ANBIMA Incident Response Workshop

Summary

ANBIMA hosted a cyber security incident response tabletop exercise at ANBIMA's offices in São Paulo. The workshop was part of the broader effort by ANBIMA to build up the understanding and application of cyber security within its member organisations.

Cyber security is a rare topic that affects organisations of all sizes, across all industries and requires a concerted, organisation-wide strategy to counter it. Attendees were provided with understanding of both the technical controls, and the required governance and oversight the business must perform to ensure that cyber security is risk is well managed.

Overall my impressions of the workshop and the attendees were that the attendees understood the risk that cyber security poses to their organisations and were proactively taking steps to improve their cyber security posture. Of particular note, there was much discussion on the day by attendees of the importance of a joined up approach between IT, Compliance and other areas of the business. An organisation-wide approach to cyber security such as this has a much greater chance of success than one which is delegated to just being an 'IT problem.

The workshop was designed to build on the results of the cybersecurity survey sent out to members in 2017. The workshop was tailored specifically for asset managers, focusing on improving the understanding and resilience against common cyber threats within small organisations.

The three tabletop scenarios covered common cyber threats that all organisations are likely to face on an ongoing basis. Each tabletop scenario would explore how the attack was progressing, how it had been able to succeed and showed how the incident response process could be conducted.

The first two scenarios covered a ransomware attack and malware which automatically spread across the network. The final scenario looks at incident response due to cloud services being targeted. In this scenario, we explored the benefits and risks of cloud services, the shared responsibility model of the cloud and the importance of securing the data within.

Next Steps

The workshop was a valuable exercise to exploring how cyber attacks can occur, and providing a framework for the incident response process. Each cyber attack scenario also showed how basic controls can be extremely effective at preventing and limiting cyber attacks. Knowledge of these basic controls can be used as an effective benchmarking exercise and attendees were also provided a number of workshop suggestions that they could take back and perform within their own organisations.

These workshops will help organisations better understand their current cyber risk levels against common threats, provide practise incident response tasks and help to improve the communication between areas of the business in the event of an incident.

It it strongly suggested that all organisations take time to perform these workshops and ensure the results of them are presented to the cyber security governance structures within their organisations.