News release

For immediate release

รัตนา ภูศรี	อรรัชตา ภควัตชัย
Brand, Marketing and Communications, Consulting	Brand, Marketing and Communications
+66 8907 76050	+66 992891792
Rattana.Phusri@th.ey.com	Onrachata.Pakawatchai@th.ey.com

ผู้นำด้านไซเบอร์ในเอเชียแปซิฟิกไม่มั่นใจในความปลอดภัยทางไซเบอร์ EY แนะ เพิ่มการป้องกัน

- **ผู้นำด้านไซเบอร์น้อยกว่าครึ่งมองว่าองค์กรมีความพร้อมรับมือภัยคุกคามด้านไซเบอร์**
- **การสร้างความสมดุลระหว่างความปลอดภัยด้านไซเบอร์และการขับเคลื่อนนวัตกรรม คือหนึ่งในความท้าทายภายในอันดับต้นๆ ขององค์กร**
- **51% มองว่า องค์กรไม่สามารถเอาชนะภัยคุกคามด้านไซเบอร์ได้ ทำได้แค่รับมือและปรับตัวให้เร็วขึ้น**

กรุงเทพฯ, 6 ธันวาคม 2566 รายงานผลการศึกษา *EY 2023 Global Cybersecurity Leadership Insights Study* ระบุว่า ถึงแม้ภัยคุกคามด้านไซเบอร์เพิ่มสูงขึ้น การลงทุนเพื่อป้องกันภัยคุกคามก็เพิ่มขึ้น ผู้นำด้านความปลอดภัยทางไซเบอร์ยังเผชิญกับความท้าทายเพื่อเพิ่มประสิทธิภาพการป้องกันภัยคุกคามที่มีต่อองค์กร

การสำรวจความคิดเห็นของผู้นำด้านความปลอดภัยทางไซเบอร์ในภูมิภาคเอเชียแปซิฟิก (APEC) ที่จัดทำโดย EY พบว่า ผู้นำน้อยกว่าครึ่ง (49%) คิดว่าองค์กรของตนสามารถรับมือภัยคุกคามด้านไซเบอร์ได้ดี ในขณะที่ 51% ยังไม่มั่นใจในประสิทธิภาพของการฝึกอบรมที่องค์กรจัดให้พนักงาน และมีเพียง 40% เท่านั้นที่พอใจกับระดับการนำแนวทางปฏิบัติที่ดีไปใช้โดยทีมนอกแผนก IT

ในขณะเดียวกัน ผลสำรวจชี้ให้เห็นว่า ต้นทุนที่เกี่ยวข้องกับการลงทุนด้านความปลอดภัยทางไซเบอร์นั้นสูงขึ้น โดยผู้นำสูงสุดในสายงานด้านไอที (CIO) ส่วนใหญ่ (66%) ตอบว่าองค์กรของพวกเขาจัดสรรงบประมาณลงทุนด้านไอทีประมาณ 1-5% ของรายได้ทั้งหมดในปี 2565 ส่วน 59% ของผู้นำกลุ่มนี้ระบุว่า ในปี 2566 นี้ การใช้จ่ายงบประมาณด้านไอทีเพิ่มขึ้นเป็น 6-10% ของรายได้ทั้งหมด ส่วนในด้านเหตุการณ์ภัยคุกคามและการรั่วไหลของข้อมูลที่เกิดขึ้นในองค์กรในปีที่ผ่านมา 45% ของผู้นำด้านไซเบอร์ระบุว่า องค์กรของตนประสบเหตุการณ์ภัยคุกคาม 25 ถึง 49 ครั้ง และพบการรั่วไหลของข้อมูลราว 10-24 ครั้ง โดย 9% ของผู้นำรายงานว่า

