

# Clever Security, Clever Business

Andy Blackwell and John Wood's new book describes the latest thinking in managing security. Read their insights on the interactions between incident management and crisis response...

**O**n Monday, November 5, 2013, an aerial view looked at a 13-hour standoff at Heathrow, Britain's gateway that looked as hectic and swarmed as thousands of passengers. He drove a rental vehicle through a security barrier onto the tarmac, then ran down to the jet, and three men... having trouble before parking the car under its aircraft. His four-year-old daughter was also in the vehicle by his side had already packed about the obstacle of her child until an ongoing security dispute. The stand security breach rapidly escalated into a hostage situation, prompting the activation of the airport's crisis management plan and the deployment of police and other specialist agencies. The standoff was eventually resolved without casualties due to the skilled actions of negotiators, and flight operations resumed the following day. However, the airport suffered significant operational and business losses from the 13-hour closure.

Various airports are fundamentally very safe. Charlotte's Carol M. Beckwith's spokesperson, Nellie Robinson, tells reporters in Berlin, that "What we have seen here in Heathrow doesn't have time and again, but we are in the concept, and that someone with high-stakes emergency situations is also very dangerous can manage to see such gaps. It is also clear that no concept is as good as it can be made to be better," she said.

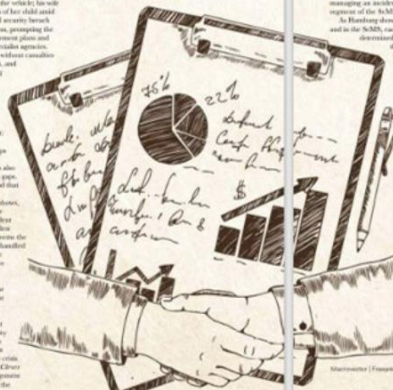
In the Heathrow Airport incident above, incidents are contained and resolved as they appear at first sight. They incident can quickly escalate out of control unless contained effectively. In this case, it seems the resolution from incident to crisis was handled well, although the state of relief of the perpetrator and his fate for his might have gone can never be known.

Crisis response is not a security capability. It is a core process provision for the management of all programs that necessitates the control of what can be called standard operating procedures.

But, in Heathrow, a security incident can escalate to a crisis, or a non-security crisis may have a security angle to it, so the security management function must provide for a smooth interface with the crisis response activities. In *Clever Security, Clever Business*, we call this the "Crisis Management Handshake" and it's an integral part of the

Security Management System (SMS).

The guidelines stemming through *Clever Security, Clever Business* is that for security and the SMS to be effective and efficient, they have to be defined thoughtfully in a way that balances the need to prevent against existing and covering them to the organization



while supporting the overall business strategy to enable growth. The fundamental aim is to manage security effectively, so that a company's security management sees the cost of the business as a strategic capability, which also presents economic security and the operational and information that can come from that. The aim is to get security just right – not too tight and not too loose (the 'Goldilocks Principle').

In a *Clever Security, Clever Business* world, the link from incident management to crisis response (the Crisis Management Handshake) is obvious, but incident management does not exist in a vacuum. The SMS is a framework of interdependent activities, and incident management is just one of those components. When they are all properly aligned and working well, the crisis response is smoother, faster and better. For example, the incident response team include personnel from business units as well as the security team and possibly from other agencies. Training them to take part in managing an incident is included in the education program of the SMS.

In *Heathrow Airport*, a crisis starts out as an incident, and in the SMS, each incident is managed by a team determined by the magnitude and reach of the incident, with an escalation mechanism to more significant incidents are managed at a higher level in the company, or in the worse case, escalated to a crisis response team.

The size of the crisis is largely determined by the speed and accuracy of crisis invocation, and often in the recognition and timing of a crisis will result in it escalating into an even greater crisis.

And although a crisis is not unpredictable, there has to be a completely pre-planned response, that does not mean we should wait for the crisis before making preparations.

Consequently, managing an unpredictable crisis requires a lot of preparation, planning and training, not in the world of knowledge a particular kind of crisis, but rather to ensure prompt and effective action for the individual and/or overall/best nature of the event.

The Crisis Management Handshake is one instance of how an incident management response provides support the company's strategic goals, in this case the resilience goal.

The book defines the goal of the Crisis Management Handshake

book review

as "To provide a smooth handover and ongoing interface with crisis management plans if a security incident occurs beyond the capability of incident management."

In a smooth handover, the first step is to activate a security crisis in prompt recognition when a security incident escalates beyond control. The preparation for that includes defining clear trigger criteria to guide who, how, and where to trigger the crisis response and establishing and practicing exercising clearly defined responsibilities, chains of command, escalation, and communication paths for the incident management link with crisis management in the handover and afterwards.

After initial, the quality of the communication link made during the incident is a major factor in the resolution and speed of the handover.

The incident management team does not stand down after handover; crisis managers may call upon them to take part in managing the crisis control or to make themselves available to provide information or advice throughout the crisis.

The other major security contribution to crisis management is the threat and risk management team. Monitoring threats and risks continuously and having the capability to make fast and accurate risk assessments as circumstances change are critical activities in crisis management. They help in identifying potential crises at the earliest opportunity, whether by resolution or major incidents, monitoring leading indicators and other warning signals for impending crises, using open and closed information sources, social media, or other means.

They also do other work for the crisis management behind the scenes, such as helping emerging challenges, developing appropriate plans and contingencies, and tracking alternative scenarios to meet the latest product challenges of political, economic, sociological, technological, legal, and environmental (PESTLE) factors that could affect decision-making.

The threat and risk team is also responsible for understanding and controlling potential points of catastrophic failure. Crisis risk review team identifies when components are not addressed and control each other – the 'watchdog effect'. For example, the team can determine and coordinate support chain vulnerabilities, particularly for infrastructure services, in anticipation of major challenges during a crisis.

CR teams, values of all hand over for the business, and security events are with their case. But in doing this, *Clever Security, Clever Business* SMS supports crisis management, so that any case are how non-security events might be managed better with similar functionalities between other departments and the crisis team. [2]

[Andy Blackwell](#) and John Wood's new book 'Clever Security, Clever Business' describes the dynamics between incident management and crisis response. "The size of the crisis is largely determined by the speed and accuracy of crisis invocation, and delays in the recognition and triaging of a crisis will result in it spiralling," they write.

<https://crisis-response.com/Publisher/Article.aspx?ID=678567>

**Free downloadable version of the CRJ article coming soon**