A Benchmark for Nonprofit Digital Responsibility
By The Center for the Digital Nonprofit, NetHope

Digital technologies are developing exponentially, bringing big economic and social benefits but also significant challenges which require new skills. As mission-driven organizations, should we go blindly into the digital future or should we instead take responsibility for our readiness? If so, what skills do we need and how are we doing?

The Digital Nonprofit Ability™ (DNA) assessment identified that the People category was holding back NGOs from advancing digital transformation. This finding led to the development of the Digital Nonprofit Skills Framework. The Digital Nonprofit Skills™ (DNS) assessment surfaced skills gaps, of which, the category of Digital Responsibility skills scored second lowest across the framework.

Being Digitally Responsible means making conscious decisions about what you are doing while you are online and accept the consequences (results) of your action.

The skills associated with Digital Responsibility are those that help an individual understand how to safely work in a digital world, while being accountable for the consequences of their digital activities.

The Center for the Digital Nonprofit identified fourteen skills contributing to Digital Responsibility, from basic cybersecurity to building a community of practice (See Appendix). While this list is not exhaustive, assessing these skills supporting Digital Responsibility allows an organization to identify strengths and gaps within their organization.

Where are Digital Responsibility gaps in nonprofit organization?

In order to further understand where gaps are, twenty-two leaders within NetHope members in Europe worked together to assess both the need and performance of Digital Responsibility skills across six job roles common in nonprofits: Senior Leaders, Program, Fundraising, Human Resources (HR), Finance, and IT. The tools used in this workshop are available to nonprofits who want to map Digital Responsibility skills within their own organization.

We first asked leaders to rank their organizations on the spectrum of Digital Responsibility, from a basic understanding of data protection to a conscious culture of safely stewarding data and digital actions (see Appendix). We observed that organizations mapped to the first two-thirds of the spectrum with clustering around the mid-point. Of note, organizations
with continental European headquarters rated themselves, on average, lower than organizations with non-continental European (e.g., Great Britain) headquarters.

For half a day, we worked in small groups to map the need and performance of Digital Responsibility skills by job function. We collected and analyzed 3,696 data points in total and discussed results. Here are the top findings¹:

Finding #1: A high need to share personally identifiable information safely
Cybersecurity issues are becoming a day-to-day struggle for nonprofits. Trends show a dramatic increase in data breach and hacking. Cisco estimates that 31 percent of organizations have experienced cyberattacks on operational technology infrastructure. In this context, it is therefore not surprising to see that the top skill needed across all job functions is “ Appropriately sharing personally identifiable information”. For nonprofits that operate globally, there is an increased demand to protect personally identifiable information. Recall that the Global Data Protection Rules (GDPR) governing personal information have recently been adopted as laws of the European Union creating an increased need for compliance and that similar regulations are being put in places in other nations. In addition, the world is experiencing a growing trend in exploitation of personal information whether it be for criminal purposes or political ones. Regardless of their roles, people working in nonprofits need stronger cybersecurity skills.

¹ As most participants were associated to the IT function, results for IT skills suffered from social desirability bias, causing performance results of the IT function to be inflated.
Finding #2: We are best at communicating safely at work

Across all organizations best performance is achieved, on average, for the skill of “Safe communication at work”. Modern technology tools such as end-to-end-encryption now included in most communication systems, complemented with secure communication awareness campaigns have likely contributed to this increase in performance. People are less worried about the safety of their work communications than they were a decade ago. However, faced with the trend of people blurring the lines between workplace and personal life, there is a need for nonprofits to consider promoting apps that are suited for both business and personal use and can thus extend the boundaries of safe communications.

Finding #3: Need to do better with cybersecurity

A survey by Willis Tower Watson in the UK reports that 61 percent of employees have “insufficient understanding” of cyber security risks. While many employees working in IT or security roles may understand the impact and risk of online behaviors, someone without a

![Figure 2. Performance of Digital Responsibility Skills by Function](image)
background doesn’t realize just how much their online activities—both the things they do, and the things they fail to do—can potentially jeopardize their organization.

Data collected from the workshop identified that the skill of greatest need with poorest performance is “Organizational baseline skills requirement around cyber security”. This was equally the case for Program, Fundraising, and HR functions. As mentioned before, the IT function tends to be more aware of these requirements and in most NGOs has the mandate to mitigate cybersecurity risks. This can explain why it scored higher. Likewise, because most online criminals seek to steal money from organizations, higher performance is demanded from the Finance function, which explains why it scores higher.

Finding #4: Online, perception is reality
In the digital world, brands are at the mercy of socially empowered people. Fake news, a couple of bad reviews, a barrage of damaging tweets, or a string of criticism-fueled posts on social media are all it takes to undo a reputation that took many years to build. The *Reputation Quotient developed by the Harris Poll* is one way to understand and measure this.

