Framework to Implement a Cybersecurity Plan

Resource Type: Articles

Topic: Data Privacy, Tech Risk, Cybersecurity

Once organizations understand what cybersecurity is and recognize that it is a threat to their operations, the next step is to assess what cyber risks the organization has. By conducting risk assessments and implementing appropriate protections, organizations can decrease the likelihood of a cybersecurity attack. Additionally, the risk assessment process often increases communication within an organization, at least temporarily, since those facilitating the assessment must speak to employees throughout the organization.

Although many risk assessment guidelines exist, standards based on the National Institute of Standards and Technology (NIST) guidelines are generally considered the best. The NIST Cybersecurity Framework includes five functions[1]:

- **Identify** cybersecurity risks
- **Protect** against potential cybersecurity events
- **Detect** cybersecurity events
- **Respond** to a cybersecurity incident
- **Recover** from a cybersecurity incident

Nonprofits, especially, should be concerned about three categories of risks and threats:

- Reputation – that an account will get compromised to send spam
- Financial – an employee, volunteer, or donor will be tricked into sending money
- Distraction – an employee's system will be compromised through automated tooling, which can cause organizations to deal with disabled systems, ransomware, or wonder what was actually accessed; this all costs a great deal of work and money

To further understand what risks an organization may face, the organization must first begin by identifying the data it collects. NIST defines risk assessments as tools "used to identify, estimate, and prioritize risk to organizational operations (i.e., mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation and use of information systems." To perform a risk assessment, begin by listing all data the organization collects and uses, and then asking who, where, what, and how. For each data type, determine 1) who owns the data, 2) where the data is stored, 3) what the level of sensitivity or confidentiality of the data is, and 4) how access controls and security measures are implemented on the data. Organizations will need to repeat this process for other digital and physical assets, including websites and servers; these assets are vulnerable to cyber-attacks as well. The next step in this process is, for each item on the list, to determine the impact of a cyber breach or attack, and the likelihood of an attack.

The protect step of the framework "supports the ability to limit or contain the impact of a potential cybersecurity event."[2] This includes activities such as training staff on cybersecurity awareness, creating policies and procedures to protect systems and data, and strengthening access control by requiring strong passwords and controlling who has access to data and when. Protecting against potential cyber events translates to proactively implementing security protocols to make an organization's systems and data more difficult for attackers to access. Detecting cybersecurity events is more challenging, as "cybersecurity incidents are often difficult to detect."[3] In fact, attackers reside within a system on average 146 days before being

detected.[4] To effectively carry out this function, organizations should implement continuous monitoring software to alert organizations of any anomalies in the system.

Should an organization fall victim to a cybersecurity attack, the primary goal in responding to the incident is to contain, or prevent the spread and impact, of the attack. Organizations will need to communicate with a variety of internal entities, including legal, HR, and IT, and external entities, including law enforcement, clients, and donors, as appropriate. Organizations must

also analyze how hackers were able to access the system, and update protocols to prevent future attacks. Recovering from a cybersecurity attack requires organizations to restore functionality to the pre-attack state. Organizations that regularly backup data and systems will have an easier time restoring information and operations.

The NIST Cybersecurity Framework is intended to scale with an organization's resources. All organizations should develop the capability to periodically conduct cybersecurity risk assessments, and identify, at least theoretically, steps to be taken if any data or systems are compromised. Using the risk assessment to guide conversations between an organization's IT, finance, programs, and executive leadership, will allow the organization to understand its vulnerabilities and make informed decisions about how much risk to absorb, and how many resources should be expended to mitigate the remaining risks.

This excerpt was originally written and published by NTEN. Risk Management Essential readers can read the full copy in "Cybersecurity for Nonprofits: A Guide." NRMC received permission from NTEN to republish this excerpt.

---

[1] Cybersecurity Framework: The Five Functions.

[2] Cybersecurity Framework: The Five Functions.

[3] Microsoft Inc. Nonprofit Guidelines for Cybersecurity and Privacy.

[4] Microsoft Inc. Advanced Threat Analytics.