert ambulances, delay surgeries, or cancel appointments, directly endangering lives. During the Ukraine war, some Western governments warned that Russia might execute destructive attacks on NATO countries' critical sectors (energy grids, transportation, etc.) – a risk that so far has been limited but remains a concern.

Public sector organisations also contend with cyber-facilitated fraud and theft. For instance, municipalities have been tricked by business email compromise schemes into transferring funds to fraudsters, and school districts have had student data stolen and held for ransom. The UK Charity Commission noted that phishing is the most common cyber-enabled fraud affecting charities, and this likely holds true in the public sector as well, where phishing of staff is often the entry point for breaches. The bottom line is that public entities face a barrage of cyber threats – from espionage (foreign APTs trying to steal government secrets or personal data) to financially motivated crime – and a successful attack can disrupt essential public services, erode citizen trust, and incur significant recovery costs.

Small and Medium Enterprises (SMEs)

SMEs form the backbone of Europe's economy and often collaborate with larger agencies and NGOs, but they too are in attackers' sights. Many SMEs supply goods or services to government or operate in critical supply chains, which makes them potential weak links that sophisticated attackers will try to exploit. For example, a manufacturing SME with unique intellectual property could be targeted by Chinese espionage actors seeking technology secrets. Or a local IT provider for several charities could be compromised to pivot into those charities' networks (supply chain attack). SMEs also suffer heavily from indiscriminate cybercrime like ransomware. Unlike global corporations, an SME might not survive the financial and reputational hit of a major breach.

According to the UK Government's Cyber Breaches Survey, the average cost of a cyber attack for a charity or small business can range from ~£460 up to £9,470 in monetary terms – and that figure doesn't capture the lost productivity and damage to stakeholder confidence. Surveys indicate that while about one-third of charities and small businesses experience a cyber incident annually, many still lack full-time security staff or advanced protections. This gap between threat level and preparedness is exactly what makes SMEs and non-profits “soft targets” in the eyes of attackers.

Overall, the impacts across these sectors include:

Operational Disruption. Whether via ransomware encrypting files or DDoS flooding servers, attacks can force organisations offline. For a charity, that might mean an inability to process donations or deliver aid; for a local government, a shutdown of online public services or even phone/email systems.

Financial Losses. Beyond any ransoms paid, there are costs for incident response, IT repair, legal fees, and regulatory fines. Such expenses can be devastating for nonprofits and small businesses with limited reserves. (E.g., under GDPR, even charities could face fines for a breach of personal data, compounding the financial damage.)

Theft of Sensitive Data. Many NGOs hold personal and demographic information on the communities they serve; public bodies have citizens' data; SMEs might hold client or intellectual property data. Breaches can lead to identity theft, jeopardise beneficiary safety (in contexts like refugee or dissident data), or result in competitive losses for businesses.

Reputational Damage and Erosion of Trust. Trust is paramount for NGOs (donors need confidence to give, beneficiaries to share info) and for public institutions (citizens expect services to be reliable and secure). A highly publicised cyber incident can weaken that trust. As an example, if a charity's donor database is hacked, supporters may hesitate to continue their contributions. If a town's council IT is repeatedly downed by attacks, residents may lose confidence in their administration's competence.

Underreporting and Knowledge Gaps. It is also important to note that many incidents likely go unreported in these sectors – some organisations may be reluctant to disclose breaches for fear of reputational harm or simply may not realise they are obligated to report. The UK Charity Commission has highlighted underreporting as an issue and urges charities to report all fraud and cyber incidents, even thwarted attempts, so that authorities can get an accurate picture of the threat and provide support. Underreporting means that the true scale of impact is probably higher than statistics suggest.

In short, geopolitical cyber threats have made the operating environment riskier for NGOs, SMEs, and public organisations in Europe. These entities must assume that determined cyber adversaries – whether politically motivated or criminal – could target them at any time. The next section of this whitepaper will shift from analysis to action: providing concrete guidance on how such organisations can build resilience through technical controls, sound organisational strategies, and strong governance. By implementing the recommendations that follow, organisations can mitigate the impacts described above and better safeguard their missions during turbulent times.

04 / THE RESPONSE

Strengthening technical resilience

Technical resilience refers to the practical cybersecurity controls and safeguards that organisations can put in place immediately to prevent attacks or limit their damage. Given the current threat landscape, NGOs, SMEs, and public-sector teams should prioritise a set of foundational security measures. Many of these align with best practices recommended by national cyber agencies (for example, the UK's National Cyber Security Centre's guidance for small charities) and can dramatically improve defences even with limited budgets. Key technical controls include:

Implement Multi-Factor Authentication (MFA) Everywhere

A top priority is to secure user accounts with MFA, especially for email, VPN/remote access, and administrator accounts. Stolen or weak passwords are a common path for attackers – in fact, three-quarters of breaches by sophisticated actors involve misuse of valid credentials rather than malware. MFA (such as one-time codes or app prompts in addition to a password) can prevent an attacker from logging in with a stolen password, thereby shutting down one of the most prevalent attack vectors. Every staff email and cloud account for the organisation should have MFA enabled. Where possible, use phishing-resistant MFA (security keys or authenticator apps rather than SMS).

