BAE SYSTEMS

Cyber Incident Readiness, Security and Operational Resilience in the face of COVID-19

Cyber Resilience, Security and IR Readiness in alternate mode

Unprecedented implementation of business continuity plans and remote working

As a result of COVID-19 many organisations and governments are finding themselves in an unprecedented situation. We have seen a large scale switch to remote and home working on a scale not seen before. Many businesses have also suspended or partially suspended many of their non-critical operations, and are struggling to maintain critical operations. This is unusual in that it is occurring globally, across all sectors, and impacting entire supply chains. It's also unusual that it is occurring for an extended period - most DR plans tend to be short term.

In response to this, many organisations have been invoking partial or full Business Continuity Plans (BCP) as part of the switch to largely remote working. This is likely to continue for in some form, for a major part of 2020.

This bulletin provides organisations with information on a series of questions and steps that should be considered, to help ensure that they are positioned to maintain their cyber incident readiness, security and operational resilience, whilst they operate in these alternate operational modes.

For many, suspending business is not an option

Many organisations do not have the option to suspend operations. They deliver services that are critical to National Interests including:

- Health Services
- National recovery efforts to the COVID-19 pandemic
- National Security and Law Enforcement
- Economic well-being
- Wider Critical National infrastructure
- Well-being of citizens and customers

And lastly, for commercial organisations, suspending operations threatens the survival of the business itself.

Business Continuity Planning did not plan for this

Organisations generally plan to run in alternate modes as part of Business Continuity Planning for a limited duration. Most Business Continuity Plans are based on restoration activities to enable to return to normal operations within set-period. Few organisations plan to run in Business Continuity modes indefinitely.

However, without plans that detail timescales and activities that map out a return to normal activities many organisations will find they increasingly struggle to maintain their continuity and operations, in manner that is sustainable.

It is also unusual (and rarely planned for within business continuity scenarios) for entire supply chains (upstream and downstream) to revert to alternate and degrades modes of working for prolonged durations.

Threats do not go away. The actors have already adapted.

Cyber-criminals and nation-state threat actors have not stopped. Since early 2020 there has been already widespread research and evidence showing how they have embraced the COVID-19 events to mount new attacks, and exploit the opportunities afforded to them by the disruption.

The usual plans and procedures may no longer be effective

Home working exposes new or different risks, and resilience 'choke' or stress points.

The departure from normal operating procedures, combined with significant stresses on staff from wider personal concerns and circumstances may increase the risk of successful attacks, or inadvertent compromise.

Changes in working environment, and unfamiliarity with the normal operation presents opportunity for an attacker, and increases the risk of compromise.

Cyber Defence in alternate working—what should organisations do?

- Ensure that you are able to detect and respond to incidents, including cyber incidents whilst in alternate modes.
- Ensure that you understand and are able to manage your business, operational and cyber resilience, even when already in partial BCP or alternate mode. What happens if an incident occurs, how will you react and respond. If you are now in your 'Plan B', What is your plan "C"? What about your upstream and downstream supply chain?
- Ensure you are able to continue managing the security of your business, assets and staff, wherever they are and however they are working.

Throughout, communicate to your staff, and ensure they have the support they need and know what to do, how to contact others, and how to ask for help.

If we are already in "Plan B", if we suffer an incident, what is "Plan C", and can we effectively deploy it?
To help you with this, we have included a number of questions that as an organisation, you should be asking yourselves, and steps that you should take to safe guard your readiness for cyber incidents, resilience and security.

To help you with this, you should:

- Review our questions that you should be asking yourself, and steps that you should be taking.
- Ensure you are satisfied that you can answer the questions, and are satisfied with the answers.
- Where applicable, take the actions recommended in our guidance.

The next pages includes a list of key questions, and steps to consider.

Do you need help with this?
If so, speak to us, we can help.

What questions should you be asking?

