Trying to separate fact from smoke: A critical review of cargo security

Erik Hoffer, Seal Committee Chairman, International Cargo Security Council, NJ, USA

The cargo security initiative is in the development and concept stages. Smoke and mirrors skew the discussions because recommendations presented by many of the experts asked to participate lack the core expertise required to recommend remedies against unforeseen threats. Many of these experts and officials lack a practical understanding of the physics behind seal security and cargo terrorism. Intimate knowledge of intelligence on threat issues is not sufficient background to recommend remedy. Specific knowledge of the physical attributes of security technology is not a substitute for understanding the threat. People who are finally asked to decide on the correct system and course of action may not be intimate with the nexus between science and viable mechanical remedy. Many of those in the know in the US Government and those consultants to the government present options based on perceptions rather than facts which can cost everyone dearly. Any approved plan will ultimately attempt to establish a level of container sealing and monitoring integrity for the entire world supply chain. The system should ideally be able to enhance homeland security, by reducing the threat of attack through cargo entering or leaving any port. By developing a workable intelligence security programme combined with viable security devices, we should be able to identify suspect cargo before it can be placed on a ship heading to its final destination.

The US's plan for cargo security

Department for Homeland Security and Customs and the Department of Border Protection, who seems to be spearheading the project which includes the plan to cover procedural security for stuffing and shipping containers, physical security for containers in transit, access to ports and cargo yards both the US and abroad, personnel integrity checks for cargo handlers, training of personnel on terrorists threats, awareness of the types of threat, secure manifest procedures and conveyance security dealing with the vessels, drays and ports handling and storing and moving cargo.

This is a broad-based plan, requiring a considerable amount of technology and refinement before a suitable solution can be found. Implementation must include appropriate physical security products used to achieve containment and control of cargo. Such technologies must be suitable to the real world of container cargo shipping. They must be cost effective for both ports and shippers and able to be readily implemented worldwide without development time. Any choice must focus on its ability to detect entry or manipulation of the doors from both an indicative and barrier prospective. Training of personnel must focus on simplicity and consistency which is often lost due to the urgency of this need. Systems that have proven to work in the here-and-now are the order of the day. Implementation of a system that requires a tremendous expenditure in infrastructure will limit approved ports, which will severely impact world trade. Such a system is both detrimental and prejudicial to shippers and ports that cannot come up to speed and thereby becomes the antithesis of free and open trade.

Who is responsible?

People whose jobs it is to secure cargo and whose goals it is to have a successful cargo security initiative are not the same people.

The MK-IIIA security lock on a container with cable.

A side view of the MK-IIIA security lock.

Those who pay the bills to ship, carry, handle, receive or load cargo are truly ambivalent about the implementation of such security procedures, products and systems. Many, if not all of them, see such an implementation as an added cost not a necessary benefit. Since their reality is cost vs. profit, not security vs. an imploded economy due to an act of terror, their perspective is radically reduced.

Not that individually they are not concerned about Homeland Security, but having 30+ years in speaking with these companies gives the author that skewed viewpoint: Shippers have always faced the threat of financial loss through theft and damage yet proactive reduction techniques are rarely used. Shippers who know the score on cargo theft in the United States, which exceeds $25 billion annually, still have inherently balked on use of the simplest tools available. The threat has never been higher for theft, tampering, drug smuggling or terrorism, yet the reluctance of most shippers remains consistently steadfast when it comes to the use of security tools at their expense. Even when confronted by a loss, most shippers complain vehemently about spending much more than a $1 on a bolt seal securing a container worth millions.

Now that the threat has become more public and it has grown to include terrorism on the list of loss conditions, have shippers begun to recognise their participation in the cure process? Not really. Tampering, smuggling (piggybacking) contraband into legitimate cargo and the use of your container to transport bombs and people around the world is suddenly real. Those who decide how much to spend for protection need to get on board with these initiatives and work as a team with governments to accomplish the mission at hand.

Technologies and solutions

With that "penny wise dollar foolish" base mindset, let's look back at the Customs initiative question and how that relates to the available technologies and viable solutions in the US.

From the port prospective: In order for a port to offer any level of security containment without opening every box they must assume that the Container Security Initiative (CSI) will help shippers to provide the security sealing when they stuff the box. Cargo in a container is just that, inside a steel box, neither visible nor accountable and highly vulnerable. A total trust relationship must exist between the shipper, dray company, port and sea carrier, who in turn has an implied trust to the receiving port, dray carrier and ultimately to the recipient. If such a relationship were to exist it must be built on secure sealing methods and technology. The control element must be the process and the seal. The seal and system must preclude and easily identify surreptitious opening en route and it must offer a formidable barrier to those trying to open it for any purpose. The most common element for securing a container has been a bolt seal placed through the handle hasp. That product, regardless of brand, manufacturer, quality or features, has only ever been good as an audit tool, and certainly never has offered or claimed to offer security. Seals placed on door handles are so easily circumvented that their utility as a security device is ridiculous. Compromising of the handle bar itself is quite easy; hence any form of seal placed on the hasp fails to offer any security.

