CYBERSNAP

Cybersecurity Culture Creators

Cybersecurity Culture Checklist

Use this checklist to assess and strengthen your organization’s cybersecurity culture. Each item reflects a best practice for fostering awareness, accountability, and resilience through a people-centric approach.

Leadership & Governance

- Leadership actively promotes cybersecurity as a core organizational value.
- Cybersecurity roles and responsibilities are clearly defined for all staff.
- A designated security champion or ambassador exists within each team or department.
- Security policies are accessible, up-to-date, and regularly communicated.

Employee Awareness & Training

- All employees receive regular, engaging cybersecurity awareness training.
- Training includes real-world scenarios, such as phishing simulations.
- New hires complete cybersecurity onboarding as part of their orientation.
- Refresher courses are provided at least annually or when new threats emerge.

Phishing & Threat Preparedness

- Employees are trained to recognize and report phishing attempts.
- Simulated phishing exercises are conducted periodically.
- Reporting suspicious emails or incidents is simple and encouraged.

Communication & Openness

- Staff are encouraged to speak up about security concerns or mistakes without fear of blame.
- Security updates, tips, and reminders are shared through multiple channels (e.g., email, intranet, meetings).
- Lessons learned from incidents are shared to foster continuous improvement.

Secure Habits & Behaviours

- Strong password practices are promoted and enforced (e.g., password managers, MFA).
- Employees lock screens and secure devices when unattended.
- Data handling and sharing guidelines are clear and followed.
- Personal and work device usage policies are established and understood.

Incident Response & Reporting

- There is a clear, well-communicated process for reporting security incidents.
- Employees know how to respond to suspected breaches or data loss.
- Incident response plans are tested and updated regularly.

Continuous Improvement

- Feedback on training and policies is regularly solicited from staff.
- Security awareness programs are updated based on new threats and organizational changes.
- Successes and milestones in building a security culture are celebrated.

Measurement & Accountability

- Progress on cybersecurity culture initiatives is tracked and reported to leadership.
- Metrics (e.g., phishing simulation results, training completion rates) are reviewed and acted upon.
- Accountability for security is built into performance reviews where appropriate.

Tip:
Review this checklist with your team and identify areas for improvement. Prioritize actions that empower people, foster open communication, and make cybersecurity a shared responsibility across your organization.

Empower your people. Communicate openly. Make security everyone’s responsibility.

Ready to become a cybersecurity hero? Contact Cybersnap today! info@cybersnap.ca / Canada: 1-647-948-7769 / U.S.A.: 1-322-244-9225