cimatri concierge IT

The Ultimate Cybersecurity Checklist For Associations

The **Ultimate Cybersecurity Checklist** for Associations

Is your data protected against theft and loss?
Does your association have the tools to combat a costly cyberattack?
Can you afford the cost and business interruptions that come with a ransomware attack?
Are your cybersecurity practices in alignment?

If your answer to any of the above questions is “no”, this checklist is for you. With our Concierge IT service, the ultimate goal is to help your association position itself as a reliable business partner capable of supporting innovation at scale.

Use this checklist to find out if you have the right tools to reach your association’s objectives.
Don't forget to score the health of your cybersecurity at the bottom.

cimatri concierge IT

1. Policy and Management

- ☐ We have a comprehensive set of security policies that are distributed to all users (staff, consultants, vendors, etc.) of IT.
- ☐ Our policies or procedures include data classifications.
- ☐ We have an IT Director who manages day-to-day operations, including IT resources, in-house IT staff, and IT vendors.
- ☐ We have an IT service desk to support users with all IT support requests 24 hours per day, 7 days per week.
- ☐ We have a designated Chief Information Security Officer (CISO) responsible for managing cybersecurity initiatives and programs.
- ☐ We consider the implications of AI in our security policy, ensuring responsible and ethical AI usage.

How did you do? Write your score here ☐

2. Access Control and Authentication

- ☐ We only allow users access the software/programs needed to perform their functions.
- ☐ We enforce strong password use for our network login and on our enterprise SaaS Applications.
- ☐ Our employees use an IT managed password management tool to track their application logins.
- ☐ We require 2FA or MFA to access our network resources o on all SaaS applications that offer that capability o on our enterprise database applications
- ☐ We require 2FA on our payroll and human resource applications.
- ☐ Passwords are required on personal mobile devices that connect to network resources.
- ☐ We perform regular access audits to make sure only users who need access can gain access.
- ☐ AI tools are monitored and controlled to prevent unauthorized access.
- ☐ We regularly update and assess our AI-based access control mechanisms to address evolving security threats.

☐ **How did you do? Write your score here**

3. Employee Training and Awareness

- ☐ We provide cybersecurity and AI security awareness training for our employees.
- ☐ We provide advanced security awareness training for all staff with privileged access to our systems or network.
- ☐ Our employees are aware of cybersecurity and AI security risks.
- ☐ Our vendors are aware of cybersecurity and AI security risks.
- ☐ We conduct periodic phishing tests on our network users.

How did you do? Write your score here ☐

4. Network and Device Security

- ☐ We conduct periodic audits and reviews of our firewall settings.
- ☐ We always use a VPN.
- ☐ We are aware of who should use a VPN and under what circumstances.
- ☐ Our firewall's software/firmware runs the most recently released version(s).
- ☐ We deploy managed virus software to all endpoints in use.
- ☐ Remote wipes are conducted with lost or stolen mobile devices.
- ☐ We regularly update and patch all software and operating systems on devices connected to the network.
- ☐ We use AI-based security systems to monitor, detect, and prevent intrusion and unusual network behavior in real time.

☐ **How did you do? Write your score here**

5. Data Security and Encryption

- ☐ We encrypt sensitive data both at rest and in transit.
- ☐ We have systems with alerts in place to monitor for suspicious activity (i.e., login from foreign countries).
- ☐ Files can be easily retrieved when accidentally removed from staff file share.
- ☐ Files stored on a laptop are recoverable.
- ☐ Our AI models are protected against adversarial attacks.

How did you do? Write your score here ☐

6. Risk Assessment and Cybersecurity Insurance

- ☐ We have cybersecurity insurance.
- ☐ We are aware of our most valuable technological assets. For example, we know what we should protect first and best.
- ☐ We have ranked the impact of various types of attacks. For example, would a ransomware attack be more damaging than a malware attack?
- ☐ We have identified potential threats and their sources. For example, do any of your vendors pose a threat because of their lax security standards?
- ☐ We have calculated the areas of greatest risk both inside and outside of our organization.
- ☐ We are able to forecast the impact of various breaches.
- ☐ We are able to determine the probability of successful attacks and have established an acceptable level of risk.
- ☐ We have a Security Operations Center monitoring all of our endpoints (Windows and Mac laptops/desktops), all devices in our network, and our key cloud services (e.g. Microsoft 365).
- ☐ We have an incident response playbook for ransomware attacks that includes containment, communications, and recovery steps.
- ☐ We regularly conduct penetration tests and vulnerability assessments to identify and address potential weaknesses in our systems and network.
- ☐ We have established a process for regularly reviewing and updating our cybersecurity policies and practices to ensure they remain effective and up-to-date.
- ☐ We have conducted a risk assessment of our AI tools and incorporated this into our wider cybersecurity risk profile.
- ☐ We have appropriate cybersecurity insurance that covers AI-specific threats and vulnerabilities.
- ☐ We have mechanisms to ensure the transparency and explainability of AI systems, for effective audit and risk assessment.

☐ **How did you do? Write your score here**

What is Your Association's **Cyber Risk**?

How'd You Score?

Count the number of checks you placed in the boxes above to measure the health of your data.

40+ Not too bad but there's always room for improvement.

30–40 Needs some work. Don't get complacent when it comes to your association's security.

20–30 Your cybersecurity isn't working for you. However, there are threats that are working 24/7 to compromise your association's IT.

0–20 Your cybersecurity problems are significantly holding you back. You need a plan immediately to combat guaranteed threats to your association.

If you scored less than 40, there are some **crucial holes** in your cybersecurity health. Get a plan in place today to resolve these issues and ensure your organization and its information is protected.

At Cimatri, our Concierge IT Service is designed to help your association climb the ladder of digital maturity. We do more than keep the lights on, we help you harness the transformational power of cloud infrastructure while bringing you the best technology, thought leaders, and white glove service that brings it all together.

If you are struggling with security and are looking for a comprehensive IT solution, learn more about how we can help here.

Email us at info@cimatri.com or call (571) 249-2719 to get started.