Cyber resiliency key to doing business in digital age

November 19, 2016 01:00
By SPECIAL TO THE NATION

ORGANISATIONS ARE highly reliant on technology as an enabler of their business. Any disruptions to normal day-to-day operations such as a natural disaster, a pandemic or a man-made disaster may have detrimental impacts on the organisation, including significant financial loss and a damaged reputation.

Most organisations have adopted a disaster-recovery (DRP) and business-continuity plan (BCP) to ensure that in the event of disasters, the organisation is able to continue operations with minimal downtime. Resilience to natural disasters or the ability to recover quickly despite a crippling disruption can in some cases save a company US$182,000 (Bt6.5 million) per hour of downtime. (footnote 1)

However, a DRP and a BCP are no longer sufficient in this age of digital transformation with organisations' high dependency on technology as an enabler and information having no borders. No company, organisation or government is immune from cyberattacks. An example is the complete breach of Ashley Madison’s user databases, financial records and other proprietary information. (footnote 2)

Cybersecurity alone is insufficient for handling cyber-disasters because it does not indicate the ability or readiness of the affected organisation to contain the pandemonium that will follow. Besides, an organisation facing a cyber-disaster will have a multitude of split-second decisions it has to make in order to respond effectively to the consequences of the attack.

Are you ready? How do you prepare?

Cyber-resiliency in action is about having detailed plans of response for all personnel and resources of the organisation – to be executed in the event of a breach. Building cyber-resiliency requires cooperation between the public and private sectors, but more than that, much greater awareness by everyone from business partners to front-line employees to those in the C-level suites.

Cyber-war gaming can help develop cyber-resiliency in an organisation by putting it through its paces with simulated cyber-scenarios in a controlled environment. This puts into practice the response plan of the organisation so team members can respond better in the advent of a crisis. This aims to achieve two outcomes for cyber-resiliency:

1. Assess and improve capabilities of personnel involved in cyber-resiliency efforts.

2. Assess and improve processes previously defined in the response plan for greater efficiency and effectiveness.

Cyber-war gaming can be delivered via various exercises within a controlled environment. For instance, tabletop exercises that are focused on testing-defined processes, the participants’ familiarity with it and their thought processes during a crisis. A cyber-war game also tests technical capabilities and infrastructure readiness to deal with any scenario in a crisis.

The purpose of cyber-war gaming is really meant to strengthen incident response and crisis management capabilities. It aims to achieve an organised approach to addressing and managing the aftermath of a cybersecurity breach or attack.

It is also focused on the attribution of an attack, and its root causes for future preventive, detective and recovery methods. Other capabilities it aims to improve are around the processes developed to deal with sudden emergency situations, which involve the legal and communications team.

An example of good versus bad crisis management is the comparison between Home Depot and Target in the United States. Both had payment systems breached. Target was hit in December 2013 and Home Depot in September 2014. Target estimated 40 million credit- and debit-card details of customers were stolen and Home Depot estimated its breach to be about 56 million. The difference can be summed up below.

Target’s senior management did not handle the breach very well, which generated a lot of bad press. One of their biggest failures was that Target took about a week after learning of the potential breach to address consumers, while Home Depot acted within about a day of discovering the breach. (footnote 3)

Finally, when a cyber-disaster strikes, an organisation is bound to see a strong negative impact from loss of public trust and reputational damage to monetary loss. A simple way to determine cyber-resiliency is to measure how quickly an organisation can recover from a disaster and the duration the negative impacts or sentiments last from day zero.

Other measurements to determine the accuracy of cyber-resiliency efforts are the following.

Minimised impact to business, quickly resuming normal business functions.

Resiliency against the recurrences of a similar cyber-disaster.

How well do you think your organisation will handle a crisis?

Footnotes:

[1] Duffy, Christopher, “A Resounding Yes! BCP and DR Can Bring Real Cost Savings”, Strategic BCP, February 17 2015, http://www.strategicbcp.com/ blog/business-continuity-cost-savings/, accessed October 6, 2016

[2] Krebs, Brian, “Online Cheating Site Ashley Madison Hacked”, Krebs on Security, July 19 2015, https://krebsonsecurity.com/2015/07/online-cheating-site-ashleymadison-hacked/, accessed October 13, 2016

[3] Hill, Catey, “Home Depot’s data breach is worse than Target’s, so where’s the outrage?”, MarketWatch, September 25 2014, http://www.marketwatch.com/story/yawn-who-cares-about-home-depots-data-breach-2014-09-24, accessed on October 18, 2016

PARICHART JIRAVACHARA is a Risk-Advisory Partner at Deloitte Thailand.