2024 Tech Survey for CYBER LIABILITY INSURANCE RENEWAL

The survey will take approximately 14 minutes to complete.

* Required

1

Please provide Parish Number, Parish Name and City **(ie, 417, All Saints, Stuart)** OR School Name OR Name of Entity (ie, Emmaus House). *

2

Please provide the name and title or primary role of the person completing this survey: *

3

Do you collect, store, host, process, control, use or share any private or sensitive information* in either paper or electronic form? *

**Private or sensitive information includes any information or data that can be used to uniquely identify a person, including, but not limited to, social security numbers or other government identification numbers, payment card information, drivers' license numbers, financial account numbers, personal identification numbers (PINs), usernames, passwords, healthcare records and email addresses.*

- ◯ Yes
- ◯ No
- ◯ N/A

4

If you answered "Yes" to the above question, please provide the approximate number of unique paper records. (Otherwise, type "n/a".) *

5

Also, if you answered "Yes", please provide the approximate number of unique electronic records. (Otherwise, type "n/a".) *

6

Do you collect, store, host, process, control, use or share any biometric information or data, such as fingerprints, voiceprints, facial, hand, iris or retinal scans, DNA, or any other biological, physical or behavioral characteristics that can be used to uniquely identify a person? *

Biometric Information
Biometrics are biological measurements — or physical characteristics — that can be used to identify individuals. For example, fingerprint mapping, facial recognition, and retina scans are all forms of biometric technology

- ◯ Yes
- ◯ No
- ◯ N/A

7

If you answered “Yes” to the above question, have you reviewed your policies relating to the collection, storage and destruction of data with a qualified attorney and confirmed compliance with applicable federal, state, local and foreign laws? *

- ◯ Yes
- ◯ No
- ◯ N/A

8

Do you use a cloud provider to store data or host applications, ie, One Drive, GoogleDrive, etc.? *

Cloud Provider
A cloud service provider is an information technology (IT) company that provides its customers with computing resources over the internet and delivers them on-demand. CSPs are well-suited for organizations and individuals who don't want the responsibility of installing software, hardware or network resources, storing data -- and maintaining them until the end of their life cycles.

- ◯ Yes
- ◯ No
- ◯ N/A

9

If you answered "Yes" to the above question, please provide the name of the cloud provider. (Otherwise, type "n/a".) *

(If you use more than one cloud provider to store data, please specify the cloud provider storing the largest quantity of sensitive customer and/or employee records (e.g., including medical records, personal health information, social security numbers, bank account details and credit card numbers) for you.)

10

Do you use anti-virus software and a firewall to protect your network (desktop computers & servers)? *

If you answer "No", coverage cannot be bound under this program.

- ◯ Yes
- ◯ No
- ◯ N/A

11

If you answered "No" to the above question, please provide details of why you do not have anti-virus software or a firewall. (Otherwise, type "n/a".) *

12

Do you encrypt all sensitive and confidential information stored on your organization's systems and networks? *

- ◯ Yes
- ◯ No
- ◯ N/A

13

If "No" to the above question, is the following control in place? *

(1) Segregation of servers that store sensitive and confidential information:

- ◯ Yes, we have a segregation of servers
- ◯ No, we don't have a segregation of servers
- ◯ Don't understand the question (please contact the Diocese)
- ◯ n/a - I answered yes to Q12

14

Also if "No", is the following in place? *

(2) Access control with role-based assignments.

- ◯ Yes, access controls with role-based assignments are in place
- ◯ No, access controls with role-based assignments are not in place
- ◯ Don't understand the question (please contact the Diocese)
- ◯ n/a - I answered yes to Q12

15

Please provide details on why you do not have any of the above security controls in place. (Otherwise, type "n/a".) *

(If you answered "No" to Q12 AND Q13 AND Q14, you may not qualify for coverage under this program.)

16

Do you use 2-factor authentication to secure all remote access to your network, including any remote desktop connections? *

If you answer "No" to this question, coverage cannot be bound under this program.

2-Factor Authentication
Two-factor authentication (2FA) is a security system that requires two separate, distinct forms of identification in order to access something. The first factor is a password and the second commonly includes a text with a code sent to your smartphone, or biometrics using your fingerprint, face, or retina.

- ◯ Yes
- ◯ No
- ◯ N/A

17

Do you use 2-factor authentication to secure remote access to your emails accounts? *

If you answer "No" to this question, coverage cannot be bound under this program.

- ◯ Yes
- ◯ No
- ◯ N/A

18

Do you use Endpoint Detection and Response (EDR) or a Next-Generation Antivirus (NGAV) software (e.g., CrowdStrike, Cylance, Carbon Black) to secure all system endpoints? *

If you answer "No" to this question, coverage cannot be bound under this program.

