MOORE ClearComm

Create a culture of cybersecurity within your company

Introduction

Creating a culture of cybersecurity within a company can be essential for protecting your data, systems and networks. It involves educating employees on the importance of cyber safety and adopting best practices and policies to ensure everyone follows safe procedures regarding their online activities. It also requires setting up checks and balances, such as regularly auditing systems and monitoring access logs to ensure no one is accessing sensitive information or putting the business at risk in any way. Additionally, having robust security protocols for remote workers, such as VPNs and two-factor authentication, helps protect the company's data from potential breaches or hacks. Companies should also create policies encouraging employees to practice safe online habits when handling sensitive information.

Issues facing Businesses in the UK

Cyber security is one of the most pressing issues facing industries across all sectors. The increasing prevalence of cybercrime has made it increasingly important for organisations to invest in and prioritise cyber security. However, this can be difficult due to needing more resources or expertise. Additionally, many companies are not up-to-date on best practices and protocols, leaving them at risk of data breaches and other forms of cyber-attack. This lack of knowledge can also lead to businesses inadvertently giving hackers access to their systems through vulnerable networks or outdated software.

Furthermore, with more employees working remotely due to the pandemic, security has added strain as companies must ensure that their systems are secure when accessed outside the workplace. Remote workers are particularly at risk from phishing scams or malicious attempts to access company information.

Organisations are responsible for protecting third-party data to which they may have access, such as customer data and financial information. They need encryption for these data types and ensure appropriate safeguards are in place if any third parties can access such sensitive information. It may also be beneficial for organisations to set up regular audits to verify the effectiveness of these safety procedures and identify any potential weak spots within their system that could leave them vulnerable. In addition, companies must keep up with emerging technologies that aim to provide better protection against cyber threats. Hence, they remain at the forefront of industry standards regarding cyber security.

How to truly affect a change of culture within your business

True change is only achievable through willing buy-in from all the necessary stakeholders, reflected in this quote by Frances Hesselbein:

> *"Culture does not change because we desire to change it. Culture changes when the organisation is transformed; the culture reflects the realities of people working together, every day."*

To that end – how do we introduce and nurture a culture of cyber security? Well, it starts at the top, with the board, directors, CEO and MD all living the core values of a security and privacy-based culture, with the following key behaviours as a constant:

- Promote cyber hygiene from the board down
- Put the staff at the heart of the cultural message and allow them to own the process
- Communicate, communicate, and communicate some more
- Adopt a position of Zero Trust from the outset

In addition, we identify 10 Steps for management to drive business culture change (generic, perhaps, but highly relevant to building a cyber culture in any organisation):

1) Define a set of desired values and behaviours
2) Align culture with strategy and processes
3) Connect culture and accountability
4) Have visible proponents / flag-wavers
5) Define the non-negotiables
6) Align culture with brand
7) Measure it
8) Don't rush it
9) Invest properly
10) Lead from the front

Is change easy to implement?

No. It`s not.

Like most things that generate positive outcomes or results, structured effort and strategy must be central to the journey. The following data provides clear evidence in respect of what is needed to effect change, evolve your process, increase diligence and trust – and to create a lasting cyber security culture:

- 47% of organizations that integrate change management are more likely to meet their objectives than those who do not *(Source: WalkMe Research)*
- 79.7% of businesses need to adapt their purpose and/or culture every two to five years, in order to remain valid and competitive *(Source: WalkMe Research)*
- More than 50% of executives say that corporate culture influences productivity *(Source: PwC)*
- 72% report that culture helps successful change initiatives happen *(Source: PwC)*

Finally, the most powerful statistic of all is one that also provides the most opportunity to learn from:

- 70% of culture change projects fail, for one, two or all of the following reasons *(Source: UK Finance)*:

1) The business hasn't bought into the vision
2) Relying on old, historical data in order to learn and effect future change
3) Perpetuation of silos, leading to the prevention of holistic change

