NSP | Nonprofit Support Program
HARTFORD FOUNDATION FOR PUBLIC GIVING

Project Plan for: Assessing & enhancing your cybersecurity

Project description

This project is to assess the state of cybersecurity at your organization and to ensure you are taking appropriate precautions to safeguard your critical data. The project scope includes evaluating your current environment and – if appropriate – purchasing and deploying additional levels of security and disaster recovery, including required software, hardware, and training to adopt the new solutions.

Solutions/tactics addressed include:

1. Adopting Multi Factor Authentication (MFA)
2. Implementing a more secure router, better Wi-Fi encryption, and/or tighter remote access
3. Ensuring proper use of anti-virus/anti-malware software
4. Planning for data backup or disaster recovery
5. Staff security training (NOTE: This item also appears in the Staff Training Project Plan. If you take on both plans, please do not request funding for this item twice)
6. Rolling out network administration policies to strengthen security, such as requiring complex passwords and password changes

Why take this on / what impact to expect:

If you complete this project, you can expect some or all of the following benefits to your staff and organization:

- Decreased probability of a staff member accidentally allowing intruders to access your network (staff errors are the number one source of ransomware attacks and security breaches)
- Reduced likelihood of a major data breach, saving the organization time, money, and reputational integrity
- Increased ability to recover from a severe ransomware attack without paying the ransom
- Lowered prospects of a data breach resulting from weak or outdated passwords (which can easily be overcome by a brute force attack)

Estimated project timeframe: 3 – 7 weeks

Project deliverables

At the end of this project, you should have made notable improvements in one or more of the following areas:

- Installation of appropriate router/firewall hardware with up-to-date subscriptions
- Setup of multi-factor authentication (MFA) for all major platforms and services
- Active use of up-to-date anti-malware/anti-virus software on all network devices
- Presence of a functional data backup
- Adoption of security policies like complex password mandates for all network users

Project milestones & who leads:

The major steps involved in executing this project and who leads them are below. Keep in mind there may be more sub-tasks than what's noted here, but these are the major steps:

Milestone	Who leads?
1. **Assess current state.** ***Do this for each of the 6 bulleted items under 'Project Description'.*** a. **What solutions are in place now (if any)?** b. **Are they robust enough to meet your needs?**	Your org or a trusted cybersecurity vendor (see list

c. **Are they properly configured to provide maximum protection?** d. **Do all staff know about them and follow them?** e. **Have they been tested to ensure that they work?**	in 'Resources' below)
2. **Create requirements/define your needs** a. **Based on the assessment above, create a list of "must-haves" & "nice-to-haves" of what you need to take on. Keep in mind you may need to prioritize some tactics over others based on areas of highest risk and which tactics/solutions offer the most protection to your organization.** b. **Understand your budget for the project. Include one-time (upfront) costs and ongoing subscription fees.**	See above
3. **Explore options** a. **Using the requirements above, evaluate potential solutions and vendors that offer what you need – use the list below as a starting place** b. **If possible, demo different solutions to understand how they work** c. **Consider what training/documentation/support is available for install & use**	See above
4. **Choose solution, install, and train users** a. **Purchase solution(s), contract for external assistance, and install the solution** b. **Ensure all elements of the solution you need are installed and tested** c. **Set up a training plan for staff to ensure they can successfully use the tools** d. **Consider your approach to ongoing support and training on cybersecurity**	Your org and/or solution vendor

Estimated project budget:

If you follow the approach outlined in this project plan template, we estimate the project budget to be as shown below. Please keep in mind this is only an estimate and final cost will vary based on your choice of solutions/vendors, hardware, etc.

Description	Cost per unit	# of units	Est. budget
Multi-Factor Authentication solution (some of your software/ solutions may have an MFA option included at no extra cost)	$0-$3 per user per month Plus, one-time setup of $400		
Router/firewall, with or without Wi-Fi capabilities	$500 Plus setup fee of $500		
Anti-virus/anti-malware software	$40 per device Plus setup fee of $300		
Data Backup / Disaster Recovery solution	$10 per device per month		
Staff Awareness Training	$250		
Network administration assistance (to work with outside vendor to establish and set up password protocols)	Set-up fee of $500		
TOTAL			

Potential solution providers/vendors for this project:

While the Nonprofit Support Program does not endorse the vendors/providers below, our work in the community indicates that many of your peers have used them for similar projects. It's essential that you research and fully evaluate solutions and vendors against your specific project requirements to ensure a good fit. Additional vendors can be found in the New England Nonprofit Consultant Directory. We've recommended additional resources under "Learn more before you decide."

Multi-Factor Authentication (MFA)

- Duo
- Microsoft Authenticator (likely the preferred option if you already use the Microsoft 365 Suite of products)
- Google Authenticator (likely the preferred option if you already use the Google Nonprofit Suite of products)

TIP: You may already be using other software products and solutions that provide you with the option to turn on MFA for your users. You should turn it on in every product/solution that offers it as an option.

Small Office / Home Office (aka "SoHo") and Business Firewall/Routers:

Firewall/router hardware offers a wide variety of security protection and custom configuration. "SoHo" models should require less outside technical expertise, but also likely provide a lower level of intruder protection. Business-grade models offer a greater level of protection, but will require more expertise to deploy, and have annual subscription fees.

- Synology (SOHO)
- Sophos (Business)
- Meraki by CISCO (Business)
- SonicWall TZ (Business)

Anti-virus and anti-malware solutions:

- Malwarebytes
- Hitman Pro Alert
- Norton Small Business
- Sophos

Data Backup and Disaster Recovery solutions:

- CrashPlan for Small Business
- Carbonite
- iDrive

Staff cybersecurity training tools:

- Discounted KnowBe4 training on TechSoup
- Proofpoint Security Awareness Training
- Sophos Phish Threat

Organizations that can help you assess your cybersecurity needs and implement these solutions:

Your organization may require assistance deploying some or all the potential components detailed in this plan. If you already have an existing IT support resource, seek input from your provider about improving your security. If you need to find a vendor to assist with decision-making and deployment, consider:

Vendors who specialize in nonprofit IT support, including security:

- Roundtable Technology
- Community IT
- Tech Impact

Network administration assistance with complex password policies and deployment:

- See preceding paragraph

Consider utilizing a Catchafire volunteer to help with select elements of your project implementation. More information about available Catchafire technology projects can be found here.

Learn more before you decide:

To learn more about how to evaluate these solutions/vendors before you proceed, consider the following resources:

- An excellent primer on multi-factor authentication
- All you wanted to know about the fundamentals of firewalls
- Why we want and need anti-virus and anti-malware software – even though some protection is already built-in to Windows
- Why nonprofits need data backup
- Did you know ~90% of security breaches are due to staff errors?
- 15 Password management best practices

Related considerations:

While you're working on this project, it is a good time to also consider the following:

- Does your staff have the time and expertise to deploy this solution internally, or do you require an outside vendor to assist? If you need help, do you have a resource?
- Is there a staff training component to any of the action items of this project? If so, who will do the training of current staff? How will future staff members get up to speed on this?