The Value of Teamwork & Crisis Management: Reflections on Gartner’s Security Summit in London

There is an opportunity in crisis.

In mid September I spent a couple of days at the Gartner Security and Risk Management Summit in London. As is the usual case when hundreds of delegates from all over the world converge in one place and hours of rich content are presented in bite-sized packages, a few sessions tend to stand out from the rest. The first was a keynote speech made by a retired captain in the United States Navy and former NASA astronaut, most famous for his role as commander of the Apollo 13 mission to the Moon, James Lovell.

Lovell spoke a lot about crisis, a fitting subject considering the nature of the summit. As many know, the Apollo 13 mission was deemed a “successful failure”; after just two days into the mission, the spacecraft suffered catastrophic damages that in most cases would mean a loss of the entire crew. But due to the team effort from the men in space, Lovell’s leadership, as well as NASA’s mission control in Houston, all three Apollo 13 astronauts returned home safely.

In Lovell’s own words, it was a classic case of crisis management. “We must always expect the unexpected,” he said during his speech, adding that it was the team’s flexibility with respect to prioritization and open communication that saved their lives. I think we could all benefit from enhancing our flexibility. Everyday people are faced with seemingly unpredictable variables, but when people band together to resolve a conflict, let go of prior expectations and think outside the box, catastrophes can be turned into opportunities. Which brings me to the topic of cyber security.

Find the proper course in times of adversity.

As alarming headlines crowd the newsfeeds confirming breaches at some of the most stalwart corporations, the awareness of our vulnerability grows. It has become too easy for hackers to penetrate what we think of as impenetrable systems. According to the 2015 Cyberthreat Defense Report North America & Europe, 71% of organizations were affected by a successful cyber attack in 2014, but only 52% expect to fall victim again in 2015. This is an alarming statistic!

The security landscape is rapidly changing and needs a solution that can match its pace. As Gartner’s very own Neil MacDonald presented in his session, prevention is no longer enough. The adversary has made it through the security barriers and if you want to remain safe, you must have tools that reveal its presence and activity in real time. The session confirmed that we have officially entered an era where detection, not prevention, should drive a security strategy, because detection alone can become the foundation of the future model we so sorely need: the ability to predict a breach and act before damage is done. This is where, as was the case with Apollo 13, preparation and execution in real-time are key.

To the moon and back.

When Lovell and his crew discovered the damage to their spacecraft, they had to take immediate action to navigate out of the crisis. While the team was put through rigorous training before the launch and each crewmember had hours of flying experience, they could not anticipate the mission's catastrophic outcome. In hindsight, what allowed them to succeed and what can help your team implement an effective security strategy boils down to two main points:

- **Teamwork.** You can plan as much as you want, but without prioritizing and open communication among teammates, even the best plans can fail. Just as the space crew needed to quickly accept that they would not be landing on the Moon and reprioritize their efforts, security teams must be agile enough to work together and react quickly to remediate an issue within their network. Better yet, teams must learn to anticipate breaches and there is no better way than to assume that they have already been breached. This is another reason why it is so important to be aware of the state of your security system and its vulnerabilities, as those can lead to the greatest loss. With every decision the crew made, their chances of making it home grew, just like with every well-planned tool you implement, your security system should become more capable of catching an attacker.

- **Risk Mitigation.** Being able to predict the many variables that can go wrong is crucial to preparation, as is protecting your business assets. The first step is to understand the main risks, articulate your findings to the leadership team, agree and then act upon a plan. The possible internal (operational) and external (public reputation) impacts of a breach should be the driving force behind a bulletproof security system. NASA was prepared because they assessed many of the risks prior to the mission. You can do the same in cyber security when you have full visibility into the state of your network.

For Lovell, the gut wrenching experience revealed the true value of teamwork. It was thanks to the team effort and leadership that they were able to use the lunar service module to assist in getting home, a vehicle never designed for that task, and splash down in the Pacific to safety 5 days, 22 hours and 54 minutes after leaving the launch pad at Kennedy Space Center. Without crisis management skills the operation would have surely failed. As we are witnessing a massive disruption in the security industry, vendors need to align with and support IT professionals, enabling them as business partners that can provide clarity and peace of mind to an increasingly worried board and C suite. Crisis management must be a part of every business plan, whether you're planning an interstellar mission or supporting the daily operations of a crew of entrepreneurs.