Content Guide

Return to office, hybrid working and remote working

Our guide to post-lockdown espionage countermeasure considerations

Context

As the UK eases lockdown restrictions, much discussion is focused on how working patterns and locations will change. Official Government advice has been to work from home where possible, and with strict lockdown phases in place for the UK at various times since March 2020, many workers have now become more used to working from home, have proven that it is effective, and have invested time and money into making their home working environment as comfortable and enjoyable as possible.

However, the draw of the office remains. Some don't have the luxury of space at home to accommodate their working requirements, and many miss the office environment for its many advantages - training, mentoring, on-tap support and advice, the sparking of creativity and innovation, that feeling of connection, and more. It is expected that the UK Government will encourage workers to return to the office once social distancing can be relaxed in acknowledgement of the productivity benefits, as well as to help the commuter-dependent economy.

So, while some organisations are fully embracing ongoing complete remote working, many are looking at hybrid and flexible working options for the foreseeable. With this in mind, what are the considerations from a security point of view?

In this five-part series, we provide our take on how organisations should consider and approach their counter-espionage strategy post-lockdown.

Step 1 - Situation analysis: Review your assets

The majority of security professionals are well versed in risk management and the concept of a risk register. The impact of Covid-19 on most organisations' risk register has been huge as we have all had to navigate dramatic shifts in working practices, and as we enter this post-lockdown phase in the UK we have to review our risk register once more through a Covid lens.

The following steps and considerations should be taken:

1. What are your critical assets?

What was critical pre-Covid and during Covid may not be critical now. For example, critical paperwork which you used to store may now not be needed (bar any legal storage requirements) if you moved to a digital solution.

2. Where are your critical assets?

With the shift to remote working, employees may now be storing more valuable information at home. If you have upped your cloud dependency or you put some solutions in place quickly when the initial lockdown happened to facilitate remote working, have you reviewed the supply chain and determined its adequacy and reliability? If your employees have been working on their own devices, how have they been storing valuable information?

However, perhaps your organisation has started to plan for a bounce back with new office locations or major refurbishments, or you're downsizing and looking to move workers to new sole occupancy or shared locations: how is this going to impact asset location?

3. Who has control of your assets?

It's important to review who has joined or left since the pandemic began, and their involvement with critical assets. The period since March 2020 may have meant some gaps in personnel exit practices or recruitment – now is the time to also review those and ensure that any missing checks or protocols have been satisfied.

Looking ahead to post-lockdown working practices, it is worthwhile being conscious of two further points which may apply going forward :

Consider how assets may be transported between locations

Whether employees are being asked to recommence full office working once more and are migrating their assets from home, or employees are going to be working in a hybrid fashion, do employees know how to transport assets securely and have the means to do so? Are their devices adequately protected for any changes, and are your systems ready to protect from any threats which are unknowingly introduced?

Consider the recommencement of international travel

International travel has not been an option for many since lockdown, but as restrictions lift it is expected that travelling overseas for business purposes will start in earnest. There may be those in your organisation who have not travelled before for business who require awareness and security briefings, and certainly, the advice needs reviewing for consideration of new threats and techniques which require mitigating.

Step 2 - Situation analysis: Review the threats

From an espionage perspective, the threat actors remain the same but their techniques have changed and will continue to change post-Covid-19. Let's explore some of those changes and how they may affect countermeasures strategy as we approach the post-lockdown era.

Hostile state

Hostile state activity is still prolific and the rate is especially high among Critical National Infrastructure and national government. In the UK, there has been increasing national security concern over the activities of China, Russia and Iran. While cyber-attacks have become more devastating as our world becomes more digitised, hostile state actors are still employing traditional techniques either alone or in combination with cyber to achieve their espionage objectives. This includes the extortion or hiring of trusted insiders, honeypot traps, planting listening devices, document theft, and more. Recently, the use of social media by hostile state actors has been highlighted by the Think Before You Link campaign, as it's claimed that at least 10,000 UK nationals have been approached by fake profiles linked to hostile states so education on this threat is crucial. Another technique growing in use is supply chain attack. In April 2021, the US National Counterintelligence & Security Center ran a campaign on supply chain attacks, and incidents such as the SolarWinds attack have highlighted the importance of assessing the supply chain network and its vulnerabilities as hostile states take action to exploit them.

Foreign state

It is widely recognised that in order to stay safe and secure, national security agencies spy on each other to remain cognisant to the emergence of new threat or changes to existing ones. When it comes to political issues which have affected UK business, Brexit, key national elections in countries such as the US, and the forging of trade alliances have created tension in recent months and this can raise the risk of espionage activity for certain industries and organisations.