Cyber Incident Response

- Does my IR readiness plan account for my alternate operating mode? – e.g. largely homeworking/ remote team?
- Have I tested my cyber incident response plans? Is the test still valid, given the current operational context and modes of working? If not, which parts are invalid, and what do I need to do in my planning and readiness to compensate?
- How do I maintain critical communications to my staff, customers and other stakeholders? How do staff communicate back, and report incidents or suspicious activity?
- Who is my chain-of-command in the event of an incident, how will we manage this and communicate? If we cannot contact people, or they are missing, what is our fall back? How will I maintain chain-of-command?
- How does remote access impact the ability of my team to coordinate and collaborate in an emergency situation?
- Do I have any single points of failure? Are my remote access solutions vulnerable to Denial of Service? What is my fall back if they are attacked?
- In the event of an attack or failure of my remote access solutions, how will I remediate and recover? What critical business operations will be impacted, and how will I provide continuity for these?
- Can I still get access to logs and conduct forensics analysis if required? How will I do this in a timely fashion?
- Who else will I need support from, and need to co-ordinate with? If they are in similar alternate working modes, how will we effectively and rapidly work together?
- If I need to "fall back" from the alternate working mode, what does this look like? How will I maintain comms? Do I have everything I need if I had to do this right now? Do my team know what to do if I become unavailable?

Cyber Resilience

- Do I understand what my business critical processes and operations are, and where the single points of failure or stress points are for each?
- Do I understand how my staff are working, and what tools, systems and networks they are using (official or unofficial)?
- Do I fully understand what supporting processes my critical operations are dependent on, and how these are manifested in alternate working modes. Do I understand who the critical staff are (internal or 3rd party)?
- Do I understand where there are new or additional single points of failure, or where existing systems, networks or process are under heightened stress? Have I adapted my networks and usage patterns to account for this?

- How close am I to the limits for these stress or single points of failure? Is there a fall back for these? How will this be invoked?
- Do I understand what incidents (cyber or otherwise) may either impact these stress points/single points of failure, or cause widespread impact to the critical operations, or process and infrastructure they depend on?
- Have I considered the impact of enhanced flexible working, due staff absences , enforced physical separation and need to care for others, on business operations and processes.
- If a further incident occurs:
  - What is my fall back or "Plan C"? How quickly can I move to plan "C" or further degraded operations?
  - Which services will be prioritised and how will I maintain critical operations?
  - How I will manage a resilience incident (however caused), and how will I respond/recover from it?
- Does my current Business Continuity/alternate mode have a 'life-expectancy'? What is the plan as we approach this? What about the supply chain (upstream and downstream), how are their alternate modes of working going to impact me?

