

Top 10 Security Tips

1. Provide **Threat Management Training** to ensure your team understands emerging security threats (e.g., phishing or exploitation of weak passwords) and is well equipped to identify and avoid them.
2. Conduct **Penetration Testing** to identify your systems and applications that are vulnerable to a cyberattack and move quickly to eliminate the vulnerabilities before a potentially devastating attack occurs.
3. Perform a **Privacy Impact Assessment** to get a detailed understanding of how sensitive data is used in your organization and recommendations for mitigating associated risks in the context of today's rapidly evolving regulatory environment.
4. Put in place an **Emergency Incident Management and Response** team that is available 24/7 and includes incident responders, malware experts, and cyber intelligence professionals to contain and remove cyber threats immediately.
5. Ensure your current and planned cloud-based systems are architected and secured in a way that addresses the unique **Cloud Security and Compliance** requirements of this complex and dynamic environment.
6. Conduct a **Risk Assessment** to identify and prioritize potential cybersecurity and other risks in your organization and implement an action plan to mitigate the identified risks.
7. Protect valuable intellectual property and consumer information and avoid potential penalties by ensuring your organization meets the **Compliance** requirements specific to your industry (e.g., PCI for payments or HIPPA for health care).
8. Conduct a **Cyberattack Readiness Assessment** to determine how equipped you are to respond to a security breach then move quickly to shore up any weak points identified in the assessment.
9. Identify experts that can immediately perform **Malware Analysis** when malicious software is detected on your systems, enabling rapid identification and quarantine of the malware to minimize negative impacts.
10. Implement a **Vendor Risk Management** program with centralized processes, policies, and controls that ensures you are managing your vendors in a way that is secure and effective and minimizes risks related to outsourcing and data privacy.