XANTRION
CYBERSECURITY • IT SUPPORT

# 2024 CYBERSECURITY TO-DO LIST

Ransomware, AI, cloud computing, and new regulations from states and the SEC, are all factors that will affect cybersecurity priorities in 2024.

We have compiled this 10-step to-do list to help you shape your cybersecurity strategy for the year.

## RANSOMWARE

1. Plan for the impact of AI on ransomware, including AI-enhanced threats and AI tools for your defense.
2. Develop an Incident Response Plan that ensures rapid response and facilitates adherence to regulatory requirements, such as state and SEC incident reporting timelines.

## THIRD-PARTY RISK MANAGEMENT

3. Perform detailed risk assessments of third-party vendors, including software vendors, if they store or handle sensitive information.

## VULNERABILITY MANAGEMENT

4. Develop a program that identifies vulnerabilities regularly and prioritizes them so you can remediate critical issues in a timely manner.

## CLOUD SECURITY

5. Evaluate whether you should provide cloud training for cybersecurity staff members and/or augment your team with cloud experts.
6. Evaluate AI and other automation for cloud management, especially those involving vulnerability or asset management.

## IDENTITY AND ACCESS MANAGEMENT

7. Ensure your cybersecurity team has identity monitoring tools that include AI or other automation which enable them to quickly detect and respond to identity compromises.
8. Consider enhancements to identity management, such as phish-resistant capabilities, especially for executives and administrative personnel with high privilege.

## GENERATIVE AI

9. Develop a company policy regarding the use of public AI tools like ChatGPT and Google Bard to prevent data privacy and security breaches.
10. Evaluate whether you should provide AI training for cybersecurity staff members and/or augment your team with AI experts.

Source: SC Magazine — 2023 Cybersecurity Year in Review
Arctic Wolf — The Human AI Partnership