

# เคยคิดใหม่ว่า Email ที่ใช้ ทำความเสียหายให้องค์กรได้

ไม่ว่าวันนี้หากจะถามใครต่อใครหลาย ๆ คนว่ากิจกรรมคอนเซ็ปต์ที่ทำงานคืออะไรใหม่เชื่อว่าการเปิด และเช็ค Email เป็นกิจกรรมของใครหลาย ๆ คน แล้วเคยคิดใหม่ว่าสักวันหนึ่งองค์กรของเราจะได้รับความเสียหาย โดยมีต้นเหตุมาจาก Email ที่เราใช้ ๆ กันอยู่ ลองคิดถึงกรณีว่ามีใครสักคนในองค์กรกับบุคคลภายนอกติดต่อกันด้วย หรือรับส่งข้อมูลที่เกี่ยวข้องกับผลประโยชน์, ความมั่นคง, ข้อมูลภายใน หรือข้อมูลในทางลับต่าง ๆ ขององค์กร และหลังจากได้รับข้อมูลแล้วคำเหล่านั้นก็ทำการลบจดหมายที่อาจจะเป็นหลักฐานสำคัญออกจากระบบไป สุดท้ายเมื่อความเสียหายบังเกิดขึ้นเราจะย้อนกลับไปได้หาหลักฐานเหล่านั้นกลับมาได้อย่างไวในเมื่อจดหมายเหล่านั้นถูกทำลายทิ้งเสียแล้ว

เหตุการณ์ที่ยกตัวอย่างมาไม่ใช่เรื่องที่เกิดขึ้นแต่อยากจะเป็นเรื่องที่เกิดขึ้นจริงในต่างประเทศ และอาจจะเกิดขึ้นกับองค์กรของคุณแล้วโดยที่คุณไม่รู้ตัว เหตุการณ์เหล่านี้ก็เกิดขึ้นที่องค์กรทางภาครัฐ และเอกชน โดยเฉพาะในสหรัฐอเมริกาต้องออกกฎหมาย และกฎหมายต่าง ๆ เพื่อควบคุมระบบ Email ขององค์กรต่าง ๆ ภายในสหรัฐ รวมถึงองค์กรต่างประเทศที่ต้องทำธุรกิจกับสหรัฐ ยกตัวอย่างเช่น

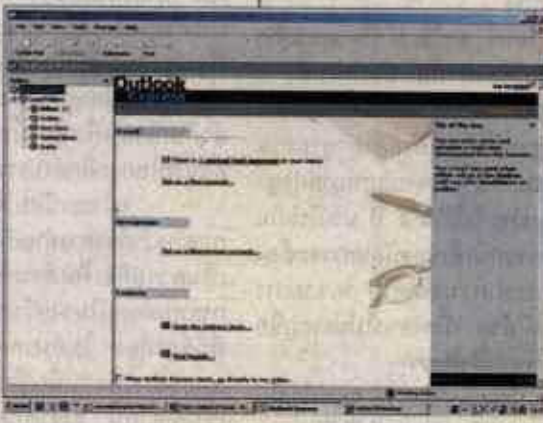
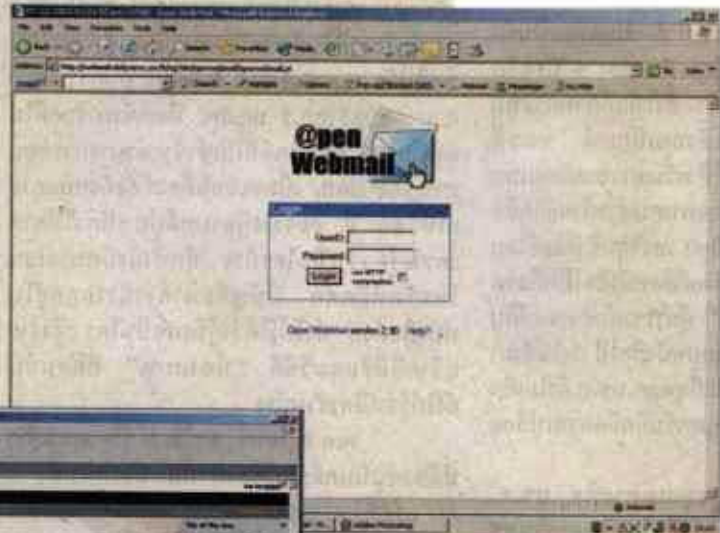
SEC 17a-4 ซึ่งเป็นข้อกำหนดหนึ่งของตลาดหลักทรัพย์สหรัฐที่กำหนดให้บริษัทโบรกเกอร์ต่าง ๆ จัดเก็บข้อมูลที่เกี่ยวข้องกับการสื่อสารทั้งภายใน และภายนอก รวมถึงข้อมูลบนระบบ Email เป็นระยะเวลา 3 ปี โดยข้อมูลที่เก็บไว้จะต้องอยู่บนสื่อ หรือมีเดียที่ไม่นอูญาคาให้แก้ไขเปลี่ยนแปลงได้ทั้งสิ้น

