TOP 9 TECH CHALLENGES
FOR NONPROFITS + SMALL BUSINESSES

Introduction

Dealing with tech challenges may be the last thing on your “to do” list when it comes to running your organization. While IT may not be your organization’s focus, it can be critical to keeping everything running and your employees productive and moving forward to achieve your goals. From network infrastructure, to backup solutions and cybersecurity, having a solid technology strategy and security protocol is critical to running your organization today.

In this document, we outline the top 9 tech challenges facing nonprofits and small businesses. We will provide high-level approaches you can take to help you address these issues within your organization, as well as a link to more in-depth information and tips for each topic:

1. Data Security
2. Data Management
3. Mobility Solutions
4. Obsolete Technology
5. Data Backup and Continuity Solutions
6. IT Policy Creation and Enforcement
7. Migration to Appropriate Cloud Solutions
8. New Technology Training
9. System Updates and Technology Replacement Budgeting

Data Security

Data security is a challenge for organizations of all sizes. One of the largest data breaches in recent history occurred at Equifax. Hackers could access personal data of 143 million people, including their names, Social Security numbers, birth dates, addresses and some driver's license numbers. While the company's security department "was aware of this vulnerability at that time, and took efforts to identify and to patch any vulnerable systems," they were slow to implement the patches and hackers exploited the flaw months after the vulnerability was identified.

While Equifax is an extreme case, it highlights how critical the human factor is to preventing data breaches, that's why we recommend starting with developing and implementing a clear, easy-to-adopt data security policy at your organization. Communicate these expectations to employees when you roll out the policy and as part of on-boarding any new employees. Update and review the policy annually (at minimum), because security protocols should evolve as technology changes.

You can create a culture of data security and mitigate the risk of human error within your organization with minimal monetary investment by following security best practices and having good internal communication and training so everyone knows what is expected.

Your first line of defense is strong passwords

In addition to having a data security policy in place, the first line of defense to securing your technology is using strong passwords that are regularly changed. Here are some tips:

- Generate a different password for each online account
- Make a random multi-word paraphrase
- Use upper and lowercase letters, punctuation, and numbers in passwords if not using a paraphrase
- Create a password that is a minimum of 14 characters long
- Change your passwords every 3-6 months and don't reuse them
- Do not store your password list in the cloud
- Use two-step verification on all services that offer it

Data Management

Today, organizations have access to myriad data. For nonprofits, that data can help inform programming, constituent relations and fundraising. For small businesses, it can help you set your goals around customer service, product development and marketing. With so much data at your finger-tips, data management can be challenging.

Key data management steps:

REVIEW: Map out all the systems that collect and store data.

DETERMINE: Store only the sensitive data you need.

VERIFY: Ensure your systems and hardware are up-to-date.

BACKUP: Determine how many days/months/years do you need retain your data and whether you can deliver data for the time period you are legally required. Make sure the backup data is secure and easy to restore.

Mobility Solutions

With a flexible, reliable mobility solution in place, organizations can realize benefits like cost savings, improved employee morale, and more efficient use of time and resources. Furthermore, new tools may provide more efficient board engagement, improve member relationship management, and increase volunteer hours for nonprofits. Appropriate planning and education will help ensure a smooth roll-out and successful outcome with any mobile device plan.

Here are some considerations for making your organization mobile-ready and secure:

- Develop a “Bring Your Own Device” policy
- Consider which solutions have proven mobile-ready applications
- Install mobile encryption when sensitive data is stored locally on a device such a laptop

Obsolete Technology

Knowing when to upgrade and install updates is critical to keeping your data secure, but it can be challenging to keep up with it all, not to mention that we typically recommend waiting on some updates, particularly for operating systems, until all the bugs are worked out. You also want to make sure your hardware and other solutions are compatible with any upgrades before installing them.

Software Updates and Patches

We often recommend waiting on some updates, particularly for operating systems, until all the bugs are worked out. In other cases, we recommend an immediate update, particularly for security patches. Deciding what and when to update can require consistent expert consultation. You'll also want to make sure your hardware and other solutions are compatible with any upgrades before installing them.

If you are managing your IT in-house, here are a few of the most common software updates you will have to manage:

- Anti-virus solutions
- Operating systems
- Firewalls
- Software including Flash Player, Adobe Reader, Java and Microsoft Office products
- Internet browsers

Retiring Obsolete Technology

It's important for organizations to have a planned strategy for retiring their technology. That can often take a back burner to more pressing organizational issues, but planning can save you money and time and help avoid the risks associated with obsolete technology.

