C-SUITE GUIDE TO CYBERSECURITY

A 9-step toolkit based on NCSC guidance for Board members, helping you to understand and reflect on the roles and responsibilities within your organisation and how they impact the wider security posture

1 EMBED CYBERSECURITY INTO YOUR WIDER OBJECTIVES

Cybersecurity should be seen as something that enables organisation's to reach their overall objectives. Good cybersecurity extends beyond technology. It's about building a culture where people are bought into the right attitudes and processes.

Questions to consider:

1. *Do we understand how cybersecurity impacts our responsibilities?*
2. *How do assure ourselves that our current approach is effective?*
3. *Who currently has responsibility for cybersecurity?*
4. *Do we have a process to ensure cyber risk integrates with business risk?*

2 DEVELOP YOUR CYBERSECURITY EXPERTISE

The latest research shows that cyber skills are in high demand. It is vital for organisations to take steps now so that they are able to deal with the turbulent changes in the cybersecurity industry.

Questions to consider:

1. *Am I well-positioned to be accountable for cybersecurity decisions?*
2. *What cyber expertise do we have, and what do we need?*
3. *Do we have a plan to address the expertise gap?*
4. *Are we building a workforce ready to tackle our cybersecurity challenges?*

3 GROW AND BUILD A STRONG SECURITY POSTURE

The latest research shows that cyber skills are in high demand. It is vital for organisations to take steps now so that they are able to deal with the turbulent changes in the cyber security industry.

Questions to consider:

1. *Do we have a strong security culture within our organisation?*
2. *What do we do to encourage a strong security culture?*

4 ESTABLISH YOUR BASELINE AND IDENTIFY WHAT MATTERS MOST

It is important to understand your technical assets and how they contribute to achieving your objectives. It's almost impossible to protect everything at all times so therefore defences should be prioritised based on importance.

Questions to consider:

1. *Have we clearly communicated our prioritised objectives and do they guide our cybersecurity efforts?*
2. *Do we understand how our technical assets help us to achieve our goals?*
3. *Are we able to track the systems, data and services we are responsible for?*

5 UNDERSTAND THE CYBER THREAT LANDSCAPE

Cyber threats are different depending on your organisation and industry. Understanding the threats most prevalent to you will enable you to most effectively tailor your approach.

Questions to consider:

1. *Which threats are most relevant to our organisation and why?*
2. *How are we staying up to date with the latest threats?*
3. *How do we use threat intelligence to inform business as usual (BAU)?*

6 RISK MANAGEMENT FOR CYBERSECURITY

Good risk management goes beyond compliance. Cybersecurity risk management should be integrated into your wider approach to risk management across your organisation.

Questions to consider:

1. *Have set out which risks we are willing to take and which are unnacceptable?*
2. *Do our processes ensure decision makers are well informed as possible?*
3. *Do we have a process that ensures cyber risk is integrated in the business?*
4. *Do we have an effective approach to managing cyber risk?*

7 IMPLEMENTING EFFECTIVE CYBERSECURITY MEASURES

Implemeting good cybersecurity measures will not only help meet regulatory requirements but will also help reduce the likelihood of a significant incident. As needs change it's important to assess if defences continue to be effective.

Questions to consider:

1. *How do we assure ourselves that our cybersecurity measures are effective?*
2. *What measures do we take to minimise the damage an attacker could do inside our network?*
3. *Do we implement cybersecurity controls against the most common attacks?*

8 COLLABORATION WITH SUPPLIERS AND PARTNERS

Attacks on suppliers can be just as damaging as one on your own network. Cybersecurity decisions should therefore take into account any new or existing relationships.

Questions to consider:

1. *Do we have a clear strategy for using suppliers? Has it been communicated?*
2. *How do we mitigate risks of sharing data with other organisations?*
3. *Are we ensuring that cybersecurity is considered in every decision?*
4. *Are we confident that we are fulfilling our security requirements?*

9 PLANNNING YOUR RESPONSE TO CYBER INCIDENTS

Attacks can have a huge impact on businesses including cost, productivity and reputation. Being prepared to quickly detect and respond will help reduce the long term impact.

Questions to consider:

1. *Do I understand my role during an attack?*
2. *Who leads on an incident and who makes the decisions?*
3. *Do we have an incident management plan?*
4. *Would we know if an incident occured?*
5. *Do we know where to go for help?*
6. *How do we learn from incidents?*

IF YOU HAVE ANY QUESTIONS OR REQUIRE ANY GUIDANCE ON ANY OF THE ABOVE, DON'T HESITATE TO GET IN TOUCH:

hello@threatprotect.co.uk +44 (0) 3334 120 120 www.threatprotect.co.uk

THREAT PROTECT