Strong identity management is crucial now that adversaries exploit identity gaps and stolen logins at an alarming rate.

Keep Software Up-to-Date and Patch Critical Vulnerabilities

Regular patching of operating systems, software applications, and devices is essential to block attackers from exploiting known security flaws. Many ransomware groups and state hackers rely on unpatched vulnerabilities to gain initial access. Organisations should enable automatic updates on all systems where feasible, and have an inventory of critical systems to ensure important patches (especially those labelled “high” or “critical” severity) are applied promptly. When major security alerts are announced (for instance, a severe vulnerability in widely used software like Microsoft Exchange or an open-source library), treat it with urgency – apply the vendor fix or workaround as soon as possible.

Timely patching could have prevented numerous breaches, and it's one of the cheapest defences available.

Backup Data Regularly and Maintain Offline Copies

Robust data backup procedures are a lifesaver in ransomware or destructive attack scenarios. Organisations should perform regular backups of key servers, databases, and files – and crucially, keep isolated offline copies of backups that ransomware cannot encrypt. For example, copy backups to external drives or secure cloud storage that isn't continuously network-mapped to primary systems. Test the restoration process periodically to ensure backups are valid. In the event that malware wipes or locks your primary data, having recent backups offline means you can recover without paying ransoms. Aim for the 3-2-1 backup rule: at least three copies of data, on two different media, with one copy off-site/offline.

Backup solutions need not be expensive; even simple automated scripts or basic cloud backup services can do the job for smaller organisations.

Defend Against Phishing and Social Engineering

Since phishing remains the #1 attack vector (94% of cyber attacks on charities involved phishing emails), technical steps to mitigate phishing are vital. Ensure that your email system has up-to-date spam filtering and malware scanning – many cloud email providers offer built-in filtering that should be maximised. Implement DMARC/SPF/DKIM email authentication to reduce spoofed emails appearing to come from your domain. Use web filtering to block known malicious links if possible. Additionally, consider deploying anti-phishing training tools: for instance, there are services that send simulated phishing emails to staff to test and train their responses. While human vigilance is part of organisational measures (discussed later), technology can block a large portion of phishing attempts before they ever reach inboxes.

Some organisations also implement browser extensions or DNS filtering that warn users if they click a suspicious link. Given the prevalence of phishing, every layer of defence (email, web, user awareness) against it is worthwhile.

Secure Configuration and Network Protections

Organisations should harden their systems by removing or disabling unnecessary services, requiring strong passwords, and using firewalls. Ensure that all default passwords (e.g. for routers, databases, or CMS admin accounts) are changed and strong. Configure firewall rules to restrict inbound traffic only to what is needed – for example, if a charity's database should not be accessed from the internet, make sure it's properly firewalled. Segment your internal network if possible: keep critical servers separate from user workstations, so that if one employee's PC is compromised, the attacker cannot easily reach the donor database or email server. Even simple network segmentation (using VLANs or firewall rules between departments) can slow an intruder's progress.

Apply the principle of least privilege – each user or system should only have the access permissions necessary for their role. This limits damage if one account is taken over. For instance, a volunteer's account probably doesn't need administrative rights on the file server; not giving excessive privileges means that account can't be used to do widespread harm.

Deploy Anti-Malware Tools and Enable Logging

Install reputable anti-virus/anti-malware software on all endpoints and keep it updated. Many modern endpoint security tools include behavioural detection that can catch unknown ransomware or trojans by their actions. While no tool is 100% effective, having this layer will stop known threats and flag suspicious activity. Equally important is turning on system logging and monitoring: make sure that important systems (servers, firewalls, etc.) record logs of security events (logins, file access, admin actions). Use a centralised log management if possible, or at least periodically review these logs. Many breaches go undetected for weeks simply because no one is looking at the alerts or system logs.

If budget permits, consider using a managed detection and response (MDR) service or open-source intrusion detection system to alert on strange behaviour (e.g., an employee account logging in at 3 AM from Russia). For small teams, even setting up email notifications for certain admin actions or using free Security Information and Event Management (SIEM) tools can provide insight. The goal is to catch an attack in its early phase (for example, detecting an attacker scanning your network or creating a new user account) before they escalate to full compromise.

Protect Websites and Online Services Against DDoS

Given the uptick in hacktivist-driven DDoS attacks, organisations that rely on public-facing websites or donation portals should prepare for potential denial-of-service attempts. Using a content delivery network (CDN) or a cloud-based DDoS protection service is a highly effective measure. Services like Cloudflare, Azure/AWS front door, or other providers can absorb and filter malicious traffic, keeping your site accessible. Often, these services are inexpensive or even free for non-profits and can be set up with minimal changes (by updating DNS settings). At a basic level, ensure your web host or IT provider has some DDoS mitigation in place. Additionally, have an emergency response plan: if your site goes under attack, know who to call (ISP, security vendor, etc.), and consider temporarily using social media or alternative channels to communicate with stakeholders.

