กรณีศึกษาที่ 1

EASYHOME ซึ่งเป็นบริษัทผลิตและจำหน่ายเครื่องใช้ไฟฟ้าในบ้าน กำลังพิจารณาว่าจ้างบริษัทเทคโนโลยีในโครงการใหม่เพื่อการช่วยพัฒนาโมบายแอพพลิเคชั่นซึ่งจะทำให้เครื่องใช้ไฟฟ้าในบ้านกลายเป็นอุปกรณ์ประเภท "สมาร์ท" ที่สามารถเชื่อมต่อกับเครือข่ายอินเทอร์เน็ต โดยมีเป้าหมายที่จะสร้างสรรค์รูปแบบการใช้ชีวิตที่เป็นไปตามความต้องการ ความชื่นชอบ และรูปแบบการใช้งานของแต่ละครัวเรือน โมบายแอพพลิเคชั่นนี้จะมีการรวบรวมและวิเคราะห์ข้อมูลจำนวนมาก ซึ่งทำให้ผู้จัดการฝ่ายรักษาความมั่นคงปลอดภัยของบริษัทฯ มีความกดดันเพิ่มขึ้น ข้อมูลที่ละเอียดอ่อนเกี่ยวกับการตัดสินใจของลูกค้า กิจวัตรของลูกค้า และข้อมูลส่วนบุคคลอื่นๆ จะถูกเก็บรักษาไว้ในฐานข้อมูลของบริษัทและประมวลผล ความมั่นคงปลอดภัยถือเป็นสิ่งสำคัญสูงสุดในระบบการจัดการข้อมูล เนื่องจากบริษัทมีข้อกังวลว่าการพัฒนานั้นจะทำให้เกิดการสื่อสารกันระหว่างอุปกรณ์ได้ ซึ่งทำให้เกิดความเป็นไปได้ที่นักเจาะระบบจะทำการแก้ไขเปลี่ยนแปลงเครื่องใช้ดังกล่าว การใช้เทคโนโลยีการสื่อสารระหว่างอุปกรณ์กับอุปกรณ์อย่างกว้างขวางน่าจะเพิ่มความเป็นไปได้ของการใช้ข้อมูลโดยมิชอบ

ท่านคณะกรรมการบริษัทต้องพิจารณาประเด็นสำคัญที่บริษัทควรคำนึงถึงในการดำเนินโครงการนี้ โปรดพิจารณาและหารือเกี่ยวกับปัญหาที่สำคัญเหล่านี้ และสิ่งที่ควรกระทำเพื่อป้องกันปัญหาเหล่านี้ตั้งแต่ต้น

Case Study 1

A home electric appliance company, EASYHOME, is considering engaging a technology company in a new project to develop a mobile application that connects home electric appliances to the Internet (i.e., makes them "smart") in order to create customized living solutions that adjust to meet the needs of a family based on their unique preferences and usage patterns. The mobile application will involve the collection and analysis of data in large quantities, thereby putting additional pressure on security managers. Sensitive data about buyer decisions, their habits, and other personal information must be kept in the company's database and processed. Security is a top priority in systems handling the data, because the company is concerned that the development will enable communication between machines, raising the possibility of appliances being manipulated by hackers. The widespread use of machine-to-machine communication is only likely to increase the risk of information misuse.

The board of directors needs to consider the key issues that the company should take into account before implementing this project. Please consider and discuss these key issues, as well as what should be done at the outset to prevent such issues.

กรณีศึกษาที่ 2

BUYBEST ซึ่งเป็นร้านค้าปลีกระดับประเทศรายใหญ่ได้รับภัยคุกคามทางไซเบอร์ ส่งผลให้ข้อมูลหมายเลขบัตรที่ใช้ในการชำระเงินประมาณ 40 ล้านบัตรถูกโจรกรรมไปพร้อมกับข้อมูลของบัญชีส่วนบุคคลของลูกค้า (อาทิ ชื่อ รายละเอียดการติดต่อ หมายเลขโทรศัพท์ เป็นต้น) อีก 70 ล้านบัญชี เป็นที่สงสัยว่าเหตุการณ์นี้เป็นผลมาจากการคุกคามระบบโดยใช้มัลแวร์ประเภทโจรกรรมข้อมูล (memory scraping attack)

คณะกรรมการบริษัทพบว่าทีมรักษาความมั่นคงปลอดภัยของบริษัทในกรุงเทพฯได้รับการแจ้งเตือนหลายครั้งจากระบบรักษาความมั่นคงปลอดภัยซอฟต์แวร์อิสระ 1 วันหลังจากที่เริ่มมีการคุกคาม และได้ส่งการแจ้งเตือนนั้นไปยังหัวหน้าคณะผู้บริหารฝ่ายเทคโนโลยีสารสนเทศ (Chief Information Officer) จากการตรวจสอบ แสดงให้เห็นว่ามีมัลแวร์ดังกล่าวปรากฏอยู่ในระบบจริง

