The Demand for Security

Dr. W. Russell Neuman, University of Michigan

Prepared for IBM Global Business Services,
Customs, Borders, and Revenue Management

October 2008

The Demand for Security

Executive Summary

For many centuries military lines of battle and clearly identified national borders defined the frontiers of security. In WWI and WWII the battlefront in effect served to define the borderline of national sovereignty. But more recently in wars of insurrection, insurgency and global terrorism, potential threats to security are no longer clearly defined by borders. In today's world, border security, homeland security and national security are inherently intertwined.

This whitepaper addresses a very pressing question for public officials, policy and budget planners and security professionals — how do we assess security in a globalized and interpenetrated world? How do we know if investment of scarce resources in security systems results in the mere appearance of security or the real thing? It is a difficult question. To answer this question, we start with the issue that motivates our concern in the first place - the demand for security.

This analysis reviews ten structural and institutional factors that arise in the domain of international border management, and travel and trade security. These factors represent significant impediments to a successfully functioning 'market for security' - permitting a rational and dynamic allocation of the limited resources. The ten factors are:

1) ***Indirect Demand*** - only very rarely do those individuals or groups seeking security actually make decisions about implementing security systems and procedures. Instead they routinely rely on expert agents, security professionals, to do it for them. There is an extensive literature about market distortions that arise from this phenomenon of 'agency'.

2) ***The Difficulty of Assessing Security Effectiveness*** - we tend to have detailed information on the cost of each security investment but only fragmentary information or no information at all on what difference each investment might make to overall system security. Because of this elusive nature of security effectiveness, critical decisions concerning 'return on investment' may be in error.

3) ***The Costs of Institutional Fragmentation*** - bureaucratic turf issues among diverse security institutions and agencies complicate the implementation of security procedures in the field.

4) ***The Challenge of International Collaboration*** - coordination within an institution or nation state is difficult enough; coordination across international boundaries is especially challenging.

5) ***The Inertia of Legacy Systems*** - The difficulty of migrating and modernizing IT systems is a broadly recognized challenge especially in the public sector. Case studies are reviewed drawing lessons for border security systems.

6) ***The Irregular Distribution of Threat Incidents*** - In many security systems, actual intrusions or security violations are rare events, sometimes generating false confidence and lax procedures.

7) ***The Multidimensionality of Threat*** - Border security agencies are held responsible for maintaining security with regard to a complex array of threats including potential terrorism, illegal migration, visa overstays, detection of diverse forms of contraband, and customs duty compliance. Public attention and the politics of funding, however, tend to focus narrowly on a few high profile cases, primarily related to terrorism.

8) ***The Dynamic Character of Threat*** - When new security techniques are put into place, those with malevolent intent will adjust their tactics and practices requiring in turn further agility and dynamism in law enforcement.

9) ***The Demand for Facilitation*** - The pressure from commercial interests in both passenger travel and cargo transport for facilitation of border crossings complicates systematic security provision.

10) ***Privacy Concerns*** - the need for appropriate protections against unauthorized and inappropriate use of personal and commercial data collected in the course of security procedures complicates security system design and legitimate exchange of information among various security units.

In the examination of these structural issues, examples are drawn from American, European and Asian case studies and initiatives in international cooperation.

Having identified and examined these issues, the analysis turns to a series of steps that should be considered in response. First and foremost is the need for structuring independent and systematic assessment of the effectiveness of security procedures expanding on the military tradition of 'red teaming'. A case is made that to insure the independence of these assessments, both new statutory guidelines and the creation of new assessment institutions may be necessary. Other strategic responses (a partial list) include:

- Increase incentives for effective use of feedback by security professionals
- Increase public education and awareness of specific risks
- Increase public awareness of benefits of sustained security
- Mandate secure and fully audited interoperability of information systems
- Rotate personnel across institutional roles
- Develop new institutional venues to facilitate collaboration
- Develop new mechanisms for multinational security systems bidding and acquisition
- Demonstrate cost savings that accrue to effective collaboration among security units
- Demonstrate security benefits that accrue to effective collaboration among security units
- Active red teaming to keep security personnel attuned to statistically rare but significant risk events
- Expand implementation of Service-Oriented Architectures (SOA) in extant and evolving IT systems
- Investment in advanced biometrics and identity management systems

The Demand for Security

"Safety from external danger is the most powerful director of national conduct."

– Alexander Hamilton
Federalist Paper No. 8

Public authorities are held responsible for many important outcomes. They are supposed to stimulate economic growth, provide for education, health and welfare services and provision public thoroughfares and postal services among other responsibilities. But one outcome rises far above all the others. That is public security. Regimes rise and fall on their capacity to provide security. The defense budget is often politically sacrosanct. In many cases it is the largest component of a national budget. Taking a stand against terrorism virtually precludes any political opposition to one's rhetoric. In the public sphere, security represents something of a sacred value, a prerequisite for all the others.

We can treat the relationship between governments and their citizenry as a marketplace. Such an analytic tool has been used by leading thinkers in political science and public affairs for many decades. Governments provide services and in return citizens, with varying enthusiasm, support the regime, pay taxes, volunteer for military service and the like. In such an analysis we find that the demand for security lies at the center of public life.

But security is also an elusive phenomenon. How do citizens actually know they are secure? How are they to assess risk? How is it possible for taxpayers to gauge their return on investment (ROI) for their collective expenditures for security systems? How do thoughtful and conscientious public officials evaluate alternative investments in security policies, practices and technologies?

The Security Shoppe

There are several classic Monty Python skits that derive from a hilarious exchange between a vendor and a customer. Most famous, perhaps, is the supply-chain challenged cheese shop and the pet shop's rather passive parrot. These scenarios of incongruous transactions resonate with audiences around the world because so many of our real world experiences in the marketplace are frustratingly Pythonesque. Hold that thought for a moment as we try to make a point about the marketplace for security.

Imagine, if you will, your favorite Python character earnestly approaching a counter to order some security.

Customer: I'd like to buy some security please

Clerk: (Cheerily) Yes, of course, you have come to just the right place. How much security do you want?

Customer: (Stroking his chin) Well, let's see, how much does it cost?

Clerk: Well that depends on the risk. If there is absolutely no risk we provide security free of charge…gratis… it is our pleasure to guarantee security. If there is some risk, as any twit can see, we are obliged to charge.

Customer: Oh, I see, well, how much do you charge?

Clerk: (Without missing a beat) Depends on the amount of risk.

Customer: Sorry, I'm new at this; just exactly how much risk is there?

Clerk: (Still smiling) Haven't a clue

Customer: (With increasing frustration) Well then, how do you bloody well know what to charge?

Clerk: That's easy. How much are you willing to pay?

[The script continues with increasingly absurd answers to rather reasonable questions.]

The unique marketplace of the supply of and demand for security is the focus of this whitepaper. In the post 9/11 world, it bears especially careful scrutiny. The once separate domains of law enforcement, border and maritime protection and military defense have become blurred and intertwined under the heading of homeland security. Fast-changing and highly complex international supply chains and instantaneous global digital communication are challenging long accepted assumptions about security best practices.

