Non-Profit Incident Response Playbook: A Step-by-Step Guide for Cyber Crisis Readiness

A Comprehensive Playbook for Non-Profit Executives by centrexIT

Version 1.1

Published June 2025

Executive Summary

For non-profit organizations, maintaining operations and donor trust in the face of cybersecurity threats is paramount. This "Non-Profit Incident Response Playbook" by centrexIT provides a practical, step-by-step guide to building a basic framework for cyber crisis readiness. It emphasizes equipping your team with a clear plan to minimize damage, accelerate recovery, and preserve trust during a cybersecurity emergency. The playbook highlights the impossibility of preventing all attacks, stressing that effective response is the best defense. It outlines four key phases: Preparation (before an incident), Detection & Containment (during an incident), Eradication & Recovery (after containment), and Post-Incident Activity (after recovery). By following the principles of simplicity, clear role assignment, transparent communication, regular testing, and a focus on mission continuity, non-profits can significantly reduce the impact of a cyberattack. The guide also underscores the importance of proactive security measures and knowing external resources, offering centrexIT's expertise for comprehensive cybersecurity assessments and tailored incident response strategies.

Key Terms and Acronyms

- Cybersecurity Incident: An event that compromises the confidentiality, integrity, or availability of an information system or the data it contains. This can include, but not limited to, data breaches, ransomware attacks, or phishing scams.

- Ransomware: A type of malicious software that encrypts a victim's files and demands payment to decrypt them.

- Phishing: A fraudulent attempt to obtain sensitive information or data, such as usernames, passwords, and credit card details, by disguising oneself as a trustworthy entity in electronic communication.

- MFA (Multi-Factor Authentication): An authentication method that requires the user to provide two or more verification factors to gain access to a resource such as an application, online account, or VPN.

- PII (Personally Identifiable Information): Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual.

- CRM (Customer Relationship Management): A technology for managing all your company's relationships and interactions with customers and potential customers.

Non-Profit Incident Response Playbook: A Step-by-Step Guide for Cyber Crisis Readiness

For non-profit organizations, every moment counts when serving your community. A cybersecurity incident—whether a data breach, ransomware attack, or phishing scam—can quickly disrupt your operations, erode donor trust, and divert critical resources from your mission. While preventing all attacks is impossible, being prepared to *respond* effectively is your best defense.

This "Non-Profit Incident Response Playbook" is a practical, step-by-step guide designed to help your organization build a basic framework for cyber crisis readiness. It’s not about complex technical jargon; it's about equipping your team with a clear plan to minimize damage, recover quickly, and maintain trust during a cybersecurity emergency.

Why Your Non-Profit Needs an Incident Response Plan

- **Minimize Damage:** A defined plan helps you contain an incident quickly, preventing it from spreading and causing more harm.
- **Faster Recovery:** Knowing exactly what to do reduces downtime and accelerates your return to normal operations.
- **Protect Reputation & Trust:** A transparent and well-managed response can preserve donor confidence and community trust.
- **Ensure Compliance:** Many data privacy regulations require a documented incident response process.
- **Reduce Financial Impact:** Proactive planning often leads to lower recovery costs.

Key Principles of Incident Response for Non-Profits

1. **Keep it Simple:** Start with a basic plan that everyone can understand and follow. You can refine it over time.

2. **Assign Roles:** Clearly define who does what, even if it's just a small team.

3. **Communicate Clearly:** Both internally and externally. Transparency (when appropriate) builds trust.

4. **Test & Review:** A plan is only good if it works. Practice it periodically.

5. **Focus on Mission Continuity:** How quickly can you get back to serving your beneficiaries and managing donations?

Your Non-Profit Incident Response Playbook: Steps to Take

Phase 1: Preparation (Before an Incident)

This is the most critical phase. Doing this groundwork saves immense stress and resources later.

1. **Form a Core Response Team:**

   * **Action:** Identify 2-5 key individuals with different skills. (e.g., Executive Director, IT lead/point person, Communications lead, Legal/Compliance, Finance).

   * **Responsibility:** Who is the primary contact for initial reports? Who leads the response?

   * **Contact Info:** Create a physical (printed) list of team members' contact information, including personal phones/emails, in case digital systems are compromised.

2. **Identify & Prioritize Critical Assets:**

   * **Action:** List your most vital data (donor database, financial records, beneficiary PII) and systems (online donation platform, CRM, email server).

   * **Responsibility:** These are the "crown jewels" to protect and recover first.

3. **Implement Foundational Security Measures (Proactive Prevention):**

   * **Action: Regular Backups:** Ensure all critical data is regularly backed up to an off-site, immutable location and *test* restorations.

   * **Multi-Factor Authentication (MFA):** Enabled for ALL accounts (email, cloud, CRM).

