ผลสำรวจไอทีชี้บริษัทในไทยได้รับประโยชน์จากการลงทุนด้านการรักษาความปลอดภัย

ผลสำรวจไอทีชี้บริษัทในไทยได้รับประโยชน์จากการลงทุนด้านการรักษาความปลอดภัย

ผลการศึกษาของบริษัทซีเอ เทคโนโลยีชี้ให้เห็นว่าบริษัทในไทย กำลังเริ่มเห็นผลการปรับปรุงจากตัวชี้วัด KPIs ทางธุรกิจ จากการลงทุนไอที รวมทั้งยอดการเจาะระบบข้อมูลที่ลดลงเช่นกัน

ผลการสำรวจล่าสุดด้านการรักษาความปลอดภัยในยุคเศรษฐกิจแอพพลิเคชั่นที่นำเสนอโดยบริษัทซีเอ เทคโนโลยี ได้ชี้ให้เห็นว่า หลายบริษัทในไทยกำลังได้รับผลตอบแทนจากการลงทุนด้านไอที โดยพิสูจน์ให้เห็นทั้งในด้านตัวชี้วัด KPIs ทางธุรกิจ ไปจนถึงยอดการเจาะระบบที่ลดลง

การศึกษาวิจัยครั้งนี้ใช้ชื่อภาษาอังกฤษว่า The Security Imperative: Driving Business Growth in the App Economyและเป็นการศึกษาในระดับโลก ที่ได้สอบถาม ผู้บริหารระดับสูงทางธุรกิจตลอดจนผู้บริหารด้านไอทีจำนวนกว่า 1770 ราย ซึ่งในจำนวนนี้มีมากกว่า 100 ราย ที่เป็น CSOหรือ CIO โดย มีประมาณ 800 รายของผู้ตอบแบบสอบถามที่มาจากประเทศที่อยู่ในภูมิภาคเอเชียแปซิฟิกและญี่ปุ่น ซึ่งรวมทั้งประเทศไทย โดยแบบสำรวจนี้ได้สอบถามว่า ผู้ตอบมีทัศนคติอย่างไร ในด้านการปฏิบัติงานด้านการรักษาความปลอดภัยไอทีและผลกระทบที่มีต่อตัวธุรกิจ

สำหรับในกรณีของประเทศไทยได้พบว่า ได้มีการปรับปรุงพัฒนาที่มีผลต่อตัวชี้วัด KPIs ทางธุรกิจ ที่ผู้ตอบแบบสอบถามได้ระบุ ว่าเป็นผลจากความริเริ่มและการรักษาความปลอดภัยใหม่ๆ เป็นไปอย่างต่อเนื่องและมีค่าเฉลี่ยที่สูงกว่าค่าเฉลี่ยของภูมิภาคเอเชียและแปซิฟิกและญี่ปุ่นโดยรวม

Qualitative Indicators
Key Performance Indicator Percentage of Thailand firms reporting improvement (%) Percentage of APJ firms reporting improvement (%)
1. Competitive Differentiation 80% 71%
2. Customer Retention 79% 72%
3. Customer Experience 78% 75%
4. Employee Recruitment and Retention 78% 70%
5. Digital Reach 69% 72%
Quantitative Indicators
Key Performance Indicator Improvement reported by Thailand firms (%) Improvement reported by APJ firms (%)
6. Customer Satisfaction 59% 44%

7. Operational Efficiency 58% 44%
8. Number of Compliance Audit Failures 57% 42%
9. Decrease in number of security breaches 56% 42%
10. Business Growth 55% 45%
11. Employee Productivity 54% 44%

นอกจากนี้ ยังพบว่า บริษัทในไทย ที่ระบุว่า มีปัญหาการเจาะระบบรักษาความปลอดภัยไอทีมีจำนวนน้อยลง ซึ่งตรงนี้ เป็นค่าเฉลี่ยที่ดีกว่า ภาพรวมของภูมิภาค โดยมีบริษัทในไทย 56 เปอร์เซ็นต์ ที่ กล่าวว่า พบปัญหาการละเมิดการรักษาความปลอดภัยน้อยลง ซึ่ง เป็นค่าตัวเลขที่ดีกว่าค่าเฉลี่ย 42 เปอร์เซ็นต์ของบริษัทในภูมิภาคเอเชียแปซิฟิกและญี่ปุ่น

