

在東南アジアの日系企業は、サイバーセキュリティアセスメントやトレーニング等、サイバーセキュリティを重要経営アジェンダと位置づけて取り組んでいる

今後起こり得るシナリオ



法規制への対応が必要となる



客観的なサイバーセキュリティ能力の証明が必要となる



サイバーインシデントが発生する

対応方針

- 準拠すべき法規制の整理
- 対応するための人員確保・体制整理
- 法規制対応のタイムライン検討

- 全般的なサイバーセキュリティアセスメントを実施し、自社のサイバーセキュリティ能力を把握および整理
- 特定システムの侵入テストを実施して脆弱性や改善ポイントが無いかを確認

- 従業員のサイバーセキュリティへの意識向上
- サイバーインシデント発生時の対応を確認

サイバーに係る取り組み(例)

1

PDPA
(個人情報保護対応)

2

Cybersecurity Assessment
(サイバーセキュリティアセスメント)

3

User Awareness Testing
(従業員の意識テスト)