To paraphrase a popular saying “what happens in digital, stays in digital” – only to be surfaced back, just-in-time, by a clever search engine. The breadcrumbs we all leave online, such as in social media, collectively influence the perception people have of our work. To be informed, donors and prospective employees have developed the habit of searching first and asking questions later—if the search results are positive. It is thus logical that the Fundraising and HR functions have the greatest need for skills to “create a positive online identity”. This is a challenge. Long gone are the days of a single website controlled by the organization. Today, most of the information about an organization is outside its control.
and managing it to a positive result requires new skills such as an understanding of the social web, empathy, online presence management, and search-engine ninja skills.

**Conclusion**

This workshop assessment of Digital Responsibility skills further documents the need to improve performance in this category at all organizational levels. It sets a benchmark for nonprofits to compare to, and highlights common needs shared by multiple job functions.

![Figure 3 Focus areas where Need is high and Performance low](image)

To effectively benchmark themselves and prioritize, an organization should use the digital skills assessment tools and guidance from the Center for the Digital Nonprofit. For further information, contact digital@nethope.org
APPENDIX: Skills for Digital Responsibility

1. Organizational baseline skills requirement around cyber security
2. Risks vulnerabilities and controls of a computer system
3. Ability to identify safe sites
4. Password protocols and practices
5. Social sites and protecting yourself
6. Identifying personally identifiable information
7. Appropriately sharing personally identifiable information
8. Protecting against Phishing, Whaling and other malicious activities
9. Safe communication at work
10. Cloud security for individuals
11. Mobile device security
12. Online security when traveling
13. Creating a positive online identity
14. Creating a community of digital responsibility
APPENDIX: Spectrum of Digital Responsibility

Level 1.0 – In your organization people work online with data, but don’t do a lot with that data. You have no confidence that people understand the vulnerabilities of sharing data online. Online work is susceptible to hacking and misuse, while a lack of basic security practices in your organization puts all online activities at risk.

Example:
- John forgot to upload Asmaan’s assessment data into the database while in the office. He has the file with him on a thumb drive, and stops at an internet café to upload the data. Unfortunately, the computer he uses had been compromised. Flustered by the discovery, he rapidly exits the café, forgetting to take back his USB stick.
- Jane has been working long hours, and is in a hurry to finish her work so she can leave. She sees an email drop into her inbox, and it looks like it is from the CEO of her organization. She isn’t expecting it, but quickly opens up and reads the note addressed directly to her. It is about the performance of her project. While she has never interacted before with the CEO about her project, Jane believes it is important to get the information now, and clicks on the link embedded in the email.
- Roberto has been on the road for a few weeks and has seen the antivirus software reminder that his security database is out of date but never took the time to download the update.
- Shani knows that she is using an old version of her software but has refused to upgrade it herself, mistakenly believing the new one is faulty, when the only difference between the two is in fact that the new one has had security flaws fixed.
- Dominique is new to the program and has proudly posted photos of the prosecuted people he works with on social media. He does not know that his phone is setup to include in each image the GPS coordinate of where they were taken, endangering the lives of the people he serves to help.

Level 2.0 – In your organization, data easily shared between teams. Teams work together online, and there is a baseline of behaviors and activities to protect and secure information. However, security isn’t reviewed regularly, and you don’t do regular updates to online safety protocols. Sometimes it’s just easier to do the work than think about protection of information.

- David has worked in the field a long time. He’s aware of the importance of protecting data – both his information and others. He’s done things the same way for years, and since he has a basic knowledge of security, David feels that he is safe in the way he handles data. David is always under a lot of pressure, and cares deeply about the people he is working to help. He has joined a new country program and doesn’t realize local hackers are more sophisticated and that sharing data here requires strong encryption before sending.
- Samir stores his passwords in a file on his computer. The file is encrypted, so he feels it is safe. He has so many passwords that he often leaves the file open to be reminded. However, Samir leaves his computer unattended for a few hours every day as he performs multiple tasks outside the office.
• Priya is a new employee and is a millennial with a strong online social network of friends and family. She posts pictures of her life and her work – after all – she wants to share this exciting work with her network! She doesn’t think about whether she should post pictures of the faces of people she is serving – after all, they aren’t in her network.

Level 3.0++ – In your organization, you are very agile – you have extensive networks and use your data well, but also use external data. Your organization makes very conscious decisions about how data is handled online, and people receive regular security updates and protocol practice. Employees are Digitally Responsible as individuals and are committed to keeping information safe no matter where they are in the world.

• In my organization, employees go thru new employee training, which includes training on online safety, security and reputation. Each employee is required to pass an assessment before they begin working. Security is updated and reviewed regularly, and employees are required to stay current with their security rating. All security incidents are shared opening as lessons learned.
• Passwords are changed every 90 days and are required to be complex and hard to guess
• Our organization has a regular cadence of communication when it comes to digital work – with safety information on using social networks, how hackers are using new phishing schemes and other vulnerabilities that help us stay secure at work and at home.
• Patricia is planning to post something publicly on the Internet. Part of her routine is to imagine with a colleague the potential sort and long-term negative consequences of online actions.