*Please Note: Cybersecurity is a rapidly evolving field. This document was last updated on February 2, 2019. Some of the technical guidance within this document may change, and some of the risks defined may increase or decrease in their potential likelihood or impact.*

# Why do Low-Risk Organizations Need Cybersecurity?

A 2018 report from the Public Interest Registry surveyed over 5,300 NGOs and demonstrated that, while nonprofits invest in information technology to conduct mission-critical activities, information security investment continues to be low.[1] Beyond low cybersecurity investment, mission-driven organizations often lack the expertise at the staff level to fend off basic online threats. Connectivity is crucial for organizations with decentralized operations or a wide volunteer base. As a result, organizations establishing such connectivity often ignore many of the basic steps that more technically mature organizations would take to preserve system security (like using formal identity systems or multi-factor authentication) in order to establish an online presence quickly.

They may not be of high risk of a cyberattack, but low-risk organizations are often resource-constrained. Therefore, the loss of control of an organizational bank account, of donor lists, or of important internal documents can have an outsized impact on organizations who otherwise might not consider cybersecurity important to their mission.

Nonprofits and public interest organizations are unlikely to make significant investments in cybersecurity. On average, small nonprofits (defined as organizations with 15 or fewer employees) have one IT person on staff, and the ratios of IT staff to non-technical staff are even more uneven in larger organizations.[2] Given that cybersecurity jobs only account for 11 percent of all IT jobs,[3] the small IT staff of most nonprofits are unlikely to provide much, if any, cybersecurity support. Nonprofits face intense competition to attract IT talent. Some studies have estimated that the global cybersecurity labor market (including both the public and private sectors) will face a shortage of 1.8 million

workers by 2022. [4] Given that 92 percent of nonprofits surveyed in a 2010 study by the John Hopkins Center for Civil Society Studies indicated a lack of funds to be a primary barrier to increasing their organization's IT capacity, it would be unrealistic to expect that these organizations have the capital to compete with the private sector to attract cybersecurity talent. [5] Nonprofits have traditionally used their missions to attract staff at sub-market rates, but still face challenges in recruiting the number of individuals needed to make up this gap.

**What makes an organization "low risk"?**

While many of the basic recommendations in this guide are applicable to all organizations, this guide is designed with "low-risk" organizations in mind. But what does it mean for an organization to be "low risk"? The "Digital Security & Grantcraft Guide" [6] published in early 2017 by the NetGain Partnership provides information for funders about how to evaluate if a grantee organization is at high risk of a cyberattack. Some of the same considerations can be applied to determining if an organization is low risk. The paper describes three basic layers of consideration: "Is the grantee high risk; is the context high risk; is the project high risk?" Each of these questions explores whether or not an element of a funded project or program is more or less at risk of a cyberattack.

Consider the following questions:

- Do you believe your organization is actively at risk of a cyberattack? Are you aware of other organizations like yours that have been actively targeted with a cyberattack?
- Does your work generate controversy, or is it viewed with hostility by government actors, government-backed organizations, or independent malicious actors?
- Are any individuals affiliated with your organization (staff, board members, advisors, etc.) engaged in work or behaviors that might draw the attention of adversaries or malicious actors?
- Do you collect, generate, or otherwise handle sensitive information (such as names, addresses, phone numbers, banking information, gender identity, or

other personally identifiable information) about a vulnerable population, or of interest to an oppressive government or malicious non-state actor?

If the answer to any of the above questions is "yes," your organization is not low risk, and this guide should not be considered sufficient for establishing a baseline security practice. While some of the recommendations in this guide may be useful for high-risk organizations, groups concerned about targeted attacks should consult a cybersecurity specialist, as well as the following resources:

- Electronic Frontier Foundation - Surveillance Self Defense: https://ssd.eff.org/
- Internews - SAFETAG Framework: https://safetag.org/
- Tactical Tech - Security in a Box: https://securityinabox.org/en/

**Organizations who identify as high risk should consult cybersecurity specialists.**

While the contents of this guide offer a baseline for any organization's cybersecurity, they should not be considered a comprehensive set of cybersecurity tools. No organization or system is ever completely "secure" – and those at greater risk must evaluate their context and individual technical circumstances to understand how to best protect themselves from online threats.

> **PLEASE NOTE:** Cybersecurity is a rapidly changing field. Many useful and reliable tools can become obsolete – even to a dangerous degree – overnight as new attacks emerge. The advice and tools offered in this report are considered reliable by the authors and a panel of cybersecurity experts as of February 2, 2019, but as this report ages, readers should consider this advice subject to deprecation.

