INSIDER THREATS ESCALATE OPERATIONAL RISK

Anne Searle

Annie Searle is Principal of Annie Searle & Associates LLC – also known as ASA Risk Consultants – an operational risk consulting and research firm that provides independent risk assessments and roadmaps for critical U.S. infrastructure sectors like banking and finance

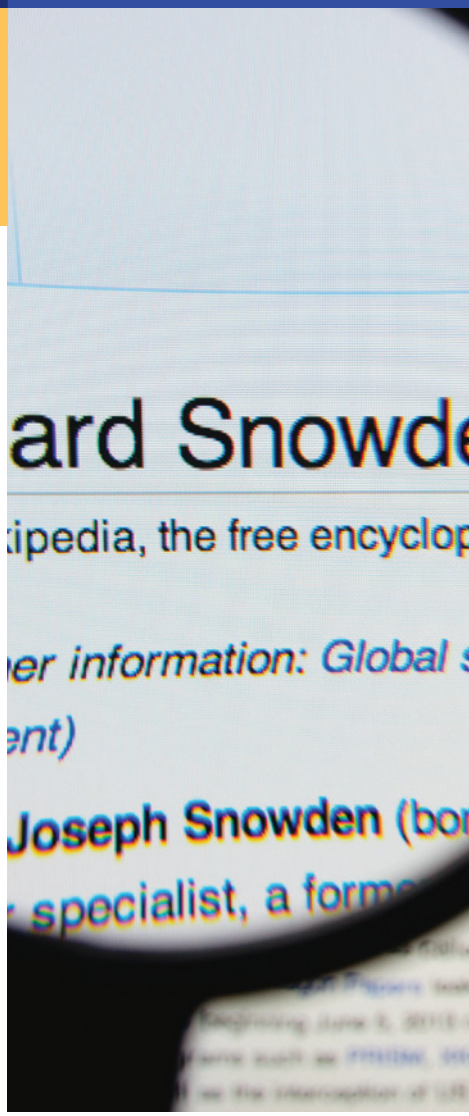
The Risk Universe columnist Annie Searle takes a look at human behavior within the firm and whether insider threats are the most significant threat to the firm

As a CEO, you want to believe your company excels at retaining the best and brightest employees and that your employees behave at all times with integrity. Yet there are enough examples to make you think more about the problems that your employees and contractors can cause – not surprising, since employees and contractors represent your largest risk, with a median loss of $140,000 per event for insider fraud (employee theft, fraud or embezzlement) and an average $20,000 in damage to the company from other insider attacks (data leaks, intellectual property theft, etc). This data comes from the 2012 Association of Certified Fraud Examiners (ACFE) Report to the Nation. Add this to the 2013 Identity Theft Resource Center Report and you will have a very clear picture of the frequency and the financial costs of various types of insider threats.

Since 2001, the Carnegie Mellon CERT (www.cert.org) has been engaged in research on insider threats and, since 2004, CERT has produced annual reports on such threats in partnership with the US Secret Service. From those reports, which can be found on the CERT website, it is possible to paint a useful picture of the ways in which a corporate culture could be at risk for heightened insider threats and to develop a checklist of behaviours that might cause management or HR departments to take additional precautions against, when appropriate.

Most executives would agree that an organisation's most valuable assets are its people and its intellectual property. Accordingly, the primary defence should be time spent training employees on insider threats. Enlightened employees become long-term employees when their orientation and training includes understanding what an organisation values, how it is protected and who owns it.

In her presentation to the 2012 BAI conference "Outing Insider Fraud," Shirley Inscoe noted that leaking bank information is the most pervasive form of financial insider fraud and identified additional types as "falsifying loan documents, selling bank or customer information, misuse of assets or position, taking money from cash drawers, identity theft and mortgage theft."



But there are more types of insider threats than financial fraud. Dawn Capelli, who at the time headed this work at the Carnegie Mellon CERT, spoke some years ago at a Shared Assessments Summit organized by The Santa Fe Group, where she summarised aspects of their work as the CERT's "Common Sense Guide on Insider Threats." This made me wonder if understanding and sharing some of the reasons that employees engage in this behaviour might facilitate managers more proactively looking for early warning signs. In the context primarily of workplace violence, I referenced some of these behaviours that managers can look for in the third chapter

of my book, Advice From A Risk Detective.

There is no doubt that putting controls in place to prevent different types of insider threats can reduce or eliminate financial or reputational loss, though it is a much more complex effort than it would have been even five years ago. Employees have a great deal of physical and electronic access by virtue of their status, as do contractors working as critical business partners. As CERT points out, both employees and contractors have practical understanding of how well or poorly policies and controls are managed. So let's explore some examples of the high level behaviours to look out for.

➤ **Anger and aggrievement** Capelli described situations in which very smart developers came to see the applications they were working on as belonging to them because they had created them, rather than the company. When circumstances deteriorate, the developer can cause damage to the application or share its code with outsiders.

➤ **Shame** A number of traders fall into this category when they feel shame for incurring large losses, which they then hide and then gamble further to correct the losses by continuing to trade larger amounts outside organisational controls. The JPMorgan Chase London Whale episode is an example of compounding losses.

➤ **Poor performance reviews** Capelli's team worked with the Secret Service and interviewed a number of former employees now serving jail time for their insider crimes. A pretty consistent theme is that the former employee had almost always been highly valued in previous performance reviews, but then received a poor review, leading to feelings of anger and aggrievement, which led to theft.

➤ **Anxiety from organisational change** When a company is being sold, anxiety that an employee will lose his/her job can cause him/her to inappropriately remove corporate information for personal use or other nefarious purposes.

In addition to providing solid orientation and training to employees and training managers to spot troubling behaviours, what else can be done? Background checks on potential hires would be the first place to start looking for flags. When interviewing potential employees, hiring managers should be checking not only for the answers they wish to hear, but also for culture fit with the firm. In high risk positions that include broad administrative-level access, a probationary period is certainly appropriate, with additional follow-up meetings between management and the new employee to ensure that the new employee has a growing understanding of the workplace.

There is no doubt that putting controls in place to prevent different types of insider threats can reduce or eliminate financial or reputational loss

If we take Edward Snowden's actions as an example, where we are looking at a large corporation with sensitive electronic property, I would recommend that employees with privileged access to both internal servers and other documents on outside servers be subject to the "two-man rule", which requires at least two people to approve an action in order for it to take place. The NSA announced the implementation of this rule only after thousands of files had walked out the virtual door with Snowden. The General Motors legal and safety divisions provide us with yet another example. We see two groups that grew to become enormous insider threats, not because they divulged confidential information, but rather because they methodically concealed negative information from their superiors. This behaviour, which has been described alternately as "overly bureaucratic" or "criminal," identifies the insider threat of the elimination or concealment of information known to be problematic or expensive to the firm. Frankly, we don't know how often suppression or concealment of information occurs in large companies – but I will looking into this type of threat in my next book, Executives and Risk: What Your Teams Won't Tell You. More to come. TRU