ผลตอบแทนที่ได้รับตรงนี้ของบริษัทในไทยได้สะท้อนให้เห็นบทบาทหลักของ บริษัทต่างๆที่ มีความเห็นว่า การรักษาความปลอดภัยไอที ควรจะเป็นรูปแบบใด นอกจากนี้ การรักษาความปลอดภัยไอที โดยเฉพาะการรักษาความปลอดภัยที่เน้นระบบไอดี ที่มีอยู่จะต้องมีศักยภาพที่สามารถทำได้มากกว่าการปกป้องตัวธุรกิจในสภาพการใช้งานปัจจุบัน โดยจำเป็นจะต้องมีขีดความสามารถที่จะสร้างความไว้วางใจ ในด้านความสัมพันธ์ในรูปแบบดิจิตอล กับผู้ใช้งานและลูกค้าซึ่งเรื่องนี้จำเป็นอย่างยิ่งสำหรับการแข่งขันในยุคเศรษฐกิจแอพพลิเคชั่นและการขยายตัวทางธุรกิจ ในไทย

• มี 93% ซึ่งจัดว่าสูงสุดในภูมิภาคเอเชียแปซิฟิกและสูงสุดในหมู่ผู้ตอบแบบสอบถามทั่วโลกระบุว่า การรักษาความปลอดภัยที่เน้นด้านไอทีมีความสำคัญอย่างยิ่งในการสร้างช่องทางในการติดต่อที่มีความปลอดภัยสำหรับพนักงาน ลูกค้าและพาร์ตเนอร์ ไม่ว่า จะอยู่ที่ไหนหรือใช้ผ่านอุปกรณ์อะไร
• มี 93% ซึ่งจัดว่า สูงสุดในภูมิภาคเอเชียแปซิฟิกและสูงสุดในหมู่ผู้ตอบแบบสอบถามทั่วโลกระบุว่า การรักษาความปลอดภัยจำเป็นต้องใช้งานได้สะดวก และไม่สร้างภาระให้กับยูสเซอร์ผู้ใช้งาน
• มี 92 เปอร์เซ็นต์ของผู้ตอบแบบสอบถามระบุว่า จำเป็นต้องจะมีต้องมีการสร้างสมดุลระหว่าง การรักษาความปลอดภัยที่เข้มแข็ง กับ การปรับตัวที่จะต้องให้ธุรกิจของตนเข้าสู่ตลาดใหม่และนำเสนอเซอร์วิสใหม่ได้สะดวกด้วย
• มี 92 เปอร์เซ็นต์ ระบุว่าการรักษาความปลอดภัยจำเป็นอย่างยิ่งในการปกป้องแบรนด์ของตนและ สามารถมองว่าเป็นตัวชี้ขาดที่สร้างความแตกต่างในการแข่งขันทางธุรกิจ
• มีมากกว่า 75 เปอร์เซ็นต์ของผู้ตอบแบบสอบถาม ได้ใช้ตัวชี้วัดต่างๆเช่น การเข้าถึงทางดิจิตอล การเติบโตทางธุรกิจ ความพึงพอใจของลูกค้า การรักษาฐานลูกค้า การจ้างพนักงาน และการรักษาตัวพนักงานที่มีความสามารถตลอดจนประสิทธิภาพในการปฏิบัติงานและกระบวนการทำงาน

“บริษัทในไทยได้แสดงให้เห็น วิสัยทัศน์ที่ยาวไกลในการใช้การรักษาความปลอดภัยไอที มาเพื่อหนุน เป้าหมายทางธุรกิจ และได้ส่งผลตอบแทนกลับมาในรูปของการพัฒนาตัวชี้วัด KPIs ทางธุรกิจที่ดีขึ้น” นิค ลิมรองประธานฝ่ายอาเซียนและจีน บริษัทซีเอ เทคโนโลยี กล่าวและเสริมว่า “ปัจจุบันเรากำลังใช้ชีวิตและทำงานอยู่ในยุคดิจิตัล ซึ่งเป็นยุคที่ผู้บริโภค มีความรอบรู้และคาดหวังมากยิ่งขึ้น ว่า ข้อมูลสำคัญส่วนบุคคลของตนที่ให้ไว้กับบริษัทจะถูกบริหาร