Sarbanes-Oxley Act (SOX) ซึ่งกำหนดให้บริษัทมหาชนที่มีหุ้นกระจายอยู่ในตลาดหลักทรัพย์จะต้องจัดเก็บข้อมูลที่เกี่ยวข้องกับกิจกรรมอันก่อให้เกิดรายรับ และรายจ่ายซึ่งจำเป็นกับการตรวจสอบ โดยรวมถึงข้อมูลของระบบ Email ไว้ไม่น้อยกว่า 7 ปี

HIPAA (Health Insurance Portability and Accountability Act of 1996) มีกฎหมายข้อหนึ่งที่เกี่ยวข้องกับการจัดเก็บ Email ที่มีข้อมูลทางการแพทย์ต่าง ๆ เอาไว้นับไม่น้อยกว่า 6 ปี ซึ่งบังคับใช้กับองค์กรต่าง ๆ ที่ข้องเกี่ยวกับกิจกรรมทางการแพทย์ไม่ว่าจะเป็นโรงพยาบาล, คลินิก, บริษัทผลิตจัดจำหน่ายยา และบริษัทประกันชีวิต เป็นต้น

การที่จะให้ระบบ Email ภายในองค์กร

ปฏิบัติตามกฎเกณฑ์ต่าง ๆ ที่กล่าวมานั้นเป็นความรับผิดชอบของเจ้าหน้าที่ด้านกฎหมาย และผู้บริหารในระดับต่าง ๆ ที่ต้องกำหนดนโยบายออกมาเพื่อให้สอดคล้องกับกฎเกณฑ์ที่กล่าวมา แต่หน่วยงานที่จะทำให้ระบบตรวจสอบเหล่านี้เกิดขึ้น และนำมาปฏิบัติได้อย่างจริงจังคงหนีไม่พ้นหน่วยงาน IT (Information Technology) ซึ่งเทคนิคที่นำมาใช้มักก็จะเกี่ยวข้องกับการทำ Email Archiving ซึ่งจะถูกนำมาใช้ในการทำสำเนาจดหมายที่มีการรับส่งกันในระบบไว้วิธีอีกจุด โดยการ



Archive ควรจะเป็นแบบ Real Time เพื่อสร้างความมั่นใจว่าจดหมายทุกฉบับที่รับส่งมีการทำสำเนาไว้ และจะไม่สูญขาดให้มี

การแก้ไขจดหมายที่ Archive ไว้เพื่อประโยชน์ในการตรวจสอบภายหลัง

คุณสมบัติของระบบ Email Archiving ที่พึงมีเพื่อรองรับกฎเกณฑ์ควรจะมีดังนี้

Email Record Capture จะทำหน้าที่ในการตรวจสอบ และทำสำเนาจดหมายที่มีการรับส่งบนระบบ Email ไปยัง Email Archiving Server แบบ Real Time ทำให้มั่นใจได้ว่าจดหมายทุกฉบับจะมีการส่งไปยังระบบ Archive ก่อนเสมอ