## Introduction to Cybersecurity

There are a range of formal and legalistic definitions of cybersecurity and information security. An example: "The protection of information and information systems from unauthorized access, use, disclosure, disruption,

modification, or destruction in order to provide confidentiality, integrity, and availability." [7] If this seems incredibly broad – that is because it is. Cybersecurity has become a wide-ranging discipline as the use of information technology has stretched across all corners of our daily lives. Because of its breadth, its rapid evolution, and the sometimes counterintuitive nature of emerging challenges, understanding cybersecurity can feel overwhelming. This can be particularly true for organizations that do not consider cybersecurity to be an integral part of their mission. This section will outline the basic tenets of cybersecurity, and includes some examples to illustrate how cybersecurity disruptions can interfere with mission priorities in organizations that have not historically considered online threats.

***In practical terms, an organization's cybersecurity is its ability to operate information and online technologies safely, accurately, and without interruption or unintended observation.***

Most experts will point to the cybersecurity "objectives" of Confidentiality, Integrity, and Availability, known colloquially as "CIA" or the "CIA Triad." These objectives are not goals, but rather, they describe the characteristics of secure information systems. No system has perfect confidentiality, integrity, or availability. These objectives can be used to articulate how a certain technique, tool, or policy might improve a system's security, or how a system's security might be diminished by an attack. These security-enhancing tools, techniques, or policies are referred to as "controls" - cybersecurity measures that can mitigate risk. The cybersecurity objectives may be briefly summarized as follows [8]:

- Confidentiality: Information is only readable by its intended audience.
- Integrity: Information is accurate and maintained in its intended state.
- Availability: Information is accessible to individuals and systems as intended.

The following sections will further describe these objectives using real-world examples.

**A Note on Privacy**

While this guide is focused on cybersecurity, there are a number of privacy issues that intersect with the security of information systems. Many of the privacy issues highlighted in the news are related to breaches of security, but

things can go wrong for privacy even without an active "attack." For example, if an organization shares a list of attendees to a past event with a partner, and that partner wants to expand its own email list to promote a similar event, this sharing might generate backlash from supporters. Individuals may lose trust in the original organization and feel they have been signed up for "spam" if they learn their information was shared without their consent.

While a number of the recommendations in this guide may improve the privacy of LROs' employees, supporters, and partners, this is not a guide to managing privacy risks. An organization's general or outside counsel can often serve as a good resource for learning more about the basics of managing privacy. The International Association of Privacy Professionals provides many tools, trainings, and even certifications in modern privacy practices for organizations who wish to expand their internal privacy expertise: https://iapp.org/.

## Confidentiality

Attacks on confidentiality make up the majority of what are often described as "data breaches." When a system loses its confidentiality, someone has gained access to information without permission, or information is inappropriately released. Attacks on confidentiality could make public information that an organization wishes to keep private, such as donor lists, financial documents, human resource files, or sensitive emails. These attacks can also victimize partners, supporters, and clients by putting their personal or financial information in the hands of criminals or other malicious actors.

> **Confidentiality Under Attack at the Utah Food Bank:** For a period of nearly two years, a security flaw in the website of the Utah Food Bank (UFB) allowed an attacker to access the personal information of individuals who submitted a donation through that site. The information, belonging to over 10,000 people (or 8% of the Food Bank's donors), included names, addresses, email addresses, credit or debit card numbers, security codes and expiration dates. The UFB underwent an extensive investigation, but was unable to ascertain the identity of the attacker. The UFB offered free credit monitoring to those affected by the breach, and had to undergo an 18-month restructuring of its website to enable more secure payment methods for its donors.

## Integrity

A system loses integrity when a person can change something without permission. For example, a student hacking into their school's system to change their grades would be an attack on the integrity of that grading system. Attacks on integrity often challenge one of the primary virtues of using information systems: that information can be maintained and shared in a way that is consistent and accurate.

> **Online Vandals Disrupt the Website Integrity of Schools and Nonprofits:** In November of 2017, a service called SchoolDesk – which provides web hosting services for thousands of schools across the US – was attacked by online vandals who altered a common system shared by many of SchoolDesk's customers. As a result, the homepages of about 800 schools were changed to display images and videos celebrating the Islamic State in Syria and the Levant. The sites were taken offline while SchoolDesk's systems were repaired, and while the attack did not disrupt the data or internal systems of school districts, it was deeply embarrassing for the affected schools. In 2015, the same groups of online vandals used a weakness in outdated versions of Wordpress – a common website design system – to display similar messages. The attack affected many small organizations who had not updated their Wordpress service, causing many to permanently lose portions of their website that were not backed up.

## Availability

Availability attacks affect the ability to access data or systems. These attacks can create restrictions for user access, can take entire websites offline, or can even hold devices hostage.