This whitepaper has a central thesis - the special dynamics of the marketplace for security generate a series of institutional impediments and market distortions leading to misallocation of resources, dangerously insufficient and delayed investment, and misleading market signals. The paper is organized around a matrix of ten institutional problem areas that sustain these market distortions. The focus here is customs and border management, so we will draw on examples in international trade and travel. The concluding section will enumerate a series of concrete steps that should be considered to respond to these challenges.

THE SECURITY MATRIX

We do not commonly use market models to think about national security and the threat of terrorism so it may strike the reader as an odd choice of analytics. Security cannot be partitioned up and sold by the dozen. Security is normally a public sector monopoly and not subject to competitive provision. It draws on fundamental human fears and emotions and many citizens would much prefer to ignore such issues rather than think hard about them. Security yields only reluctantly to such tools of analysis — and that is precisely the point of this exercise. The 9/11 attackers were devastatingly creative and fresh thinking in their conspiratorial designs. We will need to be just as creative and agile in our institutional responses, probably more so. Professional achievement and leadership in security system design and implementation demands fresh thinking.

Our analysis of the demand for security leads us to identify ten interrelated structural challenges in security systems. Each responds to the special dynamics of this domain, illustrating, yet again, that security markets do not behave like other markets typically do. We refer to these ten factors as the Trade & Travel Security Matrix. (See Figure 1)

1) The Distortion of Indirect Demand

Citizens, if asked, will demand strong borders, secure transportation and stringent protection against terrorism. But they are not called upon to manage complex multimillion-dollar procurements for video monitoring technologies, IT networks, security staff training, biometric identity systems and X-ray scanners. The ultimate citizen demand for security is filtered, interpreted and refracted through literally dozens of institutional processes. Whether the ultimate procurements reflect what an intelligent and informed citizen would judge to be prudent is open to debate.

Economic analysis provides several vocabularies for understanding these complex processes of institutionally filtered demand. One of the most common is the notion of 'indirect demand.' The key underlying concept is 'agency' - the notion that one would not enter a complicated technical marketplace directly but would rather contract with an expert agent to make decisions concerning value and benefit on one's behalf. Typical examples of expert agents are architects, investment counselors, attorneys, talent agents and home decorators. Although agents typically have a quite sophisticated understanding of a technical marketplace, its vendors and norms, for example, the classic problem of agency is that agents may have incentives and goals that conflict with the principals who hire them. Characteristically, lawyers billing by the hour may gratuitously (perhaps even subconsciously) lengthen a negotiation process or a decorator working on a percentage may opt for the more expensive chandelier.

The phenomenon of agency and indirect demand is an inevitable element of the security

Figure 1 The Trade & Travel Security Matrix

Structural Issue	Description
1) Indirect Demand	Security is a public good rather than a private one, so public demand for security is diffuse and indirect as typically large and sometimes inefficient public bureaucracies may attempt to assess 'demand' and provide a 'supply of security.'
2) The Difficulty of Assessing Security Effectiveness	Security officials only very rarely have systematic and reliable information on when security and deterrence measures are, in fact, successful.
3) The Costs of Institutional Fragmentation	In most countries the public and private institutional responsibility for security is spread out across a complex matrix of different commercial, border, law enforcement and military institutions.
4) The Challenge of International Collaboration	Border security inherently requires international cooperation and interoperable systems, always a difficult issue in matters of security and law enforcement.
5) The Inertia of Legacy Systems	Given the indirectness of demand and the limited capacity to assess the effectiveness of security systems, the normal market pressures for updating technical and supporting IT systems infrequently overcome the inertial path of least resistance in attempting to patch up aging legacy systems.
6) The Irregular Distribution of Threat Incidents	Significant threats to homeland security are relatively rare and likely to involve unique circumstances that make prediction and planning extremely difficult.
7) The Multidimensionality of Threat	Border security in particular involves elements of terrorism, illegal migration, contraband, custom duty compliance, theft, and commercial extortion, very different risk phenomena that are often conflated in the rhetoric of security policy.
8) The Dynamic Character of Threat	When new security techniques are put into place, those with malevolent intent will adjust their tactics and practices requiring in turn further agility and dynamism in law enforcement.
9) The Demand for Facilitation	There is forceful pressure from powerful commercial interests in both passenger travel and cargo transport for facilitation of border crossings through trusted traveler and authorized trader programs of various sorts.
10) Privacy Concerns	Both privacy activists and significant portions of the mass public express concern about the possible abuse of identity management systems, conveyance tracking and biometrics.

domain. Those who benefit from security routinely rely on security specialists as their 'agents'. The institutional challenge is to minimize and correct for the realistic possibility that the agents' interests and perceptions may at times vary from those of the principals and distort the dynamics of supply and demand. Although only relatively rarely addressed in security studies, these phenomena are well understood in the study of business practice and complex organizations. We will review a series of market distortion 'effects' that are particularly relevant to the provision of security systems.

The Michels Effect. The Swiss economist Robert Michels famously espoused his 'iron law of oligarchy' in his studies of organizational dynamics in Europe and the United States a century ago. It is paradoxical, he noted, that organizations created for a specific purpose such as labor unions or political parties evolve a professional elite leadership that gradually but inevitably start to define their goals in terms of the perpetuation and growth of their institution. These goals, he notes, may well be at odds with the original purposes in creating the organization. Bureaucracies, of course, are famous for defining their own staffing and budgetary growth as their primary organizational objective.

These market distorting dynamics are particularly tricky in the domain of security because, as we shall see, frequently in the analysis of the security matrix the metrics of success in the provision of security are ambiguous. One might conclude that the Michels Effect will lead to an overprovision or overinvestment in security. That may be true on occasion in the case of staffing decisions, but it turns out that there are other factors at work (discussed below) that lead in just the opposite direction - under-investment in security systems - so the dynamics are complex.

The Commons Effect. One well-recognized market dynamic of particular significance in the security arena is the 'tragedy of the commons.' Pooled or shared resources are characteristically over used and under resourced. Security is a classic example of a public good, a shared resource. Unlike most goods, security is non-rivalrous - providing more security to one individual within a perimeter does not mean providing less to others; in fact, in practical terms it means providing increased security for all. The key here is the related 'free-rider' problem. Because it is not practical to exclude someone from the benefits of a security perimeter, say an individual who refuses to contribute his share to the collective cost of security, it may be difficult to provision security resources. The individual naturally focuses on private costs and private benefits and casually calculates that some vaguely defined 'other' will take care of collective public issues such as security. The classic example would be choosing to invest in a high-tech home security alarm while voting against a property tax increase designated for the county sheriff's office.

The Complexity Effect. In the modern world the key to security is technological superiority. (Actually, as military historians are quick to remind us, technology has always played a central role. Even simple inventions like the stirrup in the Middle Ages revolutionized the role of a cavalry in warfare.) Security systems tend to be complex, large-scale, multi-element structures. Complex systems involve long periods for development, large multi-organizational development teams and large budgets. Engineering groups as part of development team may have only the vaguest idea about how elements of a system outside their immediate purview may work. If that is the case, it is easy to understand how the public at large and even those responsible for security policy and budgets are challenged by the decisions that must be made.

