Cybersecurity during Covid-19

Managing insider risk during the pandemic

May 2020

Our ways of working have changed. How can you help your organization manage insider risks in this new world?

Document changes to your controls

Some activities are so prone to insider threats that it may not be possible to carry them through, outside of a supervised office environment. Be clear on what these key roles are, and build the justification for access to premises. Any policy changes enabling activities to be performed remotely should also be recorded — putting in place additional monitoring controls. Define risk tolerances and document them.

Recalibrate your models and tooling

Staff may be working in different ways, at different times and using different access infrastructure. Expect to recalibrate detection tools. Behavioral models that may flag patterns such as frequency of remote logins, activity after hours, physical ID card / token access and even mistyped passwords may not be reliable.

Watch the holes in your filter

Processes and policies may need to adapt to prevent or detect insider threats; they may have gaps, at least for a short time. Extend logging of user activity, allowing for a retrospective review once the situation stabilizes. Meanwhile, communicate new risks to the business which arise from monitoring gaps, including regulatory implications.

Be prepared to run forensics remotely

Make arrangements to control enterprise laptops and phones remotely should the need arise and make sure you're able to conduct forensics analysis including, the physical recovery of the device if needed. Where bring-your-own-device is part of remote working, ensure policies and employment contracts enable investigating personal devices used for work processes.

Keep the human touch

Turn the video on during conference calls, and remember people matter.

Working conditions may be stressful, but this is a time to support the team and avoid feelings of resentment or disillusionment. Make sure you understand the challenges they face in balancing security and efficiency under unfamiliar conditions. Everyone will have different demands.

Pay attention to the behavior that matters

There will be a rise in security alerts as your staff try to download collaboration solutions out of necessity ("shadow IT") and make mistakes while adapting to new home working conditions. Expect the need to filter out unintentional actions, and also tolerate well-meaning actions which might otherwise have been regarded as a disciplinary matter. Tune detection tooling and disciplinary policies accordingly.

Actions have consequences

When intentional, malicious behavior is identified, act decisively, take proportional punitive action and use the case study to educate staff. Knowing that detection and monitoring tools are still operating as an effective deterrent and can help employees understand that security and privacy are still business priorities.

Contacts

Tariq Dreiza
Head of Technology
KPMG in Saudi Arabia
E: tdreiza@kpmg.com
T: +966 55 388 9928

Ton Diemont
Head of Cybersecurity
KPMG in Saudi Arabia
E: antondiemont@kpmg.com
T: +966 56 860 8393