Email record archiving and retention หลังจากได้รับจดหมายที่ถูกส่งมายัง Email Archiving Server แล้วระบบ Archive จะทำการกักตุน และเลือกเฉพาะจดหมายฉบับที่ต้องการจะจัดเก็บไว้เท่านั้น เช่นจดหมายที่ถูกส่งออกโดยผู้บริหาร หรือส่งมาให้ผู้บริหาร, จดหมายของคู่ค้าในแผนกการเงิน หรือจดหมายที่มีข้อความเกี่ยวข้องกับข้อมูลทาง

ด้านสถานะการเงินเป็นต้น หลังจากนั้นระบบ Archive จะถูกจัดเก็บไว้ในช่วงเวลา (Retention Period) ที่ต้องการเช่น 3 ปี, 7 ปี เป็นต้น ตามแต่กฎเกณฑ์ที่ถูกบังคับใช้

➤ Record Storage ขดหมายที่ถูก Archive เก็บไว้จะต้องมั่นใจได้ว่าไม่สามารถทำการเปลี่ยนแปลงแก้ไขโดยบุคคลหนึ่งบุคคลใดได้ไม่ว่าจะเป็นการเปลี่ยนแปลงผ่านทางตัวโปรแกรมระบบ Archive หรือจะเป็นการทำลายทิ้งโดยเข้าไปลบจากสื่อที่จัดเก็บระบบจดหมายที่ Archive ไว้โดยตรง ดังนั้นระบบ Archive ที่ใช้จะต้องรองรับการป้องกันเหตุการณ์เหล่านี้ และจะต้องไม่ละเลยถึงสื่อที่นำมาใช้จัดเก็บ และบันทึกจดหมายเหล่านี้ด้วยที่จะต้องรองรับการบันทึกข้อมูลโดยไมออนุญาตให้ทำการเปลี่ยนแปลงข้อมูลที่บันทึกไปแล้วได้ ซึ่งสื่อเหล่านี้มักจะใช้เทคโนโลยีแบบ

Write Once Read Many (WORM) หรือ Non-Rewritable เป็นต้น

➤ Access and retrieval ระบบ Archive ที่ใช้จะต้องตระเตรียมเครื่องมือที่จะช่วยในการสืบค้นจดหมาย และนำจดหมายฉบับที่ต้องการคืนกลับมาได้อย่างสะดวก ซึ่งระบบการสืบค้นควรจะทำให้ทั้งกับข้อความที่อยู่ใน

จดหมาย และเอกสารแนบ (Attachment) รวมถึงควรจะมีระบบรักษาความปลอดภัย และกำหนดการเข้าถึงระบบ Archive ให้เหมาะสม

➤ Auditing ระบบ Archive จะต้องมีการเฝ้าติดตามการเก็บประวัติ และเหตุการณ์ต่าง ๆ ที่เกิดขึ้นเมื่อมีการเปลี่ยนแปลงแก้ไขค่าต่าง ๆ

➤ Supervision สำหรับองค์กรบางองค์กร การ Archive Email เพื่อตรวจสอบภายหลังอาจไม่เพียงพอ ยกตัวอย่างเช่นบริษัทโบรกเกอร์ที่อาจต้องการตรวจสอบ และตรวจจับจดหมายที่มีการรับส่ง และมีข้อความ หรือข้อมูลเกี่ยวข้องกับการลงทุน, การเงิน และข้อมูลวงในของบริษัทต่าง ๆ และถูกส่งออกไปให้กับบุคคลภายนอก ซึ่งต้องการระบบ Archive ที่สามารถแจ้งเตือนให้ผู้ดูแลระบบทำการตรวจสอบจดหมายฉบับนั้น ๆ ทันทีก่อนที่จะเกิดปัญหา หรือความเสียหาย

ทั้งหมดนี้คงพอทำให้เราเองเห็นถึงแนวโน้มการใช้งาน Email ที่เราจะต้องเตรียมองค์กรของเราเพื่อมุ่งไปสู่การเป็นองค์กรที่มีธรรมาภิบาล (Good Governance) ไปฝั่งใ้, ตรวจสอบได้กับทั้งผู้ค้า, ลูกค้า และสังคมของเรา.

ทวีพงศ์ อโนทัยสินทวี  
บริษัท อีเอ็มซี อินฟอร์เมชัน  
ซิสเต็มส์ (ประเทศไทย) จำกัด