Maintaining a sustainable strengthened cyber security posture

How organisations can avoid staff burnout during an extended period of heightened cyber threat.

Introduction

During an extended period of heightened cyber threat, your systems, processes and workforce will come under pressure. This guidance explains how to maintain a strengthened cyber posture in a sustainable and efficient way, whilst prioritising staff wellbeing. Looking after your staff is not only important from an HR perspective - it also directly contributes towards maintaining an organisation's security and resilience.

> **Note:**
> If you've not already implemented the NCSC's guidance Actions to take when the cyber threat is heightened, please do so before reading this document.

What is an extended period of heightened threat?

There may be periods when the cyber threat is heightened for an extended period, for example as a result of geopolitical tensions. During these periods, organisations will experience:

- an initial *acute* phase (when they are required to strengthen their defences and address vulnerabilities), followed by
- a *protracted* phase (when a strengthened cyber posture should be maintained to manage the residual risk from the increase in threat)

Over time, the cyber threat may come down again, but it is unlikely to return to the previous baseline. Organisations might maintain aspects of their strengthened posture for the long term, in response to a changed threat landscape. The NCSC will continue to issue guidance to help organisations assess the level of the cyber threat.

How could organisations be affected?

It may be difficult to maintain a strengthened posture for a sustained period. In particular, increased workloads for cyber security staff over an extended period can harm their wellbeing and lead to lower productivity (with a potential rise in unsafe behaviours or errors).

The following steps can help your organisation sustain its security posture whilst protecting staff wellbeing.

Get the basics right

A good way to remain vigilant to the heightened cyber threat is to ensure that the basic hygiene controls within your organisation are in place and functioning correctly, as described in our guidance on Actions to take when the cyber threat is heightened. Even if there's no evidence of successful cyber attacks against your organisation, that doesn't equate to a change in adversary capability or intent; instead it could demonstrate that your cyber defences are working effectively.

Revisit your risk-based decisions

During the initial acute phase of heightened cyber threat, you will have taken risk-based decisions to introduce temporary additional defences. If the heightened cyber threat becomes protracted, then those initial risk-based decisions should be revisited to ensure that additional defences are implemented in an efficient way for the long term.

Improve long-term cyber resilience

An extended period of heightened cyber threat may reflect long-term shifts in adversary capability or intent and so you may need to strengthen your cyber security and resilience on a permanent basis. Accelerating planned action to harden networks and improve resilience capabilities will relieve pressure on your workforce over the long-term. The NCSC has published guidance that can help with this, including:

- 10 Steps to Cyber Security
- Cyber Governance for Boards
- The Cyber Action Toolkit

Empower your staff to make decisions

During a period of heightened cyber threat, senior managers will rightly want additional oversight of the response, but this can also put extra pressures on frontline teams. It may be more efficient for leaders to delegate day-to-day decision-making to appropriate levels so that leaders can focus on medium-term priorities. This approach may also provide space for a more agile response, informed by the experiences and expertise of frontline staff. For example, your staff 'on the ground' will be the best placed to review and contextualise reporting about the heightened cyber threat in the news (or across social media), to better inform your organisation's response.

Spread workloads evenly

Individuals and teams most exposed to the response can quickly become overloaded. Organisations can be more resilient if workloads are more evenly spread across a wider pool of staff, and this also provides development opportunities to less experienced staff. Staff could also be rotated in and out of frontline teams to build sustainability into the total workforce. Organisations should also be ready to surge additional staff should the threat heighten further.

Give staff a break

A period of heightened cyber threat may lead to staff working longer hours and taking fewer breaks. Over an extended period, this could have a negative impact on staff wellbeing and increase the risk of burnout. This is particularly the case for those staff whose role involves round-the-clock monitoring or requires them to be on-call. Ensure that staff spends time away from the office and can also work on other, less pressured tasks. This will provide space for staff to recharge, and boosts organisational resilience. Consider:

- how you can empower staff to take breaks and switch off (both within and outside working hours)
- how you can empower staff to take time out for themselves, including through leave or flexible working.

Look after each other

Staff involved in the response could be exposed to harmful or distressing content, difficult decisions, or high-pressure situations, all of which could negatively affect their wellbeing. This is particularly true if a period of heightened cyber threat is linked to a high-profile issue in the media, for example a conflict between nation states. Managers and team members should look out for signs that they or their colleagues are struggling, and ensure that they are equipped with the resources to respond (which will depend on the organisation and the individual). The NCSC's guidance on Putting staff welfare at the heart of incident response sets out related advice for protecting staff welfare when responding to an incident.

Engage the entire workforce

While this guidance focuses on the staff most exposed to the response, during a period of heightened cyber threat the *whole workforce* has a role to play in strengthening an organisation's cyber defences. When working at pace, it can be difficult to maintain communication between teams and individuals. This can reduce productivity as a result of siloed working and a lack of coordination. Ensure that:

- you have the right internal communications processes in place to join-up everyone involved in the response
- you help your staff to identify and report suspicious behaviour (the CPNI has produced a range of security awareness campaigns to support this)

PUBLISHED

5 July 2022

REVIEWED

5 July 2022

VERSION

1.0

WRITTEN FOR

Cyber security professionals

Large organisations

Public sector

Small & medium sized organisations