JASON R.C. NURSE

BALANCING CYBERSECURITY & PRIVACY IN THE REMOTE WORKFORCE

Remote working will only truly work if we get the balance of security and privacy right.

The COVID-19 pandemic took the world by surprise and countries are still grappling with its impact on society, the immense loss of life, and how to return to any form of normality. As remote working increased during the pandemic, so too did the cyber-attacks aiming to exploit it.

Malevolent actors viewed the pressures caused by the pandemic as the perfect opportunity to launch a variety of cyber-attacks. These targeted critical national infrastructure (e.g., ransomware and intellectual property theft attacks on healthcare and medical research organisations), businesses (via their remote workforces and often newly-adopted distributed working infrastructure), and members of the public (using a range of coronavirus-related scams) (Lallie et al., 2021). En masse, these attacks proved substantial and forced governments and organisations to rethink their approaches to cybersecurity.

Unfortunately, many issues remain for securing the post-COVID-19 remote workforce and balancing cybersecurity and privacy going forward.

SECURING TODAY'S REMOTE WORKFORCE POSES A NEW AND DIFFERENT CHALLENGE

Before COVID-19, working from home was a carefully managed reality typically reserved for those who had specific jobs, were at a prescribed level of seniority or had extenuating circumstances. In general, these individuals were trusted by the employer and were trained (either directly or via previous experience) in working effectively and securely from home. COVID-19, however, changed this situation considerably, with millions of new workers suddenly forced to work remotely with little training and in challenging home and personal environments.

My research, with colleagues (Nurse et al., 2021), has investigated the range of new cybersecurity risks present in these environments, and I discuss four of the top concerns here:

1. Security mindset

De-prioritisation of a security mindset because of heightened anxiety, stress, depression, burnout, and poor mental health generally motivated by the pandemic. As individuals concentrate more on basic needs (e.g., safety, health, family, job security), they may be less cognisant of workplace security concerns; or may assume that security is purely the organisation's responsibility. This continues to be true today because there has been little mental and psychological break/downtime for many individuals since the pandemic began.

2. Security training

Lack of security training for the remote working environment resulting in poor security practices that increase the potential of a compromising cyber-attack. Many organisations were not able to train employees adequately or build a strong security culture before they were forced to work from home. Even now as they return to offices, there is a lack of general understanding about security culture and related practices (Uchendu et al., 2021).

3. Remote working insider threat

Remote workers may, in rare cases, exploit the lack of management monitoring or oversight to steal confidential information from their employer or misuse corporate services. Although not the norm, cases of insider threat by remote workers may be motivated by perceived, or actual, job insecurity due to the pandemic; a period where many have been laid off or made redundant.

4. Returning to work

After a long period of remote working, employees returning to offices may bring infected devices into the Critical National Infrastructure (CNI) and corporate networks. Home networks are much more likely to be compromised than CNI and corporate networks, and therefore the extended period of remote working can escalate this risk. This also poses a significant challenge for employers and IT teams as they try to reintegrate employees into the office environment.

These risks are novel given the context of COVID-19, and the combination of technological, social, and psychological factors that they are based upon. Cybersecurity teams need to appreciate the socio-technical nature of the risk, and plan, create and test solutions that accommodate these factors.

"De-prioritisation of a security mindset because of heightened anxiety, stress, depression, burnout, and poor mental health generally motivated by the pandemic."

Image credit | SB Arts Media / Shutterstock.com

WHY IS PRIVACY IMPORTANT TO THIS DISCUSSION?

While security tools can be viewed as enablers of privacy (e.g., end-to-end encryption in communications software such as Zoom, Signal or WhatsApp), in some contexts, security and privacy are regarded as competing goals. For instance, as organisations sought to secure and manage remote workforces, there was a marked increase in the use of remote employee monitoring and surveillance tools. This led to several new widespread risks, this time to employees' privacy:

- **The potential infringement of employee's privacy caused by a dramatic surge in employer usage of (remote) workplace surveillance/monitoring technologies.** This could include monitoring of keystrokes, screens and websites visited. A significant reality is that in some cases, employees may be using their own technologies (iPads, smartphones, laptops) for remote working, thereby giving employers (or the companies they outsource security management to) access to vast amounts of personal employee data.
- **New forms of technology (e.g., smart technologies) emerging during the pandemic that can monitor employee emotional state could also violate privacy.** For example, such emotional and psychological data, if not properly protected, may be used to profile employees according to their wellbeing, and thus impact employment or future career prospects.

"A significant reality is that in some cases, employees may be using their own technologies for remote working, thereby giving employers (or the companies they outsource security management to) access to vast amounts of personal employee data."

Privacy is an important consideration for employers because of the need for trust between employee and employer, regardless of sector. If employees perceive that there is excessive, unwarranted monitoring, this could lessen their trust in, or commitment to, the organisation.

There is, therefore, a delicate balance to be maintained. As governments, policymakers, corporations and SMEs seek to weather the plethora of cyber-attacks that continue to emerge, developing cybersecurity solutions that also consider employee privacy concerns is paramount.

Dr Jason R.C. Nurse is an Associate Professor in Cyber Security at the University of Kent and a Visiting Academic at the University of Oxford. His research focuses on organisational cyber security, insider threat, and human aspects of security and privacy.