> **Ransomware Attacks Availability of the St. Louis Public Library:** In early 2017, the St. Louis Public Library suffered a ransomware attack. Ransomware uses strong encryption software to lock individuals out of their devices, holding the devices hostage until a ransom is paid. In this case, the ransomware's authors demanded $35,000 to release systems that had been maliciously encrypted at all 17 branches of the library. The library refused to pay the ransom, but it needed nearly a week to regain access to its systems.

> Other ransomware victims are not so lucky, and if a ransom is not paid, all the data on a device can be lost. In 2017, multiple large-scale ransomware attacks crawled from system to system, locking millions of devices around the world.

The security objectives are useful tools for discussing what kind of security any given system needs. In combination with some basic risk management considerations, the objectives can help LROs ask, "What kinds of cyberattacks are we most worried about affecting our systems, and what kinds of controls will be effective at preventing those attacks?"

## Understanding Cybersecurity Risk

Risk management is an important tool that provides a way for organizations to prioritize how to spend limited resources. Given the broad range of potential cybersecurity threats, effective use of organizational resources requires a focus on mitigating threats that are important and relevant to an organization's mission.

Risk management relies on two metrics to assess potential issues: the likelihood of an attack, and the impact of that potential attack. These two components are common for evaluating all forms of risk – including risk to finances, people, and mission. In cybersecurity, advanced risk management involves assessing particular systems for vulnerabilities and the likelihood an attacker might try to exploit those vulnerabilities – often through a process called "threat modeling" or "threat mapping."[9] While LROs are unlikely to have the time and resources to complete a detailed risk assessment exercise, they can still benefit from a less intensive effort to understand the likelihood and potential impact of some basic threat areas. This simpler exercise may be enough to determine what steps an LRO needs to take to improve its cybersecurity, and shift its organizational approach to cybersecurity towards one that is more risk-informed.

### Common Threat Areas

While cybersecurity threats will vary depending on context, LROs should focus their energy on mitigating the most common forms of attacks. Many of these

common attacks use techniques that have not changed substantially for many years, but LROs can still be victimized if they have not implemented basic security measures. The goal of LRO risk management is to deny attackers this "low hanging fruit."

Attackers targeting LROs are likely to be motivated by profit rather than by politics.[10] Whereas politically-minded attackers tend to carry out sophisticated and targeted attacks, profit-minded attackers are much more concerned with their cost margins, and a sophisticated, time-consuming, or expensive method of attack limits the breadth of their potential pool of targets.[11] This means attacks on LROs are likely to be unsophisticated, automated, and targeted at simple, known systems vulnerabilities. Three types of common attacks described below represent the most common threats LROs will likely face online:

**Account Compromise:** According to Verizon, the most common tactic used to facilitate data breaches in 2018 was the reuse of stolen usernames and passwords.[12] The proliferation of stolen passwords and usernames (also known as "account credentials") online – combined with the reality that people tend to recycle the same passwords across accounts – means that one of the most common forms of online attacks doesn't require any "hacking" at all. By buying or otherwise accessing dumps of already-compromised logins, attackers can attempt to take over multiple accounts owned by the same user. Account credentials are the "front door" to many sensitive or important services, and their design is generally unfriendly to humans (they are hard to memorize, hard to share, etc.). This means account credentials are often the easiest way to gain access to the most delicate of information - why do any complicated "hacking" if you can just get someone to send you their password in an email, or find a reused password in old breach data?

**Phishing:** Phishing is the use of email or another digital communications platform to trick an individual into disclosing sensitive information that can then be used to carry out a cyberattack. Phishing attacks generally require low technical sophistication to execute, often relying on simple techniques like sending emails with links to fake websites that prompt individuals to "log in" with their usernames and passwords, when really they are submitting this sensitive information directly to the attacker. Phishing emails can also trick

individuals into opening attachments that include malicious software. While it may seem embarrassing to fall for a phishing email, these attacks often fool even the most sophisticated targets, and in many ways it is the simplicity of this type of attack that makes it so dangerous. Phishing is the entry point for a range of attacks, so the consequences of being phished can vary widely. Some of those consequences can include the loss of control of important accounts (such as banking, email, or social media accounts), the infection of devices with malicious software, or the theft of important data.

**Data Promiscuity:** The sprawl of data – both online and across internal systems – is a reality that can have many potential negative outcomes for an organization. Poor data security practices within an organization greatly increase the likelihood of an attacker siphoning off information from its systems. Poor internal access controls may allow employees of an organization to access privileged information – such as HR files – inappropriately. Especially for organizations with significant staff turnover, it is often challenging to manage and secure internal access to information. For example: every time an organization shares a password with an employee or grants them access to sensitive systems, then forgets to revoke that employee's access or change passwords once the employee leaves the organization or changes roles, an opportunity arises for an accidental or malicious leakage of information.