จัดการในรูปแบบใด ดังนั้นถ้าจะบรรลุเป้าหมายในด้านการเปลี่ยนผ่านสู่ยุคดิจิตอลให้สำเร็จ บริษัทธุรกิจจะต้อง มีพื้นฐานด้านการรักษาความปลอดภัยเป็นหลักเพื่อสร้างสัมพันธ์กับลูกค้าที่ไว้วางใจได้เสมอ”

การใช้งาน ระบบรักษาความปลอดภัยที่เน้นไอดีขั้นสูง ช่วยสร้างผลตอบแทนทางธุรกิจและลดปัญหาการเจาะระบบข้อมูล

จากการศึกษาที่มีในระดับภูมิภาค ยังได้จัดสถานะบริษัทผู้ตอบแบบสอบถาม ในด้านที่เกี่ยวกับการรักษาความปลอดภัยต่างๆ เช่นดูจาก ประสบการณ์การใช้งานของยูสเซอร์ ระบบบริหารจัดการไอดีและการเข้าถึงข้อมูลและประเด็นการเจาะระบบข้อมูล โดยข้อมูลนี้ได้ช่วยให้บริษัทซีเอ เทคโนโลยีและบริษัทวิจัยColeman Parkesซึ่งทำหน้าที่เป็นผู้ศึกษาวิจัยในครั้งนี้ ในการสร้าง โมเดลจำลองเพื่อแยกแยะว่า บริษัทต่างๆ ของผู้ตอบแบบสอบถามอยู่ในระดับขั้นสูง ระดับพื้นฐานหรือยังมีการใช้งานในวงจำกัด

โดยสภาพทั่วไปแล้ว ผลลัพธ์ที่ได้ของบริษัทในภูมิภาคเอเชียแปซิฟิกและญี่ปุ่นสามารถจำแนกได้ว่าส่วนใหญ่ของผู้ตอบแบบสอบถาม จะเป็นผู้ใช้งานระบบการรักษาความปลอดภัย ที่เน้นหนักในด้านไอดี ในระดับเบสิกอยู่ 64% ซึ่งเน้นหนักไปที่การใช้งานหลักๆ เช่นการบริหารจัดการรหัสผ่าน ระบบ SSO รวมทั้งการวิเคราะห์และการรายงานผลในบางด้าน

ในขณะที่มีอีก 28 เปอร์เซ็นต์ จัดได้ว่าเป็น บริษัทที่ใช้งานในระดับสูง โดย เน้นไปที่ด้านต่างๆ เช่นการรักษาความปลอดภัยที่ยืดหยุ่นปรับตัวได้ การวิเคราะห์ระบบพฤติกรรมการใช้งาน และการสนับสนุน การรักษาความปลอดภัยข้ามช่องทางต่างๆ

ถึงแม้บริษัทผู้ใช้งานในภูมิภาคเอเชียแปซิฟิกโดยทั่วไปจะมีการปรับปรุงพัฒนาขึ้น ใน ทางธุรกิจซึ่งเป็นผลมาจากความริเริ่มในการใช้จากระบบรักษาความปลอดภัยก็ตาม การสำรวจนี้ยังได้แสดงให้เห็นว่าบริษัทผู้ใช้งานในระดับสูงโดยทั่วไปแล้วจะระบุว่ามีผลตอบแทนที่เด่นชัดมากกว่า โดยเฉพาะอย่างยิ่งในด้านประสบการณ์การใช้งานของลูกค้า การปฏิบัติงานทางธุรกิจและการรักษาความปลอดภัย

- บริษัทที่ผู้ใช้งานระดับสูง มี ยอดเติบโตทางธุรกิจ และ มีรายได้ใหม่ๆ เข้ามา กว่า 58% ในขณะที่บริษัทที่ใช้งานในระดับ พื้นฐาน มียอดปรับปรุงพัฒนาขึ้นเพียง 44%

