

Case Scenario

The Business & Communication Insurance (B&C Insurance) began business as a private health insurer, established by Gary RT.L & family in 1965 through the Health Insurance Commission. This company was set up to compete with private "for-profit" funds. The company's headquarters is located in New York and has offices in various other countries including Spain, Australia and Hong Kong. The CEO of the B&C Insurance recently received a ransom email from an unknown company claiming that they have access to the company strategic plans and personal details of 200,000 clients. A sample of personal details of 200 clients was included in the email as a 'proof'.

Ransom emails are normally sent through unreliable external networks that are outside the company's security boundary. The CEO consulted the senior management and they acted promptly to investigate and contain the threat with the aid of forensic computer specialists. The first step was to validate the threat. The management team found a discussion on a hacker site in the dark net that had personal information of 200,000 clients of B&C Insurance for sale. This also included the details of the 200 clients, provided in the ransom email as 'proof'. The investigation also confirmed that the details of the 200 customers are genuine.

The senior management considered the need to identify threats and give practical guidance on how to manage the risks of identity fraud to be of utmost importance. Therefore, a team of consultants was appointed to prepare a series of reports to identify various threats and to develop cybersecurity crisis management plans in order to respond to potential threats/ risks of sophisticated hackers penetrating into the internal systems of the company and accessing client information.

As the cybersecurity specialist in the team, you have been asked to write a report to identify the threat types and key factors involved. In doing so, you are required to identify the most 'at-risk' components, create awareness among the staff of such high-risk components and how to manage them. In addition, this report is to help key stakeholders, including the executive managers, to make decisions on what course of actions must be undertaken to mitigate potential threats.