**Malware:** Malicious software (or "malware") is a broad threat area, but one that encompasses many of the terms that people generally associate with cybersecurity, such as viruses, worms, and trojan horses. Malware generally takes advantage of a flaw in a system's design (a "vulnerability") to make the system act in a manner that is not intended. Many people have experienced firsthand a form of malware "exploiting" a vulnerability on a system or device they own or rely on. While a malware attack is one of the more clear and present dangers online, the technical vulnerabilities malware exploits often get fixed before the attack can be carried out. Attackers who use malware rely on individuals and organizations not updating their software frequently. They focus on systems with out-of-date web browsers or other common software (like Microsoft Office or Adobe Acrobat) with known vulnerabilities to maximize the reach of their attack.

For example, one type of malware is ransomware, which uses encryption software to lock up a device so its basic functions and data are inaccessible unless and until the victim pays a ransom. . Ransomware has seen an explosive increase in growth in recent years. [13] Like most malware, it takes advantage of known security vulnerabilities in common software or operating systems. Like other forms of malware, it often requires some user interaction to operate (e.g. a user must click "ok" when prompted to install a piece of unknown software). However, recent variants of ransomware have used powerful methods stolen from intelligence agencies that enable the software to run on victims' computers with minimal user interaction. [14]

---


1. Nonprofit Tech for Good, *2018 Global NGO Technology Report* (Reston, VA: Public Interest Registry, 2018), http://techreport.ngo/.
2. Lyndal Cairns, "Nonprofit Technology Staffing and Investments Report," *Non-Profit Technology Network*, May 2017, https://www.nten.org/article/your-guide-to-nonprofit-it-investment/.
3. Burning Glass, "Job Market Intelligence: Cybersecurity Jobs, 2015," *Burning Glass Technologies*, July 2015, http://burning-glass.com/research/cybersecurity/.
4. Frost & Sullivan, *2017 Global Information Security Workforce Study: Benchmarking Workforce Capacity and Response to Cyber Risk* (Clearwater, FL: Center for Cyber Safety and Education), 2017, https://iamcybersafe.org/wp-content/uploads/2017/06/Europe-GISWS.pdf.
5. Stephanie L Geller, Alan J Abramson, and Erwin de Leon, *The Nonprofit Technology Gap–Myth or Reality* (Johns Hopkins Listening Post Project, Communique 20, 2010), http://ejewishphilanthropy.com/wordpress/wp-content/uploads/2010/12/Nonprofit-Technology-Gap-Dec.-2010.pdf.
6. "Digital Security & Grantcraft Guide," Ford Foundation, accessed February 15, 2018, https://www.fordfoundation.org/library/reports-and-studies/digital-security-grantcraft-guide/.
7. Federal Information Processing Standard 199. "Standards for Security Categorization of Federal Information and Information Systems." (2004): https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf.
8. These definitions are simplified for this document. More formal definitions can be found in *CNSSI 4009* or NIST Special Publication 800-53.
9. "Hacked! Crooks Are Grabbing Nonprofit Websites and Demanding Ransom." *The NonProfit Times* (blog). Accessed December 20, 2017. http://www.thenonprofittimes.com/news-articles/hacked-crooks-grabbing-nonprofit-websites-demanding-ransom/, "More than 10,000 Utah Food Bank Donors Notified of Breach." SC Media US, August 31, 2015. https://www.scmagazine.com/the-data-breach-blog/more-than-10000-utah-food-bank-donors-notified-of-breach/article/532920/.

10. "800 US Schools' Websites Hacked with Saddam Hussein Photo, 'I Love Islamic State' Message." International Business Times UK, November 7, 2017. http://www.ibtimes.co.uk/pro-isis-hackers-hijack-800-us-schools-sites-saddam-hussein-photo-i-love-islamic-state-message-1646210.
11. "When ISIS Hacks Your Website." *Nick Fogle* (blog), January 7, 2015. http://nickfogle.com/hacked-by-isis/.
12. "St. Louis Public Library Recovers from Ransomware Attack." Threatpost. Accessed December 20, 2017. https://threatpost.com/st-louis-public-library-recovers-from-ransomware-attack/123297/.
13. For organizations who are interested in learning more about threat modeling, the Electronic Frontier Foundation has an introductory guide on the topic: https://ssd.eff.org/en/module/assessing-your-risks.
14. "The Verizon 2018 Data Breach Investigations Report" Verizon Enterprise Solutions, accessed February 1, 2019, https://enterprise.verizon.com/resources/reports/dbir/.