In summary, markets work best when the consumer is informed, responsible and receiving feedback on market decisions. In the institutionally complex and mediated indirect market for security, none of these important mechanisms is fully engaged and working to maintain efficiency. The fundamental character of security systems in the modern world leads us to conclude that the market will unavoidably be indirect. The challenge is to compensate as carefully as possible for the potential market distortions that typically result. Some recom-

"Upon discovering that Weeki Wachee Springs, his Florida roadside water park had been included on the Department of Homeland Security's list of over 80,000 potential terrorist targets, its marketing and promotion manager, John Athanason, turned reflective. 'I can't imagine bin Laden trying to blow up the mermaids,' he mused, 'but with terrorists, who knows what they're thinking'."

— John Mueller, Professor of Security Studies, Ohio State

mendations in that vein are included in the final sections of this whitepaper. Of the difficulties of the indirect market for security, the most troublesome missing market mechanism is the lack of timely, accurate and systematic feedback. That issue is addressed in the following element of the matrix.

2) The Difficulty of Assessing the Effectiveness of Security Systems

One might characterize security assessment as the paradox of the missing denominator. Customs and immigration officials, for example, have learned to have statistics about seized contraband, false visa and asylum applications at the ready. The following facts, for example, have been prominently featured in recent annual reports and press releases.

UK Customs officers seized 1.6 billion cigarettes and 5.4 million liters of illegally imported beer, wine and spirits in 2003.

Australian authorities seized 610kg of cocaine and 90.6kg of amphetamine type stimulants in 2005-06.

On Feb 27, 2008 near Yuma Arizona the US Border Patrol seized a Ford F250 and a Jeep Cherokee carrying 3,340 pounds of marijuana with an estimated street value of $2,670,000.

Since the creation of the Immigration and Customs Enforcement unit in the US Department of Homeland Security, ICE fugitive operations teams have arrested more than 44,000 illegal aliens, including 33,343 fugitives and 10,777 non-fugitives. Of these, more than 20,000 had criminal records.

The South African Revenue Service conducted 4,706 anti-smuggling seizures, seizures of counterfeit goods valued at R354-million, as well as the seizure of cigarettes worth 250 million Rand.

The Indian Central Board of Excise and Customs recently seized 22,333.741 Kgs of smuggled silver valued at 19,336,676 Rupees.

The official world of customs and border management, of course, lives by such official statistics and the occasionally gripping details of an uncovered illegal operation. But in the calculation of success and efficiency of border security operations these are only numerators. The denominators are unknown. What is the ratio of success to failure? Security authorities know how many were caught, but cannot accurately assess how many were missed. A particular irony is the American Border Patrol's dogged pursuit of typically small groups of would be illegal aliens on the Mexican border as it is widely acknowledged that over 12 million illegal immigrants currently reside in the US. The Border Patrol is dutifully and appropriately fulfilling its mission, of course. It is the broader border policy context that is paradoxical.

It is relatively easy to report that arrests or seizures have risen or declined. But it is difficult to document whether either might represent a constant but unknown percentage of varying levels of illegal attempts. A central element of border security, of course, is not just arrest and seizure but deterrence. This critical factor all but defies meaningful assessment. How is it possible to systematically determine how many smugglers, customs fee avoiders or illegal immigrants were literally deterred from attempting illegal acts because of increased surveillance or new security procedures?

Red Teams and White Hats.

Actually, it is possible to systematically assess the capacities and possible weaknesses of security systems. This prospect of systematic assessment will become a central element of this paper's recommendations. In military culture the practice of testing formations and strategies with simulations or war games is often referred to as 'red teaming' as the simulated enemy is designated as the red team and the regular military unit as the blue team. In computer security the terminology is 'white hat hackers' as an outside team of computer specialists is hired to test an IT system's security through a variety of intrusion or denial of service techniques.

Taking the attacker's view can be a challenge for many government and business leaders, but it is an essential step toward accurate prioritization of threats.

—Brad Westpfahl, IBM

"The eBorder initiative was surprisingly successful in eliciting interagency cooperation. I believe it was a result of two factors - first, there was high-level sponsorship, and second, it was well organized so each agency saw a direct benefit from active participation."

-Senior Official in the UK Border & Immigration Agency

Surprisingly, given the obvious advantages and benefits of systematic red teaming, it is only infrequently utilized in military and computer security contexts and extremely rarely in customs, border and identity systems. Why would this be so? Four related factors appear to be at work.

First, red teaming runs counter to the culture and traditions of the security domain. Professional advancement is associated with designing security systems and procedures, not breaking them, even with positive intent. Considerable effort is sometimes exerted to avoid being assigned to the red team. Law enforcement officials, although it provides a clear professional advantage, simply find it difficult to 'think' like the violators they pursue.

Second, red teaming is disruptive. If an invasive white hat cyber attack disrupts an IT system, the system still has to be repaired. Significant down time is not practical on many real-world systems. There are natural concerns about possible vestigial damage to databases and source code. Keeping systems up and running tends to exhaust staffing and technical resources precluding serious investment in red teaming.

Third, security officials prefer to rely on what they consider 'real' data from naturally occurring intrusions and violations detected by routine monitoring systems, although, as noted above, there remains the problem of the missing denominator.

Fourth, and perhaps most significantly, officials seldom seek out what might turn out to be bad news. Why ask for trouble? Why cause trouble for your colleagues with whom you may be working for many years? It may seem glib to characterize highly intelligent and hard working security professionals as instinctively avoiding bad news, but it is a sociological reality that merits some attention. From the point of view of the institutional decision maker in situ, with limited resources and many demands, priorities need to be set and red teaming tends to sink to near the bottom of the list. If some security procedures are found to be ineffective, that may result in a reduction of budget and staffing — hardly an optimal outcome. If weaknesses are detected, they need to be explained. It is a bit of a lose-lose proposition.

Assessing the effectiveness of security systems is fundamental to the notion of a market for security. Question number one - what is the return on investment for each element in the system? We tend to have detailed information on the cost of each security investment but only fragmentary information on what difference each investment might make to overall system security. Because of the elusive nature of the phenomenon of security effectiveness, the security ROI equation may frequently be out of balance.

3) The Costs of Institutional Fragmentation

Perhaps in another decade most of the world's nation states will have integrated agencies responsible for homeland security, border control and customs; but currently the norm is separate agencies. The processing of identity documents, passports, visas, border crossings, water and air ports of entry, commercial customs, agricultural inspection, coastal security, national security, infrastructure security and local law enforcement most often represent separate institutional silos with sometimes competing bureaucratic interests, different procedural traditions and limited intercommunication which frustrates coordination. It represents a very significant institutional challenge.

The American effort, for example, to bring together 22 separate agencies and 180,000 federal employees under the banner of a new cabinet level Department of Homeland Security has been a limited success. Secretary Chertoff has candidly acknowledged that many turf issues remain and the federal Office of Personnel Management reported in 2006 that DHS ranked last or near last among 36 federal agencies in personnel morale and management capacity.

The turf and coordination issues turn out to be well-studied questions in the study of business and complex organizations. A series of classic works by Stanford sociologist James March and colleagues published originally in

"Controlling information is power, and they don't want to let it go — it is as fundamental as that."

New York City Police Commissioner Raymond W. Kelly explaining difficulties coordinating anti-terrorist intelligence with the FBI

the 1950s provide the basic analytic vocabulary. They examine the conditions under which subunit goals come to differ from other subunits and at times conflict with the overall goals of the entire organization. As authority is delegated to subunits to take advantage of their specialized expertise, the subunit staff comes to internalize those subunit goals, emphasize their importance and minimize the expertise and goals of other subunits in a natural competition for scarce internal resources. Harvard's Graham Allison conducted the classic case study in this area in his research on how each of the armed services came to loggerheads in advising President Kennedy during the Cuban Missile Crisis, each emphasizing their special capacities in land, sea and air military power.

