ROKE

Lockdown: Behavioural Threats in a Covid-19 World

Enhancing resilience to cyber crime in a disrupted world

ROKE

In December 2019, a virus was found in Wuhan, China. Five months later and Covid-19 has grasped the world's attention. The impact has been primarily physiological, with thousands of tragic fatalities. However, the social and economic damage cannot be underestimated. Millions of us sit under lockdown procedures, radically altering our way of life.

The threats we face are not only biological. Due to our disrupted routines, we grant new opportunities to cyber criminals. Many reports have highlighted the technical bugs in collaboration tools. However, few consider our behavioural vulnerabilities. This article looks to identify the user-centred risks in the Covid-19 environment. It then outline approaches that may enhance our resilience. Through sensible measures, we can mitigate threats, whether biological or virtual.

Working from home

Most of us are unfamiliar with extended periods of remote communication. This places us at risk of social engineering, where criminals can impersonate distant colleagues. Through reciprocity (calling a favour) and authority (giving orders), they might then extract valuable data. The use of internal VoIP services (e.g. Skype) may make correspondents easier to identify. However, when we yearn for human interaction, we might overshare sensitive details. Within higher threat models, such as whaling, foes could even use DeepFake to mimic audio and video. It is important that we remain cautious during these uncertain times.

While remote working can be convenient, it does present new threats. Our houses are increasingly populated with smart home devices. Although they offer useful automation, low-end gadgets are notoriously vulnerable. This might embed eyes and ears into our new workspaces. Whereas we are accustomed to our offices, we might misclassify homes as a "safe space". Families should not be excluded from this threat model. We naturally trust our close relations, with self-disclosure key to maintaining this bond. However, cohabiters could develop a detailed picture of our work activities. Sensitive data must remain private, even within a crowded lounge.

Though it's hard to admit, most companies are vulnerable to insider threats. The Covid-19 upheaval does not mitigate this risk, but only exacerbate it. Staff morale might be decreased due to uncertainty and social isolation. Workers might also face financial pressures, particularly if salaries are reduced. This generates a perfect environment for extortion. Remote monitoring can go some way to managing this risk. However, anomalous behaviour will be harder to spot in such anomalous conditions.

Novel communication

The lockdown has led to a rapid shift towards virtual collaboration. Technical vulnerabilities are well-documented, but the user should not be overlooked. While we consider ourselves logical, we are all subject to bounded rationality. This concept describes the heuristics and cognitive biases which limit our decision-making. Prior to the pandemic, we might act impulsively when tired or pressured. These abnormal

times are likely to further encourage illogical behaviour. For example, the availability heuristic may cause us to overestimate Covid-19 prevalence. Hyperbolic discounting might then inspire knee-jerk reactions over prudent planning. We are only human, and the best defence to our biases is to understand them.

Millions of people are utilising new technologies, with little prior familiarity. These tools are often complex, seeking to combine audio, video and file-sharing functionality. Furthermore, the drive for normality pressurises quick adoption. As we act on imperfect mental models and incomplete information, user errors will enhance our vulnerability. The threat is likely to be greater for those with less tech experience, such as the young or elderly. It will take time for this new digital environment to reach homeostasis.

Conferencing software has gained enormous popularity during lockdown. These applications aid both productive work and social communication. However, such popularity might encourage extortion attempts. In the past, Denial-of-Service (DoS) attacks have been used to blackmail sites. If targets refuse to pay, their capabilities are knocked offline. When markets are competitive, victims might prefer to settle than lose their edge. Fortunately, some protection is available through cloud providers.

It is not only services that can face extortion. Adversaries might exploit our increased dependence on virtual communication. Ransomware encrypts a system, rendering infected files unintelligible. Only once the ransom is paid, usually in a cryptocurrency (e.g. Bitcoin), is access restored. Victims have an economic dilemma between regaining files and incentivising attacks. Following payment, foes might repeatedly target this easy option. In the past, firms have weathered ransomware through manual workarounds. With Covid-19 limiting these processes, companies may be resigned to pay up.

Vulnerable infrastructure

It should be no surprise that our national infrastructure is at its limits. As might be expected, healthcare is facing enormous workloads. Unfortunately, this domain has also proved most vulnerable to cyber-attacks. During the WannaCry campaign, criminals capitalised on outdated NHS systems. While laptops can be patched, medical machinery is constrained by its accreditation. With the sector stretched, non-healthcare staff are populating many roles. This inexperience could be exploited by adversaries. Although some hackers have called a truce, Covid-19 might drive a digital epidemic.