Competitors

On our Twitter feed, we regularly post incidents of corporate espionage and it is clear that these have not stopped during the pandemic. Emerging from a challenging period, the risk of unscrupulous competitors looking to strengthen their recovery by reducing their risk, getting ahead of the curve, or simply ensuring their survival by whatever means, is high. Increasingly competitors are looking at the recruitment of trusted insiders to achieve their goals, but other traditional technical techniques are just as damaging.

Insider risks

The impact of Covid-19 on the working population has been huge. Changes to job security, the stress of juggling childcare and homeschooling alongside work commitments, the health impact of Covid-19 on either the employee directly or a family member, less than ideal home working conditions, and the general emotional toll of the pandemic has resulted in poor mental and physical health. During this time, the security risks posed by unintentional insiders have increased. When it comes to deliberate insiders, with the rise in activity by hostile state and competitors it can be expected that the insider risk is going to be high during this next era.

Cybercriminals and Organised Crime Groups

Criminals have been motivated by the pandemic to hit the most vulnerable groups in society by praying on fear, confusion and heightened stress levels. Rates of phishing have rocketed and common themes reported to NCSC have focused around Covid-19 testing and vaccines. Similarly, for businesses, scams have focused on imitating official authorities such as HMRC who reported a 73% rise in reported phishing emails from March to September 2020 compared to the previous six months. Ransomware has also been an escalating issue, with many high-profile cases and incidents of data breaches and leaks, and APT activity has become more damaging and targeted. Having the most up-to-date cyber protection is key at all times, but employee awareness and knowledge of what to do when faced with an attack are as important, if not more so, hence investment in training is crucial.

Step 3 - Situation analysis: Review your current countermeasures strategy

Having reviewed your assets and the threats now posed to them, it's time to review your current countermeasures strategy and whether this is effective in protecting your organisation against the risks posed by espionage.

Principally, you will no doubt have changes to your risk register and so you will then have changes to either the specific countermeasures you employ, where they are executed, when they are executed or a combination of all these.

One of the major factors which will likely contribute to changes in your countermeasures strategy will be changes in working practices. Where people are working and the work they are conducting there is going to be changing over the coming months. If you are implementing remote or hybrid working for the foreseeable future, you will need to consider whether the homes of those handling sensitive assets require a formal assessment of technical threats since the adversary will be targeting where they reside and, as a result, the application of specific countermeasures. Travelling to and from office locations once more will require consideration of asset storage and transport.

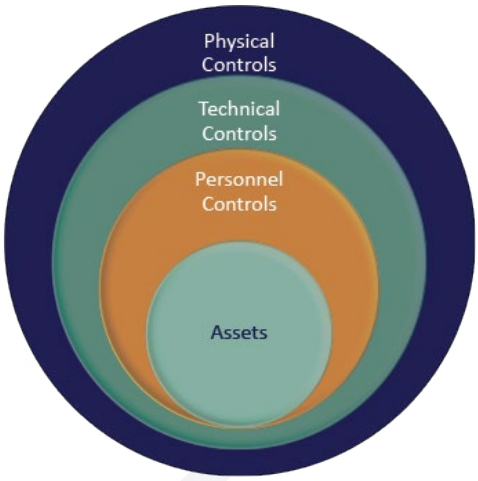
Offices for some organisations will be changing. Perhaps you are downsizing, relocating, looking at shared office space or reorganising office space for more collaborative working and hotdesks. All of these changes pose challenges in ensuring the protection of sensitive information and conversations, and you will need to be mindful of how physical and technical controls need to mirror changes to the physical working environment.

Alongside physical and technical controls, reviewing your personnel controls will be crucial. Even if your asset locations and working practices are not going to be drastically different, as you navigate the easing of restrictions your employees will require support and education to both help them to successfully navigate security changes and to also adjust personally. Avoiding disaffection is crucial to avoid greater insider risk.

At a time when a programme of communication is being planned across the organisation, most likely by HR and Communications departments, there is a key opportunity to include security messages and education. The Centre for Protection of National Infrastructure (CPNI) has produced some excellent guidance on personnel and people security post-lockdown.

Step 4 - Strategy building: Develop a post-lockdown layered, blended countermeasures strategy

When implementing an effective counter-espionage strategy, at Esoteric we strongly believe in a layered 'Defence In Depth' approach which is a trusted information security concept.



