Security Culture Audit

In the battle against cyberattacks, employees are often viewed as the cracks in an organisation's defence. This is primarily not because of any malice on the part of the workers, but rather because an absence of an ingrained security-minded culture which can often lead an employee, strictly out of curiosity or mindless impulse, to click and fall prey to a phishing scam, compromising the entire business.

While it is not uncommon for people to be hooked by phishing, no company should consider these mistakes acceptable. On the contrary, employees should be the company's first line of defence, acting as human firewalls against costly data breaches, business interruption and regulatory noncompliance.

Establishing A Security Culture

You can advocate for as many security strategies as you want, but if your culture does not reward certain behaviours to ward off social engineering attacks, no amount of security technology thrown at the problem will work. To quote workplace guru Peter Drucker, "Culture eats strategy for breakfast."

A complacent culture is the biggest obstacle to getting employees to respect security protocols and adhere to best practices. Changing cultural attitudes demands a top-down approach, yet even with management buy-in, it will still take a lot of effort and patience to guide employees to adopt safer behaviours and habits.

Improving security awareness starts with gaining a high-level understanding of what a security culture comprises. To help create a more security-minded workforce, let us look at seven key dimensions of culture and what you can do in each of these areas to enrich a culture that promotes security-mindfulness.

1. Employee Attitudes Toward Security and Policies

Attitudes toward organizational security policy can be changed by reinforcing positive norms and through effective communication, such as:

- Celebrating achievements and rituals.
- Acknowledging employee concerns.
- Involving other members of the organisation in planning.
- Exemplifying behaviours by sharing examples of correct and desired behaviours.
- Motivating employees by testing responses to phishing simulations.

2. Behaviours

By "behaviours," I mean employee actions that have direct or indirect impacts on the security of the organisation. Unintentional "misbehaviours" can include carelessly clicking on phishing links, visiting non-work-related websites, inadvertently posting confidential data on unsecured servers, or selecting a simple password (123456 is still commonplace).

How can we positively influence behaviours?

- Use a focused approach to different training methods.
- Implement short communications that are easily available to employees.
- Identify important processes and assess employees' knowledge of their existence.
- Provide easily accessible security policies so everyone knows what behaviour is expected.

3. Cognitive Processes Surrounding Security

While knowledge itself isn't likely to have a direct impact on behaviour, the cognitive processes used to acquire knowledge related to security have a direct (and indirect) influence on other dimensions that are relevant to improving security culture.

How can we positively influence cognition?

- Establish clear expectations from the start.
- Emphasize the vital role each employee has in sustaining the security of the organisation.
- Share stories that advertise security-related social norms that support a sense of belonging.
- Ensure your security awareness training is tailored to the needs and learning styles of the individual.

4. Quality of Communication

Cybersecurity is an interdepartmental effort, not just the responsibility of the IT department -- and interdepartmental collaboration requires a culture that prizes good communication using techniques that:

- Resonate with your audience: Whether addressing senior management or front- line staff, the information should be digestible and relevant to them. Listen. Find out what is important to them and why.
- Keep people appraised: Attitudes toward security measures are more likely to be positive if everyone understands why certain protocols are necessary to secure the organisation.
- Encourage positive expression: The more often an attitude is expressed, the stronger it becomes. Build a network of security evangelists across different business areas.

5. Compliance with Security Policies

Compliance depends on communication, cooperation, and coordination, ensuring that security policies are adequately implemented and adhered to at all levels. Employees' understanding of and adherence to written policies can be improved by:

- Improving the quality of communication channels (including regular meetings) to discuss security-related issues and report incidents.
- Increasing understanding and awareness of the policies, including procedures to implement them into daily work tasks and habits.

6. Organisational Unwritten Rules or Norms

Behaviours that support security need to be identified, taught, and reinforced. When correct behaviours are normal, adherence to these norms can be encouraged through the following mechanisms:

- Design campaigns that advertise security-related social norms. Encourage employees to share their stories (using blogs, newsletters, and emails) to raise awareness of the consequences of noncompliance and to see others rewarded for adherence to norms.
- Internal communication channels should be open and accessible to address any uncertainty and to encourage everyone to report on phishing attempts, suspect content, and breaches.
- Well-published, slowly stepped-up disciplinary actions can be used as a legitimate deterrent and help to establish group norms by identifying and broadcasting unacceptable behaviours.

7. Individual Responsibilities

Security is everyone's responsibility, not just IT's. How people understand those responsibilities is a key component to establishing a successful security culture. Workers are responsible for securing their own assets, even if they are not working on sensitive material. This knowledge will make people less likely to put the organisation at risk through careless actions.

Managers should talk with team members regarding their responsibilities and how they can improve the security culture of the team and organisation. They should encourage dialogue between themselves, team members and security officers.

Assessing security risks makes it easier to see where the weaknesses are, helping to create targeted training for employees. When your organisation is armed with a strong, in-depth security culture, you will have the best possible defence against cybercrime.