ARCTIC WOLF

The IT Director's Cybersecurity Checklist

For IT directors, a lack of resources is a critical reality when it comes to cybersecurity.

Few IT teams have the necessary talent and budget to meet the increasing threat landscape. The number of bad actors profiting by illicit means continues to grow. And the software and the techniques they use are more sophisticated than ever before.

That's just for starters. The number of entry points continues to climb exponentially. Physical devices are proliferating, from mobiles to those used for the Internet of Things. What's more, today's businesses rely on technology with roots from a variety of sources, such as software coming from third-party SaaS or IaaS providers, from one-off vendor purchases, and from cloud solutions. The attack surface stretches beyond what just a few years ago was unfathomable.

So, what can an IT director do to keep your organization ahead of mounting threats to stay safe and secure? The Center for Internet Security (CIS) recommends starting with basic, often-overlooked precautions when it comes to building a solid security posture.

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

Inventory and Control Hardware and Software Assets

You can't secure assets you don't know you have. Reducing your organization's attack surface starts by having a complete view of all devices on your network. IT teams should make every effort to document and manage authorized devices and the software the devices run. IT teams must also quickly disconnect from their network all unauthorized devices, as well devices that run potentially dangerous software.

- ✓ Secure business devices, and outline and enforce strong security guidelines for personal devices. Don't let unsecured devices onto the network. Use guest networks for visitors.
- ✓ Utilize inventory tools throughout the organization to facilitate up-to-date records of existing software and hardware.
- ✓ Oversee all user access to the business network, record authentication errors and unauthorized access, and sweep the network for unusual user behavior.
- ✓ Create an escalation workflow for afterhours incidents involving unauthorized devices.

Continuously Manage Vulnerabilities

The IT team must have 24x7 real-time cybersecurity operations that can manage vulnerabilities, monitor and detect threats, and respond to malicious and risky activity in real time.

- ✓ Prioritize responses so that vulnerabilities and intrusions that pose the highest risk and greatest threat are addressed first, instead of concentrating on less critical and non-essential tasks.
- ✓ Be ready to answer how security impacts business decisions, including where risk exists and how risks are mitigated.

Control Administrative Privileges

Administrative credentials are like the keys to your organization's front door, and a favorite target for cybercriminals seeking access to your data. Simple, re-used passwords and administrative accounts in disarray make stealing critical data easy for bad actors.

- ✓ Ensure all employees use password managers, single sign-on, and multi-factor authorization as part of their cyber hygiene.
- ✓ Set a password policy that requires unique and complex passwords for every employee.
- ✓ Make sure your staff is updated on security training and warned about current known threats, such as phishing attacks. Preparing and educating staff members makes them part of the solution.
- ✓ Ensure IT team members have admin access to all 3rd-party software applications that access confidential or potentially sensitive data.

Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers

Manufacturers design default configurations with user experience and ease-of-use in mind; security tends to be an afterthought. Basic controls, old protocols, preinstallation of unneeded bloatware, and open ports are easy targets for cybercriminals. Good configuration doesn't stop when users get access to devices, as you'll need to watch continuously for changes when systems are patched or updated.

- ✓ Ensure the IT team records past events and incidents—such as configuration changes, anomalies to inbound and outbound traffic, unusual behavior by privileged users, etc.—to build a complete picture of threats.
- ✓ Maintain documented security configuration standards for all operating systems and software in use.
- ✓ Utilize a Security Content Automation Protocol (SCAP)-compliant configuration monitoring system.

Maintain, Monitor, and Analyze Audit Logs

Without audit logs, attacks may go unnoticed and uninvestigated, leaving the door open to additional attacks and untold potential damages.

