Huntsman®
Defence-Grade Cyber Security

Obtaining Cyber Insurance Cover, including Renewals, in 2022 – 2023

Topic 2b

Activating UK NCSC & US NIST guidelines:

BEYOND ENDPOINT CONTROL - FOR VISIBILITY OF CYBER-RISK PREVENTION, CONTAINMENT & RECOVERY

As a decision-maker within your organisation, you may be familiar with the cyber security and risk mitigation strategies recommended by the UK's National Cyber Security Centre (NCSC) & the US Department of Commerce's National Institute of Standards & Technology (NIST), to help organisations protect their systems against ransomware and cyber threats more generally.

If you've had to reset your password from your favourite phrase to a combination of letters, numbers and characters that are hard to remember, or if you are required to use an Authenticator app to gain access to files or parts of your system, then your team has potentially already implemented at least some of the suggested security mitigation strategies.

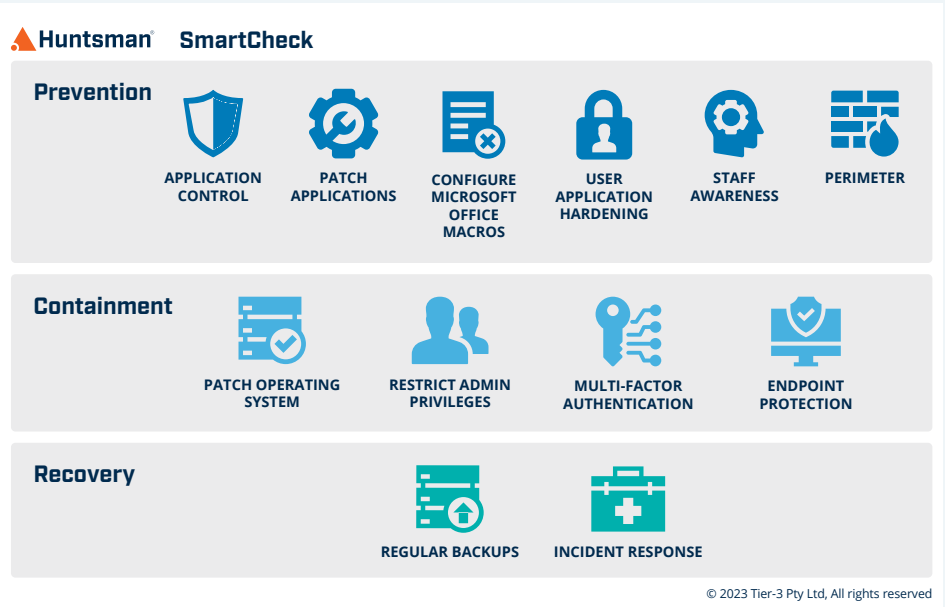
▶ Question 1

Have your teams implemented any or all of the NSCS or NIST guidelines, to protect your Microsoft Windows-based connected networks and systems? How do you have ongoing assurance of this?

It might seem like a question for your IT team, but this question is now also directed to your executives, board, risk managers and any others involved in the in the renewal of your cyber-insurance policy in the coming 12 months.

The likelihood of cyber-attack and the potential costs to organisations associated with such an attack has risen considerably in the last little while, and the style of attack varies too. This means that organisations need to demonstrate a range of prevention, containment, and recovery steps as a part of their risk controls.

In order to consolidate and use the guidance from these global thought-leaders, we have distilled the NCSC & NIST guidance advice down to 12 Safeguards that are key to supporting organisations to assess ransomware readiness, inform risk management activities and act as a set of highly effective baseline cyber security controls.

