Red Helix

How to Foster a Positive and Proactive Security Culture

Having a positive and proactive security culture in your organisation is essential to securing your business. No matter how much tooling and technology are in place, your human firewall is your first line of defence.

Encouraging employees to speak up when they see something that looks wrong or inform you of the potential loopholes or fall-backs in your current training and awareness program makes you far more resilient and responsive to your security needs. That is why it is crucial to create a positive and proactive security culture, based on honesty and transparency.

Small steps to encourage a positive security culture:

Engage with senior leadership.

If your board and senior managers are not completing the security awareness training or are receiving exemptions when they fail phishing tests, it sets a bad example for the rest of the business.

Informing the senior leadership of the risks involved by putting it in a framework that resonates with their department's objectives can be beneficial. For example, if you are talking to the CFO putting it in the context of the financial loss a breach can cause, or if you are talking to the CHRO (Chief HR Officer) putting a breach in context of employee wellbeing and the increase in staff turnover that is suffered when an attack takes place.

Have clear metrics to monitor employee awareness and engagement.

These could be things such as training metrics e.g. 98% of the business scored 80% or higher on our security awareness training, or 65% of our company identified and alerted us to the phishing email. By tracking these metrics over time, you can see if your training is still engaging your co-workers or if it is time to use a different method of training or testing.

Clearly communicate the risks to your company

Whilst it is important to communicate to your colleagues the risks, avoid using fear-based communications. Instead, ensure that employees understand the significance of their role in maintaining the human firewall, and how a company data breach does not just affect the business but their personal employee data as well.

Inform them about new essential training and reward those who complete it, even with simple gestures like a thank-you email. Keeping communication lines open and reminding employees who to contact in case of issues fosters a supportive environment.

Foster an open Environment for Reporting

Creating a culture where employees feel safe and valued for reporting issues will lead to a more proactive and vigilant workforce. Recognise and address reported concerns promptly to reinforce the importance of their contributions.

Encourage employees to speak up when they notice anything suspicious or identify potential loopholes in the current security measures. It is vital to have a clear reporting model so employees know exactly who and where to report to and the next steps that will occur once they have reported something.

Provide Ongoing Education and Training

Security awareness is not a one-time event but an ongoing process. Regularly update training materials to keep them relevant and engaging. Use a mix of videos, interactive sessions, and real-life scenarios to cater to different learning styles. Continuously educating employees about the latest threats and best practices ensures that they remain vigilant and prepared.

Building a positive and proactive security culture requires commitment and continuous effort from all levels of the organisation. By engaging senior leadership, establishing clear metrics, communicating risks effectively, fostering an open reporting environment, and providing ongoing education, you can significantly strengthen your human firewall. In turn, this creates a more secure and resilient business.

Red Helix

W - https://www.redhelix.com/