Recently an ISO standard 17712 was developed in Europe by a group of well intentioned scientists. Note that I did not say security professionals since, in my view they are anything but. The perception of the report, which was immediately embraced by many who also fail to have a proper understanding of the vulnerability of the door handle, was immediate. Because they chose not to solicit any other qualified forum, the US Government created a mandate regarding the use of this standard and worked from that point forward.

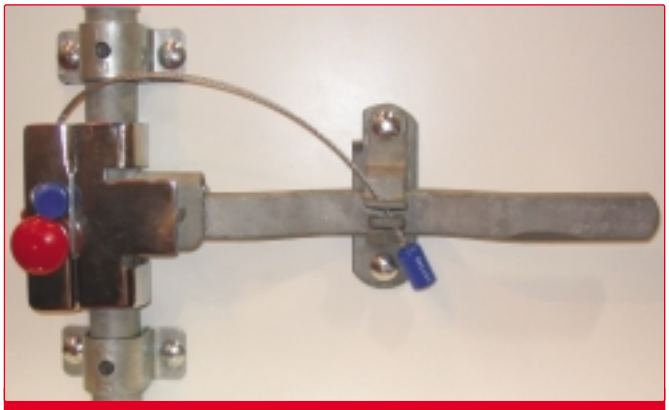
Standards are necessary to achieve consistency in most things, however standards that deal exclusively with the physical attributes of a science and not the appropriate application of the technology fail on all fronts. They create a misperception which is then carried forward and thereby jaundices the process. The ISO standards are clearly a misrepresentation of the facts as they relate to vulnerability. They fail to account for the utility of a seal and focus on the physical attributes. As scientists and not security professionals, their lack of knowledge has set the standards for security back by four years.

Realtime security

When dealing with a threat such as cargo terrorism, expecting any security from the 'now revered bolt seal' would be ludicrous.

The next area is the perceived need for real time security information on containers and their contents. It is obvious to anyone that has ever seen a port or a container yard or a ship is that the environment that these containers move and are stored in, is hostile at best. Salt, cold, heat, water, shock, rough handling, stacking and truck mounting are hard on steel much less electronics. Most technologies that have been tried in the past to transmit information from containers fail because they either break down in salt, rust, become damaged and unusable and or they are broken off during transit. To think that a delicate Radio Frequency Identification (RFID) tag could withstand this environment is questionable. The SAIC report dated July 11, 2003 clearly identified their short comings. The report is available on-line and is entitled *Cargo Handling Cooperative Program*.

To try and place sensitive and expensive electronic elements into or on to a container and ask that they be monitored by a port security system would be asking for trouble. Who will pay for it? Can it be recovered? Who is responsible to monitor it and where? How will we affix it to the containers? Can it stand up? What will it take to read it? What frequency will it operate under? What are the standards? What software will be chosen? Who owns the problem it if it fails?



The Navablock theft deterrent device with cable seal.

Products such as active RFID tags have been touted as the coming technology for almost five years but they fall way short of being viable when it comes to security. In fact they offer no security at any level. They barely have been used in any industry because they cannot be read around or in contact with metal, they cross talk, they break, the batteries wear out, they cannot take abuse, they are expensive and this just touches on some of their short comings. They are great in a controlled environment as locators, as inventory tools and as data collectors; they are not ready for security applications.

RFID tags are expensive to use, to own, to verify, to get back and to audit. To analyse the RFID industry as it relates to security you need to understand very basic electronics. Radio signals are blocked by metal such as containers are made of. Hundreds of containers in a yard facing different directions require many expensive antennas and a costly infrastructure system. Each system of each manufacturer may be different so which will people use since there is no agreement on an electronic operating platform?

