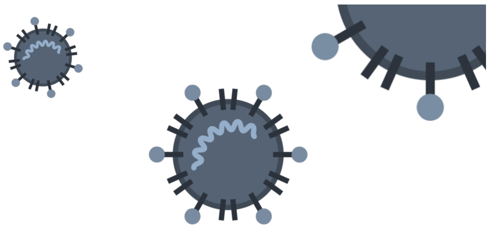
CPNI
Centre for the Protection
of National Infrastructure



Protective Security Throughout Covid-19

PUBLISH DATE:
April 2020

CLASSIFICATION:
Official

Advice Note to Risk Owners: Shaping your security posture and measures to manage the evolving risks during the pandemic

The Centre for Protection of National Infrastructure (CPNI) is the National Technical Authority for Physical and Personnel protective security advice. We have been working with our partners in the National Cyber Security Centre (NCSC) to provide tools and guidance products to help government, infrastructure and business to adapt their security posture as the Covid-19 crisis develops.

Whilst CPNI usually advises national infrastructure operators on national security threats, in the current landscape, the definition of what is critical is rapidly changing. As such, CPNI are reaching wider than our standard remit to help those organisations who are currently or could become key to the crisis recovery efforts.

This guidance document has been commissioned to provide new and existing customers of CPNI with a framework for reassessing their security risks in the current climate, ensuring that your most important risks are addressed. This document sits within an evolving suite which will help consider specific concerns, such as Guard Force provision and operation of Automated Access Control Systems for a safe and secure environment.

Background

The Covid-19 pandemic is unlike any crisis that has been faced by the United Kingdom in living memory. There have been unprecedented shifts in the way the country operates, changes to legislation and changes to which parts of the national infrastructure are under the greatest pressure and are critical to keeping the country operating.

All organisations have adapted the way they operate in order to protect lives during the pandemic; be that reducing operations to keep staff and the public safe or shifting production to deliver essential products and services to help combat the pandemic. These changes will have happened swiftly and will have had an impact on the security risks being faced, meaning there will have been little time to build the security posture and culture to operate around them.

These sudden changes are set against a backdrop of uncertain staffing levels as staff numbers reduce due to sickness, self-isolation, shielding or caring impacts. This reduction in operational staff has an impact on the ability to deliver the essential output but will also be felt in terms of reduction in security staff and as such reduced security capacity.

Governance

Protective Security Management Systems (PSeMS)
Pandemic Self-Assessment Checklist

Effective and empowered governance structures are essential to managing organisational responses to the pandemic, including those related to protective security. Your organisation has had to deal with, and will continue to deal with, exceptional issues which require security responses. These security decisions may be needed under tight time pressures, relate to a changed landscape in which your organisation is currently working and without the level of information that traditionally would enable these decisions. The Protective Security Management Systems (PSeMS) tool has been enhanced by the inclusion of a pandemic specific self-assessment checklist to help identify strengths and weaknesses within organisational structures.

Evolving Risks

Your security risks will have been affected by the countrywide changes surrounding the Covid-19 crisis and will continue to change as the various business recovery phases develop. The broad phases which organisations will face are outlined in the Security Planning section below.

Whilst it is understandable that some risks may not have been understood in the earliest phases of crisis management, it is essential to reassess security risks as each of the phases develops. This will help security leadership to:

- **Ensure your security measures continue to be fit for purpose**
- **Identify where security policy may need changing**
- **Understand opportunities and requirements for security to support business**
- **Highlight vulnerabilities which are introduced due to changing working practices**
- **Ensure equipment and personnel are in place to support future phases**
- **Engage staff so measures are understood and operated as intended**
- **Plan for efficient removal of temporary or re-implementation of previous measures**
- **Review current risks as the environment changes**

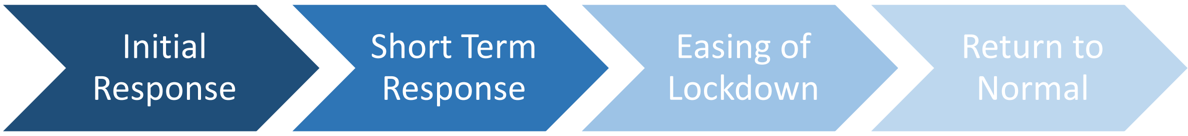
The Protective Security Risk Management guidance available from CPNI, discusses security risk assessment in more detail via https://www.cpni.gov.uk/rmm/protective-security-risk-management.