Most DDoS attacks are short-lived, but being prepared can make that downtime even shorter and less impactful.

Encrypt Sensitive Data and Communications

To reduce the impact of a breach, encrypt sensitive data at rest and in transit. Full-disk encryption on laptops and servers ensures that if a device is stolen or an attacker copies data, they can't read it without the key. Use VPN encryption for any remote access or when staff are connecting over untrusted networks. For communications, encourage the use of end-to-end encrypted messaging (for internal discussions or when sharing confidential info with partners). Encryption will not stop an intrusion, but it adds an extra hurdle for attackers trying to leverage stolen data – in some cases making the difference between a reportable breach and a non-incident (if the data was encrypted and unusable to the thief).

Plan and Practice Incident Response (IR)

While this borders on organisational process, it's worth listing as a technical preparedness measure. Have an incident response plan that outlines what to do if various attack scenarios occur (ransomware, website defacement, data breach, etc.). Include technical steps like isolating infected machines, contacting your web hosting provider, or switching to backup systems. Keep an emergency contact list (IT staff, external security consultants, law enforcement, cyber insurance hotline, etc.). Practice the plan with tabletop exercises or drills. The faster and more methodical your technical response, the less damage an incident will cause. For example, if ransomware hits, knowing how to quickly quarantine systems and begin restoration from backups can turn a potential catastrophe into a manageable IT outage.

Many of the above controls align with frameworks such as the Cyber Essentials scheme (in the UK) or the CIS Critical Security Controls. They are considered baseline "cyber hygiene." For NGOs and small organisations, implementing these measures can seem daunting, but guidance is readily available – the UK Charity Commission, for instance, worked with the NCSC to publish concise cybercrime guidance for charities emphasising affordable steps and a culture of awareness. By taking advantage of free resources (like NCSC's "Small Charity Guide" or toolkits from groups like the CyberPeace Institute), even organisations without dedicated IT security staff can put in place strong defences.

The important thing is to start with the basics: access control, patching, backups, phishing protection. These steps address the most common threats. As the saying goes, you don't have to outrun the bear; you just have to outrun the other guy – implementing fundamental security will discourage opportunistic attackers and ensure that you are not the easiest target in the wild.

05 / THE RESPONSE

Adapting organisational strategy

Technology alone is not enough. Building true cyber resilience requires an organisational strategy that adapts over time – balancing immediate actions with medium-term improvements and a sustainable long-term approach. Below, we outline strategic measures in the short, medium, and long term that NGOs, SMEs, and public organisations should pursue to strengthen their security posture amid volatile geopolitical conditions.

Short-term priorities | Next 3–6 months

In the short term, organisations should focus on quick wins and urgent risk mitigations to address the most glaring vulnerabilities:

Perform a Rapid Risk Assessment

Identify your most critical assets and biggest threats. For example, map out what data you hold that might be of interest to state actors (e.g. personal data on activists), or which systems absolutely must stay online (e.g. a hospital's patient management system). Evaluate your current security measures against likely threat scenarios. This doesn't need to be a massive audit – even a focused workshop with IT staff and management can pinpoint gaps. The outcome should be a prioritised list of risks to tackle immediately (such as “our staff email isn't on MFA – fix that now” or “our website is vulnerable to defacement – implement a protection this quarter”).

Improve Security Hygiene and Awareness Right Away

As you implement the technical measures from the previous section, ensure everyone in the organisation is aware of the heightened threat environment. Conduct an immediate awareness refresher training for all staff and volunteers. Emphasise phishing detection (perhaps share recent examples of phishing attempts, especially any that might tie to current events or your sector). Remind people how to report anything suspicious. This doesn't have to be formal; even a short all-hands meeting or an email bulletin with “Top 5 cyber tips” can raise vigilance. Given that many successful attacks start with human error, cultivating a security-conscious culture is a quick win that trustees and managers should champion.

Leadership can set the tone by communicating that cybersecurity is everyone's responsibility in these uncertain times.

Establish Incident Response Basics

If you do not already have an incident response plan, create at least a basic one now. Identify an incident response team or point person (even if that's an external IT provider you will call). Define how to handle common attack types: who would take the lead, how to isolate affected systems, and how to communicate internally and externally. Share the plan with staff so they know whom to alert and how (e.g. “If you suspect a cyber attack, call this number immediately, 24/7”). Also, gather important information in advance: key contacts for cyber incidents (ISP, cyber insurance, local authorities, etc.), backup restoration instructions, and access to critical account credentials in case of emergency.

These steps ensure that when an incident hits, the team can respond swiftly and effectively, minimising confusion and delays.

