Recovering from a cyber crisis: The Maersk Case

On 27 June 2017, Maersk, the Danish shipping giant, faced the costliest cyberattack in the world to date. 97% of the digital infrastructure of the company was compromised. Critical applications like the cargo booking system were unavailable. Customer contact details had been wiped out. Even business recovery plans were scrambled. As a result, ships, containers and merchandise were blocked in ports around the world.

As the pressure built up from clients losing millions by the day and as authorities started knocking at his door, Adam Banks, Chief Technology and Information Officer at Maersk, faced the arduous task to rebuild the entire network infrastructure from scratch and in no time. Five lessons from the man who prevented a shipping giant from sinking.

Lesson 1: be transparent, including with clients

Maersk decided early on to communicate extensively internally and externally about the crisis mitigation activities and timeline. This decision would prove instrumental in securing third-party assistance that was critical to rebuilding the network infrastructure.

Lesson 2: no matter your size or industry, get cybersecurity into your crisis plans now

As an asset-centric company, Maersk's most valuable assets are its vessels and terminals. As such, crisis management plans revolved around the latter, not the underlying technological infrastructure. Maersk had to borrow plans from financial firms, right into the crisis, to elaborate a mitigation strategy. A key lesson for Adam Banks was the imperative requirement to separate business continuity and disaster recovery plans, so as to limit the adverse effects of cascading technological dependencies.

Lesson 3: prepare the board for agile leadership

When all communication systems are down, when contact details have been wiped out from mobile phones, there is no other option than resort to face-to-face decision making, fast track procurement processes, and ad-hoc leadership processes. As technology suddenly became the scarcest resource in the company, the Chief Technology Information Officer effectively embraced a major leadership role during the crisis management. The resulting temporary management structure helped prioritize crisis decisions and execute strategy in all departments, from operations to finance, ensuring that rebuilding the infrastructure as fast as possible was priority number one. An agile leadership culture and shared trust amongst C-level execs is essential to do this.

Lesson 4: build and maintain a trusted network to be able to get help fast

Maersk had call-down contracts in place with multiple consultancies and was effectively able to draw in forensics expertise rapidly to unscramble compromised backups. The real challenge was to replace 3,500 servers in a week and prevent reinfection. Few consultancies, if any, have the ability to dispatch hundreds of network engineers globally and overnight. And so, Maersk's leadership reached out to the C-level executives of its clients: they sent hundreds of engineers to support the recovery efforts and played a major role in turning things around. Transparency with clients, as described previously, was the precondition to this unprecedented cooperation effort.

Maersk also asked several governments for help. If the company gave a lot information, they did not get anything back. More, government agencies did not share it at national or international level, so that Maersk wasted precious time repeating the same thing over and over again. To accelerate mitigation of global crises, Banks says governments should seek to harmonize practices to simplify incident reporting. They should also better exchange victim information multilaterally to let victims focus on response and recovery.

Lesson 5: practice

Banks admits now, there is no better way to prepare for crises than to exercise: "Experience is a good school, but the fees are high". Maersk certainly paid a high price, but it proved resilient enough to get through. Not all companies would. In the aftermath of the crisis, Maersk revamped its entire crisis management approach and upgraded its insurance policy to include cyber incidents.

Since then, Banks has been travelling the world sharing his story, hoping others will learn from Maersk to get ready before it is too late.