Endpoint Detection and Response
Endpoint Detection and Response (EDR), also referred to as endpoint detection and threat response (EDTR), is an endpoint security solution that continuously monitors end-user devices to detect and respond to cyber threats like ransomware and malware.

- ◯ Yes
- ◯ No
- ◯ N/A

19

If you do use an Endpoint Detection and Response (EDR) or a Next-Generation Antivirus (NGAV) software, please provide the name of your provider. (Otherwise, type "n/a".) *

(Examples of providers: CrowdStrike, Cylance, Carbon Black)

20

Email Filtering Software
An email filtering service is a process of filtering emails that are inbound to the user's mailbox and outgoing from the user's server. Inbound email filtering checks and filters the incoming emails for spam, malware, suspicious links, etc. and also organizes the messages into different categories or folders.

Do you use an email filtering solution designed to prevent phishing or ransomware attacks (in addition to any filtering solution(s) provided by your email provider)? *

If you answer "No" to this question, coverage cannot be bound under this program.

- ◯ Yes
- ◯ No
- ◯ N/A

21

If you do use Email Filtering Software, please provide the name of your filtering solution provider. (Otherwise, type "n/a".) *

22

Data Backup
The practice of copying data from a primary to a secondary location, to protect it in case of a disaster, accident or malicious action.

Do you use a data backup solution for all critical data? *

If you answer "No" to this question, coverage cannot be bound under this program.

- ◯ Yes, it runs daily
- ◯ Yes, it runs weekly
- ◯ Yes, it runs monthly
- ◯ No
- ◯ Don't know
- ◯ I don't understand the question (please contact the Diocese)
- ◯ N/A

23

Is your data backup solution segregated and/or disconnected from your network in such a way to reduce or eliminate the risk of the backup of the backup being compromised in a malware or ransomware attack that spreads through out the network? *

If you answer "No" to this question, coverage cannot be bound under this program.

Malware
Malware (short for “malicious software”) is a file or code, typically delivered over a network, that infects, explores, steals or conducts virtually any behavior an attacker wants. And because malware comes in so many variants, there are numerous methods to infect computer systems. Though varied in type and capabilities, malware usually has one of the following objectives:

Provide remote control for an attacker to use an infected machine.

Send spam from the infected machine to unsuspecting targets.

Investigate the infected user’s local network.

Steal sensitive data.

Ransomware
Ransomware is a type of malicious software that infects a computer and restricts users' access to it until a ransom is paid to unlock it. Ransomware variants have been observed for several years and often attempt to extort money from victims by displaying an on-screen alert.

- ◯ Yes
- ◯ No
- ◯ N/A

24

Do all employees with financial or accounting responsibilities at your church or school complete social engineering training which is manipulation techniques to gain private information, access, or valuables? *

Social Engineering Training
Social engineering is a popular technique because criminals can bypass the technical side of security, such as firewalls, vulnerability scanning, and penetration testing, and get information directly from an individual. Because of its popularity and increasing sophistication, social engineering is a huge vulnerability to businesses since all employees are susceptible to social engineering attempts. This is why training your workforce on social engineering should be a top priority.

- ◯ Yes
- ◯ No
- ◯ N/A

25

If you answered "Yes" to the above question, does such training include phishing simulation? *

Simulated Phishing
Simulated phishing or a phishing test is where deceptive emails, similar to malicious emails, are sent by an organization to their own staff to gauge their response to phishing and similar email attacks. The emails themselves are often a form of training, but such testing is normally done in conjunction with prior training; and often followed up with more training elements. This is especially the case for those who "fail" by opening email attachments, clicking on included weblinks, or entering credentials.

- ◯ Yes
- ◯ No
- ◯ N/A

26

In the past 12 months, has your parish or school received any complaints or written demands or been a subject in litigation involving matters of privacy injury, breach of private information, network security, defamation, content infringement, identity theft, denial of service attacks, computer virus infections, theft of information, damage to third party networks or the ability of third parties to rely on the Applicant's network? *

- ◯ Yes
- ◯ No
- ◯ N/A

27

In the past 12 months, has your parish or school been the subject of any government action, investigation or other proceedings regarding any alleged violation of privacy law or regulation? *

- ◯ Yes
- ◯ No
- ◯ N/A

28

In the past 12 months, has your parish or school been notified customers, clients or any third party of any security breach or privacy breach? *

- ◯ Yes
- ◯ No
- ◯ N/A

29

In the past 12 months, has your parish or school received any cyber extortion demand or threat? *