While we tend to recommend a 3-4-year life cycle of computers, devices are more like 1-3 years, depending on the device. It's smart to plan to retire 20-30% of your technology each year to ensure no device is older than four years old.

Data Backup and Continuity Solutions

Business continuity requires the development of policies and procedures for risk mitigation and service disruptions, whether it's caused by human error or natural disaster. Essential operations should be identified and redundant systems put in place to ensure workplace continuity.

Key concepts include:

- Online file back-up
- Back-up security
- Back-up functionality
- Back-up restoration
- Back-up file access
- In-house vs. cloud back-up
- Mobile device back-up

Creating and Enforcing It Policies

Our customers often struggle with developing, updating and enforcing IT management and security policies. A comprehensive IT management and security policy is critical to protecting the privacy, accuracy, security, and integrity of your data. Furthermore, it should be easy to understand, follow and enforce. The goal is to find a balance between policies and procedures that support physical and virtual security while ensuring employees have access to the data when and where they need it.

We recommend developing a comprehensive IT management and security policy that includes the following topics:

- Acceptable Use
- Media Access / Portable Storage
- Mobile Devices
- Password Security
- Laptop Security
- Administrative Rights
- Remote Access
- Network Data

Migrating to Appropriate Cloud Solutions

When developing a cloud migration plan, you will need to assess your current technology, including both hardware and software. For instance, if you have an in-house server that needs to be replaced in the next six months, this is an opportune time to consider migrating that infrastructure to a cloud solution. It will likely save on the capital expense of replacing the server while reducing the risk of data loss.

Before migrating your in-house infrastructure to the cloud, it's important to consider the following:

- What are your organizational goals and how can technology help achieve them?
- What is your current infrastructure and where is your hardware in its replacement cycle?
- Do the critical applications meet your needs and are cloud solutions offered that have the same or increased functionality?

Training Your Staff on New Technologies

While the benefits of the new technologies you want to implement may be evident to you, they're not always immediately embraced by the team. This can cause disruption if proper tech training is not part of the roll-out.

Secure leadership buy-in prior to the roll-out. Managers know their staff best and are responsible for ensuring the solutions in their departments are adopted. Take the time to meet with them, hear their concerns, learn about the challenges their staff are facing, and work together to build a technology and security infrastructure that is both practicable and useful.

Before rolling out any new technology, it's good to be aware of some of the top reasons employees may resist the change so you can address them:

- They don't see the benefit to themselves
- They think what they use now is working just fine
- They don't think they'll understand how to use it
- They've been through technology changes that didn't go smoothly

When you have your team together to learn a new technology, use the opportunity to review data security protocols and your IT policies.

Budgeting for System Updates and Technology Replacement

Most organizations work from a strategic plan to guide them to achieve their growth goals. However, many organizations overlook the value of developing a plan for their technology and how it can support that strategic plan. Adopting a disciplined approach to technology replacement and budgeting accordingly can help avoid surprise expenses, save money, mitigate data security risks, and increase productivity.

There is a strong interdependency between the hardware you use and the software your company relies on. Make sure they are in sync and if mobile is your focus, your solutions should be strong on this front. When developing a technology replacement cycle, we encourage our customers to rethink their IT infrastructure and software because most critical applications, including CRM, payroll, and accounting software, have a cloud strategy that was not available a few years ago. Cloud solutions can help relieve capital expenditures by reducing the need to replace obsolete technology, and they typically offer greater flexibility and functionality for your employees.

Another important benefit of keeping your systems and hardware current is data security. Obsolete technology may no longer be supported and may not receive the latest security patches, leaving your data wide open to malicious attacks.

As you start thinking about next year's budget, there is no better time to develop a technology replacement plan. Your nonprofit will be healthier, your team more productive and your budget will have fewer surprises if you plan according to the life cycle now dictated by today's technology industry.

About ASG

ASG, Inc. was established in 2000 and is a privately-owned IT services company headquartered in Boston, MA. We are the technology support infrastructure for professional organizations and nonprofits throughout the country. We specialize in small business IT support for companies that range from 10 to 300 employees.

We believe…people matter, objects don't. In other words, technology is just one more tool to help employee productivity and support the goals of your organization and it's our mission to deliver reliable IT services and small business IT consulting while delivering superior customer support.