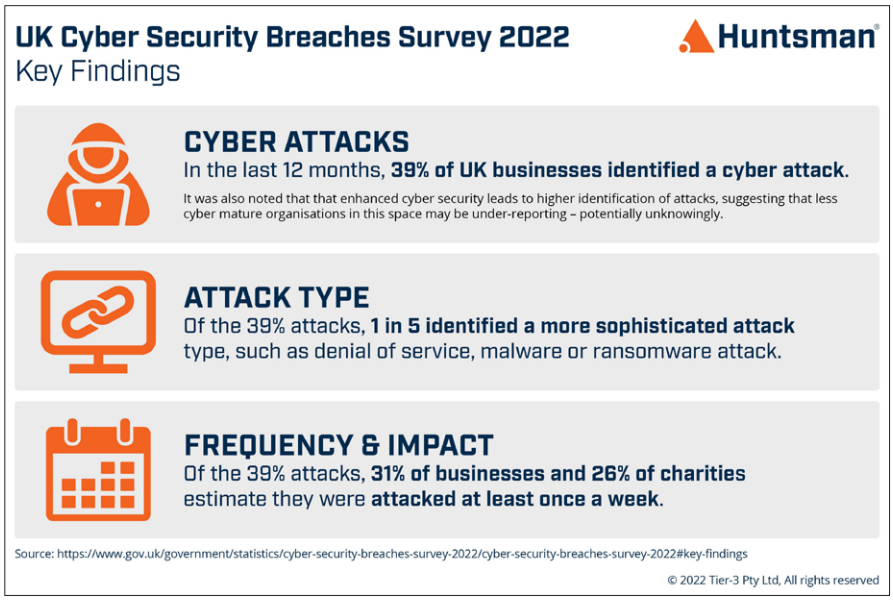


QUICK READ:
12 Safeguards aligned with UK NCSC & US NIST guidance

No single cyber security control can protect against every situation. The cyber security concept of defence-in-depth anticipates multiple independent security controls operating in concert to protect you across the attack sequence. Ransomware readiness or resistance is best achieved when the effectiveness of these security controls is maintained across each phase of an attack. This applies equally to other attack types.

The NCSC and NIST security control guidance can be categorised into the cyber-attack sequence of **Prevention**, **Containment** and **Recovery**. In order to support organisations to implement this advice, Huntsman Security's 12 safeguards (integrated into the SmartCheck software application), assess key control effectiveness across these three attack phases.

A single point solution, such as Multi-Factor Authentication (MFA) or simply strengthening your password strategies, is not enough. Because a single point solution can represent a single point of failure, NCSC and NIST guidance seek to address the concept of Defence-in-Depth. By monitoring the effectiveness of multiple strategies, data-driven assessment can provide significantly better visibility and improved quality of information about your cyber security posture (at each phase?).



In looking at the Cyber Security Breaches Survey 2022 results from the UK Government, it is evident that there are a range of ways that UK organisations are being targeted, and so there needs to be a more comprehensive approach to defend and protect their data and systems, and ultimately their product & service delivery to customers.

The next steps for your executive, board, and risk teams are to firstly determine the extent to which you have implemented this powerful set of 12 risk mitigation strategies, and secondly, to regularly assess the operating efficiency of each of those controls.

Question 2

Did you know that reporting on your organisation's implementation of a cyber risk governance framework can support cyber insurance renewal? Did you know that it's now a tool that underwriters can use to evidence your cyber maturity?

As ransomware and cyber risks increase, it is recommended that organisations get ahead of the onerous reinsurance process – now starting 2 to 3 months before their current policy ends.

Huntsman Security's Insurance Renewal Initial Report driven by the SmartCheck software application, streamlines the process of IT risk assessment or posture measurement for organisations, as it aligns directly to the NCSC & NIST guidelines, and with its accurate measurement and simple dashboard, it identifies vulnerabilities that might leave your entire organisation at risk.

With security gaps highlighted via a SmartCheck assessment, your in-house ICT team can remediate against the 'to do list' provided , and if required, re-audit your environment to quantify and verify any cyber posture improvement that might improve your insurance terms.

This new step in insurance coverage is valuable for any organisation that prioritises cyber insurance as a risk-control, and now seeks quantifiable data to verify its cyber posture, to:

- Visualise & measure the cyber risk controls that will affect your insurance terms and eligibility for cover
- Understand your cyber posture with a data-driven application designed to measure your cyber resilience across detection, containment and recovery
- Use these changing insurance requirements to improve your security controls and maintain your access to insurance as a risk management option

Your risk profile is the single most important factor in informing renewal success.

Huntsman Security's SmartCheck software application strengthens your internal capacity to address these emerging cyber risk areas, support renewal of your cyber insurance, and manage your broader cyber security controls.

Download SmartCheck brochure

Download

Start the Preliminary Stage of your Cyber Insurance Renewal process with an Insurance Renewal Initial Report driven by:

SmartCheck

Measure your cyber risk

With on-going access to resilience reports, cyber maturity metrics, remediation "To-Do" Lists, and the ability to regularly 'Re-Audit' your environment for 12-months.

ALIGNED WITH GUIDELINES FROM THE UK'S NATIONAL CYBER SECURITY CENTRE (NCSC) AND THE US DEPARTMENT OF COMMERCE'S NATIONAL INSTITUTE OF STANDARDS & TECHNOLOGY (NIST). [from £7,500].

Contact Us e: info@huntsmansecurity.com

Huntsman®
huntsmansecurity.com