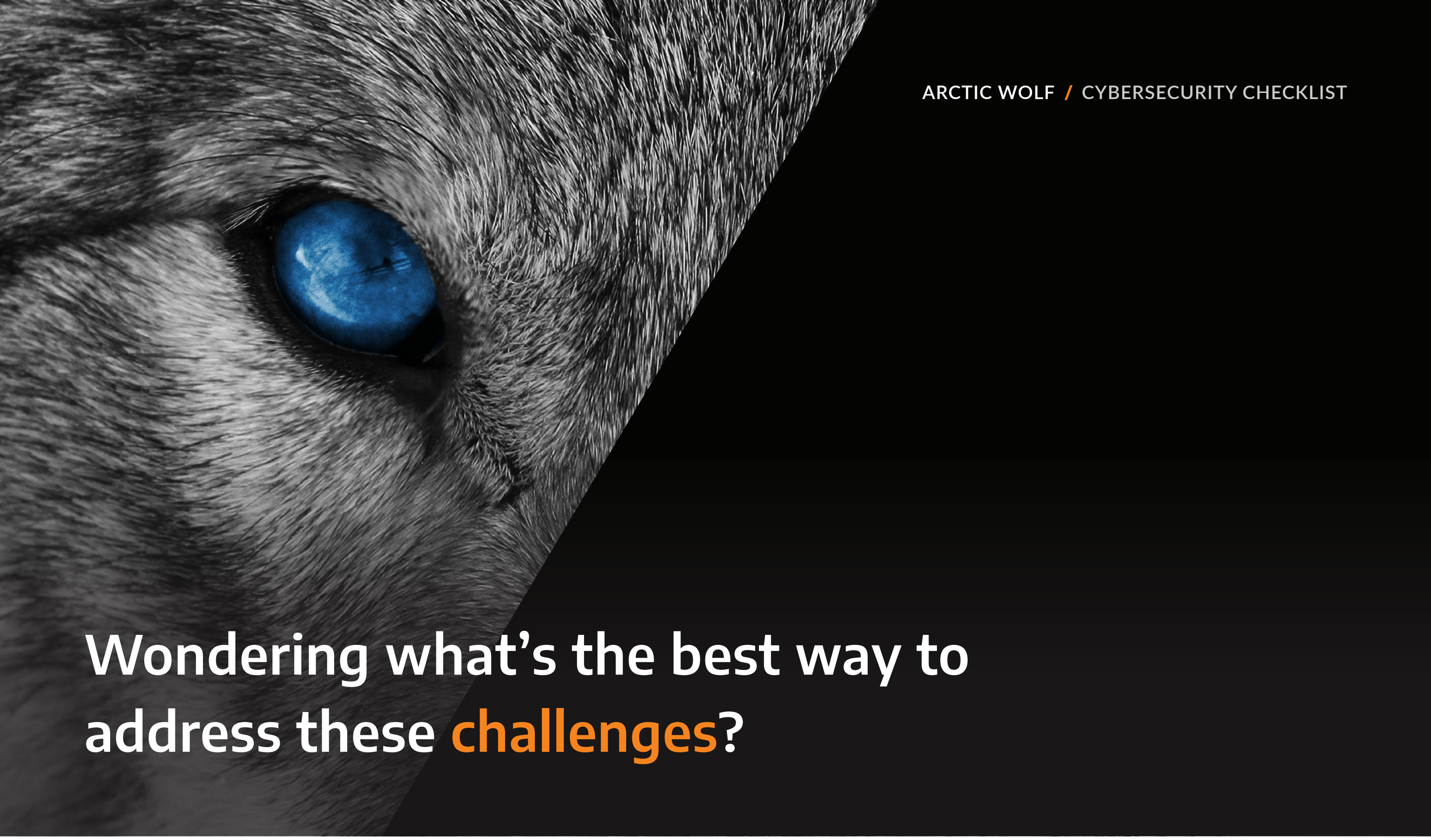
Most IT teams keep audit records for compliance purposes, but attackers know there are many organizations who lack the time or resources to review logs on a regular basis, which provides a generous window of time to access systems and data undetected.

- ✓ Enable local logging on all systems and devices.
- ✓ Have a plan to analyze and review log data in real time.

Bonus Tips: Security is a Process, Not a Project

Staying secure is not always painless, and it requires a certain amount of diligence from your entire organization. This means fostering a strong security culture from day one so that all employees—not just those in IT—employ strong security practices whenever they use their work devices or access your network. They must also be aware of physical security concerns and company practices to ensure access control and a safe and secure workplace that intruders can't exploit.

- ✓ Ensure HR policies and onboarding cover best security practices. This starts with creating a clear company security policy and communicating security expectations on an ongoing basis.
- ✓ Determine budgetary needs and plan ahead so cybersecurity defenses can scale sufficiently as the organization continues to grow.
- ✓ Stay on top of compliance. Attend virtual and in-person events to understand how new regulations impact your business. Consult corporate counsel to ensure your security standards satisfy federal and state cybersecurity guidelines.
- ✓ Suggest where insurance, added controls, or new tools could improve compliance with upcoming regulations and guidelines, especially as your business expands into new markets.



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

Discover how Arctic Wolf SOC-as-a-service helps you check off every item on the list in the most comprehensive, secure, and affordable way possible.

ABOUT ARCTIC WOLF

Arctic Wolf Networks delivers the industry-leading security operations center (SOC)-as-a-service that redefines the economics of cybersecurity. Arctic Wolf™ Managed Detection and Response and Managed Risk services are anchored by the Arctic Wolf Concierge Security™ Team who provides custom threat hunting, alerting, and reporting. The Arctic Wolf purpose-built, cloud-based SOC-as-a-service offers 24×7 monitoring, risk management, threat detection, and response.

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

ARCTIC WOLF

SOC2 Type II Certified

AICPA SOC

ISO 27001 CERTIFIED CYBERGUARD COMPLIANCE

Contact Us

arcticwolf.com
1.888.272.8429
ask@arcticwolf.com