Staff Engagement

Engaging your staff and their representation groups is a crucial step when defining security policies and procedures; one which is made much more difficult during times of constant change with reduced staffing levels. Your Human Resources business partners will be in a position to assist your staff engagement during this time which will further help to maintain your security culture in unprecedented times.

Your staff should be considered as an essential layer in your security, their awareness of the environment will enable reporting of suspicious behaviours. This applies equally to staff who are furloughed or working from home, allowing suspicious activity via their personal or office devices to be recognised and reported. Staff who are on extended periods away from the office should also be briefed on how they should secure and monitor their office hardware, access passes and credit cards to ensure that these are not being compromised. CPNI have released a guidance document to support your personnel security measures during the pandemic which can be accessed via https://www.cpni.gov.uk/system/files/documents/a3/4e/Pandemic%20Security%20Behaviours%20v4.pdf

Security Planning


Initial Response
Short Term Response
Easing of Lockdown
Return to Normal

These are generic planning steps that can be considered in order to understand how your security may need to adapt as the Covid-19 crisis progresses back to business as usual. Engaging the team leading the organisational response, security can be modified to suit the current and future operating model.

Not all security resourcing is provided in house; security workforce providers, maintainers and suppliers of security equipment are all being put under similar pressures. Engaging with these key security stakeholders will ensure that your planned actions are able to be supported throughout your return to normal operations.

Due to the evolving nature of this event, any plans put in place need to be agile in how they may approach issues going forward. Whilst these are laid out in a linear fashion, thought should be given to the fact that these steps may be carried out in any order, steps missed or repeated, depending on how the crisis unfolds and what the government led response mandates.

1. Initial Response

The initial crisis management will have been focussed on protection of staff and public as well as understanding which outputs and services are essential. It is quite understandable that in these initial moments, security was not in the forefront of people's minds. As the crisis develops however, the security risks should be considered and any vulnerabilities which have been created during the initial response should be identified and managed appropriately.

There may have been a sudden and sharp change in how facilities are staffed, which contracted staff are kept away from your sites due to their organisational policies, and which staff are conducting duties from home. The National Cyber Security Centre has produced a guide on how to manage information risks associated with increased working from home which can be accessed via https://www.ncsc.gov.uk/guidance/home-working. Alongside this, your ongoing personnel management should be considering how to best support your staff.

2. Short-mid Term Response

Once the initial crisis management stage comes to an end, the operational outputs will settle to a sustained base level. Security policies and procedures should be reviewed to ensure that they are fit for purpose and that accepted risks are fully understood by the leadership team.

Once the required minimum staffing to deliver the essential functions has been agreed, security resourcing can be planned around this.

3. Easing of Lockdown

As the restrictions begin to be lifted by the government and business starts to increase beyond the bare minimum operations, people will inevitably return to work, and business outputs will start to return to normal.

This relaxing of restrictions will see many other businesses take similar steps which may impact on supply of equipment or services which are critical to your operation. It may also reduce the speed with which you can re-commission security equipment which hadn't been in use during the lockdown period due to the lack of qualified staff. Engagement with your supply chain and understanding what level of service they can guarantee is essential to your outline planning and ensuring returning to normal operations in a safe and secure way.

By working with the HR business partners, the number and phasing of staff returning to work can be planned for by security teams. This will ensure that security resource planning can support any individual issues around the return to work (such as reset of passwords or PINs or provision of new passes where they have been lost or cancelled etc.) but also support the duties being carried out as a result of the increased activity (increased number of external visitors, opening of additional entrances to support the number of staff within a site etc.). The HR business partners may also provide an opportunity to reaffirm staff as to some of the security policies that are in place which may have been forgotten, changed or were relaxed to enable greater productivity whilst working from home, before they return to work which reduces the demand on your security staff.

4. Return to Normal Operations

Business as usual, when the organisation is able to operate unrestricted may not be the same as the operating environment seen at the end of 2019. This means that your security posture will also need to change.

There may be permanent changes to the way in which certain duties are carried out as people and organisations embrace new working practices which have developed throughout the crisis. Working closely with all stakeholders, any new ways of working can be properly risk assessed, and proportionate security measures and policies put in place to support the new ways of delivering the key organisational outputs.

Resources

Going forward, as issues are encountered and resolved, CPNI along with our colleagues in the NCSC and partners across government will release issue specific guidance to assist in the safe and secure operation of your sites. Further guidance will be signposted via our website at www.cpni.gov.uk.