BLOG POST

Preparing for the long haul: the cyber threat from Russia

Although the UK has not experienced severe cyber attacks in relation to Russia's invasion of Ukraine, now is not the time for complacency.

Dr Marsha Quallo-Wright

In January 2022, ahead of Russia's invasion of Ukraine, we asked all UK organisations to bolster their cyber defences.

We knew that cyber was part of Russia's military doctrine, and we had seen that previous Russian cyber activity against Ukrainian targets had caused spillover effects around the world.

In the five months since that guidance was published, we have seen significant cyber activity in Ukraine, with sustained intent from Russia to destroy or disrupt Ukrainian government and military systems. This has had effects beyond Ukraine's borders; the UK government stated Russia was behind a cyber attack on a global communications company, on the eve of the invasion, which affected windfarms and internet users in central Europe.

So our initial concerns were well-founded. And while, to date, UK organisations have not experienced significant cyber attacks as a result of Russia's invasion, now is not the time for complacency. The absence of successful cyber attacks doesn't equate to a change in adversary capability or intent; indeed it may be evidence that our additional cyber defences are working effectively.

Russia has not achieved the rapid military victory in Ukraine that President Putin expected and there's no obvious end in sight. While we are not aware of any current specific threats to UK organisations, the cyber threat to the UK remains heightened, and we expect it to stay that way for some time. **Accordingly,**

organisations should respond to this potentially protracted period of heightened cyber threat from Russia by maintaining a strengthened cyber posture.

Of course, this puts additional pressure on your systems, your processes and your workforce. Cyber security teams were already under mounting pressure in the months leading up to the invasion of Ukraine: handling a global pandemic, a rise in ransomware attacks and the Log4j vulnerability, alongside the usual levels of ongoing malign cyber activity. These extended periods of intense pressure on cyber security teams raise the risk of poor wellbeing and even burnout, with a potential associated rise in unsafe behaviours and errors. Staff welfare is a critical component of an organisation's security and resilience.

That is why we have published the new guidance on maintaining a strengthened cyber security posture in a sustainable way. It contains advice for business leaders and managers about how to manage the residual risk from an extended period of heightened cyber threat whilst prioritising staff wellbeing, and stresses the importance of:

- revisiting risk-based decisions to ensure defences are implemented in an efficient way for the long term
- empowering frontline staff to take decisions about prioritisation
- ensuring that workloads are spread across individuals and teams and that frontline staff can take breaks to recharge
- providing resources to managers and teams to recognise the signs of someone who is struggling

While the cyber threat arising from the war in Ukraine may diminish over time, it is unlikely to return to the previous baseline and new threats may emerge. Your best *long-term* response to changes in cyber threat (*without* your staff having to work 24/7) is to permanently improve your organisation's cyber security and resilience by building more secure networks and bolstering your resilience capabilities, as described in NCSC guidance 10 Steps to Cyber Security.

The NCSC will continue to issue guidance to help organisations assess the level of the cyber threat and take appropriate action in response; if you would like our support please get in touch using the usual channels.

Dr Marsha Quallo-Wright
Deputy Director for Private Sector CNI, NCSC

WRITTEN BY

Dr Marsha Quallo-Wright
Deputy Director for Private Sector CNI, NCSC

PUBLISHED

5 July 2022

WRITTEN FOR

Small & medium sized organisations

Large organisations

Cyber security professionals

Public sector

PART OF BLOG

NCSC publications