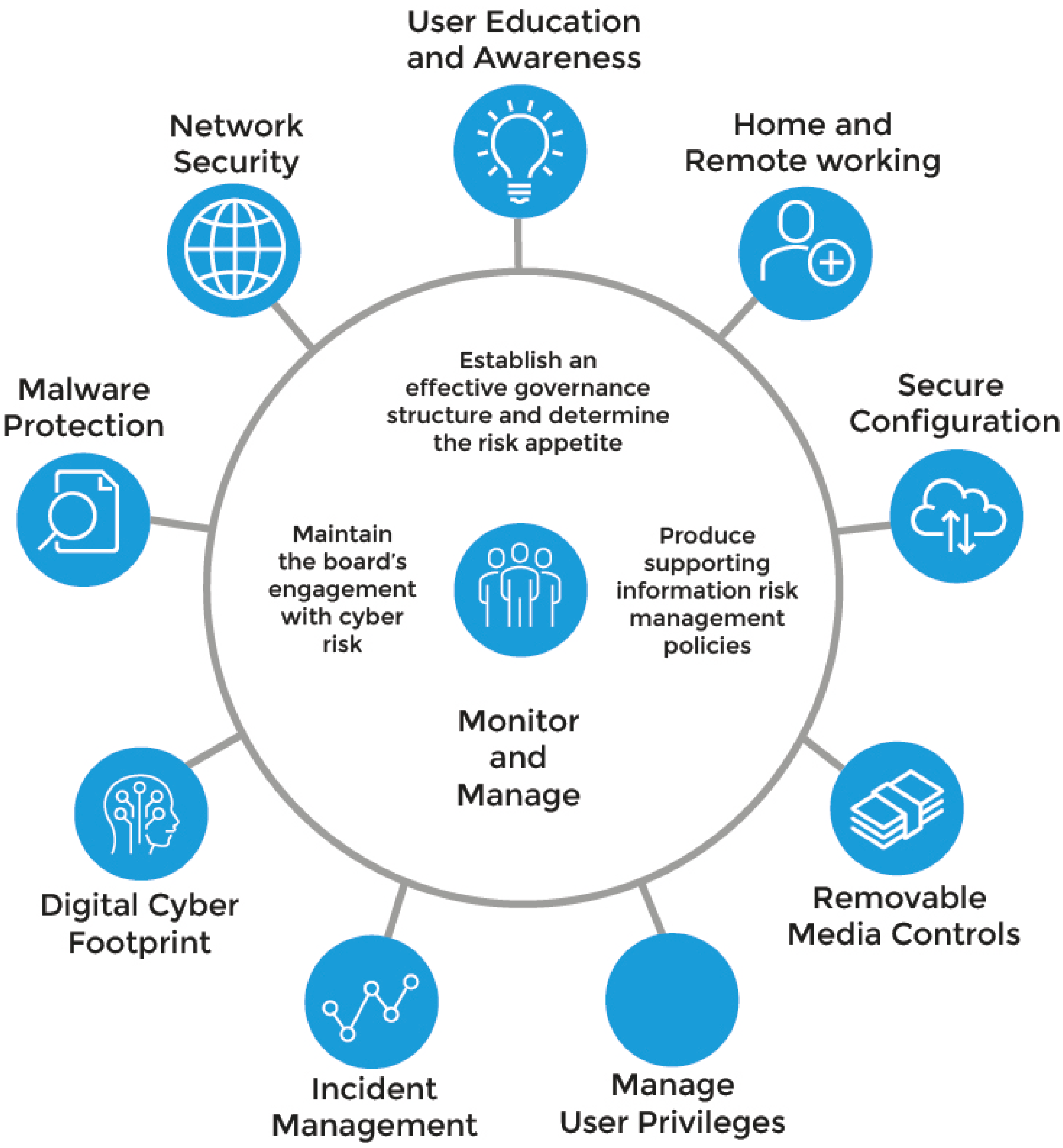
Benefits of creating a culture of Cyber Security within a business

To create a culture of cyber security within an organisation, there needs to be a clear understanding of the importance of security and what is expected from every employee. This should be followed up with training and awareness sessions for all staff members to better understand the risks associated with cyber breaches and how to protect against them.

Furthermore, companies should ensure protocols are in place when handling sensitive data, such as encryption or two-factor authentication. Additionally, organisations should ensure they have a plan outlining actions to take if any data breaches occur. It may also be beneficial for companies to have regular cyber audits and drills so that employees are aware of best practices and prepared in an emergency. Finally, organisations must establish clear policies around the use of technology at work so that everyone is on the same page regarding issues such as appropriate email usage or online behaviour.

Strategy

It is clear that to create a successful culture that embraces cyber security; the organisation sets out to implement a framework that includes a deep understanding of cyber security and the associated risk and a robust mitigation plan. A successful framework should consist of:


User Education and Awareness
Home and Remote working
Secure Configuration
Removable Media Controls
Manage User Privileges
Incident Management
Digital Cyber Footprint
Malware Protection
Network Security
Establish an effective governance structure and determine the risk appetite
Maintain the board's engagement with cyber risk
Produce supporting information risk management policies
Monitor and Manage

In addition to this framework, the organisation should become Cyber Essentials certified, a UK government-backed certification that helps businesses protect themselves against cyber threats.

It is designed to ensure companies have implemented basic cybersecurity measures to protect themselves against common online threats. Cyber Essentials certification also includes £25,000 of cyber liability insurance (for business with a turnover of less than £20million)

Please read our information on Cyber Essentials here (Link)

About Us:

Moore ClearComm is part of Moore Kingston Smith, a dynamic, leading professional UK firm of accountants and professional business advisers.

Our services include Data Privacy, Cyber Security, Business Continuity and Information Security for organisations worldwide.

As trusted advisers to businesses and not-for-profit organisations, we are passionate about helping our clients achieve their ambitions. Our highly experienced people have the strategic insight, drive and dedication to deliver results and help mitigate Data Privacy and Cyber Security risk.

As part of Moore Kingston Smith, a leading member of the Moore Global Network. An international family of over 30,000 people across more than 100 countries, members connect and collaborate to care for our clients' needs – at a local, national and international levels.