Electronic readers needed to interrogate active tags are typically antenna based and must be deployed throughout a container yard. This infrastructure requirement would be extremely costly and provide little else than a location scan but with many serious shortcomings. RFID tags can be removed and replaced, they can be broken off and therefore not read at all, making that container invisible without a physical check, which makes the need for RFID redundant if you have to go out and find it. The tags need to be applied at origin. Can you see shippers in Jakarta holding up a shipment because they need tags! RFID tags have no relationship to the lock mechanism hence they provide no security at any level just location and data if they were to work. Tags are expensive and must be funded by shippers who will get no tangible benefit from them and no possibility of recovery and re-use. The tags must be able to be read at every port and by every carrier in order to render any level of reliable real time information. The infrastructure of many foreign ports has not reached the computer level much less that of RFID readers. The information is only as good as the software, and interfacing software between many companies and operating systems is a joke. Rights of authorship on the choice of software and hardware out of all of the existing tag manufacturers would begin World War 3 in the industry. The requirements of a port to implement a new infrastructure to accept all possible tags and integrate them to one common Local Area Network (LAN) to read them would be a five-year project at best. To accept RFID information implies that the tags would solve some portion of the problem when in fact they would create a logistical and database nightmare. Indeed, the data collection and retention element of RFID has now become a tremendous debate.

The MKIIB lock is used on a container.

No one wants their information regarding shipments, volumes, frequency, supplier and recipient data floating in cyber space. Without physical interaction with the container and its lock or seal you can never be certain that the box was never opened, only that the tag is somewhere in your yard, hopefully still attached to the original container and not on the floor! Security can only be achieved when it begins at the beginning, offers the appropriate protection based on the threat and has audit characteristics and physical checks throughout the logistic cycle.

Conclusion

Being critical is only useful when you can support that doctrine with credible solutions. Containers are unprotected storage warehouses that have many ways to beat them. Nothing can be done to secure a container completely, however the fact that the doors are the easiest and most readily available portal of entry dictates that they be the first line of defense.

Barrier defense systems work best to keep people out, yet indicative systems make it easier to detect if someone got in. To avoid surreptitious entry, a good system will employ both indicative seals such as self voiding door seals and barrier seals such as cables or locking bars.

Locking bars secure the keeper bars of the container itself and prevent the door from being opened. The fact that lock bars keep out everyone without a dremil wheel means that they are the most suitable barrier device available. These are typically cost-effective tools that area easy to apply and impossible to remove with common tools outside a cutting wheel. Cable seals which also wrap and retain the keeper bars present a reasonable second tier approach. They are removable with bolt cutters, but they typically cannot be replaced as a bolt can.

Last but not least, are indicative self adhesive seals applied across the doors to indicate openings? Indicative sealing devices used without visual scrutiny yield no results. All security seals and security countermeasures require a detailed written plan, training and consistency. No security product can offer complete protection yet when used correctly, consistently and monitored bars, cables and seals can give us a leg up on protecting the world's supply chain.

ABOUT THE AUTHOR

Mr. Hoffer is a graduate of Northeastern University holding a Bachelor of Science degree in industrial psychology. He also holds an associates degree in transportation and traffic management.

Mr. Hoffer is president and CEO of CGM Security Solutions, Inc., which he created in 1977. For the past 37 years he has designed and patented a number of theft control products. His training in theft control science started with his military career in 1965 where he worked in Vietnam.

Mr. Hoffer and CGM hold top secret clearances. Mr. Hoffer owns numerous patents in cargo security technology and for tractor and trailer security products.

For the past 4 years Mr. Hoffer has been the chairman of educational events for the International Cargo Security Council, Chairman of the Seal Committee and the co-chairman of the ICSC GMATS Masters degree programme. He is also a member of the Transportation Consumer Protection Council, the Maritime Security Counsel, the International Organization of Packaging Professionals, the Conference of Logistics Managers, the Truckload Carriers and American Trucking Association and the American Society for Industrial Security. He frequently teaches at the ASIS national seminars, the U.S. Merchant Marine Academy, and at venues across the United States.

ABOUT THE ORGANISATION

The International Cargo Security Council is a professional association of cargo transportation and security professionals from the entire spectrum of cargo security: Air, truck/rail, maritime, and intermodal. Its success hinges on each member's personal concern for the safe and secure movement of the nation's commerce.

The ICSC Seal Committee is made up of 25 member companies that manufacture, distribute, or consult regarding seals or seal security. As a group the committee is very active in writing best practices and standards. Last year it assisted the ISO by drafting its opinions and concerns regarding the development of the ISO/PAS 17712 document. The Committee is also very active with all US government agencies including the Department of Homeland Security, Customs and Border Protection, and the Transportation Security Administration.

ENQUIRIES

Erik Hoffer
CGM Security Solutions
Punta Gorda
FL 33955
USA

Tel: +1 (941) 575-0243
NJ office tel: +1 (732) 448-1400
Web site: www.tamper.com

International Cargo Security Council
#3 Church Circle – No. 292
Annapolis
MD 21401-1933
USA

Tel: +1 (410) 571-7913
Fax: +1 (410) 571-8294
E-mail: admin@cargosecurity.com
Web site: www.cargosecurity.com