Church Security Assessment Questions

Question	Weight	If Yes, Enter Weight
Does your church have information security policies and procedures in place?	6	
Do you know the legal requirements for reporting data breaches that apply to your church (local, state, federal, & industry-specific)?	5	
Do you check and update your security plans every year?	5	
Is there a specific team or individual within your church responsible for managing information technology?	4	
Has your church developed a crisis management plan and assembled a team to handle potential data breaches or cyber incidents?	4	
Does your church have a careful way to manage changes to the security settings of computers, servers, and other devices?	4	
Do you train your staff and volunteers each year about keeping information safe and spotting tricks that could steal company secrets?	6	
Do you maintain an inventory of all hardware devices connected to your network?	4	
Has anyone from outside your church ever checked how safe your computer systems are?	3	
Does your church have a system in place for creating and storing backup copies of crucial data?	5	
Do you regularly update and/or patch the software on your computers (recommended at least quarterly)? Are all laptops and mobile devices that can access your church's systems protected with passwords or special codes?	5	
Are all devices that can access your church's systems protected with passwords?	4	
Do the users of devices have administrator privileges?	5	
Do all of your applications require unique logins for each user?	5	
Does your church enforce the use of strong, complex passwords?	5	
Does your church keep track of all the software on the network to make sure only approved programs are installed?	4	
Has your church set up a separate network specifically for visitors and non-employees?	4	
Is your network divided into distinct sections to protect different types of assets?	3	
Does your church make you use two ways to prove who you are (like a password and a code sent to your phone) when you log into email or other services from outside?	5	
Does your church's website employ HTTPS encryption to safeguard all transmissions of sensitive data?	4	
Are all devices that can access your church's systems equipped with antivirus software and firewall protections?	3	
Do you have a way to check if vendors and suppliers (ie., online giving) are safe and what risks they might bring to your church?	5	
Do you perform background checks on all employees and volunteers?	2	
	Total	

100-90:
Organizations scoring in this range demonstrate exceptional cybersecurity maturity. They have comprehensive policies, procedures, and technical controls in place, with a proactive approach to security that includes regular assessments, employee training, and incident response preparedness. These organizations are well-equipped to handle current and emerging cyber threats, showing a strong commitment to protecting their digital assets and maintaining compliance with relevant regulations.

89-80:
Organizations in this range exhibit strong cybersecurity practices, with most key elements of a mature security program in place. While there may be some areas for improvement, these organizations generally have effective policies, regular security assessments, and good awareness among staff. They are likely to be resilient against many common cyber threats but may benefit from fine-tuning certain aspects of their security strategy to reach the highest level of maturity.

79-70:
Organizations scoring in this range have implemented several important cybersecurity measures but still have significant room for improvement. While they may have some solid practices in place, there are likely gaps in their security posture that could leave them vulnerable to certain types of attacks. These organizations should focus on addressing their weak points, enhancing employee training, and implementing more robust technical controls to improve their overall security maturity.

Below 70:
Organizations scoring below 70 demonstrate a concerning lack of cybersecurity maturity. They likely have significant gaps in their security policies, procedures, and technical controls, leaving them highly vulnerable to various threats. These organizations urgently need to prioritize cybersecurity, implement fundamental security measures, and develop a comprehensive strategy to protect their digital assets and sensitive information.