Engage with External Support and Intelligence

In the short term, connect with resources that can keep you informed about threats and assist if needed. Subscribe to threat alert services (many national CERTs or cybersecurity centres issue free alerts for your sector). For instance, the EU Cybersecurity Agency (ENISA) and country-level agencies (like CERT-EU, NCSC in the UK, BSI in Germany, etc.) often share warnings about active campaigns (such as state-sponsored phishing targeting NGOs). Make sure you are on these mailing lists or portals. If feasible, reach out to peer organisations – for example, other NGOs in your network – to share information about any suspicious activities (this can informally form a support community).

Short-term, you might also consider pro bono or low-cost security services: some cybersecurity companies and non-profits offer free security assessments or tools for charities (e.g., scanning your website for vulnerabilities). Taking advantage of these can quickly improve your understanding of your exposure.

Consider Cyber Insurance and Emergency Funding

Finally, as a short-term risk transfer measure, evaluate if cyber insurance is appropriate for your organisation. Cyber insurance can provide access to incident response experts and financial coverage for certain losses. Policies for small organisations are not overly expensive, and given the rising risks, this safety net could be worthwhile. That said, insurance is not a substitute for good security – insurers will expect you to have basic protections in place and may not pay out if negligence is found. If insurance isn't an option, at least plan financially for incidents: set aside an emergency fund (even a modest amount) for cybersecurity response, so that paying for a clean-up or legal advice doesn't completely derail your budget.

Medium-term strategy | Next 6–18 months

In the medium term, organisations should take a more structured and strategic approach to cybersecurity, integrating it into business plans and projects:

Develop a Formal Cybersecurity Strategy or Improvement Plan

Based on the initial risk assessment and any gaps identified, craft a plan that outlines how you will raise your cybersecurity maturity over the next year or so. This might include projects like migrating to a more secure cloud setup, implementing a new identity management solution, obtaining a security certification, or increasing staff training frequency. Set achievable goals for each quarter (for example, “Q1: enable MFA for all systems and finish network segmentation; Q2: conduct a third-party security audit and implement recommendations; Q3: run a cyber incident simulation exercise; Q4: achieve compliance with XYZ standard”). A written strategy, approved by leadership, helps ensure cybersecurity remains a focus even as other priorities compete for attention.

It also signals to funders or stakeholders that you are taking the issue seriously.

Invest in Training and Building Expertise

Over the medium term, allocate resources to deepen the cybersecurity knowledge within your organisation. This can involve sending IT staff (or whoever manages your systems) for specialised training or certifications, so they can better handle threats. It also includes establishing a regular security awareness programme for all employees – not just a one-off, but ongoing education. Many organisations do brief quarterly refreshers or use automated phishing email tests to keep people on their toes. The goal is to embed security into the organisational culture: clicking on strange links should become as taboo as not wearing an ID badge in the office.

Employee vigilance is a critical layer of defence, especially against social engineering, so continuous education is key.

Strengthen Vendor and Supply Chain Security

As you improve internal defences, don't overlook the security of third-party providers and suppliers. Medium-term, introduce processes to vet the cybersecurity of any critical vendors (e.g., cloud hosts, payment processors, IT consultants). Include cybersecurity expectations in contracts – for example, require that vendors notify you of their own breaches or have certain certifications. If you are a smaller NGO relying on a volunteer web developer or a small MSP (Managed Service Provider), have a frank discussion about how they are protecting your data. Supply chain attacks have risen, so an adversary might try to compromise your organisation through a weak link like a shared IT service.

Therefore, start maintaining an inventory of key suppliers and assess their risk. Simple steps include: using trusted, well-known providers for critical services; keeping software supply chain (plugins, open-source libraries) updated; and avoiding or tightly controlling remote access tools that vendors use (ensure they use MFA too).

Adopt Security Frameworks or Certifications

Aim to benchmark and formalise your cybersecurity practices by aligning with a recognised framework. For instance, an SME or charity could pursue Cyber Essentials certification (in the UK) which verifies that basic controls are in place. Larger organisations might aim for ISO 27001 (an information security management standard) or implement the NIST Cybersecurity Framework's recommendations. In the public sector, many will need to comply with the EU's NIS2 Directive and related national laws which mandate risk management measures and incident reporting for essential services. Embracing these frameworks in the medium term will not only improve your security systematically but also ensure governance accountability and regulatory compliance.

For example, NIS2 requires organisations in sectors like health, transportation, water, energy, and public administration to implement minimum technical measures (such as access control, encryption, incident response planning) and could hold management liable for non-compliance. Preparing for such requirements by gradually upgrading your policies and controls is a prudent medium-term strategy.

Enhance Detection and Response Capabilities

With basic protections in place from the short term, the medium term is when you elevate your ability not just to prevent, but to detect and respond to threats. This might involve deploying more advanced monitoring tools or services. Some organisations subscribe to threat intelligence feeds relevant to their sector, so they get alerts on specific threats (e.g., a charity might get intel about a phishing campaign targeting NGOs). Others might contract a part-time security monitoring service or join an Information Sharing and Analysis Centre (ISAC) if one exists for their sector. For instance, the healthcare sector often has ISACs that share real-time threat info.

