TÜVRheinland®
Risktec

RISKworld / The Newsletter of Risktec Solutions / Spring 2021

Cyber Health Check: Developing and maintaining a healthy cyber security culture

Over the years, significant emphasis has been placed on managing the cyber threat via design solutions, such as air gaps and fire walls. This is, perhaps, not surprising because cyber security is undoubtedly a very technical domain. However, an organisation's approach to cyber security needs to not only address technology and associated procedures, but also requires a proactive cyber security culture.

WHAT IS GOOD CYBER SECURITY CULTURE?

Good cyber security culture is an integral part of an organisational culture. This means that in addition to technical cyber security solutions, the values, beliefs and behaviours of employees in relation to cyber security all play a crucial role in the overall level of security. If cyber security awareness is the basic knowledge of cyber security issues, then good cyber security culture is the resultant behavioural patterns and dedication of all employees to implementing that knowledge and adhering to the organisation's policies and procedures.

However, when it comes to cyber security, there is a tendency to focus almost exclusively on the technical issues, which often do not take into account the needs of the employees, their roles and how they actually complete their work on a day-to-day basis. This approach is likely to give senior management an unrealistic view of the actual security resilience. It can result in leaders believing they are completely secure because of the latest technologies that have been implemented at great cost or the rigorous and highly restrictive policies that have been explained to personnel.


© Shutterstock

Managers may not be aware of the non-technical shortfalls in the organisation. It is well known, for example, that when a restrictive procedure makes it hard for someone to do their job, or when the procedure is no longer practical, it is human nature for employees to find workarounds and unofficial ways of carrying out tasks to get the job done on time.

Without a positive cyber security culture, personnel are less likely to engage with the leaders responsible for the organisation's cyber security. As such, the security team will be unaware of workarounds because no one is bringing them the 'bad news'. Not only does this portray an inaccurate picture of the organisation's cyber security, but it also misses the opportunity for valuable input into how policies or processes could be improved.

BENEFITS OF A HEALTHY CYBER SECURITY CULTURE

The key benefits of an effective security culture include:

- A workforce that is more likely to incorporate cyber security into decision-making processes, making it more likely to act in a cyber security focused manner; and employees that are more likely to understand why they are required to do things in a certain way.
- An increase in compliance with cyber security procedures, as well as a greater understanding of how those policies and procedures actually affect employees and their day-to-day activities.
- A greater awareness of the cyber threats the organisation faces.
- Reduced risk from insiders, because they are more likely to have cyber security at the forefront of their mind during their day-to-day tasks, are less likely to look for shortcuts and are more likely to alert responsible parties to non-compliance or incidents.
- A greater openness from employees, more insight into their thoughts and behaviours, and a better all-round workplace environment.

HOW TO IMPROVE CYBER SECURITY CULTURE?

There are a number of steps that can be taken to develop a healthy cyber security culture within an organisation:

Lead by example

Leaders should lead by example; if cyber security is clearly a serious concern to them, then the workforce is more likely to take cyber security seriously too. People observe what their leaders say and do. If the actions they take are inconsistent with what they say – for example, if a meeting room has a large glossy poster on the wall setting out cyber security best practice, but a leader leaves behind an open laptop when the meeting ends – then people will conclude that cyber security is actually not that important.

Leaders should ensure the workforce knows that they are taking cyber security seriously, are vocal as to why it is being taken seriously, and follow the rules themselves.

Put employees at the heart of security

When it comes to cyber security, employees are frequently referred to as the 'weak link', but with a mature cyber security culture they don't have to be. A company's cyber security response comprises technology, people and processes in equal measure. It is more a matter of finding a balance that enables employees to achieve their goals efficiently, with cyber security 'baked in'.

Instil responsibility in all

Ensuring that employees understand exactly how they benefit from the success of the organisation and how crucial cyber security is to that success is the key to instilling a sense of personal responsibility in everyone. If people feel personally invested in cyber security then it is more likely to become a core belief and drive their workplace behaviours.

Go beyond awareness training

Whilst cyber security awareness training is crucial, it is not a complete cyber security solution. Understanding cyber threats is important, but employees also need to know why and how they are specifically important and relevant to them, and what the consequences of poor cyber security might look like – so when they leave the classroom those feelings stay with them. A healthy cyber security culture keeps cyber security at the forefront of an employee's mind and helps it to become an integral part of their working life, and not something that is left at the door as soon as the training session finishes.

Recognition and reward

Praise and recognition goes a long way to turning a one-off action into a regular habit and group mentality. When it comes to fostering good culture of any kind, it is worth bearing in mind that the carrot always trumps the stick.

Build a security minded community

A strong cyber security focused community is the backbone to any good cyber security culture. This can be achieved by traditional community-building techniques, such as speaking to the different areas of the business, finding out their level of interest in cyber security, giving them a voice for their opinions on the matter and opening it up for debate.

A few ways to help grow a cyber security focused community within the organisation include:

- Hosting a forum where relevant cyber security matters can be discussed.
- Hosting educational one-to-ones or monthly meetings.
- Monthly cyber security Q&As.
- Bulletins that highlight cyber security topics or announce the 'cyber hero of the month'.

CONCLUSION

Developing a proactive cyber security culture within an organisation is a never-ending process of community building, educating, listening and improving. This process ultimately leads to a more optimised balance of cyber security technology, procedures and behaviour, and a more secure organisation as a whole.

Contact: Liam Humphreys
enquiries@risktec.tuv.com