The Episcopal Diocese *of* Olympia
The Episcopal Church in Western Washington
www.ecww.org

Cybersecurity and Data Recovery

05/25/2021
VERSION 1.0

From the Office of the Bishop

1551 Tenth Avenue East | Seattle, Washington 98102
206-325-4200 *telephone* | 206-325-4631 *fax* | 800-488-4978 *wa* | *online at*

TABLE OF CONTENTS

Intro

While cybersecurity and data recovery are two independent disciplines, they are closely linked when it comes to protecting your organization from malicious digital attack. As we continue to use digital technology more and more in the 21st century, cybersecurity and data recovery become more and more a critical concern. It is not just a requirement for large IT firms, financial institutions, or government agencies. It affects everyone, up to and including your faith organizations. The purpose of this paper is to present a roadmap for churches and faith organizations to prepare for and respond to potential cybersecurity and data recovery issues that may arise for themselves and their organizations.

Where to Begin

All organizations that have digital and IT functions which are important to the organization want to make sure they have consistent, reliable, and robust systems and tools. They want and need to secure their data, network, equipment, and tools to work efficiently. The connectivity of all these pieces becomes more important but also poses a potential security risk to the organization. These can be divided into three areas:

- Data - the digital information important to the success of the organization. Think about the different types of data that your organization uses on a regular basis. What are the tools that would be used to access this data? Where is this data stored? How is this data protected and secured?
- Identity - how the users are allowed to interact. When we think of “identity”, ask how your users in the organization are allowed to access your information. Are there different access limits for some people than for others? How is that controlled?
- Network - how these pieces are all connected together. Are there any protections to control network access? Are people allowed to connect from places outside of the organization’s offices?

Add into this the physical equipment, software, business processes and applications that each of the three components use and you begin to see the complexity and necessity of securing these assets.

Cybersecurity

Whereas at one time, hacking or security breaches were considered a novel curiosity or prank, it is now a multi-billion-dollar business which targets many different groups and organizations. The single biggest reason for these attacks is simple – gathering data. Through the data, one can potentially gain information on finances, medical records, intellectual property, mailing lists, email addresses, etc. The possibilities are endless. Its variants include ransomware of its victims, stealing data and reselling it, destroying it, or injecting malware which can either corrupt data or quietly

spy and collect data for a long period of time without your knowledge. Security has taken a prominent role as these attacks increase. These attacks have become more sophisticated, and they touch so many different aspects of our daily lives.

Hope for the best, but prepare for the worst

Sadly, cybersecurity is a defensive game. They attack, you defend. You never get to go on offense. Securing data is very important regardless of whether you are a target or not, because eventually you will be. We and our organizations are dependent on having sustainable, dependable, and efficient network systems as well as reliable and secure applications. By creating and maintaining secure, configured systems and applications we can help reduce but not eliminate the risk of attack. How you prepare and respond becomes very important.

Cyber Resilience

What we want to achieve is to create a sense of cyber resilience for your organization. Cyber resilience involves the idea of keeping the operations of the organization going during and after cyber-attacks. Security goals and methodologies change from simply protecting the organization from attacks to ensuring that business functions will not be severely interrupted by attacks.

Training

There are a number of sites and organizations which offer user training in security. You can search online for these using the search terms “cybersecurity user training”. These trainings help inform users on how to recognize and avoid many types of cyber-attacks, including computer viruses, worms, Trojans, rootkits, ransomware, and spyware. While many of these cybercriminals create and deploy the cyber-attacks, the weakest link in our defense is the unknowing end user who actually initializes the attack by clicking on something they shouldn’t have.

Cybersecurity Action Items

This security checklist is a good start in a cybersecurity arsenal. While it is not exhaustive, it does cover many of the basics.

- **Secure Servers and Computers:** There are three things to do to secure your computers and servers. 1) If you have a server at your facility that you connect to, it should be in a controlled room with limited access. This should be either a room that can be locked or in an enclosed cabinet that can also be locked. 2) There should be a firewall in place between your computer and your cable or DSL modem. Check with your provider to see if they

provide that as part of the modem. 3) Your computers and workstations should be password protected for access and there should be the ability to lock the computer when you are not working at it or you need to step away from it for a period of time.