- ◯ Yes
- ◯ No
- ◯ N/A

30

In the past 12 months, has your parish or school sustained any unscheduled network outage or interruption for any reason? *

- ◯ Yes
- ◯ No
- ◯ N/A

31

In the past 12 months, has your parish or school sustained any property damage or business interruption losses as a result of a cyber-attack? *

- ◯ Yes
- ◯ No
- ◯ N/A

32

In the past 12 months, has your parish or school sustained any losses due to wire transfer fraud, telecommunications fraud or phishing fraud? *

- ◯ Yes
- ◯ No
- ◯ N/A

33

In the past 12 months, has any IT service provider that your church or school relies on sustain an unscheduled network outage or interruption lasting longer than 4 hours? *

- ◯ Yes
- ◯ No
- ◯ N/A

34

If you answered "Yes" to the above question, did the you experience an interruption in business due to the service providers outage or interruption? *

- ◯ Yes
- ◯ No
- ◯ N/A

35

Does the parish/school have a password policy in place which includes length and strength requirements? *

Examples would be minimum of 15 characters, one capital letter, one symbol, two numbers.

Password Policy
A password policy defines the password strength rules that are used to determine whether a new password is valid. A password strength rule is a rule to which a password must conform. For example, password strength rules might specify that the minimum number of characters of a password must be 5.

- ◯ Yes, and it includes length and strength requirements
- ◯ Yes, but it does NOT include length and strength requirements.
- ◯ No, we do not have a policy in place
- ◯ N/A

36

Does your policy require passwords to expire and be reset after a minimum of 90 days? *

- ◯ Yes
- ◯ No
- ◯ N/A

37

Do software applications containing confidential information require a separate user based password? *

- ◯ Yes
- ◯ No
- ◯ N/A

38

Is a user-based password required to access each parish/school computer? *

If uncertain, enter CTRL-ALT-DEL to lock the computers screen. A password should be required to unlock the screen.

- ◯ Yes
- ◯ No
- ◯ N/A

39

Does each parish/school computer have password-protected hibernation enabled? *(If uncertain, go to settings for the computer, select System/Power & sleep, Screen should be set to 15 minutes. Then select Accounts/Sign-in options, Require sign-in should be set to "When PC wakes up from sleep". This setting should only be accessible by an administrator.)* *

- ◯ Yes
- ◯ No
- ◯ N/A

40

Is there a wireless network operating within your parish/school property? *

Wireless Network
Wireless networks are computer networks that are not connected by cables of any kind. The use of a wireless network enables enterprises to avoid the costly process of introducing cables into buildings or as a connection between different equipment locations.

- ◯ Yes
- ◯ No
- ◯ N/A

41

Is the wireless network secured by WEP, WPA, or WPA2? *

- ◯ Yes, WEP
- ◯ Yes, WPA
- ◯ Yes, WPA2
- ◯ Yes, WPA3
- ◯ No
- ◯ N/A
- ◯ I don't understand the question (please contact the Diocese)
- ◯ I don't know what we have

42

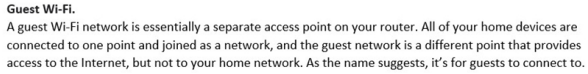
Is the wireless access password protected? *

For example, if you connect a personal device to WiFi, do you have to put in a password?

- ◯ Yes
- ◯ No
- ◯ N/A

43

Do you allow guests on the same wireless network that the office/school staff uses? *



- ◯ Yes
- ◯ No
- ◯ N/A

44

Are parish-issued mobile devices utilized for parish/school business? *

Mobile devices include laptops, tablets, cell phones, and USB storage devices.

- ◯ Yes
- ◯ No
- ◯ N/A

45

Do you allow personal devices (laptops, tablets, thumb drives, portable drives) to be used for parish/school business? *

- ◯ Yes
- ◯ No

46

If you DO allow personal devices to be used for parish/school business, please describe the **type of business allowed on non parish-issued mobile devices.** (Otherwise, type "n/a".) *

47

Are any mobile devices, parish issued or personal, allowed to connect to the Parish/School's network either through VPN or email? *

- ◯ Yes, parish-issued only
- ◯ Yes, personal and parish issued
- ◯ No
- ◯ N/A

48

Are the devices encrypted? *

- ◯ Yes
- ◯ No
- ◯ N/A

49

Are the devices password protected? *

- ◯ Yes
- ◯ No
- ◯ N/A

50

Is there a Mobile Device Use Policy in place? *

- ◯ Yes
- ◯ No
- ◯ N/A

51

Please use the space below for any additional comments. *Thank you for your assistance in this important survey as we approach the renewal process for cyber-liability coverage for all entities within the Diocese of Des Moines.*