Inter-agency (or subunit) competition is not entirely a negative phenomenon. The fact that staff internalize and invest energy in the goals of the subunit is generally a positive organizational outcome. Some level of properly managed competition among units can also represent a positive development. Dysfunctionality, however, derives from three undesirable conditions:

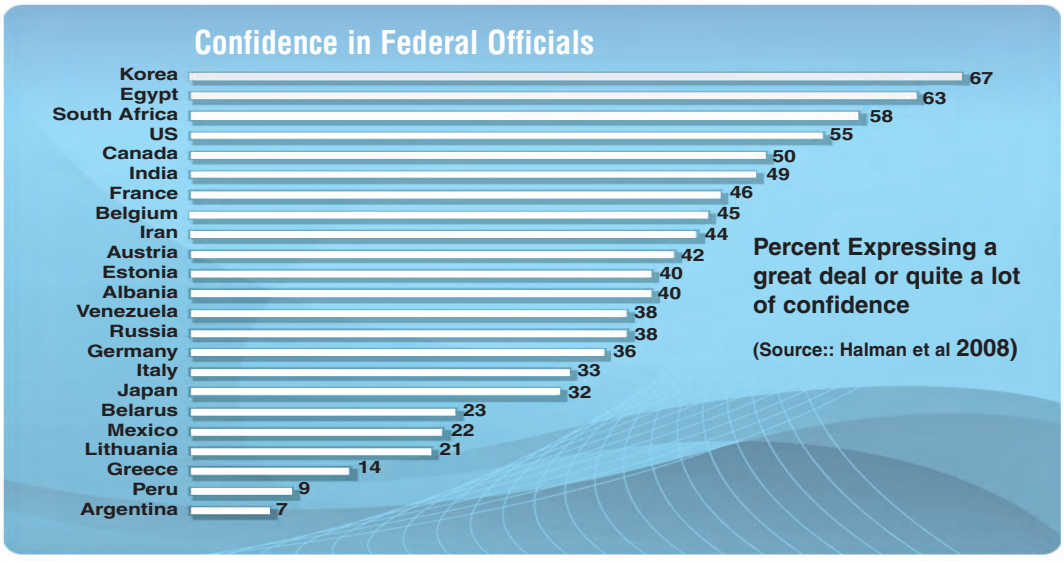
- When subunit competition leads to distortion in information processing and decision making within the subunit,
- When subunit competition leads to a decrease in information sharing across subunits or a systematic bias in what information is shared,
- When subunit goals begin diverge from broader organizational goals.

These challenges are especially difficult in the area of border security because subunit cultures have evolved and crystallized over many years and are resistant to reform. Further, because systematic assessment of security outcomes is elusive, the capacity to allocate resources among units is complicated and competition for resources proceeds on ideological rather than performance-based principles. Finally, because in the domain of security it is important to protect confidentiality of 'sources and methods,' sharing information such as watch lists is particularly difficult both across subunits and across organizations.

4) The Challenge of International Collaboration

Customs, ports and border management issues are inherently international. Although each side of a border transaction is managed by a nation state, the processes inevitably involve the movement of goods and people internationally. Especially in a globalized, electronically connected, post 9/11 world, success in this domain will hinge on the creation and maintenance of reliable and secure real-time international systems of information exchange and information verification.

Old-fashioned one-sided notions of national defense and boundary maintenance associated with images of moats or walls and fences provide inappropriate models for the future.



"Some people have been critical of the efforts of US-VISIT, but if you look around the world you will see in nation after nation that they are copying our architecture for border systems."

— Senior Official at the US Department of Homeland Security

The Great Wall of China provides a wonderful architectural and spiritual symbol but a poor model for modern border management. (It turned out to be a poor historical model as well as it famously failed to prevent the Manchu invasion in the Seventeenth century.)

Although it is well recognized that international collaboration is desirable, the different cultures and the shape of public demand in different countries makes it clear that a one-size-fits-all solution may be unrealistic. Note, for example, the dramatic variation from country to country in the chart above in relative expression of confidence in federal officials. (These are overall ratings; evaluations of border and customs officials may differ significantly from these data.)

International collaboration, however, remains a particularly difficult challenge in the security arena. Part of the problem derives from the fact that the international organizational venues for cooperation largely replicate the internal agency fragmentation of responsibility. The World Customs Organization (WCO) restricts itself to customs issues. The International Civilian Aviation Organization (ICAO) focuses with some success on technical interoperability standards for travel documents. Various UN agencies and diverse NGOs address immigration and asylum issues. Regional organizations such as APEC and ASEAN sponsor some travel security initiatives. The G8 and the associated Roma-Lyon venue have attempted to address issues of security coordination and information exchange from time to time. INTERPOL continues to provide a data system I-24/7 for exchanging information on lost and stolen passport numbers. The International Maritime Organization (IMO) addresses issues associated with maritime safety such as the International Ship and Port Facility Security Code (ISPS) as an amendment to the Safety of Life at Sea Convention (SOLAS.) All in all, the alphabet soup of international entities is fragmented, intimidatingly complex, unevenly organized and resourced, competitive, bound by numerous historical traditions, and generally supported by a weak tradition of international law that constrains the prospect of enforcing compliance and cooperation.

5) The Inertia of Legacy Systems

The difficulty of migrating and modernizing IT systems is a broadly recognized challenge in both the public and the private sector. Unlike some of the other factors addressed, this one is not particularly unique to the border security domain, but it represents an important problem nonetheless. And the appropriate response is not unique either - it is the thoughtful and strategic implementation of Service Oriented Architectures.

Although there are upgrade efforts currently underway, for example, the United States primary data system for border inspection and customs, including the controversial matter of Passenger Name Record (PNR) review for international air travel, remains a primitive green-screen, mainframe-based architecture -The Enforcement Communication System/ InterAgency Border Inspection System (TECS/IBIS) — setting something of a dubious record of thirty years of service. A recent examination found only one other institution (the City of Indianapolis) still using this ancient IT architecture. Managed by US DHS CPB in Newington, Virginia, the on-line and batch components consist of nearly 4,000 programs supporting a database of more than a billion records, 2 million transactions per day and a geographically dispersed user community of 30,000 users at 1,800 sites.

How do such overtaxed and overextended security data systems persist? The answer is straightforward and probably familiar to most IT specialists, especially in the public sector. At the margin, it always appears to decision makers to be easier to add one more element or patch or extension to an existing system than to undertake the long, expensive and risky task of re-engineering the full enterprise architecture.

UC Berkeley's Shapiro and Varian have studied the phenomenon and found it so powerful that they recommend it as a business strategy in the software business - calling it 'Lock-In' which has something of a better ring to it than the inertia of legacy systems.

