CREATING A CULTURE OF SECURITY

The value of even the most robust brands can be decimated overnight by the consequences of security breaches—and at almost any point in the supply chain. But few companies take this threat seriously enough, says Hugh Kenneth Branch

Devising, adopting and applying tactics to protect a brand owner's product is a perpetual moving target, especially in these times of continuous technology transformations, a worldwide recession and sinking bottom lines. Companies must scramble to trump creative counterfeiters, cheats and swindlers that are in direct competition with brand owners.

Complicating this state of affairs is the wired-up network of worldwide, instant communication and 24/7 news cycles that force businesses to defend their reputation and brands with lightning speed in the face of a security crisis. A business can find itself stigmatised without any direct involvement in the predicament of a particular brand, suffering the adverse consequences of a ripple effect.

For instance, as of late February, several hundred companies have voluntarily recalled more than 2,500 peanut products in the US and more than 300 products in Canada due to salmonella poisoning. As that list continues to grow, food companies will lose millions of dollars. But in reality, only a small percentage of products were tainted from a peanut plant in Georgia.

Most business owners understand that in the current economy, growth will be difficult at best. This makes it more critical than ever to defend the products they produce. An abundance of aid exists to accomplish such an enterprise. Advances in state-of-the-art technology have mushroomed in recent years. At the same time, more brand owners are pushing suppliers to adopt recognised security standards.

And they should. Brand owners and their security managers must insist that suppliers meet some level of a security benchmark to protect the company and its brand.

Nonetheless, many businesses still don't get it, especially in the US, which lags behind other regions of the globe where security systems are considered *de rigueur*. Many US brand owners lack comprehensive security planning and training, allow gaps in satellite facilities, only casually monitor supply networks and ignore recognised security standards. A better culture of security is needed to establish quality protection.

One of the greatest threats to any company or brand is neglect, complacency and ignorance when it comes to confronting security threats. It is essential to educate senior managers as to the changing tactics and strategies of offenders, and that has been a substantial part of our mission at PICA Corporation in our 26-year history.

"Since 9/11, which occurred when I lived and worked in New York City, companies have really begun to take security and loss prevention more seriously," says Vincent Volpi Jr, PICA's chairman and chief executive officer. "Before, these services were seen as a drain on the bottom line. Afterward, their ability to add value through asset protection and brand integrity started to be recognised."

The big picture

As a certified auditor for ISO 27000 (Information Security Management Systems), ISO 28000 (Security Management Systems for Supply Chains) and C-TPAT (Customs Trade Partnership Against Terrorism), I know the value of assessing businesses for security standards. The assessment is basically a checklist covering eight areas of widely accepted managed risk.

Yet, some companies hesitate. Assessments can slow down business operations, but it's critical to think of the big picture when implementing security measures. Ensuring the security of the product throughout the supply chain is critical for any company. Senior managers driven by profit and loss statements must recognise that their entire business can be seriously jeopardised by slipshod security.

To establish comprehensive security for a supply network, organisations need a team to build a foundation that includes a preparation phase, technology solution evaluation, information technology integration, and enforcement co-ordination and management of the entire system. It is a cost, but tactical band-aids will not work in the long run.

Volpi believes that the key to successful loss prevention is a proactive and integrated security programme that creates a culture of security in the organisation, and that in abbreviated form should be made available to the public.

"Professionals in the field can carefully add value by helping to protect and promote brand and shareholder value while they search out and find fraud, waste and risk that can directly impact profits," Volpi says. "Those endeavours actually make security a 'profit centre' so that services like these become an investment with a return."

Brand owners would do well to consider many off-the-shelf technologies that can be integrated or combined with information systems to communicate security threats in real time. Some perform missions beyond a security function, which helps justify their use.

Examples of successful technological innovations include:

- Nano-micro message carriers, which are invisible to the human eye. These can be used on more than 400 materials
- Machine-readable forensic codes made up of chemical or synthetic DNA buried behind labels or product packages and used for asset management. The codes have an anti-theft capability and their data can be sent over the Internet
- Encrypted barcodes and passive radio frequency identifier (RFID) tags that can link to GPS for intelligence mapping, investigator management and selective recall of products.
- Active RFID and data loggers that warn of unauthorised pallet, carton or shrink-wrap opening to help ensure consumer safety from an infected product. These are used to record temperature changes, extended humidity and shock exposure to products or cargo.

Technology and a combination of technology integrated into a company's existing information system can mitigate threats to brand owners for vehicle, cargo and organised retail theft. It can also curb unauthorised repackaging of goods, warranty and return fraud, diversion of products and counterfeiting.

Hugh Kenneth Branch is a senior director of security consulting with PICA Corporation. He can be contacted at: kbranch@pica.net

Hugh Kenneth Branch

Hugh Kenneth Branch is a retired 25-year army veteran. He has been a security consultant for the past 18 years, specialising in logistics crime, fraud prevention and brand protection. He recently developed a technologies programme to provide real-time systems to protect products, cargo and vehicles.

He is a certified ISO security management auditor, skilled in preparing clients to comply with C-TPAT, EU-AEO and the Sarbanes Oxley Act.