Medium-term, you should also refine your incident response processes through drills. Consider performing a simulated cyber incident (tabletop exercise) with key staff and leadership to practice decision-making under a cyber crisis scenario. This helps iron out roles and communication paths before a real incident hits. Essentially, move from a reactive posture to a proactive and prepared stance.

Communicate and Integrate Security into Organisational Planning

During medium-term implementation, make sure cybersecurity is not siloed as an “IT issue.” It should be discussed in management meetings and integrated into project planning. For example, if you’re launching a new programme that involves collecting data on beneficiaries, incorporate the IT security team’s input from the design phase (privacy considerations, secure data storage, etc.). If you’re planning an expansion to a new region, assess if that region poses unique cyber risks (maybe new threat actors or compliance needs). The more security is woven into the fabric of the organisation’s projects, the less likely that glaring holes will be left open.

This period is also a good time to engage with your board or trustees on the topic – provide them updates on what’s being done to mitigate cyber risks, so they are kept in the loop and can support resource allocation. Many boards now recognise cyber risk as a top-tier organisational risk (akin to financial or reputational risk), and keeping them informed helps ensure sustained commitment.

Long-term strategy | 18 months and beyond

In the long run, the goal is to make cybersecurity part of the organisation’s DNA and resilience strategy, so that it evolves with emerging threats and technologies:

Establish a Cybersecurity Governance Structure

For long-term sustainability, define clear governance for cybersecurity. This could mean having a dedicated cybersecurity or IT risk committee at the board level, or assigning a member of senior management as the accountable “Cybersecurity Champion”. Larger organisations might hire a Chief Information Security Officer (CISO) or assign security responsibilities to an existing executive. Smaller ones may continue to rely on external expertise, but they should at least have an internal point of contact who liaises with external IT/security providers and keeps leadership apprised. Governance also means setting metrics and reporting mechanisms: e.g., the board receives a quarterly cyber risk report, including any incidents or number of phishing attempts blocked, etc.

Making cybersecurity governance formal ensures ongoing oversight and continuous improvement, rather than a one-time effort.

Continuously Update Policies and Procedures

Over the long term, all the policies you develop (acceptable use, incident response, data protection, etc.) should be living documents. Set a schedule to review and update them annually or whenever a major change occurs (like a new data regulation or a new type of threat). For example, if AI-driven social engineering becomes prevalent, update your policies/training to cover how to verify identities in communications. Ensure that new employees are onboarded with these policies in mind (security briefing as part of orientation) and that departing employees are offboarded securely (removing access promptly). Long-term resilience is about institutionalising these practices, so that even if key staff leave, the processes remain.

Invest in Advanced Tools Judiciously

As technology evolves, consider which advanced cybersecurity solutions might benefit your organisation and plan for them in your IT roadmap. This could include things like zero-trust network architecture (which, for instance, continually verifies users and devices, minimising implicit trust on internal networks), more sophisticated endpoint detection and response (EDR) tools, or cloud security posture management if you heavily use cloud services. However, avoid chasing shiny new tech for its own sake – each investment should address a clear need or gap identified in your risk management. Long-term planning also involves budgeting for the lifecycle of systems: legacy systems often pose security risks (as they stop receiving updates), so have a strategy for phasing out or isolating legacy IT.

For example, many public sector bodies still have some old applications – if you can't replace them immediately, plan mitigations (like network isolating them) and work toward replacement in the long run.

Scenario Planning and Resilience Building

Expand your thinking beyond just cyber attacks to overall operational resilience. Conduct scenario planning for worst-case situations – e.g., “What if we faced a coordinated attack during a geopolitical crisis that takes out our communications and leaks sensitive data?” By gaming out extreme scenarios, you can identify additional resilience measures: perhaps having backup communication methods (like SMS alerts or public hotlines if email is down), or relationships with partner organisations that can step in to assist if you are hit. Incorporate cyber incidents into your broader business continuity and disaster recovery planning. After the experiences of the past few years, many organisations realise that continuity plans must account for things like prolonged IT outages or loss of data integrity due to cyber incidents.

Make resilience an organisation-wide priority: everyone should know that if something bad happens, there is a plan to keep critical services running, even if that means reverting to manual processes temporarily.

Stay Informed and Adaptable

The threat landscape in 3-5 years may look very different (consider how five years ago, ransomware was a nascent threat and “hacktivism” was less pronounced – now they dominate headlines). So, commit to staying informed about cybersecurity trends and adapting accordingly. This could mean maintaining membership in industry groups, attending occasional security webinars or conferences relevant to your sector, or simply setting aside time for your IT/security staff to research and update their knowledge. Encourage a mindset of continuous learning and adaptation. For example, if artificial intelligence (AI) starts enabling more convincing phishing or automated attacks, be ready to train staff on that and explore AI-based defensive tools.