   * **Security Awareness Training:** Ongoing for ALL staff and volunteers (phishing, safe Browse).

   * **Software Updates:** Keep all operating systems and applications patched.

   * **Antivirus/Endpoint Protection:** On all devices.

   * **Responsibility:** Consistent application of these basics is your first line of defense.

4. **Establish Communication Channels (Internal & External):**

   * **Action: Internal:** How will your team communicate if email is down? (e.g., dedicated secure messaging app, phone tree).

   * **External:** Draft basic templates for potential communications to donors, partners, and regulators. Identify a spokesperson.

   * **Responsibility:** Pre-planning avoids chaotic messaging during a crisis.

5. **Know Your External Resources:**

   * **Action:** Have contact information for:

   * Your IT lead and/or IT support partner (like centrexIT).

   * Cybersecurity legal counsel (if applicable).

   * Your cyber insurance provider (if you have a policy).

   * Relevant law enforcement (FBI, local police if appropriate).

   * **Responsibility:** Don't wait until an incident to find these numbers.

Phase 2: Detection & Containment (During an Incident)

Once an incident is suspected, rapid action is key.

1. Detect & Verify:

* **Action:** How will you know if an incident is occurring? (e.g., suspicious emails reported by staff, unusual system behavior, locked files).

* **Responsibility:** Anyone who suspects an incident *must* immediately report it to the core response team.

2. Isolate & Contain:

* **Action:** The priority is to stop the spread.

    This might involve:

        * Disconnecting infected devices from the network.

        * Changing compromised passwords (especially for administrator accounts).

        * Blocking malicious IP addresses.

        * Taking affected systems offline.

    * **Responsibility:** The IT lead/point person, guided by the response team.

3. Preserve Evidence:

    * **Action:** While containing, try to gather any relevant information (e.g., screenshots of suspicious activity, logs, unusual files).

    * **Responsibility:** This helps experts investigate and learn from the incident.

Phase 3: Eradication & Recovery (After Containment)

Cleaning up and getting back to business.

1. Eradicate the Threat:

* **Action:** Remove malware, close vulnerabilities, and ensure the attacker is completely removed from your systems. This often requires expert assistance.

* **Responsibility:** IT lead/partner.

2. Recover & Restore:

* **Action:** Restore systems and data from clean backups. Verify integrity before bringing systems back online.

* **Responsibility:** IT lead/partner.

3. Post-Incident Analysis:

* **Action:** Once recovered, review what happened, how the plan performed, and what lessons were learned.

* **Responsibility:** Core response team.

Phase 4: Post-Incident Activity (After Recovery)

Learning and rebuilding.

1. Notify Stakeholders (if required):

* **Action:** If sensitive data is compromised, you may have legal or ethical obligations to notify affected donors, beneficiaries, or regulators. Work with legal counsel.

* **Responsibility:** Communications lead, legal/compliance.

2. Enhance Defenses:

* **Action:** Implement lessons learned. Patch new vulnerabilities, update training, and strengthen policies.

* **Responsibility:** Core response team, IT lead/partner.

3. Review & Update Plan:

* **Action:** Update your incident response playbook based on recent experiences and evolving threats.

* **Responsibility:** Core response team.

Don't Wait for a Crisis: Be Prepared

Implementing even a basic incident response plan can dramatically reduce the impact of a cyberattack on your non-profit. It shows responsible stewardship, protects your mission, and builds resilience for the future.

While this playbook provides a solid foundation, developing a strong, tailored incident response strategy and building truly resilient systems often benefits from expert guidance.

Ready to ensure your non-profit is truly prepared for any cyber crisis?

Contact centrexIT for a Cybersecurity Assessment and to develop a tailored Incident Response Plan for your mission.

Strengthening Cybersecurity in the Non-Profit Sector

The regulatory and threat landscapes in the life sciences industry are evolving rapidly, creating new challenges for organizations striving to remain compliant and secure. A proactive and well-aligned cybersecurity strategy is essential—not only for audit readiness, but also to mitigate the risks associated with increasingly sophisticated cyber threats.

To support this need, **centrexIT offers a structured cybersecurity assessment tailored to the unique needs of life sciences organizations**. This playbook is designed to provide clear visibility into compliance exposure and overall security posture.

For more information or to initiate an assessment, contact our team at **(619) 651-8700** or complete the form on our contact page. When using the form, please select "cybersecurity concerns" to help us direct your inquiry efficiently. To ensure your request is routed appropriately, please select "cybersecurity concerns" as your topic of interest.

centrexIT. (2025). *Non-Profit Incident Response Playbook: A Step-by-Step Guide for Cyber Crisis Readiness*. Version 1.1.