The process of full-scale system upgrades is intimidatingly complex. Famous cases like the FBI's Trilogy Virtual Case File Program upgrade between 2000 and 2005 cost over $100 million (some estimates run twice that figure) only ultimately to be abandoned as unworkable. The Bureau has been forced to rely on the antiquated 1970s-era ACS system while a new upgrade design is being undertaken and is scheduled to be completed in 2009. The lessons from that awkward failure are, none theless, worthy of attention as the project demonstrated a systematic failure of traditional software engineering practices:

- Lack of a viable overall architectural model from the outset which led to poor design decisions.
- Micromanagement of software developers.
- Multiple changes in specification.
- Scope creep as the requirements were added to the system design while the upgrade continued to fall further behind schedule.
- Code bloat due to changing specifications and scope creep.
- Ongoing staff turnover.
- Assigning additional staff to the project as it was falling behind, which made it later still, sometimes referred to as Brooks's law.
- Planned use of a flash cutover deployment which added risk and development problems
- The engagement of DOJ personnel with minimal computer science background as managers and engineers.

Sometimes the problems with legacy systems are simply a matter of insecure process design. One of the least secure passport issuance systems is still in place in Germany, a situation frequently pointed out by our German colleagues who are addressing the issue. The system is highly decentralized relying on issuance from local authorities in part a legacy of the post WWII defederalization effort of the occupying allied powers. Because there is no central national identity database and no biometric confirmation, individuals can request and will routinely be issued multiple passports under potentially different identities. The authorities are well aware of the problem, but turf issues and institutional inertia are likely to delay system redesign and implementation.

6) The Irregular Distribution of Threat Incidents

Thus far in this analysis we have been focusing primarily on the supply side of the demand-supply equation addressing various institutional complexities in responding to demand. In the next three elements of the matrix, however, we turn our attention to the character of the threat events that stimulate demand for security in the first place. In each case we confront characteristics of demand not typically encountered in commercial marketplace dynamics.

Security threats are rare events. This is fortunate, of course. The less frequent the better. But this distribution of threat incidents generates special problems for the normal functioning of demand and supply. To respond intelligently, we need to employ sophisticated modeling and simulation tools.

The classic case is widely recognized and the subject of numerous anecdotes. We refer to the frequently repeated phenomenon of strengthening security after a prominent threat event rather than before it. Perhaps it should simply be written off as human nature. The childhood epigrammatic version of this lesson (probably a legacy of the rural origins of popular cultural) takes the form of closing the barn door after the horse has taken flight. For the professional programmatic design of security systems, however, this is a serious design challenge. Extended periods without threat lead to an undue sense of security, lax procedures and inattention. Post threat tensions may lead to an overreaction and inefficient and inappropriate security responses. Military texts address this issue as a challenge for military preparedness in garrison and a challenge for long term military budgeting. It is, in effect, a classic distortion of demand and supply dynamics attributed to the functioning of collective human cognition. Fortunately, mathematicians and economists have developed useful tools for addressing these classic issues.

The Good Reverend Bayes. Amateur mathematician Thomas Bayes' posthumously published theoretical treatise on probability in 1764 has become not just a classic but the basis of an entire subfield of statistical modeling especially

appropriate for the analysis of rare events. Without going into his famous equation and the underlying mathematics in detail it may useful to describe its logic in straightforward prose.

Basically his model draws the analyst's attention to what we have come to call 'priors' or prior estimates. This is particularly useful, for example, in security design in response to natural disasters. From a careful analysis of historical data we can calculate security precautions necessary for protection from a 100-year flood. We understand the likelihood that this level of defense being necessary in any given year is one in one hundred. Depending on the costs at the margin we may or may not be convinced that the appropriate security investment level would be determined by a 1000-year flood. In any case, it represents a useful way to think appropriately about relatively rare threat events.

In the domain of security design, we recognize the importance of assessing threats over longer periods of time. If we have information that a serious threat has occurred once in the last two days — a problem. If we know also that this observed threat in the last two days has manifested itself twice in the last ten years — a problem in appropriate perspective. Over reaction to threat can be just as dangerous as under reaction if it leads to misallocating priorities in security provisioning.

A Downsian Analysis. Economist Anthony Downs studied public reactions to social problems and developed a staged model of quickly growing and gradually declining support for collective response. The basic element in his model is the realization that publics have limited attention spans. Although Downs did not include this in his original analysis, the phenomenon is well represented in public support for military engagements over time. Long wars test public patience.

Accordingly, we confront a paradox of sustained funding for border and transport security procedures and technologies. Public support for security investment is derived from attention to dramatic (if rare) events. People buy fire insurance for their own home after witnessing a dramatic fire at a neighbor's home. That may make psychological sense but not actuarial sense. The challenge to border and security professionals is to manage what may turn out to be a cyclical level of funding into an optimally designed continuity of security. In the design of security architectures it is useful to take full advantage hard historical and actuarial statistics on risk (whenever available) and the helpful models of the good Reverend Bayes.

"There is a real sea change underway in national visa issuance policy around the world. It used to be based simply on the national origin of the applicant. Now visa authorities are keying their review procedures on specific groups from within other countries."

-Senior Official in the European Commission

7) The Multidimensionality of Threat

There is a shorthand language that develops in border and customs management and planning. The reference is to the 'bad guys.' We design our systems so the bad guys can't get through. Such language is handy in hearings and with journalists. It is straightforward shorthand and universally understood. The undifferentiated bad guys.

Usually in the post 9/11 world the phrase is interpreted as a reference to terrorists. In some contexts it might be interpreted as a reference to hardened criminals and smugglers or simply illegal immigrants. In any case, it is procedurally convenient in justifying security budgets and procedures to highlight the most dramatic of threats. This may be seen as a derivative of factor six above concerning the distribution of threat events.

Mundane threats such as simple theft in cargo supply chains may be less dramatic than terrorism, but are nonetheless a central element of meaningful security investment. The bottom line is that although it might be seductively easy to aggregate threat, careful planning requires disaggregation. Again, we propose a strategy of sophisticated threat simulation and assessment to guide security design and investment.

Border security professionals are under continuous pressure to control costs and minimize inconvenience and delay to travel and trade. Nonetheless, they are held responsible for maintaining security with regard to a diverse set of risks ranging from a variety of forms of terrorism, to illegal migration, diverse contraband issues, custom duty compliance, theft, and even commercial extortion. Security proce-

dures need to be carefully and continuously 'tuned' to match the full array of risks. Journalists and pundits may find it useful to think in terms of catching the 'bad guys.' In designing security systems, security professionals cannot afford to.

"You can bet terrorists will attempt to qualify their operatives for the trusted traveler programs. It's a problem."

- Senior Official, European Union

8) The Dynamic Character of Threat

Security is a dynamic business. Smugglers, illegal aliens, terrorists, and multiple asylum seekers come to understand border and customs security procedures with some sophistication and adjust their tactics accordingly. It is technically akin to an arms race. As passport agencies may add antifraud technologies to their travel documents, malevolent individuals will employ their own advanced technologies in response to counteract them. Dynamic security requires dynamic procedural and system design through sophisticated modeling and ongoing red-team assessment.

Security procedures, however, tend to be highly routinized. Since in most cases, violations are rare (Factor Six) and/or many violations may go undetected (Factor Two) there is a tendency to be lulled into a false sense that older security procedures remain effective longer than is in fact the case.

We are reminded again of the Great Wall of China, the Maginot Line and related wall-like border technologies, that if not sustained, tested (Factor Two) and upgraded (Factors Five and Eight) provide a dangerously misleading sense of security. A constant and unchanging defense against a dynamic threat is an uneven match.