เหตุการณ์เหล่านี้ส่งผลให้มีค่าใช้จ่ายรวมกันกว่าสองร้อยล้านบาท

เพ็ญนภา พุกกะรัตน์ หุ้นส่วนและหัวหน้าสายงานบริการที่ปรึกษาเทคโนโลยี EY ประเทศไทย กล่าวว่า "จำนวนการโจมตีด้านไซเบอร์ที่เพิ่มขึ้นทั่วโลกส่งผลให้องค์กรหันมาให้ความสนใจและลงทุนในด้านความปลอดภัยทางไซเบอร์เพิ่มขึ้น แนวโน้มนี้เกิดขึ้นในประเทศไทยเช่นเดียวกัน ความปลอดภัยด้านไซเบอร์ได้กลายเป็นหนึ่งในการลงทุนสำคัญอันดับต้นๆ สำหรับองค์กร โดยเฉพาะองค์กรในอุตสาหกรรมที่มีความเสี่ยงสูงจากภัยคุกคามด้านไซเบอร์ เช่น กลุ่มผู้ให้บริการทางการเงิน กลุ่มอุตสาหกรรมด้านสุขภาพ (Healthcare) อุตสาหกรรมค้าปลีก และการค้าออนไลน์ (อีคอมเมิร์ซ) โดยซีไอโอต้องมุ่งเน้นศึกษาข้อกำหนดด้านกฎระเบียบและติดตามการเปลี่ยนแปลงของภัยคุกคามด้านไซเบอร์ที่ดำเนินไปอย่างต่อเนื่อง เพื่อสร้างการป้องกันการโจมตีทางไซเบอร์ที่มีประสิทธิภาพให้องค์กร"

ความท้าทายของการนำเทคโนโลยีความปลอดภัยด้านไซเบอร์มาปรับใช้

จากผลสำรวจ องค์กรส่วนใหญ่มีการนำเทคโนโลยีความปลอดภัยทางไซเบอร์มาใช้แล้วอย่างน้อยหนึ่งเทคโนโลยี โดยที่ใช้กันมากที่สุดคือเทคโนโลยีปัญญาประดิษฐ์ (Artificial Intelligence – AI) และ/หรือการเรียนรู้ของเครื่อง (Machine Learning – ML) การรักษาความปลอดภัยแบบ zero trust และการยืนยันตนแบบไร้รหัสผ่าน (Passwordless Authentication) อย่างไรก็ตาม แม้ว่าซีไอโอมุ่งมั่นที่จะยกระดับความปลอดภัยด้านไซเบอร์ แต่ยังต้องเผชิญกับความท้าทายที่เกิดขึ้นในองค์กร โดยความท้าทายสามอันดับแรกคือ การมีพื้นที่หรือช่องทางการโจมตีมากเกินไป (52%) ความยากในการสร้างความสมดุลระหว่างความปลอดภัยด้านไซเบอร์และการขับเคลื่อนนวัตกรรม (50%) และงบประมาณด้านความปลอดภัยทางไซเบอร์ที่ไม่เพียงพอ (44%)

กมลวรรณ ตันพิชัย หุ้นส่วนและที่ปรึกษาด้านความปลอดภัยทางไซเบอร์ EY ประเทศไทย กล่าวว่า

"ถึงแม้องค์กรจะมีการตั้งค่าควบคุมการเข้าถึงและลดความซับซ้อนในการจัดการด้านไซเบอร์ แต่การมีพื้นที่ให้โจมตีมากเกินไปยังเป็นความท้าทายสำคัญที่ต้องรับมือ นอกจากนั้น ความไม่ชัดเจนของกลยุทธ์ความปลอดภัยด้านไซเบอร์ก็ถือเป็นความท้าทายเช่นกัน เนื่องจากผู้บริหารอาจสับสนระหว่างการขับเคลื่อนนวัตกรรมขององค์กรกับความจำเป็นในการนำเทคโนโลยีป้องกันความปลอดภัยทางไซเบอร์มาใช้ นอกจากนี้ งบประมาณที่ไม่เพียงพอและพนักงานที่ขาดทักษะที่จำเป็นก็เป็นหนึ่งในอุปสรรคต่อการบริหารจัดการความปลอดภัยด้านไซเบอร์อย่างมีประสิทธิภาพ ซึ่งอาจส่งผลให้องค์กรไม่พร้อมรับมือกับภัยคุกคามที่เปลี่ยนแปลงตลอดเวลา"