Defence In Depth approach to information security

While we specialise in technical surveillance countermeasures (TSCM), mitigating the technical threat is only one part of an effective protective strategy when considering that a determined adversary commonly employs numerous attack techniques to achieve its objective. Examples of this include using social engineering to gain access to administrative systems and implement a cyber-attack, or navigating weak recruitment checks to plant an insider who successfully installs quick plant listening devices or steals sensitive files.

Now, as we navigate changes to the risk register but see a continued degree of uncertainty for the foreseeable future, it is important to have a countermeasures strategy that will support flexibility and change.

Blending layered countermeasures will provide greater flexibility at this time. Blending in the sense of applying countermeasures that provide connectivity, interaction and mitigate multiple threats. For example, technology can enable greater futureproofing for all of your countermeasure layers, as well as providing benefits of improved metric visibility, wider system integration and automation. In the realm of TSCM, an In-Place Monitoring System in your most sensitive conversation areas such as a boardroom can help to provide a greater level of assurance of technical threat protection on an ongoing basis. Investing in portable TSCM equipment, such as our TSCM Lite equipment, and training your manned guarding to sweep key areas or offices before sensitive briefings or meetings can flag any concerns and help ascertain whether you need a professional survey completed, while providing an audit of regular inspections. At the same time, providing a level of TSCM training will ensure they have heightened awareness of the espionage threat which should help to flag any incidents or concerns.

As indicated in our earlier posts, a focus on personnel controls is key at this time to help counter insider risks. Disaffection as a result of feeling anxious about returning to the office is a key risk and can give rise to malicious insider activity. Unintentional insider risk is also at risk of escalating if security culture is not a focus of communication and education at this time, and there is ample opportunity to implement this now. An organisation's people can be its greatest weakness in security terms, as well as its greatest asset. You may need to review your new starters to identify any gaps in induction training, review your leavers to ensure assets have been returned to the organisation, implement awareness briefings and training to ensure employees know of the latest threats, review physical access control privileges as people return to the office, and more. But don't forget that all layers need to be strong. What impact is being Covid-secure having on your physical controls for example? Are you needing to make changes to ventilation with open windows and doors? If so, do you need more manned guarding resource to mitigate the risks this poses?

Step 5 - Implementation: Scenario plan. Program flexibility. Communicate.

It is unlikely that any changes to your countermeasures strategy will result in a dramatic shift or 'push the button' moment. What will be important is scenario planning, flexibility and communication.

You will need to be prepared to review frequently, and that is as much to allow for ongoing uncertainty over Covid-19 as for organisational factors. The easing of lockdown restrictions, changes in working practices and associated countermeasures which are effective in Summer 2021 will most likely have changed by Summer 2022. It is worth having scenario plans, for example, if new national or local lockdowns occur. If you have managed to implement a layered, blended countermeasures approach, then it should then be the case that you have less actionable changes to make if lockdowns reoccur vs. a more rigid, location-dependent or asset-specific strategy. To help you to navigate uncertainty and adapt successfully, review your security suppliers to determine their flexibility and how they can support you.

There will be some controls that you will need to implement to prepare for employees returning to the office, and especially so if you are working to an official re-opening date. Planning ahead will be required for measures such as security briefings to ensure that awareness is high when employees start commuting once more and are in the environment. Similarly, from a TSCM perspective, it is advisable to have a survey completed before employees return, both for practical reasons and to have a 'clean bill of health' after offices have been unoccupied and potentially vulnerable to attack. Equally, if your office or site locations have changed due to growth or downsizing, and especially if you have moved to shared occupancy, or undergone building or refurbishment work, a TSCM survey is highly recommended.

Working together with colleagues will be important to more successfully mitigate insider risks. Forming an insider risk task force with the combined specialisms and knowledge of Human Resources, Communications, Security, Facilities and Risk Management will most likely yield a more cohesive, effective strategy and ensure that resulting communications are more integrated and targeted for better reception by employees.

During the coming weeks and months, you may find it useful to consult different sources of advice and guidance. At Esoteric we are ready to advise, provide consultancy and deliver our services to help you to counter the espionage and eavesdropping threats. We also recommend the following sources of information:

NCSC guidance for SMEs , large organisations & public sector

CPNI overview of espionage, Advice & Guidance & Protective Security Risk Management overview

Want to find out more about Esoteric and how we can protect your business? Get in touch with us via:

Esoteric Ltd UK.
The Links Business Centre, Old Woking Road, Old Woking, Surrey, GU22 8BF
+44 1483 740 423 | mail@esotericltd.com

Follow us at: esoteric-ltd @Esotericltd

esotericltd.com