The modern passport system was established during the First World War. (It is interesting to note that throughout the middle ages various and sometimes multiple identification papers were required of travelers (passaporti and billette de sante) but after the Treaty of Vienna in 1815 and for the next century it became customary not to require any identification at all for international travel.) Since the 1920s we have witnessed an increasing sophistication of printing, human identification, forgery prevention and electronic interoperability of travel documents. Three fundamental technologies are currently revolutionizing passport technology yet again. The first technology is biometrics, moving beyond the simple photograph and the human judgment of a border official as to whether a live individual matches a small photo portrait. The second is certification by a cryptographically secure digital signature to confirm that no element of an electronically stored identity document has been tampered with. These first two elements have been successfully formalized and standardized by the International Civilian Aviation Organization (ICAO) technical group on machine readable travel documents. The third technology is a real-time secure global data network for authentication of travel documents. Several initiatives for this third technology have been proposed, but none is currently active.

The ICAO work represents a very positive model of appropriately dynamic response to dynamic risk. The inclusion of a digital chip in passports represents a very significant step forward. But the successful utilization of the information on the chip and data security capacity of the chip's architecture as part of a real-time data system will require ongoing attention and investment.

9) The Demand for Travel and Trade Facilitation

Much of what we have addressed thus far has focused on inter-institutional miscommunication and market distortions within the multiple institutional layers of modern security systems. The final two factors of this analytic matrix, however, draw attention to institutions and individuals outside of the security domain that sometimes function to challenge or constrain the imposition of security procedures - active travelers and traders interested in facilitation and optimization of movement and privacy policy specialists.

Some security professionals have grown impatient and dismissive of the concerns these individuals raise. In some rare cases the irritation

"If we are to succeed in getting the US to take data protection seriously we will need to demonstrate the actual costs in dollars and cents of the liability for misuse of data and identity fraud."

— Senior Official in the UK Information Commissioner's Office

is so great, these institutions come to be viewed as oppositional, inimical and fundamentally anti-security, functionally not unlike the 'bad guys' who try to circumvent security systems. Passenger and cargo carriers, border area economic concerns and tourism related industrial groups routinely challenge security procedures they view as generating unjustified costs and delays. A market perspective may be especially useful in modeling policy for these last two factors, and help to reduce the prospect of cross-institutional conflict.

In this view, travelers and traders are by the nature of their role simply incented to look at the cost side of the cost-benefit equation. Because of Factors One and Two, the costs of insecurity are obscured and institutionally distant, only the direct costs of security procedures are prominently visible. Because of Factor Six, the relative rarity of significant threats leads to miscalculation of its true long term costs - I won't wear my seatbelt today, I'm not very likely to have an accident today anyway.

The market perspective suggests two structural responses to institutional conflicts along these fault lines. In economic terms, both attempt to increase the capacity for market signaling across domains. First, traders and travelers would benefit from more complete, systematic and accurate data on the real costs for insecurity, ultimately costs they themselves must bear. Second, security professionals would benefit from more complete, systematic and accurate data on the real costs of travel and trade delays and security transaction costs. The first is seldom addressed; the need for security is most often addressed rhetorically and anecdotally. The second is more frequently addressed. Border and customs officials routinely collect and publicize data on delays and processing statistics and take facilitation seriously as part of their job. Self-administered official statistics on facilitation, however, can sometimes be selective and self-serving, so there may be room for meaningful improvement here as well.

10) The Demand for Data Protection

Concerns raised about privacy and data protection sometimes constrain security practice, but the dynamics here are somewhat different than trade and travel facilitation. Here the concern is not about cost and delay, it is about potential abuse and misuse of security data systems. In the difficult job of catching and convicting violators, so the logic goes, security and law enforcement professionals want access to as much data as possible, for as many uses as practical and for a long as the data might be useful. Since the potential usefulness of data may become evident later, to maximize data collection and maximize length of data storage is to maximize security.

But as a practical matter, in routine security procedures

- Data is lost
- Data collected for an explicitly contracted purpose becomes used for other unrelated purposes (function creep)
- Data is accessed illicitly by unauthorized individuals for personal motives

There is extensive data on the distribution of public concern about privacy and three primary characteristics of this distribution stand out. First, in most nations there is a small and very active and well-informed community of privacy policy specialists. The corresponding public at large is much less concerned and informed. Second, level of elite and mass concern about privacy varies dramatically in different geographic areas. It is highest in Europe, modest in North America and lowest in Asia. Third, level of mass public concern with privacy varies in response to dramatic public events. Generally (using the US as an example) one third are simply unconcerned, one third are concerned but only at the time of a dramatic public incident, and one third report a sustained concern and attentiveness to privacy issues.

Over time, perhaps much like a classic business cycle, we can expect a cyclical pattern of alternative attentiveness to security and to privacy. In many cases policy and procurement will result at the high points and corresponding

low points in these historical cycles. The events of 9/11 had dramatic effects on the public perceptions of the privacy-security trade-off in the US and elsewhere around the world. Interestingly, those effects returned to the pre-9/11 levels in about 18 months.

A market perspective in this domain would lead to a strategy on the part of security and law enforcement professionals not simply to demand maximal personal data collection for maximal periods of storage concerning travelers, traders and their associated consignments, but to calculate the optimal amount of information and the optimal storage period based on the current level data protection concern and associated policy restrictions.

Using the US-EU Passenger Name Record negotiations as an exemplar, one might have concluded that the strategy of demanding maximal data and data storage periods on the US side has led to significant delays in what might otherwise have been calculated to be an optimally practical level of security-relevant information available to authorities on both sides of the Atlantic. These are classic problems in operations research, and the well-known models there could usefully be put to work to optimize information selection and structure on both passengers and cargo for demonstrated security benefit while reducing risk of inappropriate and unauthorized use of personal and commercial data.

A well-known principle in data protection policy is the principle of proportionality - the collection, transmission and storage of personal data should be authorized in proportion to demonstrated necessity. When the necessity resides in the domain of transportation and border security, one confronts a double bind. First, as addressed in Factor Two above, data on effectiveness of security systems is most often incomplete and frequently biased by institutionalized data collection procedures. Second, as addressed in Factors Three and Four above, security professionals for very good reasons are reluctant to share information on security sources and methods for fear of compromising them. In response to these challenges, applying traditional principles of operations research, one would propose the establishment of a trusted third party - an institutional arrangement that would permit rational, systematic and proportional design and implementation of security procedures without compromising the security of the procedures themselves. This logic could prove useful in both the national inter-institutional coordination problem (Factor Three) and in international fora (Factor Four.)

"The new policy initiative of Franco Frattini [the European Commission's Vice President for Justice, Freedom & Security] and Wolfgang Schaüble [the German Federal Minister for Home Affairs] on Passenger Name Records has stunned the European security policy community. Instead of standing up to the US, they seem to have adopted the very logic of the US in ignoring European traditions on data protection policy."

— European Think Tank Policy Analyst

IMPROVING SECURITY IN TRAVEL AND TRADE

We have reviewed a matrix of ten institutional factors, most of them quite specific to the domain of travel and trade, which represent possible impediments to the capacity of commercial and public institutions to respond to the increased demand for reliable and effective security systems in the post 9/11 world. Our strategy has been to take the perspective of the 'naïve' economist who asks, straightforwardly enough, if there is increased demand for security, why can't the market effectively respond to this increased demand? We have examined ten possible factors that may contribute to an awkward disconnect between demand and supply.