The pandemic has led to unprecedented unemployment across the UK. Millions of individuals are furloughed and facing an uncertain future. While the government is providing support, reduced manpower may undermine our resilience. For example, if IT helpdesks are thinned, they might be slow to counter threats. Companies must balance their books while managing security. Although the furlough scheme is beneficial, it may encourage fraud and identity theft. Universal Credit has also been targeted, seeking to capitalise on a flooded system. Parties should take care that their funds aren't claimed by others.

Communication and (mis)information. With the news agenda dominated by Covid-19, we are swamped with content. Unfortunately, it can be challenging to distinguish facts from fake news. On such a complex topic, sometimes the misinformation is unintentional. Research suggests that viral campaigns are driven by emotion rather than reason. Furthermore, being tribal animals, we relish the belonging that such homophily promotes. However, on a matter of such importance, the impact may be fatal. Disinformation will be used as a weapon by hostile states. Such information warfare may hit economies, with western markets having more to lose than most adversaries. Rivals might also seek to destabilise societies, particularly those with polarising restrictions. While autocrats can tighten their grip, liberal democracies will be buffeted by controversial debates.

While phishing is a familiar threat, criminals are now taking advantage of Covid-19. Some campaigns may exploit authority bias and masquerade as reputable sources (e.g. the World Health Organisation).

This might appear credible, particularly when the government uses SMS. Others might claim miracle cures, seeking to capitalise on our emotional biases. In either case, it provides an opportunity to steal credentials and personal data. We should remain vigilant, despite the instability plaguing our lives.

As communication moves online, we experience the good and the bad. While social media can reduce isolation, it often hosts offensive content. Throughout Covid-19, hate speech has been spread on digital platforms. With many frustrated by the pandemic, such anger can be easily misdirected. Restrictions may also enhance cyber-bullying, since victims have no option but to go online. Closed schools have pushed millions of children towards digital immersion. Unfortunately, this can play into the hands of virtual predators. Online disinhibition might lead kids to underestimate the risk they face. Illegal imagery is predicted to increase on the dark web, at a time where law enforcement is stretched.

Return to abnormality

Although the future is uncertain, we can expect restrictions for an extended period. This will cause increased temptation for non-compliance. Most of this is likely to be physical, through unnecessary journeys and social gatherings. However, reduced morale might drive apathetic security, particularly when it's a secondary goal. Restrictions may begin to adjust criminal tactics, with foes adopting paths of least resistance. For example, NHS IDs have been targeted, since they enable greater mobility. As services become digital by necessity, crime may become cyber-crime.

The Covid-19 restrictions will be eventually lifted. However, this will not represent a return to prior normality. The disruption of an unlocked society cannot be underestimated, particularly if home nations adopt different policies. This has been evidenced in the past weeks, where partial adjustments have led to public uncertainty. Companies and staff will have to re-adapt to new environments. Some firms might not return, while others will be undermanned. Particularly in the initial months, our attention might revert back to the physical. Criminals could then target distracted staff to capitalise.

ROKE

Protection

The scale of this pandemic is unprecedented in modern times. As such, we are constrained in the actions we can take. Furthermore, considering the economic complexity, we must be careful to balance the risk. For companies to function, employees require access to their systems. Although workarounds might present vulnerabilities, they may be a commercial necessity. For example, while sensitive discussions have been face-to-face, they now must continue via virtual means. A certain risk tolerance is needed to ensure we can weather the storm. This is particularly vital when capabilities support critical operations or the national response.