ผู้ถือหุ้นของบริษัทได้กล่าวหาว่าทีมรักษาความมั่นคงปลอดภัยของบริษัทได้ทราบหรือควรที่จะได้ทราบแล้วว่าภัยคุกคามทางไซเบอร์จะก่อให้เกิดความเสียหายด้านการเงินและชื่อเสียงอย่างมากต่อบริษัท แต่ก็ไม่ได้ดำเนินการที่จะเป็นการป้องกันภัยคุกคามทางไซเบอร์ ผู้ถือหุ้นกล่าวหาด้วยว่าทีมรักษาความมั่นคงปลอดภัยไม่ได้ดำเนินการตามที่เหมาะสมในทันทีที่เกิดภัยคุกคาม ทั้งนี้ คณะกรรมการบริษัทมีหน้าที่ในการดูแลผลประโยชน์ของบริษัทและผู้ถือหุ้นด้วยการปฏิบัติหน้าที่ตามที่ได้รับความไว้วางใจ และด้วยความซื่อสัตย์สุจริต และระมัดระวังตามสมควร ในการปฏิบัติหน้าที่ คณะกรรมการบริษัทจะต้องกำกับดูแลการบริหารจัดการ นโยบาย วิธีปฏิบัติ และการควบคุมการดำเนินการทางการเงินของบริษัทอย่างเหมาะสมและรอบคอบ ผู้ถือหุ้นกล่าวว่าเนื่องจากการที่คณะกรรมการบริษัทละเลยไม่ปฏิบัติหน้าที่ของตน คณะกรรมการบริษัทจึงควรต้องรับผิดต่อการละเมิดหน้าที่ในการดูแลผลประโยชน์ การสูญเสียสินทรัพย์ของบริษัท การบริหารจัดการที่ผิดพลาดอย่างร้ายแรง และการปฏิบัติหน้าที่โดยมิชอบ

จากเหตุการณ์นี้ ท่านคิดว่าอะไรคือการดำเนินการที่คณะกรรมการบริษัทพึงทราบและพึงกระทำเพื่อป้องกันการคุกคามทางไซเบอร์ เพื่อที่จะลดหรือจัดการความรับผิดที่อาจเกิดขึ้นได้ภายหลังจากที่เกิดภัยคุกคามทางไซเบอร์

Case Study 2

A large national retail store, BUYBEST, suffered a cyber-attack that resulted in around 40 million payment card numbers being stolen. In addition, 70 million customers' personal account data (i.e., names, addresses, telephone numbers, etc.) were also stolen. The incident is suspected to be the result of a memory scraping attack.

The board of directors has found that the company's security team in Bangkok had received alerts from a software security system 1 day after the attack was launched and sent them to the Chief Information Officer. The investigation indicates that malicious software had appeared in the system.

The shareholders of the company allege that the company's security team knew or ought to have known that a cyberattack would cause substantial financial and reputational damage to the company, and that they failed to take actions that would have prevented the cyberattack. They also allege that the company's security team failed to act reasonably once the attack occurred. The shareholders allege that all directors owe a fiduciary obligation of trust, loyalty, good faith, and due care to the company and its shareholders. To discharge their duties, the directors were required to exercise reasonable and prudent supervision over management, policies, practices, and controls of the financial affairs of the company. The shareholders contend that as a result of their failures to prevent the attack and mitigate the damage it caused, the directors are liable for breach of fiduciary duties, wasting corporate assets, gross mismanagement, and abuse of their positions.

Based on this summary of the incident, what steps, if any, could the board of directors have taken in an attempt to prevent the cyberattack such that it would have minimized their potential liability once the attack actually occurred?

กรณีศึกษาที่ 3

TECHWORK ซึ่งเป็นบริษัทวิศวกรรมในประเทศไทย ถูกโจมตีระบบคอมพิวเตอร์ เจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศได้รายงานต่อผู้จัดการ และผู้จัดการได้แจ้งต่อคณะกรรมการบริษัทในทันที

จากเหตุการณ์ดังกล่าว บริษัทเกรงว่าอาจมีการเข้าถึงข้อมูลที่เป็นความลับบางอย่างของบริษัทและบุคคลภายนอก ซึ่งรวมถึงคู่ค้าของบริษัท ที่จัดเก็บอยู่ในฐานข้อมูลของบริษัท เช่น ข้อมูลของบริษัทเทคโนโลยี พันธมิตรการวิจัยและพัฒนา ผู้จัดหาสินค้า และลูกค้า ต่อมาคณะกรรมการบริษัททราบถึงเหตุการณ์ว่ามีข้อมูลที่เป็นความลับบางอย่างจากฐานข้อมูลของบริษัทได้ถูกเผยแพร่บนเว็บไซต์แห่งหนึ่งนามว่า"Tradesecretsrevealed.com" ไปแล้ว