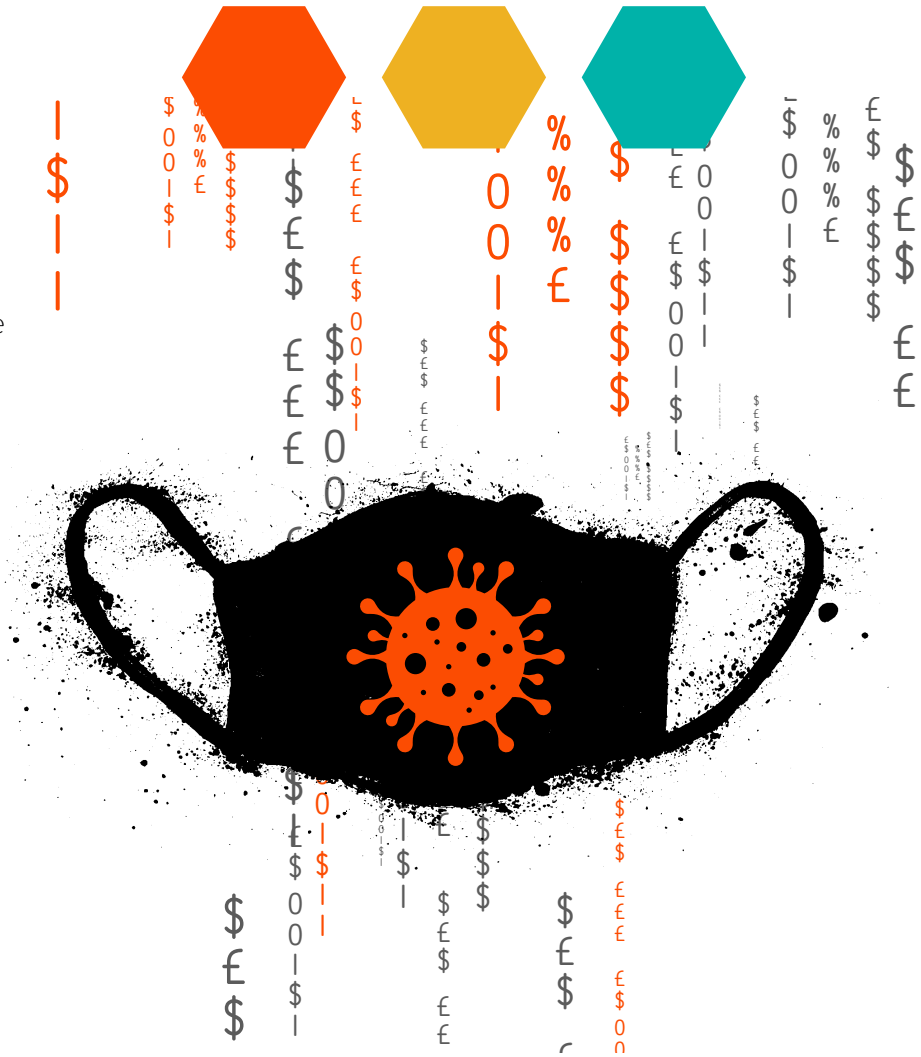
Cyber Security

- Have I taken on board available guidance on home and remote working (e.g. from the NCSC)? Am I confident that I have this covered?
- Do I understand the remote environments in which my staff are operating, incl. shared accommodation, environments etc.?
- Do I understand the channels staff are using to collaborate and communicate. Is there relevant and updated guidance on this?
- Does my business have a means of authenticating communications with staff, especially when using unusual channels?
- Do I (as a business) understand the security risks with the above, and equally importantly, do my staff understand the security risk?
- Are my staff aware and alert for social engineering and phishing? Do staff have an easy and readily available means of asking for help if they need to?
- Are my security, networks and IT teams able operate effectively in alternate operating modes and perform all their security duties, e.g. monitoring? Which duties are impacted, how will my privileged users work remotely?
- Am I able to, and how will I continue to, keep track of, maintain, patch and configure my services, applications and equipment, remote or otherwise?
- Do staff understand what they should and should not do. What policies and procedures have changed, which have not? Is this being clearly communicated to all?
- How am I managing my people processes, including joiners and leavers, e.g. induction and onboarding, along with leaver processes?
- For critical processes that require onsite delivery or operations, how am I ensuring continuity (e.g. skeleton staffing, transport etc.), along with maintaining secure and safe environments for those onsite staff?

What steps should you be taking now?

Cyber Incident Response

- Review IR readiness and plans in view of remote working scenarios. Work out how to access all the systems and information, even when under attack. Identify primary and secondary plans for each.
- Document and share your revised IR Plan with your staff and response teams. Be clear how the chain of command will be established, confirmed and maintained.
- Document the fall back approach if key staff in the chain-of-command are uncontactable or out of action.
- Stress test your comms and response process. Identify where the stress points are, and reinforce or add capacity? (e.g. secondary remote access channels and communications channels. Access to management networks.) be clear on how you will access and manage these as part of a response if your core remote access and control has been taken out.
- How will you get critical staff to site if required? If so, is there a plan for this. Ensure there are options that are not reliant on third party services (e.g. public transport) to do this.
- Make sure staff understand how you will communicate, and if you need authenticate individuals, how this will be done. Communicate the plan to staff now.
- Confirm how you will continue to communicate and collaborate with your suppliers, customers and other stakeholders. How you will you "authenticate"?
- Make a plan for accessing security and IT logs and conduct of forensics. If this needs to be done remotely, using primary or secondary access channels, is there sufficient bandwidth? What is the impact to other users?
- Identify where critical support would be needed from suppliers. Confirm they are able to provide this, identify workarounds if not.
- If you had an incident right now – does the readiness plan work? Revise it so it does.



Cyber Resilience

- Identify business critical processes and operations, and associated single points of failure or stress points for each. Identify the dependent services, and what point failure in other services (e.g. being able to maintain systems) becomes an issue.
- Ensure you understand how your staff are working, and what tools, systems and networks they are using (official, or unofficial). Provide pragmatic guide on the safe use of other channels and tools.
- Set out guidance on flexible working to cover external staff commitments and responsibilities (e.g. carers, childcare etc.). Ensure each team understand the flexible working within the team itself, and how to communicate, collaborate and work together now that staff may be balancing many duties and working very flexibly.
- Confirm how you will manage, maintain and operate each of the critical systems, operations and processes, and how long you can tolerate loss of systems and processes they are dependent on. Make a plan to work around this that works.
- Identify where the new stress points or single points of failure are from alternate mode working. How close to the limits/capacity are you? Make a plan to deal with additional failures and incidents.
- If a further incident occurs:
    - Document what the fall back or "plan C" is.
    - Work out which services will be prioritised and how to maintain critical operations.
- Communicate the plan to staff. Tell people what it is.

