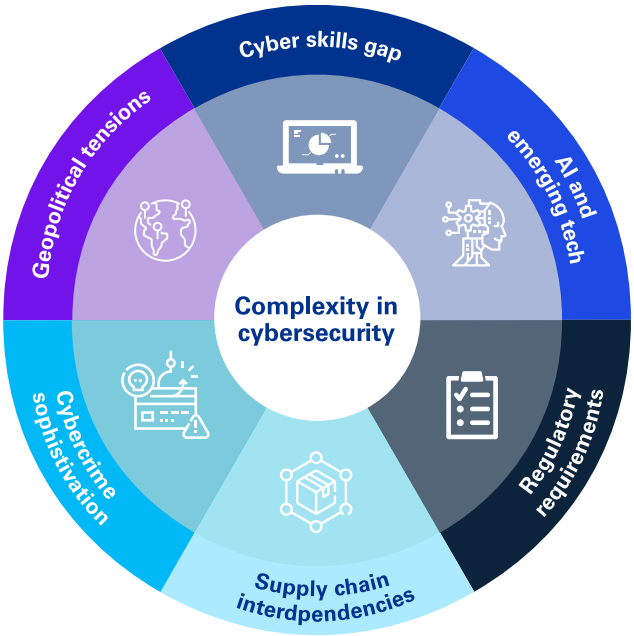
KPMG

Audit Committee Forum No.57

Embedding Trust in an AI-Driven World: Cybersecurity Insights 2025

Cybersecurity is becoming increasingly complex



Reference: Global Cybersecurity Outlook 2025 (World Economic Forum)

Eight key cybersecurity considerations for 2025

1

The ever-evolving role of the CISO

What CISOs and their teams focus on, and how they interact with the rest of the organization is fluid, as the cybersecurity function becomes more broadly embedded within and better understood across the organization.

2

The power of the people

As organizations continue to transform their business models in the face of new digital disruptions, many are experiencing real challenges around workload, which is exacerbating the long-discussed cyber skills gap. AI and automation can help, but there is an underlying risk of talent attrition as many teams struggle to cope.

3

Embed trust as AI proliferates

AI is here to stay and has a place in virtually every organizational function, but there are a number of key cyber and privacy challenges that have the potential to affect the adoption and deployment of AI.

4

Harness AI for cyber: Racing ahead vs racing safely

Many factors appear to be contributing to the buzz around AI adoption, from a lack of training to the fear of missing out and possibly falling behind. A key challenge is weighing the potential benefits of integrating AI into cyber and privacy functions against the potential risks.

5

Platform consolidation: Embrace the potential but recognize the risks

Increasingly, many global organizations are looking to reduce the complexity and cost of their technology. Organizations that choose to do so by consolidating tools and services on to a single, or a limited number of platforms should seek to identify and navigate the inherent risks.

6

The digital identity imperative

Although there are several initiatives around digital identity sprouting up worldwide, interoperability between systems and enhanced authentication due to the emergence of deepfakes remain challenging, whether because of regulations, risk appetite, and/or public opinion regarding the processing of personal and biometric data.

7

Smart security for smart ecosystems

The rise of smart devices and products worldwide is challenging and changing traditional views and approaches toward security, prompting many regulators to introduce new regimes to ensure these products meet basic security requirements.

8

Resilience by design: Cybersecurity for businesses and society

Resilience is becoming central to the CISO agenda as the prospect of attackers using ransomware or other malicious means to cause large-scale industrial disruption, risking both data and human lives, remains alarming.

Reference: https://kpmg.com/xx/en/our-insights/ai-and-technology/cybersecurity-considerations-2025.html

KPMG in Thailand

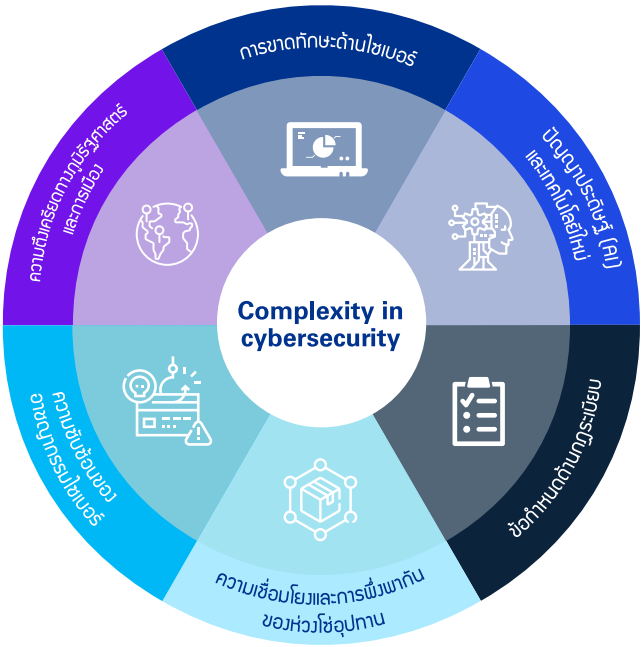
kpmg.com/th

KPMG

Audit Committee Forum No.57

Embedding Trust in an AI-Driven World: Cybersecurity Insights 2025

ความปลอดภัยทางไซเบอร์: ความท้าทายที่ซับซ้อนมากขึ้น



อ้างอิง: Global Cybersecurity Outlook 2025 (World Economic Forum)

8 ประเด็นความปลอดภัยทางไซเบอร์ขององค์กรในปี 2568

1

CISO จากผู้เฝ้าระวังสู่ผู้นำการเปลี่ยนแปลง

Chief Information Security Officer (CISO) ต้องมีความเข้าใจในเป้าหมายทางธุรกิจ ประโยชน์และความเสี่ยงของเทคโนโลยีใหม่ๆ ที่สามารถเสริมความแข็งแกร่งให้กับกลยุทธ์ทางธุรกิจ และกำหนดมาตรการในการบริหารจัดการความเสี่ยงที่เหมาะสมจากภัยคุกคามทั้งภายในและภายนอก

