May 20, 2021 21:20 BST

Executive Analysis: Three actions to reduce insider threats while working remotely

The shift to remote working during lockdown has presented specific security challenges for organisations: 39% of respondents to our survey of 290 cyber security decision makers reported that insider threats have increased in the last six months, and 51% believed that an increase in remote working was the main cause for this.

Whether they are malicious or accidental, insider threats can take various forms including disruption to systems, theft of intellectual property and fraud. However, all insider threats can expose organisations to cyber risk, so it's

vital that you take action to address them.

In a separate post, our chief technical officer, Ollie Whitehouse, explores some of the technical issues around insider threats that your CIO or CISO should consider. In this briefing, we reflect on those issues from an executive's perspective, giving you practical advice to reduce your organisation's risk of insider threats while working remotely.

Optimise your controls

According to our research, 29% of decision makers agreed that a lack of appropriate controls had contributed to their increase in insider threats. This can partly be explained by the fact that organisations have been forced to establish new remote working infrastructures quickly, without always understanding the risks of doing so. In many cases, these infrastructures will have included exceptions to pre-lockdown security controls such as greater leniency when granting access to files and the disabling of multi-factor authentication. However, these exceptions could all make it easier for insiders to compromise sensitive information while appearing legitimate.

With this in mind, organisations should ensure that they have a strong Identity and Access Management (IAM) framework in place across their remote working set-up. IAM covers the policies, processes and systems that govern the roles and access privileges of individual network users. Ideally, this should include clear policies around who can access certain systems, data or functionalities and why, and the circumstances in which those privileges could change according to the business's need.

Among other things, IAM should also mandate users to establish their identity before authenticating that identity with multiple factors including passwords, two-factor authentication or biometrics. However, it's important that your IAM controls aren't so strict that they deny users the privileges they need to carry out their day job. In these circumstances, people will often develop workarounds, heightening the risk of accidental insider threats and wasting time and resources required to investigate them.

To mitigate against this, ensure that someone is actively checking incident logs to bucket insider incidents into accidental and malicious categories. If you're regularly seeing accidental security alerts, speak to your people and your IT team to ensure that your controls are fit-for-purpose and consider

adjusting them accordingly. When they are optimised in this way and combined with the concept of least privilege, which only provides users with the minimum levels of access and permissions needed to do their job, IAM controls can be a powerful defence against insider threats.

Improve your detection capabilities

Often, there is no obvious pattern to indicate that an insider threat attack is imminent or ongoing. However, 39% of decision makers that suffered an increase in insider attacks in the last six months blamed a lack of detection capabilities, indicating significant room for improvement in this area.

To detect insider incidents as early as possible, implement a logging or monitoring system to provide visibility of activity across the network and create clear benchmarks for what constitutes 'normal' vs 'anomalous' behaviour for each individual system. For this solution to be effective and to avoid missing suspicious activity, it's also important to appoint someone with responsibility for regularly checking alerts and output. Pop-ups that warn a user that their activity is being monitored when they try to access restricted areas can also be helpful deterrents against insider activity, and can be used as part of a detection solution.

As part of this detection of network traffic, monitor for indications of mass data exfiltration or large data transfers via removable media such as USB flash drives. This could indicate that an insider is transferring data from the organisation maliciously, so it's important that you can identify this quickly and easily. Fingerprinting data and analysing it as it passes the boundary of a company through Data Loss Prevention (DLP) solutions can be effective safeguards here.

Train your people

Of the respondents that reported an increase in insider-related incidents in the last six months, a third believed that a lack of training or awareness within their organisation was behind this. As such, it is important that cyber security teams take a holistic view to defending against insider threats, focusing on training and awareness alongside technical controls and detection measures.

Firstly, ensure that your training programmes are updated to reflect people's new ways of working and that the content of the material includes real, current events and incidents that people can relate to. For example, we have seen a rise in phishing attacks that label ransomware with titles including COVID-19 in the last 12 months, so share examples of these attacks with your employees. This will increase the impact of the training and be more likely to bring about meaningful change in people's behaviours.

Next, ensure that your employees know what key indicators of a potential insider threat looks like and empower them to anonymously report suspicious activity to senior management.

Organisations should also tailor their training to the specific threats to your organisation. We have seen many organisations use the same generic security awareness materials for all staff without updating them on a regular basis. However, the insider threat landscape has evolved through remote working, offering more opportunities to access and compromise vital assets, so this approach is ineffective.

With this in mind, you should tailor training according to users' roles. For example, someone responsible for monitoring incident logs should receive different training to an everyday user. Additionally, those with escalated privileges should be informed on best practice around the security of the assets that they can access so that they can spot any malicious activity towards those assets.

No training program will ever completely remove the likelihood of an employee clicking on a suspicious link. However, these measures will help employees to feel more engaged with the security of their organisation, flag suspicious activity earlier than they would have done and be less inclined to consider a malicious attack themselves, all lowering the risk of an insider attack.

Conclusion

It's important to have empathy when dealing with insider threats. Personal changes and challenges have accompanied the operational shift to remote working, leaving people juggling the demands of their partners, children and pets alongside their professional responsibilities.

This process has meant that traditional working hours and practices, well known by cyber defence teams, have become very different. For example, early starts to get on top of work before taking over the home schooling so partners can focus on their work for the rest of the day are now commonplace, as are new ways of sharing data, files and access via cloud-based software that businesses have integrated under lockdown.

Previously, all of these things could have been flagged as suspicious activity, but it's vital that you don't alienate employees by casting doubt on their behaviour while working remotely. Ultimately, this new way of working is here to stay, so it's vital to make it as easy as possible for people to follow security guidelines rather than asking them to change their new behaviours.

By optimising their controls, increasing their detection capabilities and upskilling their staff, organisations can go a long way to reducing their risk of insider threats while working from home.

Insight Space – People

This Executive Analysis is part of our latest edition of Insight Space which tackles the importance of people when it comes to ensuring an organisation is truly resilient.

We've put together technical and executive insights, case studies and practical advice focusing on how organisations can manage their people risk.

*Find out more **here***

About NCC Group

NCC Group exists to make the world safer and more secure.

As global experts in cyber security and risk mitigation, NCC Group is trusted by over 14,000 customers to protect their most critical assets from the ever-changing threat landscape.

With the company's knowledge, experience, and investment in research and innovation, it is best placed to help organisations assess, develop and

manage their cyber resilience posture.

With circa 2,000 colleagues in 12 countries, NCC Group has a significant market presence in North America, Europe and the UK, and a rapidly growing footprint in Asia Pacific with offices in Australia, Japan and Singapore.

Contacts

NCC Group Press Office
Press Contact
All media enquires relating to NCC Group plc
press@nccgroup.com
+44 7824 412 405
+44 7976 234 970