- 58 เปอร์เซ็นต์ของบริษัทผู้ใช้งานระดับสูงระบุว่ามีการปรับปรุงพัฒนาในด้านผลิตภาพงานของพนักงานเพิ่มขึ้น ในขณะที่ บริษัทใช้งานในระดับพื้นฐาน ระบุว่ามีการพัฒนาเพิ่มขึ้นเพียง 44 เปอร์เซ็นต์
- บริษัทผู้ใช้งานระดับสูงระบุว่า มีการพัฒนากว่า 49 เปอร์เซ็นต์ ในเรื่องการแก้ปัญหา ความล้มเหลวในการตรวจสอบระบบ ในขณะที่บริษัทที่ใช้งานขั้นพื้นฐานระบุว่ามีเพียง 38 เปอร์เซ็นต์ เท่านั้น
- สำหรับในกรณีของการเจาะระบบข้อมูลนั้น บริษัทที่ใช้งานระบบไอทีการรักษาความปลอดภัยที่เน้นไอดีดีขั้นสูงระบุว่ามีการลดลงของการเจาะระบบ ถึง 35 เปอร์เซ็นต์ในขณะที่บริษัทที่ใช้งานในระดับพื้นฐานมีการปรับปรุงใน

เรื่องนี้ขึ้นเพียง 12 เปอร์เซ็นต์ เท่านั้น

นอกจากนี้ ยังได้สำรวจพบว่า ที่พบว่ามีการเจาะระบบลดลงนั้น บริษัทที่ใช้งานขั้นสูงในด้านการรักษาความปลอดภัยที่เน้นไอดี ในภูมิภาคเอเชียแปซิฟิกและญี่ปุ่น ยังได้พบว่า

- มี 86 เปอร์เซ็นต์ การใช้มาตรการป้องกันล่วงหน้า ในการสกัดการเจาะระบบ
- 82% เน้นไปที่อุปกรณ์โมบายและแอพพลิเคชั่น
- 73% เน้นหนักที่ การใช้งานระบบยืนยันตัวเองที่มีความเข้มแข็ง และ ระบบเป็นขั้นตอนมากขึ้น
- มี 68% ที่มีการตรวจสอบมาตรการรักษาความปลอดภัย เพื่อจะเน้นโฟกัสไปที่ บริเวณที่มีความเสี่ยงสูงเช่น ไอดีของผู้ใช้งานที่ได้รับสิทธิ์พิเศษ และการเปลี่ยนรูปแบบองค์กรให้ มีความสอดคล้อง ต่อหน้าที่รับผิดชอบด้านการรักษาความปลอดภัยมากขึ้น
- มี 59% ที่ให้การศึกษาอบรม ด้านรักษาการรักษาความปลอดภัยกับตัวบุคลากรในองค์กรมากขึ้น

เกี่ยวกับ ซีเอ เทคโนโลยี

ซีเอ เทคโนโลยี (NASDAQ: CA) เป็นผู้จัดหาโซลูชั่นเพื่อการบริหารจัดการไอที ซึ่งช่วยให้ลูกค้าสามารถจัดการและรักษาความปลอดภัยในสภาพแวดล้อมของระบบไอทีที่ซับซ้อนเพื่อรองรับการให้บริการธุรกิจได้อย่างคล่องตัว ทั้งนี้ องค์กรต่างๆ ใช้ประโยชน์จากซอฟต์แวร์และโซลูชั่นในกลุ่ม SaaS ของซีเอ เทคโนโลยี เพื่อสร้างนวัตกรรม ปรับเปลี่ยนโครงสร้างพื้นฐาน และรักษาความปลอดภัยของข้อมูลและอัตลักษณ์ต่างๆ นับตั้งแต่ระดับดาต้าเซ็นเตอร์ไปจนถึงระบบคลาวด์ อ่านข้อมูลเพิ่มเติมเกี่ยวกับซีเอ เทคโนโลยี ได้ที่ www.ca.com