2

พลังของคน: หัวใจของความปลอดภัย

CISO ต้องมีกลยุทธ์ในการดึงดูดและรักษาบุคลากรที่มีความสามารถหลากหลาย พร้อมเสริมทักษะให้ทีมงานสามารถทำงานร่วมกับระบบ AI ได้อย่างมีประสิทธิภาพ CISO ต้องมุ่งเน้นที่การเชื่อมช่องว่างระหว่างทีมรักษาความปลอดภัยและพนักงานในส่วนอื่นๆ ขององค์กร เสริมสร้างความรู้ด้านความปลอดภัยทางไซเบอร์ และส่งเสริมวัฒนธรรมที่ทุกคนมีส่วนร่วมในการป้องกันภัยคุกคามทางไซเบอร์

3

AI กับความไว้วางใจ

องค์กรต้องให้ความสำคัญกับการกำกับดูแลข้อมูลที่เข้มงวด สอดคล้องกับหลักจริยธรรม และให้ความสำคัญกับคุณภาพของข้อมูลที่ใช้ การประเมิน AI อย่างต่อเนื่องเพื่อป้องกันผลกระทบด้านความปลอดภัยทางไซเบอร์ ไม่เพียงช่วยปรับปรุงประสิทธิภาพของโมเดล AI แต่ยังสร้างความไว้วางใจแก่ผู้มีส่วนได้ส่วนเสียในการใช้ข้อมูลอย่างมีความรับผิดชอบและโปร่งใส

4

ตรวจสอบด้านความปลอดภัยไซเบอร์ก่อนเร่งใช้งาน AI

ก่อนที่จะนำ AI มาใช้ องค์กรต้องมั่นใจว่ามีรากฐานด้านความปลอดภัยทางไซเบอร์ที่แข็งแกร่ง และมีการจัดการที่เหมาะสม ไม่ว่าจะเป็นการอัปเดตระบบ การควบคุมการเข้าถึง การฝึกอบรมทีมงาน และแก้ไขช่องโหว่ที่มี

5

การรวมแพลตฟอร์มเพื่อเพิ่มประสิทธิภาพและลดความเสี่ยง

องค์กรอาจเลือกใช้เครื่องมือความปลอดภัยที่หลากหลายเพื่อปกป้องข้อมูลของตน และป้องกันธุรกิจจากภัยคุกคามออนไลน์ ทางเลือกในการรวมแพลตฟอร์มอาจเป็นแนวคิดที่ดีที่ช่วยให้องค์กรต่างๆ สามารถจัดการกับเครื่องมือเหล่านี้ได้ง่าย รวมถึงมีประสิทธิภาพและมีการควบคุมที่ดีขึ้น ขณะเดียวกันก็มีความเสี่ยงที่ต้องพิจารณาควบคู่กัน CISO ควรคำนึงถึงความเสี่ยงที่เกิดจากการมีผู้ให้บริการหลักเพียงไม่กี่ราย โดยอาจพิจารณาผู้ให้บริการสำรองเพิ่มเติม เพื่อกระจายความเสี่ยงและเพิ่มความยืดหยุ่นในการดำเนินงาน

6

ตัวตนทางดิจิทัล (Digital Identity): เกราะป้องกันยุคใหม่

จากภัยคุกคามอย่าง Deepfake และการแอบอ้างตัวตนใน Internet of Things (IoT) องค์กรควรพัฒนากระบวนการยืนยันตัวตนที่ทันสมัย เช่น ไบโอเมตริก รวมถึงใช้หลักการให้สิทธิพิเศษน้อยที่สุด เพื่อการพิสูจน์ยืนยันตัวตน และลดการเข้าถึงระบบโดยไม่จำเป็น นอกจากนี้ ต้องมีการสอบทานและปรับปรุงตัวตนทางดิจิทัลในระบบงานที่สำคัญอย่างสม่ำเสมอ

7

ความปลอดภัยอัจฉริยะสำหรับระบบนิเวศอัจฉริยะ (Smart security for Smart ecosystem)

อุปกรณ์อัจฉริยะ (Smart Devices) ต่างๆ อาจส่งผลให้เกิดช่องโหว่และความเสี่ยงใหม่ องค์กรควรนำแนวคิด Security by Design มาใช้ในการออกแบบและพัฒนาทุกกระบวนการ โดยเน้นความปลอดภัยเป็นหลักตั้งแต่ต้น เพื่อปกป้องข้อมูลสำคัญที่อยู่ในอุปกรณ์

8

สร้างความยืดหยุ่นผ่านการออกแบบ

การสร้างความยืดหยุ่น (Resilience) คือการลดช่องทางที่มีความเสี่ยงต่อการถูกจู่โจม การตรวจจับและจัดการสถานการณ์ที่ไม่พึงประสงค์ที่รวดเร็ว ซึ่งจะช่วยลดผลกระทบที่อาจเกิดจากการถูกโจมตีทางไซเบอร์และทำให้องค์กรสามารถฟื้นตัวได้อย่างรวดเร็ว CISO ควรจัดให้มีทรัพยากร เครื่องมือ และเทคโนโลยีที่จำเป็นเพื่อรับมือกับภัยคุกคามที่อาจเกิดขึ้น

อ้างอิง: 8 ประเด็นความปลอดภัยทางไซเบอร์องค์กร: ปรับกลยุทธ์รับความเสี่ยงปี 2025

KPMG in Thailand

kpmg.com/th