Steve O'Malley, *Security Team Leader, ISO TC-8 and Director, Maritime & Supply Chain Security, SAIC*

Francis D'Addario, *Emeritus Faculty of Protection Innovation, Security Executive Council and former CSO, Starbucks*

Daniel Collins, *Solution Sales Leader, Customs, Ports and Border Management, IBM Public Sector, Americas*

Richard A. Lefler, *Dean of Emeritus Faculty of the Security Executive Council and former CSO, American Express*

Question: What can I do to ensure my supply chain is adequately protected?

Somehow the goal of anti-terrorism has replaced the goal of good corporate governance in the management of supply chains. Does an act of terrorism impact the supply chain differently than a criminal act or a natural disaster? In the aftermath, the answer is "no" — in all cases, infrastructure may be damaged, people hurt and operations will need to be restored.

Theft of goods, toxic chemicals in toys, poisons in foods, e-coli in vegetables, contaminated or counterfeit pharmaceuticals and illicit items inserted into legitimate shipments — these are real and current issues. Corporate due diligence that combats these types of threats will pose a more formidable barrier to terrorists who wish to attack our supply chains than externally imposed security programs.

What can I do to protect my supply chain? First accept that it is yours, not your suppliers', 3PL's or carriers'. You can outsource these functions, but liability ultimately remains yours. Second, maintain quality control over what enters your supply chain. Be able to track the shipment; if it is delayed or rerouted, have a mechanism to investigate. Maintain the ability to isolate the shipment should issues arise. Companies that apply proper corporate governance will find meeting the requirements of externally imposed security programs routine.

Supply chain risks can be the showstopper for any enterprise when left unmitigated. Consumer and stakeholder confidence depend on our ability to ethically provide quality products on time. Brand reputation is earned from delivering on that promise.

Stakeholders expect "all hazards" risk mitigation, from raw materials through shipment to manufacturing and distribution destinations. That means mapping the risk geography and mitigation authentication for assets including facilities, personnel and trusted agent services, and quality control processes.

A people, process and technology methodology enables us to determine that all hazards are understood and may be prioritized for mitigation. That was Starbucks Coffee's risk-based approach to its Guatemalan supply chain. An early adopter of C-TPAT and ISO supply chain guidelines, Starbucks also participated in Operation Safe Commerce, GE CommerceGuard and Sealock pilots. The results offered proof of an ROI-capable supply chain protection plan.

We cannot subrogate consumer or stakeholder expectations for supply chain protection. We must continually monitor risk conditions and key mitigation processes. We must have the leadership courage to champion supply chain protection, particularly in uncertain economic times when cost savings at any price potentially endanger protection programming.

In tough times, investing in your supply chains seems like a common-sense decision. The double whammy of a difficult economy and faulty implementation of your supply chain security isn't survivable. Undoubtedly, some will make the wrong decisions and pay for it in civil lawsuits or complete loss of the business.

The temptation is to rely on your partners in the chain to do their jobs. But when all actors in your supply chain are faced with the same economic pressures, can you rely on them not to make the wrong decisions? A consistent understanding, commitment and follow-through to a standard and agreements for supply chain security is one of the keys to your company's good reputation and success.

Your investment in wise application of technologies is required when considering the trust quotient of the chain and the partners represented by it. Don't forget supply chain security rests atop public safety and brand image. Advanced technologies like RFID labeling and tagging, satellite and GPS tracking, advanced behavioral and geospatial video analytics, computer simulation of supply chains for scenario planning and biometrics for access control and identity management might seem like luxuries in tough times. What can you do? Champion the right stuff.

Thoughtful, proactive security program partnering with legal, finance, and risk management operations forms an umbrella of protection in a global economy in which interdependence and cross-border trade continue to grow rapidly. Experience continually reminds us that no matter how robust our proactive programs, events can happen that will disrupt the global supply chain. Geo-political disruptions including war, terrorism and crime will occur. Natural disasters and outbreaks of disease will strike. As Nassim Nicholas Taleb writes in *The Black Swan*, when highly improbable events do occur they often create widespread disruption and upheaval. An example: The recent credit market collapse had an immediate, dramatic effect on the Baltic Dry index measuring global shipping and subsequently on shipments themselves.

Front-end risk mitigation is critical, but we need to remember that residual risks remain — some of them quite large. It is important to use some precious resources to be able to quickly detect emerging events. Following detection, the ability to rapidly communicate to all parties quickly and on an ongoing basis is important. Finally, constant crisis management and business continuity planning are essential to being able to adapt rapidly. Detection, communication and planned responses get you to the front of the line in tough times.

NEXT MONTH'S QUESTION: Should Web 2.0 applications be allowed to be accessed from company computers?

For more information about the Security Executive Council, please visit www.securityexecutivecouncil.com/?sourceCode=std.