In the long run, organisations that treat cybersecurity as an ongoing journey – not a one-time project – will be best positioned to handle whatever new threats emerge.

In sum, an effective organisational strategy for cyber resilience is multi-layered and phased. Start with urgent fixes and awareness in the short term, build out structured programmes and partnerships in the medium term, and solidify governance and adaptive capabilities for the long term. This strategic approach ensures that improvements are sustained and that the organisation is not just reacting to the latest crisis, but proactively preparing for the future. As one security adage goes, “Hope is not a strategy” – instead of hoping not to be attacked, organisations must plan and act in advance, given the inevitability of threats in today's landscape.

06 / THE RESPONSE

Enhancing governance and policy

Governance and policy form the foundation of a resilient cybersecurity posture, ensuring that there is accountability, clarity, and alignment with laws and best practices. For NGOs, charities, SMEs, and public bodies, establishing strong governance means that cybersecurity is managed at the highest levels and integrated into organisational policy frameworks. Below are key considerations for improving governance and policy in light of the cyber risks we have discussed:

Board and Leadership Oversight

It is crucial that top leadership (board of directors, trustees, or senior executives) actively oversees cyber risk management. Cybersecurity should be a regular item on the agenda of board meetings or leadership team meetings. Leaders do not need to be technical experts, but they do need to ask the right questions and set expectations. For example, boards should ask: What are our top cyber risks? What are we doing to mitigate them? When was our last security assessment? The tone from the top matters; if the board prioritises cybersecurity, the rest of the organisation will follow. The UK Charity Commission explicitly reminds trustees that “it is every trustee’s responsibility to ensure they’ve done all they reasonably can to protect their charity from harm”, and this ethos applies broadly – leadership must treat cyber threats as seriously as any other strategic risk.

Many organisations are now including cybersecurity in their annual reports or risk disclosures, highlighting that it’s being governed at the highest level.

Clear Policies and Procedures

Develop a suite of security-related policies that outline expected behaviour and processes. Key policies typically include:

Acceptable Use Policy. defining how employees, volunteers, or partners can use organisation IT assets (e.g., rules about using work email, installing software, using personal devices, etc.).

Access Control Policy. covering how access rights are granted and revoked, password management rules, and MFA usage requirements.

Data Protection and Privacy Policy. detailing how sensitive data (personal data of beneficiaries, donors, etc.) is handled, in compliance with regulations like GDPR. Remember, under GDPR, charities and companies must protect personal data and report certain data breaches within 72 hours to authorities, so your policy should include breach notification procedures.

Incident Response Plan/Policy. a document that guides the incident handling process (which we discussed earlier), including communications strategy (who communicates with the public, with law enforcement, etc. in a breach scenario).

Business Continuity/Disaster Recovery Plan. covering how to restore operations after major disruptions, including cyber incidents.

Vendor Management Policy. if not separate, incorporate in another policy how third-party risks are managed (security requirements for vendors).

These policies should be tailored to your organisation’s size and complexity – a small NGO may keep them simple – but they should provide enough guidance that there’s no confusion about roles or

procedures. For example, a good incident response policy will clearly state when an incident must be escalated to management or when law enforcement should be contacted. Having these policies in writing also enforces consistency: new staff can be given the policies to read, and everyone knows the rules of the road. Make sure policies are communicated and easily accessible (e.g., on an intranet or in an employee handbook).

Assign Roles and Responsibilities

Governance means defining who is responsible for what in the realm of cybersecurity. Identify the person or team responsible for managing day-to-day security (it could be an IT manager wearing the security hat). Identify who is the Data Protection Officer (if required by GDPR, some organisations need a formal DPO). For larger entities, form a cross-functional cybersecurity committee that includes IT, operations, HR, and executive representation – this ensures different perspectives in decision-making and that security isn't isolated. Importantly, specify escalation paths: staff should know how to report security issues (and that they won't be penalised for reporting accidental clicks or mistakes – a just culture is important so issues aren't hidden).

Likewise, if a serious breach occurs, it should be clear which senior executive becomes the incident manager and which board member is the liaison. By clarifying roles, you avoid paralysis during incidents and embed security into job duties. Some charities have even added cybersecurity responsibilities into certain job descriptions (e.g., the finance director might also oversee fraud and cyber risk, given the overlap with fraud cases).

Regulatory Compliance and Legal Obligations

Ensure your governance framework accounts for all relevant cyber and data protection regulations in your jurisdiction and sector. In Europe, the foremost is the General Data Protection Regulation (GDPR), which applies to any organisation processing personal data – this means you must implement appropriate security controls to safeguard personal data and follow breach reporting rules.

Non-compliance can lead to hefty fines, so treat data protection as a board-level compliance issue.