ลดความซับซ้อนเพื่ออยู่รอด

องค์กรที่นำเทคโนโลยีความปลอดภัยทางไซเบอร์มาใช้งานจะมีจำนวนเพิ่มขึ้น ซึ่งจะนำมาซึ่งความเสี่ยงใหม่ๆ ซีไอโอในกลุ่มประเทศเอเปคกว่าครึ่ง (52%) มองว่าองค์กรไม่สามารถเอาชนะภัยคุกคามด้านไซเบอร์ได้ ทำได้แค่รับมือและปรับตัวให้เร็วขึ้น รายงานการศึกษาได้ระบุถึง 4 แนวทางที่องค์กรสามารถลดความซับซ้อนและช่วยให้การรับมือภัยคุกคามด้านไซเบอร์มีประสิทธิภาพมากขึ้น คือ 1. ตรวจสอบระบบเก่าที่ซ้ำซ้อนหรือบูรณาการอย่างไม่มีประสิทธิภาพ 2. พิจารณาใช้ระบบอัตโนมัติ รวมถึง DevSecOps และ SOAR 3. ใช้เทคโนโลยีความปลอดภัยด้านไซเบอร์ที่มาพร้อมกับแพลตฟอร์ม 4. ใช้แนวทาง Co-sourcing และ Managed services เพื่อลดความซับซ้อนของโครงสร้างพื้นฐาน เพิ่มการมองเห็น และจัดการต้นทุนอย่างมีประสิทธิภาพ

เพ็ญนภา กล่าวว่า “องค์กรไม่ควรมองว่า ผู้ให้บริการเทคโนโลยีสามารถจัดการความเสี่ยงทางไซเบอร์ได้ทั้งหมด พนักงานทั้งองค์กรจำเป็นต้องได้รับการปลูกฝังและให้ความรู้ในเรื่องการรักษาความปลอดภัยด้านไซเบอร์ ด้วยการจัดโปรแกรมฝึกอบรม นอกจากนั้น ต้องประเมินความเสี่ยงอย่างสม่ำเสมอเพื่อระบุจุดที่มีความเสี่ยง จัดลำดับความสำคัญของมาตรการรักษาความปลอดภัย รวมทั้งมีแผนรับมือที่จัดทำเป็นเอกสารไว้อย่างชัดเจน และมีการทดสอบการใช้งานเป็นประจำ เพื่อให้มั่นใจว่าจะสามารถรับมือและจัดการกับภัยคุกคามทางไซเบอร์ในหลากหลายรูปแบบได้อย่างมีประสิทธิผล

“การปลูกฝังวัฒนธรรมด้านความปลอดภัยทางไซเบอร์ทั่วทั้งองค์กรจะช่วยสร้างมูลค่าเพิ่ม สร้างความมั่นใจเพื่อสร้างสรรค์นวัตกรรม และสร้างโอกาสทางธุรกิจให้กับองค์กร”

-จบ-

ข้อความถึงบรรณาธิการ

อ่านรายงานผลการศึกษา EY 2023 Global Cybersecurity Leadership Insights Study ได้ที่นี่

About EY

EY exists to build a better working world, helping create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. For more information about our organization, please visit ey.com.

About EY Consulting Services

In Consulting, we are building a better working world by transforming businesses through the power of people, technology, and innovation. It's our ambition to become the world's leading transformation consultants. The diversity and skills of 70,000+ people will help clients realize transformation by putting humans at the center, delivering

technology at speed and leveraging innovation at scale. These core drivers of “Transformation Realized” will create long-term value for people, clients and society.

For more information about our Consulting organization, please visit ey.com/consulting

APAC no. 15001235