คณะกรรมการบริษัทจึงจำเป็นต้องเรียกประชุมพิเศษภายในอีกไม่กี่ชั่วโมงข้างหน้า เพื่อหารือถึงกลยุทธ์และวิธีการที่จะจัดการเหตุการณ์นี้ คำถามดังต่อไปนี้ได้ถูกหยิบยกให้ท่านพิจารณา ในฐานะกรรมการบริษัท กล่าวคือ หน้าที่และความเสี่ยงอะไรบ้างที่อาจเกิดขึ้นต่อข้อมูลที่เป็นความลับของบุคคลอื่นซึ่งอาจรวมอยู่ในข้อมูลที่ถูกโจรกรรม รวมทั้งการดำเนินการที่อาจทำได้อันเนื่องจากการเปิดเผยข้อมูลบนเว็บไซต์นั้นและแนวทางแก้ไขที่ควรมีในอนาคต

Case Study 3

An engineering company in Thailand, TECHWORK, had its computer system hacked. The IT officer reported the incident to the manager, who then immediately informed the board of directors.

The company fears that some of its own confidential information has been accessed, as has that of third parties stored in its system, including that belonging to various business partners such as technology companies, research and development agents, suppliers, and customers. By the time the board of directors learns of the incident, some of the confidential information has already been published on a website named "Tradesecretsrevealed.com."

The board of directors needs to convene a special meeting in the next few hours to discuss a strategy for handling this incident. The following questions have been addressed to you as one of the board members: What duties and potential exposure apply to the third party confidential information that might have been included in the theft? What action, if any, can be taken as a result of the disclosure on the website. What should be done to prevent a similar hack in the future?

กรณีศึกษาที่ 4

คณะกรรมการของบริษัทA&B ซึ่งเป็นบริษัทสินค้าอุปโภคบริโภคระหว่างประเทศในกรุงเทพฯ และมีสำนักงานสาขาอยู่ในประเทศต่างๆ ทั่วภูมิภาคเอเชีย รวมถึงสิงคโปร์ ฮ่องกง มาเลเซีย และอินโดนีเซีย ได้รับข้อเสนอการควบรวมกิจการที่เป็นความลับจากบริษัทสินค้าอุปโภคบริโภคข้ามชาติรายใหญ่อีกรายหนึ่ง

ในบ่ายวันศุกร์หนึ่งก่อนวันหยุดยาว หัวหน้าคณะผู้บริหารสูงสุดฝ่ายเทคโนโลยีสารสนเทศ (Chief Information Officer) ได้รับอีเมล์เรียกค่าไถ่จากแหล่งที่มาที่ไม่รู้จัก โดยระบุว่าพวกเขาทราบถึงแผนการควบรวมกิจการและมีข้อมูลส่วนบุคคลของลูกค้าจำนวน 100,000 ราย ตัวอย่างของข้อมูลส่วนบุคคลของลูกค้าจำนวน 500 รายได้ถูกรวมมาในอีเมล์เรียกค่าไถ่ด้วยเพื่อเป็นการพิสูจน์ ผู้เรียกค่าไถ่ขู่ว่าพวกเขาจะเปิดเผยแผนการควบรวมกิจการและขายข้อมูลลูกค้า เว้นแต่จะได้รับค่าไถ่เป็นจำนวนมากในสกุลเงินบิทคอยน์จากทางบริษัท

ในฐานะที่ท่านเป็นหนึ่งในคณะกรรมการบริษัท ท่านเห็นว่าคณะกรรมการบริษัทควรดำเนินการใดเพื่อที่จะตอบโต้ต่อข้อเรียกร้องเกี่ยวกับค่าไถ่เป็นอย่างแรก และขั้นตอนต่อๆ ไปที่เหมาะสมที่สุดเพื่อจัดการกับเหตุการณ์นี้ โปรดพิจารณากระบวนการสื่อสารระหว่างบุคคล/องค์กร/หน่วยงานที่เกี่ยวข้อง และแผนการแก้ไขเยียวยา

Case Study 4

The board of directors of "A&B," an international consumer goods company in Bangkok with offices in various countries across Asia including Singapore, Hong Kong, Japan, Malaysia, and Indonesia, was considering a confidential merger offer made by another large multinational consumer products company.

On a Friday afternoon, before a long holiday, the Chief Information Officer received a ransom email from an unknown source stating that they knew about the merger plans and had personal details of 100,000 customers. A sample of personal details for 500 customers was included in the ransom email as proof. Unless a significant ransom was paid in Bitcoin, they would leak the merger plans and sell the customer information.

You are one of the directors. What is the first thing the board of directors should do in response to the ransom request? What are the most reasonable steps that the board of directors should take to deal with this incident? In your response, please consider the communications processes among relevant persons, organizations, and authorities, as well as remedial plans.