Actions to take when the cyber threat is heightened

When organisations might face a greater threat, and the steps to take to improve security.

Balancing cyber risk and defence

The threat an organisation faces may vary over time. At any point, there is a need to strike a balance between the current threat, the measures needed to defend against it, the implications and cost of those defences and the overall risk this presents to the organisation.

There may be times when the cyber threat to an organisation is greater than usual. Moving to heightened alert can:

- help prioritise necessary cyber security work
- offer a temporary boost to defences
- give organisations the best chance of preventing a cyber attack when it may be more likely, and recovering quickly if it happens

This guidance explains in what circumstances the cyber threat might change, and outlines the steps an organisation can take in response to a heightened cyber threat.

Factors affecting an organisation's cyber risk

An organisation's view of its cyber risk might change if new information emerges that the threat has heightened. This might be because of a temporary uplift in adversary capability, if for example there is a zero-day vulnerability in a widely used service that capable threat actors are actively exploiting. Or it could be more specific to a particular organisation, sector or even country, resulting from hacktivism or geopolitical tensions.

These diverse factors mean that organisations of all sizes must take steps to ensure they can respond to these events. It is rare for an organisation to be able to influence the threat level, so actions usually focus on reducing your *vulnerability* to attack in the first place and reducing the impact of a successful attack. Even the most sophisticated and determined attacker will use known vulnerabilities, misconfigurations or credential attacks (such as password spraying, attempting use of breached passwords or authentication token reuse) if they can. Removing their ability to use these techniques can reduce the cyber risk to your organisation.

Actions to take

The most important thing for organisations of all sizes is to make sure that the fundamentals of cyber security are in place to protect their devices, networks and systems. The actions below are about ensuring that basic cyber hygiene controls are in place and functioning correctly. This is important under all circumstances but critical during periods of heightened cyber threat.

An organisation is unlikely to be able to make widespread system changes quickly in response to a change in threat, but organisations should make every effort to implement these actions as a priority.

+ Show all

Check your system patching Show

Verify access controls Show

Ensure defences are working Show

Logging and monitoring Show

Review your backups Show

Incident plan Show

Check your internet footprint Show

Phishing response Show

Third party access Show

NCSC services Show

Brief your wider organisation Hide

- Ensure that other teams understand the situation and the heightened threat. Getting buy-in from the rest of the business is crucial in being able to complete the actions described here.

- Ensure colleagues in other areas understand the possible impact on their teams' workloads and tasking. Make sure everyone knows how to report suspected security events and why reporting during a period of heightened threat is so important.

Advanced actions

Large organisations should carry out all the actions outlined above, to ensure that the most fundamental security measures are in place. Organisations and sector regulators using the Cyber Assessment Framework to help them understand cyber risk should note that the CAF contains guidance on all the areas included in the actions above. If your organisation has deprioritised these areas of the CAF, you are advised to revisit those decisions immediately when the threat is heightened.

In addition, those organisations with more resources available should also consider the following steps:

- If your organisation has plans in place to make cyber security improvements over time, you should review whether to accelerate the implementation of key mitigating measures, accepting that this will likely require reprioritisation of resources or investment.
- No technology service or system is entirely risk free and mature organisations take balanced and informed risk-based decisions. When the threat is heightened, organisations should revisit key risk-based decisions and validate whether the organisation is willing to continue to tolerate those risks or whether it is better to invest in remediation or accept a capability reduction.
- Some system functions, such as rich data exchange from untrusted networks, may inherently bring a greater level of cyber risk. Large organisations should assess whether it is appropriate to accept a temporary reduction in functionality to reduce the threat exposure.
- Larger organisations will have mechanisms for assessing, testing and applying software patches at scale. When the threat is heightened, your organisations may wish to take a more aggressive approach to patching security vulnerabilities, accepting that this may have a service impact itself.
- During this time, large organisations should consider delaying any significant system changes that are not security related.
- If you have an operational security team or SOC it may be helpful to consider arrangements for extended operational hours or to put in place contingency plans to scale up operations quickly if a cyber incident occurs.
- If you have systems in place that can take automated action or notifications based on threat intelligence, you might also consider procuring threat feeds that may give you information relevant to the period of heightened threat.

PUBLISHED

17 January 2022

REVIEWED

17 January 2022

VERSION

1.0

WRITTEN FOR

Public sector

Large organisations

Cyber security professionals