- **Password managers**: A password manager helps you create a unique password for each online service you use. Having a unique password ensures that if one service you use is hacked, the compromised password won't allow access to all of your other accounts. Suggestions for password managers include 1Password, LastPass, Dashlane, KeyPass and Keychain. You can also go to https://haveibeenpwned.com/ to see if your password has been hacked.
- **Creating strong passcodes on mobile devices**: Many passcodes are numeric only. You should use a 6+ set of number minimally to provide extra security. Use TouchID or FaceID if it is available. Have a strict lock policy on your devices.
- **Two-factor authentication (2FA)**: In traditional username and password practice, you enter your username and your password, press enter and it logs you into whatever system you are attempting to log into. Two-factor authentication or 2FA utilizes two different pieces, something that the user knows (your password) and something that the user has. This would be your mobile phone or what's called a hardware token. After entering the username/password, a text message is sent to your phone with a numeric code that you enter to complete the login process.
- **Encryption**: If your phone or computer is ever stolen, a thief may try to read or export your personal data. If your device is unencrypted, hackers will have access to anything stored on that device, including photos, emails, documents, and contacts. Note that encryption may not be an option for every operating system. Search for "encrypt hard drive" for more information.
- **Freezing one's credit**: This may not directly affect your organization, but it is a good tip for individuals. Due to the many security breaches that have led to the loss of data belonging to billions of users with different companies, you should assume that your SSN, credit report, and other personal details are known by hackers. To prevent hackers from opening new lines of credit using this information, enable a freeze on your credit through the three credit agencies, Experian, Equifax and TransUnion. This is a free service and these can be temporarily unfrozen by you if you need to allow credit checks.
- **VPNs:** Virtual Private Networks (VPN) help to protect internet access by offering a secure internet connection that is encrypted so that all the data you send or receive cannot be read by people snooping on a network. These are especially important when you are on an open public WiFi network. They are available on all operating systems. Search for "VPN providers" for options. Note that this will be a paid feature.
- **Webcam covers and privacy screens**: There are websites that contain malicious scripts that can open your webcam without asking for permission and take pictures or videos. In addition, using your computer in public places exposes you to shoulder-surfing, where malicious people simply watch and steal sensitive data when you enter it into a website or system. Webcam covers make it impossible for hackers to see anything if they hijack the webcam and the privacy screen is a filter that blocks visibility of a screen outside of 60 degrees.

- **Privacy-first browsers, and search engines**: You should use a web browser and search engine that protects you from tracking, fingerprinting, and unwanted advertisements. For browsers, consider Brave, Safari, and Firefox. For search engines consider duckduckgo.com instead of Google since Google (including Chrome) collects data and does target advertising.
- **Email providers**: There are privacy-friendly email providers like ProtonMail, FastMail, and Tutanota. Never send sensitive information or identifiable password information via email unless it is encrypted. A good alternative is to send the password via text message without any other identifying information and send only the associated user name via email.
- **Reviewing app permissions**: There is an increase in the number of apps that have been requesting excessive permissions to sensitive data that is not required for their primary purpose and functionality. You should review all applications that have access to your photos, camera, location, and microphone. Be sure that you trust these apps with sensitive permissions and review them regularly.
- **Social media privacy settings**: A lot of personal information can be obtained on social media networks without much hassle. Social media platforms often have privacy controls which most users ignore or do not bother checking. Lock down access to your social media account. Also, many of those so called “polls” on social media platforms asking your favorite animal, or how far are you from where you were born are ways to garner information that can be used to answer standard privacy questions which allow back access into bank accounts. Don’t post responses to these.
- **Learn about phishing attacks**: Hackers do not solely depend on using advanced software to breach accounts. Sometimes, they just request access from users under false pretenses. Using social engineering, hackers can trick you into sharing sensitive credentials. Once the users enter their details, the hackers proceed to use the details on the correct websites and steal money or data. Learn how to spot them and avoid falling into their trap.
- **Keeping devices updated**: This is something that is extremely important but often overlooked. Keeping the software up to date on your computers and apps is vital since these updates contain patches to fix potential hacking and virus threats. Also remember to update other devices such as routers and Internet of Things.

