ARCTIC WOLF

The CIO's Cybersecurity Checklist

CIOs used to struggle to get their boards and C-suites invested in cybersecurity as a business priority.

Now? It's at the top of most companies' agendas. A cyberattack today can halt operations, erode customer trust, and expose a company to lawsuits and regulatory fines. Organizations large and small from all over the world are at risk, making cybersecurity a top concern for management.

Effective cybersecurity starts at the top. It needs to be a built-in function of business strategy, championed by employees across the organization. For the CIO, that means clear leadership and a comprehensive cybersecurity strategy that includes constant vigilance, a comprehensive view of stakeholders, and strict compliance.

Use this checklist to develop your cybersecurity strategy, step-by-step:

Analyze Risk

The threat landscape is enormous and continues to expand. The first step in building a cybersecurity strategy is to assess where and how your business may be attacked.

- Identify every potential access point so it can be effectively monitored. Entry points range from infrastructure and in-house applications to SaaS solutions and cloud services. Physical devices continue to multiply, raising the challenge. Your organization must secure laptops and mobile devices, both business and personal, and devices used in the burgeoning Internet of Things.
- Oversee all access to secure the network. Review employee, partner, customer, SaaS/cloud provider, and all third-party vendor access. People are one of the greatest risks to the business, whether because of malice or human error.

See Risks in Real Time

CIOs need a real-time, 24/7 view of internal risk, not only to secure the network, but to ensure effective reporting to the rest of the C-suite and the board.

- Establish a vulnerability management system either in-house or through a provider that can display in a dashboard an overview of the current threat level to the organization, past events and incidents that have occurred, and any authentication errors or unauthorized access in a single pane of glass. This will give the most complete picture of the entire network.
- Review reports on any attempted or successful cyberattacks such as brute force attacks, and malware or phishing attempts. This data will support initiatives to update and patch the network, as well as educate on current threat levels and risks.

Monitor the Cloud

As a CIO you need an overview of the cloud environment, so make sure your organization monitors cloud assets and services in addition to its internal business network.

- Build a complete picture of user and administrator access and behavior. This will tip off the team in case hackers obtain credentials or malicious insiders are active.
- Confirm the team can keep tabs on third-party API access, which may be used in man-in-the-middle (MITM) attacks.

Engage All Stakeholders

Armed with real-time information, a CIO can engage the entire leadership team about the organization's cybersecurity strategy.

- Instill consciously secure behavior from the top down to ensure that business devices are properly secured and that only secure devices are used for business activity. Review security controls and processes regularly with the leadership team.
- Provide training and development for all staff members and enforce the cybersecurity policies of the organization. This will minimize human error and prepare all staff to meet the current threat landscape.

Keep Compliance Up to Date

The CIO has to take the final responsibility for compliance with regulations and legislation in order to give staff and customers peace of mind on the reliability of the business and the safety of their personal data.

- Ensure data protection tools and policies are implemented and followed. Accountability is a core principle of data protection. Not only are companies responsible for personal information, they also must demonstrate compliance, especially in industries like finance, healthcare, and law.
- Hire a data protection officer and establish written contracts with external partners to ensure compliance across the business.
- Record all data breaches so that you can, where necessary, report these to relevant authorities. Or look to integrate with a partner who will document and report on vulnerabilities and breaches.

Be Ready to Report

Leveraging threat detection and response capabilities combined with vulnerability management will sufficiently prepare the CIO to effectively report to the board.

- Be able to provide a comprehensive overview of cyber risk at any given moment, leveraging a partner's security expertise if needed. This feeds into the development and implementation of risk management and business continuity plans.
- Be ready to show why an adequate budget for cybersecurity is needed. Detailed reporting centered around existing threats and proper incident response procedures and planning helps make the case.

Invest in a Security Operations Center

For most CIOs, even with the full support of the C-suite and business leadership along with engagement from staff, staying on top of everything is no easy task.

A security operations center (SOC) offers the people, process, and technology you need to manage cyber risk and meet all compliance requirements, along with the round-the-clock expertise needed to hunt down and respond to threats.

- Put in place a SOC (in-house or as-a-service) that not only monitors and assesses risk, but also responds to incidents 24/7 with a dedicated team of experts, such as Arctic Wolf's Concierge Security® Team.
- Look for a solution that also includes centralized logging of all network events and a detailed framework for managing compliance in accordance with security regulations and guidelines.

Wondering what's the best way to address these challenges?

Discover how Arctic Wolf® helps you check off every item on the list in the most comprehensive, secure, and affordable way possible.

ABOUT ARCTIC WOLF

Arctic Wolf® is the market leader in security operations. Using the cloud-native Arctic Wolf® Platform, we provide security operations as a concierge service. Highly trained Concierge Security® experts work as an extension of your team to provide 24x7 monitoring, detection, and response, as well as ongoing risk management to proactively protect systems and data while continually strengthening your security posture.

For more information about Arctic Wolf, visit arcticwolf.com.

ARCTIC WOLF

AW_CIO-Cybersecurity-Checklist_0520

SOC2 Type II Certified

ISO 27001 CERTIFIED CYBERGUARD COMPLIANCE

Contact Us

arcticwolf.com
1.888.272.8429
ask@arcticwolf.com