Additionally, the new NIS2 Directive in the EU (and similar national laws) expands the set of organisations that must adhere to specific cybersecurity measures and incident reporting. Public sector organisations and many mid-sized companies in sectors like health, transport, water, energy, and digital services are covered.

Governance should ensure that the organisation conducts a gap analysis against these requirements and addresses any deficiencies. For example, NIS2 mandates that management bodies approve cybersecurity risk measures and can be held accountable for breaches – so boards may need training on these duties. There may also be sector-specific regulations (financial services, for instance, have their own cyber rules; the healthcare sector might have patient data security requirements beyond GDPR). An emerging area of compliance is the expectation to report cyber incidents to authorities beyond just privacy breaches – some countries are setting up central reporting for any significant cyber attack (for instance, in the UK, certain charities might be expected to report incidents to the Charity Commission, which as noted has guidance on what to report).

Make sure someone in governance is tasked with keeping track of these obligations and that your incident response plan includes when to notify regulators or law enforcement.

Establish an Internal Culture of Cyber Awareness and Ethics

Governance is not just paperwork – it's also about setting values and culture. The board and senior leaders should promote an ethical, vigilant culture regarding cybersecurity. This means encouraging transparency (report mistakes, report near-misses), emphasising that security is integral to the mission (e.g., a charity cannot help others if its systems are compromised), and allocating time and budget to security initiatives. Leadership should support initiatives like regular training, drills, and perhaps even incentives for good security practices (some organisations do fun competitions or recognise employees who report phishing emails, etc.). When employees see that top management cares about and invests in cybersecurity, they are more likely to take it seriously too.

Creating a cyber-aware culture has been highlighted by regulators as a key defence. This could involve simple practices like including a cybersecurity tip in each staff newsletter or having an annual “cybersecurity month” with events or challenges.

Coordination with Stakeholders and Partners

Many NGOs and public sector bodies work in partnership with other organisations. Governance should extend to how you handle cybersecurity in those relationships. For instance, if you are a sub-grantee to a larger NGO, do you have agreements on data handling and breach notification between you? If you're a local government collaborating with a national agency, are there protocols to share cyber threat information? At the governance level, try to formalise such cooperation. One useful step is to sign up for any information-sharing forums or emergency support networks relevant to your sector. There are initiatives where, say, NGOs can quickly get help from volunteer cybersecurity experts in a crisis (the CyberPeace Institute runs a “CyberPeace Builders” programme offering free assistance to NGOs, for example).

Knowing these resources and weaving them into your policies (e.g., your incident response policy might note that you can reach out to X partner or Y emergency hotline) is wise.

Audit and Accountability

Incorporate cybersecurity into your audit and assurance processes. This could mean commissioning periodic independent security audits or penetration tests to get an objective view of your defences. It also means tracking internally whether policies are being followed. For example, perform periodic checks that user accounts are being disabled when employees leave (a common policy that sometimes falls through the cracks). If you have a risk register (a common governance tool listing all key risks), ensure cyber risks are included and updated regularly. The board should receive reports on these – e.g., an annual cybersecurity report summarising incidents, improvements made, audit findings, and plans.

An effective governance approach treats cybersecurity as an ongoing cycle of assess -> improve -> monitor -> report. If something goes wrong (like a breach), do an after-action review and feed the lessons back into policy updates and training. This continuous improvement loop is crucial for accountability. In some cases, regulators or donors might ask for evidence of your cybersecurity measures – having this documented trail of governance actions, policies, and improvements will demonstrate your commitment and diligence.

In conclusion, robust governance and clear policies are what bind all other cybersecurity efforts together. They ensure there is leadership buy-in, structured management, and compliance with external requirements. Especially in an era of heightened cyber threats, regulators and stakeholders expect organisations to have more than ad hoc defences – they expect to see governance frameworks in place. As one example, when the UK Charity Commission refreshed its guidance in 2024 amid rising cyber incidents, it stressed that trustees must foster a culture of awareness and use available guidance to

protect their charity. Governance is about doing exactly that: setting the tone at the top, formalising the approach, and making sure that when lightning strikes – be it a state-sponsored hack or a criminal scam – the organisation is not caught rudderless.

With the right governance, even smaller entities can punch above their weight in cybersecurity, because they will react in a coordinated, compliant, and thoughtful manner, rather than in panic.

07 / THE TAKEAWAY

Conclusion

The convergence of geopolitical conflicts and cybersecurity has made the past few years some of the most challenging on record for organisations operating in Europe. The war in Ukraine, escalating great-power cyber competition, and flashpoints like the Israel-Gaza conflict have all contributed to a threat environment where no organisation can afford complacency. NGOs, SMEs, charities, and public sector agencies – often on the front lines of serving communities – find themselves facing threats ranging from state-backed espionage and disruptive hacks to financially motivated cybercrime and ideologically driven attacks. While the situation is undoubtedly serious, this whitepaper has illustrated that there are practical steps and strategies to manage and mitigate these risks.

