KPMG

Maintain high standards

Cyber risk

Reaction | Resilience | Recovery | New Reality
COVID-19

—

kpmg.nl

Remaining vigilant

Cyber risk

Why strong cyber risk management is crucial in time of Corona?

— Organisations are rolling out new remote working and cloud infrastructure at a fast pace and are being forced to implement new ad hoc security models and approaches to secure that infrastructure. This results in alleviated cyber security risks.

— In addition banks will face cost pressure as result of the crisis. Also in the cyber security domain while being called upon by regulators and policy makers to remain vigilant of cyber security risks.

Key challenges faced

- ✗ Dealing with COVID-19 themed cyber threats. Increased risk of phishing attacks and email frauds due to remote working
- ✗ Managing escalating costs of IT security when budgets are constraint and costs saving as required
- ✗ Current Business Continuity plans do assume that not every organisation's Business Continuity Plan is simultaneously triggered
- ✗ Accelerated moves to the cloud requiring adaptation of security models
- ✗ Concerns about security and viability of managed service providers
- ✗ Increased pressure for automation to deal with regulatory changes and meet compliance requirements

How to respond

- ✓ Focus on embedding pragmatic remote working security controls to deal with threats, including education of employees
- ✓ Act to secure cloud and other ad-hoc collaboration environment and seek assurance on security controls of managed services providers
- ✓ Review and enhance business continuity management frameworks, covering larger, more frequent and globally simultaneous events
- ✓ Test robustness of your cyber resilience and optimise controls while reducing cost of ownership
- ✓ Plan to migrate to a security operating model that allows for greater automation

Remaining vigilant

How we can help

Cyber incident response support and prevention

In the current digital threat landscape, we continue to help our banking and other clients to prevent and resolve cyber incidents and deal with the security and privacy of new working models, including the rapid reconfiguration of security controls.

Business continuity risk assessments

Recognising the need of taking a new and broader approach for Business Continuity Planning and Operational Resilience, we can assist in drafting these new approaches as well verify the effectiveness of these plans by organising sector-wide crisis management exercises.

Advice and implementation on automation of the Cyber Security function

We can help with rationalisation and automation of security controls, resulting in cost savings and ultimately developing a more data driven resilient security model.

Cloud security

New working models require built-in security and privacy processes working across disciplines and ecosystems. We assist banks by providing a strategic approach to governing information on the Cloud and enhancing the Cyber posture by leveraging advanced AI technology.

John Hermans
Cyber, Governance and Risk
+31 6 5136 6389
hermans.john@kpmg.nl