Each of these ten factors represents a special organizational or structural challenge that distorts what might otherwise be an effective and appropriate dynamic equilibrium between the informed demand and professional supply of effective security in travel and trade. We need not reiterate the familiar statistics about the increasing importance of a secure supply chain and international passenger system in this age of globalization. The increased demand for security in response to intensified conflict, organized crime and global terrorism is neither ambiguous nor controversial. But what lessons might we draw from this analysis for improving the security of travel and trade?

First and foremost, the case needs to be made for independent and systematic assessment of security procedures. It is noted above that the 9/11 hijackers were devastatingly creative and agile in implementing their horrific acts of terrorism.

The professionals responsible for security in travel and trade are well aware that it is not going to be business as usual. But it could be argued that a coherent strategy of response has not yet been articulated.

Security professionals, given their diverse and sometimes competing institutional affiliations and for the reasons discussed above, may not be the optimal starting point for promoting systematic assessment. They may acknowledge its importance in the abstract; they may respond thoughtfully and creatively if and as the culture of security institutions evolves; but they are not likely to be the most effective initiators. If not the front lines of global security systems, then where would one turn?

Second, a strategy worth exploration is to move up the 'food chain' to the level of policy planning, legislation and budgeting. Budget professionals live in a culture of ROI - return on investment. Budget professionals in the security domain have come to accept a very limited definition of 'return.' Instead of measuring return as security, the actual detection and deterrence of threat, they follow the evolved norms and expectations and measure return as the number of security procedures and the size of security staff - so many Euros provides for so many border inspectors, x-ray machines and security cameras. Such logic, unfortunately, is tautological.

If the budgeting process for security systems includes a proportional requirement for funding systematic and institutionally independent effectiveness assessment, perhaps one or two percent of allocated funds, the capacity to allocate scarce resources more effectively would be greatly enhanced. In a phrase, a new budgetary requirement - no red teaming, no new resources.

The main mission for which the Military Organization is responsible is:
The overthrow of the godless regimes and their replacement with an Islamic regime. Other missions consist of the following:

1. Gathering information about the enemy, the land, the installations, and the neighbors.
2. Kidnapping enemy personnel, documents, secrets, and arms.
3. Assassinating enemy personnel as well as foreign tourists.
4. Freeing the brothers who are captured by the enemy.
5. Spreading rumors and writing statements that instigate people against the enemy.
6. Blasting and destroying the places of amusement, immorality.
7. Blasting and destroying the embassies and attacking vital economic centers.
8. Blasting and destroying bridges leading into and out of the cities.

The Military Organization dictates a number of requirements to assist it in confrontation and endurance. These are:

1. Forged documents and counterfeit currency
2. Apartments and hiding places
3. Communication means
4. Transportation means
5. Information
6. Arms and ammunition
7. Transport

—Al Qaeda Manual, recovered from a follower in Manchester England

Third, if taking security return-on-investment seriously requires legislation, then the effort will require public support and public engagement. This is probably a very good idea in its own right - a public information and education campaign. The public at large, as discussed above, is not well informed about security procedures and how at times their own individual behaviors may make security more difficult to maintain. The argument that increased security in response to increased threat requires more than just throwing money at the problem should be resonant with a sometimes jaded public.

Fourth, an impediment that spans many of the factors listed above derives from the structural difficulties associated with traditional procurement and contracting processes. Acquisitions tend to focus point-solution investments rather than end-to-end solutions that could deliver more comprehensive security system improvements. It is likely that the indirect demand problems we have identified could be significantly reduced through use of contracts that include Service Level Agreements that incent contractors and systems integrators to provide high levels of end-to-end service as measured by independently assessed security metrics (see appendix) rather than the typical cost-plus-fee contracts.

Fifth, and finally, most of what has been suggested thus far focuses on national-level efforts. Clearly, international cooperation and collaboration is required. New security demands may require new institutional venues to hammer out the details. One very promising effort at international security data exchange, for example, is the Four-Nations Initiative involving Australia, Canada, the US and the UK. Initial tests on exchanging asylum applicant data have proven to be stunningly successful. But the principal staff involved in these tests came to realize that next steps at implementation would be particularly difficult because there was no obvious institutional venue for a multi-national tender for engaging systems development expertise and technology.

Figure 2 expands these five fundamental strategic responses with concrete examples for each of the ten factors discussed in this report. It is evident that a piecemeal response to these impediments to security is unlikely to be successful. For example, suppose a successful case is made that independent institutions should undertake a red-team style evaluation of security weaknesses and new institutions are created and become active. That would be an important start, but if security personnel have little incentive to attend to or respond to these red-team evaluations, their effectiveness is diluted and indeed their sustainability over time may be challenged.

These 'next steps' are just that, only a start. The primary purpose of this analysis is not to provide an explicit blueprint or timeline, but rather to raise provocative questions and suggest some new lines of analysis. This project does not represent the first attempt to apply market-dynamic and institutional modeling to the realm of security (as demonstrated by the attached bibliography.) But, hopefully, if the benefit of this approach becomes evident, it will also not be the last.

Figure 2 Strategic Responses to Trade & Travel Security Impediments

Structural Issue	Structual Response
1) Indirect Demand	• Develop feedback mechanisms to improve security system design and implementation • Increase incentives for effective use of feedback by security professionals • Increase public education and awareness of specific risks • Increase public awareness of benefits of sustained security
2) The Difficulty of Assessing Security Effectiveness	• Develop independent institutions to design and implement broadly focused and ongoing red-teaming evaluations
3) The Costs of Institutional Fragmentation	• Mandate secure and fully audited interoperability of information systems • Rotate personnel across institutional roles • As appropriate, centralize and systematize institutional responsibility for security functions • Employ new data mining and multi-database analytic technologies to identify threats more accurately from distributed information sources
4) The Challenge of International Collaboration	• Develop new institutional venues to facilitate collaboration • Develop new mechanisms for multinational security systems bidding and acquisition • Demonstrate cost savings that accrue to effective collaboration • Demonstrate security benefits that accrue to effective collaboration
5) The Inertia of Legacy Systems	• Expand implementation of Service Oriented Architectures in extant and evolving IT systems
6) The Irregular Distribution of Threat Incidents	• Active red teaming to keep security personnel attuned to statistically rare but significant risk events
7) The Multidimensionality of Threat	• Independently targeted security evaluations and systems tests draw the attention of responsible appropriators and security systems designers to the multidimensionality of risk events
8) The Dynamic Character of Threat	• Investment in advanced biometrics and identity management systems • Inculcate a culture of flexibility and agility in implementation of security systems • Provide new incentives for security personnel to uncover new techniques designed to avoid detection
9) The Demand for Facilitation	• Increase public education and awareness of the costs of insecurity to balance public attention to the costs and inconvenience of security procedures
10) Privacy Concerns	• Invest in expanded data security and data usage auditing so that data protection concerns can be met without diminishing the amount of data available to security personnel • Utilize multi-factor authentication technologies to prevent and deter unauthorized use of personal data

Appendix

Security Performance Metric

"The federal government spends over $2 trillion a year on approximately 1,000 federal programs. In most cases we do not know what we are getting for our money."