By understanding the trends – how geopolitical instability fuels cyber attacks and which sectors are most affected – organisations can better anticipate what might come next. More importantly, by following the guidance on technical controls, strategy, and governance, even resource-limited organisations can significantly harden their defences. Technical resilience measures like MFA, patching, backups, and phishing protection form a crucial first line of defence that addresses the most common attack vectors. An adaptable organisational strategy ensures that cybersecurity improvements are not one-time fixes but an evolving programme – with immediate actions to tackle urgent issues, medium-term plans to build capability, and long-term integration of security into the organisational fabric.

Strong governance and policy provides the oversight, accountability, and cultural emphasis needed to sustain these efforts, aligning them with legal requirements and instilling cyber awareness from the boardroom to the frontline.

Building cyber resilience is an ongoing journey. There may be setbacks – almost every organisation will experience some cybersecurity incident eventually. However, resilient organisations respond and recover with minimal damage. They learn from incidents and continuously improve. They also recognise that cybersecurity is not just an IT issue, but a fundamental aspect of risk management and ethical responsibility in the digital age. A cyber attack on a charity or public service is an attack on the community it serves; by protecting itself, the organisation protects its stakeholders.

In practical terms, leaders of NGOs and public institutions in Europe should take away the following key points from this discussion:

- Stay alert to geopolitical developments and related cyber threats – if tensions rise, be ready to increase your cyber monitoring and vigilance.
- Focus on cyber hygiene – basic measures stop the majority of attacks, and many resources exist (often free) to guide implementation.
- Empower your people through training and clear policies – humans can be the weakest link or your strongest asset, depending on how well they are prepared.
- Engage with peers, authorities, and experts – you are not alone in this; share information and seek help when needed (early reporting of incidents can often reduce harm).
- Embed security into organisational values and plans – make it part of “the way we do things,” supported by management and checked by governance.

Resilience in the face of cyber uncertainty is achievable. Europe's organisations have shown remarkable adaptability through recent crises, from the COVID-19 pandemic to the Ukraine refugee emergency; cybersecurity is another field where that adaptability must be applied. By taking action now, guided by reputable practices and informed by the latest threat intelligence, NGOs, SMEs, and public sector entities can withstand and weather the cyber storms stirred up by global instability. In doing so, they ensure that their crucial missions – whether it's humanitarian relief, social support, healthcare, education, or governance – can continue uninterrupted, maintaining the trust of those who rely on them.

This whitepaper has drawn on a range of expert sources and reports to provide the most up-to-date insights and recommendations. For further reading and detailed guidance, please refer to the cited sources and the additional resources below.

08 / REFERENCE

Sources and further reading

European Union Agency for Cybersecurity (ENISA), Threat Landscape 2023 – Key findings on top threats, affected sectors, and geopolitical influences.

CrowdStrike, 2025 Global Threat Report – Surge in nation-state cyber operations (notably 150% increase in China-nexus espionage) and evolving attacker tactics.

Reuters (Oct 2023), “Hackers hit aid groups responding to Israel and Gaza crisis” – Report on DDoS attacks against humanitarian NGOs during the Israel-Hamas conflict.

CyberPeace Institute (Nov 2023), “Escalation of Threats in the Middle East” – Analysis of cyberattack trends (DDoS, defacements) amid the Israel-Palestine hostilities, and involvement of hacktivist groups.

UK Charity Commission (Nov 2024), press release “Regulator refreshes guidance as it reveals 600 cases related to fraud in the last year” – Statistics on cyber incidents in the UK charity sector and emphasis on trustee responsibilities^[3].

Armstrong Watson (Dec 2024), “The importance of cyber security for the not-for-profit sector” – Overview of risks facing charities, with UK Cyber Breaches Survey stats (32% charities hit by cyber attack, phishing prevalence).

Devex (Feb 2022), “Exclusive: ICRC says cyberattack was ‘state-like’ in nature” – Details of the Red Cross breach and its implications for humanitarian sector.

Dutch NCSC (July 2023), Cyber Security Assessment Netherlands 2023 – Noted incidents like pro-Russian hacktivists targeting European hospitals in retaliation for Ukraine support^[2].

These sources and others provide deeper context and practical checklists for organisations aiming to enhance their cyber resilience. By leveraging such knowledge and fostering a proactive security culture, organisations in Europe can face the future with greater confidence – prepared, resilient, and steadfast in pursuing their critical missions despite the geopolitical headwinds.

Linked references

[1] Armstrong Watson — The importance of cyber security for the not-for-profit sector

[2] NCTV — Cyber Security Assessment Netherlands 2023 (PDF)

[3] UK Charity Commission — Regulator refreshes guidance on fraud and cybercrime

INVENIRE RISK

Risk expertise. Connected.

invenirerisk.com/contact | info@invenirerisk.com

October 2025 edition. Published in this branded format in October 2026. The sources above are retained from the supplied manuscript; no later developments have been substituted.