Data Backup and Disaster Recovery

Data backup and recovery procedures are many times the most overlooked items an organization contends with. Backups need to be consistent and diligent and for many organizations, backups are infrequent or even nonexistent. The same type of effort (or lack thereof) for disaster recovery holds even more true. To be effective, backups and recovery requires much more planning and effort. It isn’t particularly hard, but it needs to be put into place and followed consistently.

Data backup and disaster recovery processes need to be documented for your organization. This document will be your roadmap for recovery. For data backups, an inventory needs to be done to

determine what data is critical to be backed up. Assess whether it is important to back up programs or the data the programs use. For example, backing up the Word program may be important, but the Word files are more important since you can always re-install Word, but not the files unless they are backed up. In addition, there are many important church related documents that will need to be backed up as well. Refer to the diocesan retention schedule at: https://archives.ecww.org/wp-content/uploads/2020/12/Records-Retention-Schedule-2020.pdf for information on which files are considered vital or that need to be kept permanently. Determine where these files reside and how often you want to back them up. There are programs like Carbonite which will automate the backup process to the cloud, or you can manually do this backup to a removable hard drive or USB device. If you do your own backups, store the backups somewhere other than your office such as your home or a safe deposit box. This will help to protect you in case of physical damage to your computers or building.

When you work on your disaster recovery plan, design your plan with these two ideas in mind: RTO (Recovery Time Objective) and RPO (Recovery Point Objective). RTO defines the time to recover your IT infrastructure and services following a disaster to ensure business continuity. If you set your RTO as 2 hours, then you should be able to continue normal business operations within this timeframe in case of any disaster. RPO determines your tolerance to the amount of data that your organization can afford to lose during a disaster. It also helps you measure how long it can take between the last data backup and a disaster without seriously damaging your business. RPO is useful for determining how often to perform data backups. Together, RTO and RPO goals are the basis for a solid and realistic disaster recovery plan.

Steps for Creating a Disaster Recovery Plan

Disaster recovery plans vary from organization to organization, therefore the particular implementations of the areas of focus which we will discuss may be different for different organizations. Below are the main areas of focus that a typical organization needs to address in creating a disaster recovery plan.

Having ready backups, alternative hot sites to take over operations during cyber-attacks, and faster incident response measures to ensure that organizations can mitigate and recover from attacks will go a long way to drastically reduce the amount of disruption a cyber-attack can cause. Here is an example of a nonprofit security checklist that can be downloaded and used to help with the process.

Impact Analysis and Risk Assessment

The first thing to do when designing a disaster recovery plan is to evaluate the impact that a disaster would have on various parts of the organization. Are some parts more critical to get back

up than others? Ask the staff how long they could operate without a functioning IT infrastructure. From here you can calculate your RTO and RPO information to know the critical paths and what the staff needs to recover.

Recovery Strategies

The next step is to determine whether the resources you have currently in place are sufficient to meet the RTO and RPO goals you have identified. Determine whether or not you have enough staff, backup infrastructure and network bandwidth to meet your goals. If new hardware and/or software is required, will you be able to acquire it quickly if needed? Answering questions like these will help to identify gaps or problem areas in your strategy.

Develop Recovery Plan

Here is where you will create your plan. You will want to develop an overall plan framework which defines the different components of your plan. You will identify people who will be responsible of executing the plan. Write out the specific disaster recovery procedures required to complete the plan. Document any special information required to follow the procedures as well as any manual workarounds if contingencies are necessary. Have others review the plan for feedback and any areas that may need further explanation or attention.

Test Recovery Plan

Now that the plan is created, you will need to test it. Do dry runs with different scenarios to see if the plan works and meets the needs of the organization. Train staff who will be part of the disaster recovery process so that they know their parts and responsibilities and how to perform them. Document the results of these tests and review them to identify any areas that need to be addressed.

Remember that this is a living document. It is not a one-time exercise that you can put on a shelf and never be bothered with again. Review it regularly as things can change. There may be items in the plan that are no longer relevant or as important. New, undocumented items will come up and will need updating in the document. Staffing changes are the norm and new employees need to be aware of this document and their role in making it a success. One cannot become complacent because the next hack or ransomware could be you or your organization.