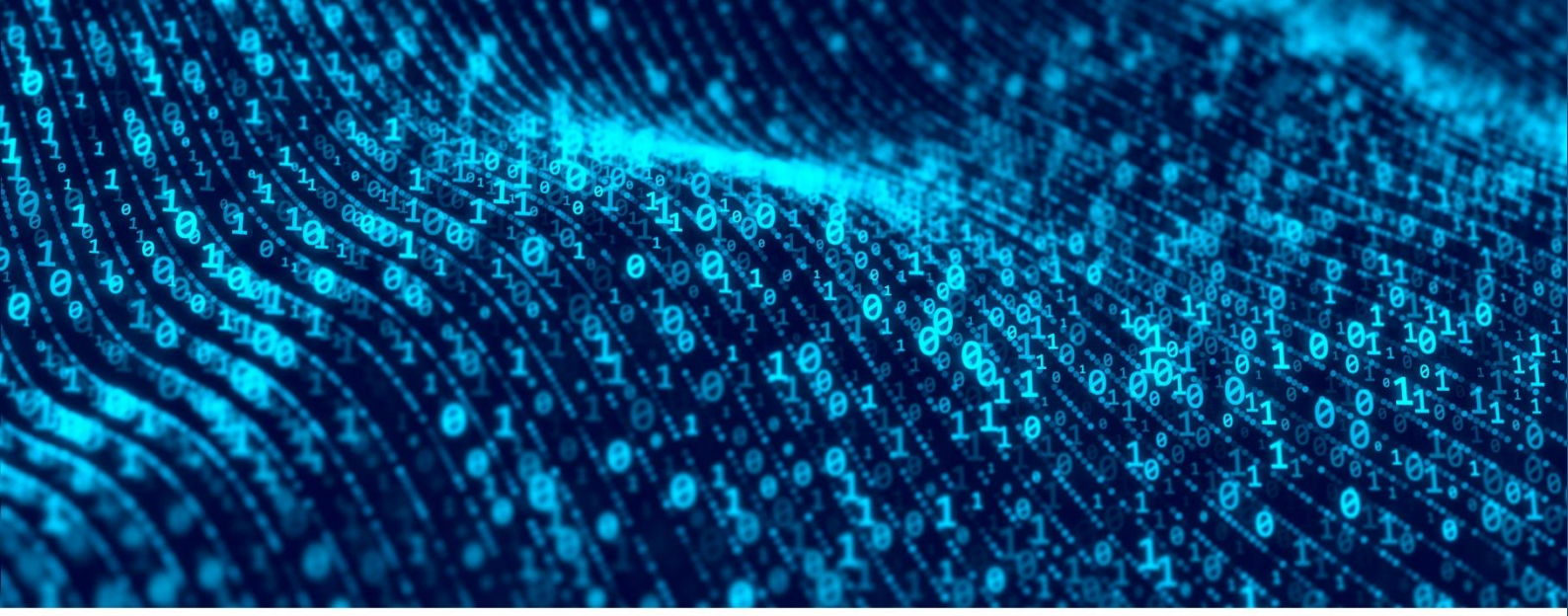
When we seek to mitigate risks, there are some simple principles to adopt. These can be grouped into three categories: physical, virtual and psychological. While our home offices may be imperfect, they need not threaten security. Protect your documents as you always have, through lock screens and locked drawers. If smart devices can be relocated, store the gadgets during the working day. Our vacant offices should not be forgotten, with monitoring necessary to deter incursions. Although this comes at a cost, it is far less than the potential damage. Finally, of greatest importance is your own health. Continue to follow the government guidelines to minimise your Covid-19 risk.

Since the threat is virtual, there are several protections we can implement. At an absolute minimum, individuals should only use recently-updated applications. Older versions contain vulnerabilities, with recent popularity encouraging criminal interest. If these tools are unfamiliar, resist the pressure for instant adoption. It is more important that apps are used correctly than quickly. When breaches do occur, back-ups can prove vital. Ransomware can be overcome if targeted files are quickly restored. Unfortunately, with remote devices and intermittent connectivity, recovery may not be trivial.

Finally, we should not underestimate the importance of psychological resilience. While our machines might continue as usual, our minds are disrupted. To minimise our vulnerability, we should not hesitate from taking frequent breaks. Not only is this shown to increase productivity, but should enhance attentiveness and morale. Fake news is as viral as the pandemic, but we can take steps to limit its spread. Apply critical thinking and don't share what appears sensational. Though it might seem distant, we will eventually return to a new normal. This transition risks posing further disruption. Use any downtime to prepare yourself for the post-Covid world.

Support

At Roke, we recognise that security goes beyond chipsets and ciphers. Through our Human Science capability, we help clients identify behavioural threats and opportunities. Our expertise ranges from usability and behaviour change to managing misinformation. In these uncertain times, systems are only as strong as their weakest link. Roke supports their clients from hardware to human.



ROKE

We believe in improving the world through innovation. We do it by bringing the physical and digital together in ways that revolutionise industries.

That's why we've fostered an environment where some of the world's finest minds have the freedom, support and trust to succeed.

Roke is a team of curious and deeply technical engineers dedicated to safely unlocking the economic and societal potential of connected real-world assets. Our 60 year heritage and deep knowledge in sensors, communications, cyber and AI means our people are uniquely placed to combine and apply these technologies in ways that keep people safe whilst unlocking value. For our clients, we're a trusted partner that welcomes any problem confident that our consulting, research, innovation and product development will help them revolutionise and improve their world.

If you're bringing the physical and digital worlds together, we'd love to talk.

Roke Manor Research Ltd
Romsey, Hampshire, SO51 0ZN, UK
T: +44 (0)1794 833000
info@roke.co.uk www.roke.co.uk