Cyber Security

- Review and take on board guidance on home and remote working such as from the NCSC. Make sure you are confident you have this covered.
- Review and make sure you understand the security risks from alternate mode of working, in terms of staff location/remote working, vulnerability of your sites, and use of new channels and communications. Acknowledge that staff may have very different accommodation circumstances and external commitments and constraints. Take account of this and with your communications.
- Make sure staff aware, and alert for social engineering and phishing, and can access easy and readily available means of asking for help if they need to.
- Ensure there are measures of authenticating staff using out of band channels if required, and that these are understood by staff.
- Prioritise critical security, networks and IT team duties, ensure this is understood by the teams, and make sure the means to deliver these are available using secondary remote access channels if required. Make sure they know what these are.
- Put out guidance to staff on what they should and should not do, including what policies may have changed. This should cover corporate and non-corporate services, including communication channels and securing remote environments. This should not be a complete rewrite of policy, but rather digestible information at a glance.

Getting help

If you have reviewed the questions above and need help addressing them or are not satisfied with your current position, we can offer the following services to help you.

Core Objectives:

- Assess ability to effectively detect, respond, remediate and recover from incidents, whilst in alternate working mode.
- Identify additional or heightened business and operational resilience risks (such as new critical single points of failure, or network stress points) due to working in alternate mode. Identify and highlight additional or heightened security risks to your business as a result of alternate mode working.
- Assess ability to maintain security of business information assets, whilst in alternate working modes.
- Recommendations to reduce alternate mode risks, where possible.

These are intended to provide a short, sharp tactical assessment, and will be based on the information available to you now, so as to provide output as soon as reasonably possible to help you through the current situation. By comparison, our standard offerings for non-acute situations would go into more depth and detail, with extended timelines.

Services for alternate operational modes:

Cyber Incident Response Readiness Review

Cyber Incident Response Readiness and Resilience Review

Cyber Incident Response Readiness, Resilience and Security* Review

*As part of the shift to alternate working patterns, we expect the majority of organisations to have already taken security considerations into account, including communications, guidance and support to staff. For organisations that have not managed to do this, we can extend our incident response and cyber resilience assessments, to cover wider security risks.

Further Information and advice:

Contact us for access to our threat intelligence reports, including:

- COVID-19 Campaigns - threat research summary of attacks exploiting the COVID-19 crisis.
- Remote Working Tools - Current threats in a COVID-19 world.
- Lazarus in Indonesia, and exploitation of COVID-19 as part their campaign.

Advice from the NCSC: NCSC Guidance on home-working: https://www.ncsc.gov.uk/guidance/home-working

Be aware of coronavirus scams and look out for suspicious emails: https://www.ncsc.gov.uk/guidance/suspicious-email-actions

We are BAE Systems

At BAE Systems, we provide some of the world's most advanced technology, defence, aerospace and security solutions.

We employ a skilled workforce of 82,500 people in over 40 countries. Working with customers and local partners, our products and services deliver military capability, protect people and national security, and keep critical information and infrastructure secure.

Global Headquarters
BAE Systems
Surrey Research Park
Guildford
Surrey GU2 7RQ
United Kingdom
T: +44 (0) 1483 816000

BAE Systems
8000 Towers Crescent Drive
13th Floor
Vienna, VA 22182
USA
T: +1 720 696 9830

BAE Systems
Level 1
14 Childers St
Canberra, ACT 2601
Australia
T: +61 1300 027 001

BAE Systems
Suite 905 Arjaan Office Tower,
Dubai Media City
Dubai
T: +971 (0) 4556 4700

BAE Systems
1 Raffles Place #42-01, Tower 1
Singapore 048616
Singapore
T: +65 6499 5000

BAE Systems, Surrey Research Park, Guildford, Surrey, GU2 7RQ, UK

E: learn@baesystems.com | W: baesystems.com/threatdefence

linkedin.com/company/baesystemsai

twitter.com/baesystems_ai