How to establish an executive protection programme

+

Data classification: Kidnapping, Hostages and Extortion

Gen2models: Structured scenario analysis

Frontline ORM in the Oil & Gas Industry

Annie Searle: Vendor risk and intellectual property

www.riskuniverse.com

The Risk Universe

Eye of the tiger

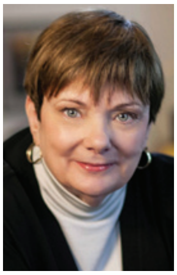
Protecting senior executives is paramount for all firms - this scenario focuses on Tiger Robbery

ISSUE 23

November 2013

VENDOR RISK AND INTELLECTUAL PROPERTY

The Risk Universe columnist Annie Searle addresses the very important operational risk of third-party vendor management



Annie 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.

B British and American operational risk experts have had a lot to absorb since Edward Snowden started releasing documents he filched during his time as a Booz Allen contractor at the National Security Agency (NSA). There may very well be a handful of NSA executives who have a good idea of just how much material will eventually be published by media, but I think most of us (including the Obama administration) are surprised at the range and variety of the materials about British and American projects involving targeted surveillance. Just when we think we have seen the last set of materials, more appear. In succession, we have been able to read about programs such as Prism, Boundless Informant, XKeyscore, and Tempora -- as well as documents that expose how successful the NSA has been at latching on to data from both Google and Yahoo through penetration of its secure links among global data centers.

Many of us had been aware of the government's heavy reliance upon contractors to do its work, especially since threat analysis was ratcheted up after 9/11. Like the government, we just assumed that companies like Booz Allen did a good job of vetting the persons they hired to work on classified information. Recently we learned that it was not only Booz Allen's background checks that were deficient. In 2009, while Snowden was working for the CIA "his supervisor wrote a derogatory report in his personnel file, noting a distinct change in the young man's behavior and work habits, as well as a troubling suspicion." [*New York Times*, October 11, 2013]. The supervisor's suspicion was that he was trying to break into classified files. Evidently that information stayed buried in his personnel file or "fell through the cracks," and was not picked up on a subsequent background check for his more recent position as a contractor at Booz Allen.

Operational risk that stems from vendors and their contractors is, in fact, one of the most critical risks that business faces in an increasingly complex world. The US government may be the largest entity to contract with vendors, but the practice of using contractors permeates most mid-sized and large companies. Gaps in vendor controls can be found in any of the four lenses through which we view operational risk – people, broken or failed processes, systems, and external events.

In a March 2012 Impact Factor study, more than 100 companies were surveyed on their use of supply chains. The results were not encouraging. Half of those surveyed spent $50,000 or less annually to audit and assess suppliers. And 80% of those surveyed indicated they manage only the primary vendor, not what are often multiple layers of suppliers and subcontractors. With increased outsourcing and offshoring over the past five years, the stakes have never been higher. Economic turmoil, more natural disasters and political change around the globe have produced additional complexity for vendors and for their clients.

As companies grow, their

intellectual property is often not well protected. In a Carnegie Mellon CERT study on such threats, contractors were the heart of the problem: in one case, a contract janitor stole customer account information from hard copy documents lying out on desks and used it to obtain credit cards in the customers' names (loss= over $200,000); and in another case, a contractor stole and sold trade secret drawings intended for shredding (loss = $100 million). For more information on Carnegie Mellon's CERT research, go to http://www.cert.org/insider_threat/. Though we don't have a great deal of detail on how contractor Edward Snowden obtained access above his own level to so many documents, one can infer that the NSA has now tightened up its access controls as well as its internal logging routines.

The first place to start in managing the risk around vendors and intellectual property is with the contract that is created. Here's specific advice by operational lens:

People Require back ground checks scaled in sophistication to the criticality of the business processes you are giving the vendor. Identify whether the vendor is using subcontractors and require background checks there if appropriate. Be mindful also of the small companies you need to run your business, like janitors or couriers.

Process Bind the vendor on all compliance-related issues (in particular, their own business continuity and data security programs and those of their subcontractors). Ask them to show you their plans for how they will service your account in the event of events like natural disasters, pandemics, or acts of terrorism in this or other countries. Write into the contract the time frame in which you expect the vendor's attention during such events. Above all, trap for potential worst case scenarios and for additional layers of subcontractors.

Operational risk that stems from vendors and their contractors is, in fact, one of the most critical risks that business faces

Systems Require proof of additional layers of redundancy that the vendor has in place. Consider geopolitical location if data centers are involved. Insist upon site inspection visits to critical vendors. Before you contract a cloud vendor, determine in advance how you will audit that vendor and write it into the contract.

External events Closely review the vendor's business continuity and security plans. Find critical gaps in both your own and your vendor's plans based on increased global complexity for transactions processing.

Vendor risk management has two parts: getting the contract language right; and active monitoring of critical vendors. The commonest problem I see is that small vendors are not scrutinized in the same way that large technology vendors are, even though small vendors often have direct access to intellectual property.

Finally, build your own corporate assumptions on service and recovery into each contract: what priority will your company have with a cash courier, for example, during a severe weather event? Once you've worked out all those details and embedded the understanding in the contract, then insist upon key vendor participation in the scenario testing you do throughout the year. And keep your board of directors apprised several times a year on the controls you have in place to avert financial loss or reputational damage. TRU