Huntsman®

Top 10 Questions about Cyber Security Management

For Executives and Directors

An effective cyber security management regime requires the integrated operation of a professional cyber security team to undertake activities that include risk assessment, vulnerability detection, mitigating security controls, measurement of their effectiveness and finally the visibility and reporting of residual risk.

When successfully orchestrated into a systematic workflow, KPIs of cyber security controls inform the effective risk management processes and the executive oversight of the IT security management process. Directors and senior Executives need accurate IT risk information to enable their efforts and inform their decisions.

This list of questions will assist Directors and senior Executives in interpreting cyber security information and prompt deeper inquiry where KPIs clearly point to the need for more detail.

1. **What are our cyber security management and reporting obligations?**
   In asking this question, consider that obligations may vary on regulations, industry sector, and participation in particular supply chains. For example, for more specific cyber security guidance and advice refer to: *https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks*

2. **Do we have a sufficiently defined risk appetite that considers NCSC or NIST recommendations and advisories, the security management maturity of industry peers and the value of our assets? In particular, do we:**
   a. Assess the sensitivity of our IT systems and assets?
   b. Determine the effectiveness of these assets' security defences?
   c. Supplement our existing efforts with additional risk mitigation controls?
   d. Set ambitions for our security maturity level?

3. **What is the most appropriate security framework for cyber risk management for our business? In particular:**
   a. What was the basis for this decision making?
   b. Do we have external contracts or funding bodies, that may require us to align to a specific standard in the next 12-months?
   c. Is there an industry standard?
   d. Can our chosen framework be easily implemented and maintained?
   e. Are our reporting obligations still to be agreed with Government?

4. What are the minimum level security controls required by our insurer for cyber insurance "eligibility"? How do we actively verify our efforts when it is time for renewal?

5. How do we assess that security mitigation strategies are in place and operating effectively? In particular:

   a. What mitigation controls do we measure to inform that decision?
   b. Do we engage independent auditors, penetration testers or do we self-assess?
   c. Do we use qualitative questionnaires or quantitative measurement?
   d. Do we have visibility of the state of our security controls and artefacts?

6. Do we have an ongoing risk mitigation program to regularly identify and manage compliance gaps?

7. Do we maintain a systematic evidence-based risk management process to inform and manage our IT risk governance and oversight?

8. Do we undertake systematic cyber security risk assessment to also include our key 3rd party suppliers?

9. Have we added cyber risk reporting to our Management and Board agendas and how often do we consider our industry and regulatory obligations, that facilitate the asking of the right questions and ensure appropriate governance?

10. How regularly do we review the adequacy of our cyber security controls? Is this a formalised component of our systematic governance processes?

Good leadership and governance start with communications and the empowerment of your team. These questions are geared to support Executives, Directors and Sub-Committees to continue their cyber risk conversations and identify current areas of residual risk and the effectiveness of the controls in place to manage them.

Depending on the scope and size of your in-house team, you may want to consider an out-of-the-box application to align with the UK's National Cyber Security Centre (NCSC), and the US Department of Commerce's National Institute of Standards & Technology (NIST).

Huntsman Security's SmartCheck is used by government departments and commercial organisations to quickly and accurately measure their cyber security posture to inform data-driven cyber security decision making.

Further reading

https://www.ncsc.gov.uk/collection/board-toolkit/cyber-security-regulation-and-directors-duties-in-the-uk

Want to find out more?

Download the brochure.

SmartCheck

Or **contact us** to talk to one of our team today.

© 2023 Tier-3 Pty Ltd, All rights reserved