— White House Office of Management and Budget, 2002

Defining meaningful and reliable performance metrics is, in general, a difficult challenge. Doing so in the context of security systems pitted against indeterminate threat is an extraordinarily difficult challenge. Extending this process to the inherently international context of travel and trade is more difficult still. If we are to succeed in developing a serious culture of security ROI, we may benefit from reviewing the available case studies in related domains.

The US government's INFOSEC Research Council listed security metrics on its famous Hard Problem List in 2005. They find existing metrics to be of 'questionable utility' and notoriously difficult to 'evaluate, interpret and use intelligently.' Their analysis, because of their institutional position, focuses on the IT domain and coordination within the US context. The complexity in the international security arena is even more daunting.

The Coordination Science Institute of the University of Illinois lists the following gaps in existing security metrics.

- Existing methods focus narrowly and exclusively on a single aspect of security
- Institutional inputs are often not available
- Most technical metrics focus solely on process rather than achievement
- Different metrics are not integrated to provide a comprehensive view

It may be useful to step back for some perspective on the difficult question of public sector performance measures. In the American case the modern round of concern with programmatic evaluation came in 1966 with President Johnson's Planning, Programming and Budgeting System (PPBS) championed by Secretary McNamara at DOD and based on private sector models of 'output budgeting.' Some variants of this early initiative are still in use at the Pentagon and in the United Kingdom. In the Nixon era the effort was continued under the rubric of Managing By Objective (MBO) in this case influenced by the well-known management guru Peter Drucker. President Carter expanded the effort under the banner of zero-based budgeting. President Clinton and Vice President Gore championed a National Partnership to Reinvent Government in an effort to create

a government that "works better, costs less, and gets results Americans care about." The 1993 Government Performance and Results Act (GPRA) set new standards and procedures for performance metrics and continues today under the responsibility of the OMB utilizing the Program Assessment Rating Tool (PART). President George W. Bush continues the tradition of strong White House support for the effort under the rubric of the President's Management Agenda (PMA). This represents four decades of successive waves of evaluation effort. The initial reports revealed that only 6% of federal programs were judged to be effective and 50% simply could not be evaluated because a lack of performance indicators. More recently compiled OMB statistics identify higher levels of effectiveness and fewer programs unable to be evaluated, but it is not yet clear whether these result from bureaucratic nuance in filling out forms or real improvement in field effectiveness.

In 2002 David Walker, Comptroller General of the United States in testimony before Congress took note of the opportunity the creation of the new DHS provided to clarify and enhance the effectiveness of American trade and travel security. His key recommendation was the establishment of 'specific expectations for performance and accountability including establishing goals and performance indicators.' His office (OMB) followed up and in 2005 utilized the PART process to assess the performance of 32 programs in DHS for fiscal years 2004-2006. On the basis of answers to 25 questions relating to a program's purpose, planning, management, results and accountability, OMB concluded performance was effective for 4 programs, moderately effective for 6 programs, and adequate for 6 programs and results were not demonstrated for the remaining 16 programs. This may or may not represent testimony on DHS's achievements to date, but it certainly confirms that an accepted culture of public sector assessment and ROI is not yet in place.

The Washington Beltway and think tank communities have been promoting a process of 'scorecarding' drawn from the private sector tradition of Enterprise Performance Management and applying it to public sector processes. Kevin Coleman published a paper recently putting these ideas to work in the domain of homeland security and border management. He notes for example: “Careful consideration must be given to the design of a metrics and measures system. Improper or imbalanced measures can often create bad behaviors and gaming of the system. For example, for the DHS, if you were to measure the number of persons arrested without an opposing measure like the number of persons whose arrests were upheld and remanded for trial, or those convicted - you could create a situation where arrests were being made without clear, valid and credible reason to improve the appearance of success. The ideal is to implement a 'balanced performance scorecard' throughout the enterprise, because that framework helps foster alignment between all the individual operational components. The scorecard structure contains three major categories - effectiveness, efficiency and results. Careful attention has been given so as not to have an imbalance that promotes bad behaviors or gaming of the system.”

The scorecard he proposes is illustrated below. It may strike some observers as incomplete and potentially misleading because it relies, as do most PART evaluations, on event statistics - all numerator and no denominator. It is included here to illustrate the state of the literature in homeland program assessment.

Figure 3 Coleman Exemplary DHS Scorecard

The development of programmatic assessment of security investment in Europe and elsewhere in the world is also at an early stage. One potentially promising model for possible emulation, however, is the creation of the European Network and Information Security Agency (ENISA) as an independent entity to publicize security standards and assess programmatic success in the European context. The focus in this case is on IT security, but the model could be applied more broadly to cooperative initiatives in other security arenas. To maintain the independence and reliability of the reporting process to standard operating model is to contract with outside vendors such as auditing firms to conduct surveys and analyses of security practices and issue public awareness.

Another intriguing model in the European context is a new and evolving legal concept known as the Connexity Criterion. It evolved from some legal cases that questioned whether public sector expenses justified by a state of emergency declaration were in fact connected to the state of emergency. Legal scholars have been expanding the notion to apply more broadly to provide a legal basis for having agencies justify budgeted expenses in terms of measurable accomplishments. Again, it is very early in the evolution of these initiatives to know whether they may prove to be effective. But it is useful to note that one novel approach in this area has been a legal one initiated by judicial mandate.

In Australia a tradition has evolved to publish an annual report entitled *Managing the Border: Immigration Compliance* to assess the effectiveness of border and immigration security procedures and systems. It is a public document and arguably has a sustained positive affect on public sector practice and public awareness but it relies heavily on event statistics and therefore suffers from the endemic missing denominator problem. The Japanese Ministry of Foreign Affairs has developed a unique approach that may also provide a model worthy of emulation in this arena. In addition to more traditional security assessments they have prepared and promulgated a security self-assessment tool for private sector entities in travel and shipping to help them evaluate security issues and respond to vulnerabilities. This is particularly promising given the obvious need for private-public coordination and partnership in this field.

In summary, we might conclude that although there is wide recognition that systematic assessment of security systems is important and necessary, it is not yet possible to point to a set of best practices and a sophisticated set of assessment tools. Now that the challenges of post 9/11 security have been widely recognized, and budget constraints for security systems investment have been addressed in national states and regional entities around the world — the time is right for new initiatives in the domain of security ROI.

Demand for Security

Resource Bibliography

Agre, Philip E. and Marc Rotenberg, Eds. (1997). **Technology and Privacy: The New Landscape.** Cambridge: MIT Press.

Allison, Graham T. (1971). **The Essence of Decision: Explaining the Cuban Missile Crisis.** New York: Harper Collins.

Anrig, Bernhard, James Backhouse, Emmanuel Benoist, Ana Isabel Canhoto, Sabine Delaitre, Claudia Diaz, Marit Hansen, David-Olivier Jaquet-Chiffelle, Thierry Nabeth and Árpád Rab (2006). **Identity in a Networked World: Use Cases and Scenarios.** Brussels: Future of Identity in the Information Society Consortium.

Baldwin, Thomas E., Arkalgud Ramaprasad and Michael E. Samsa (2008). "Understanding Public Confidence in Government to Prevent Terrorist Attacks." **Journal of Homeland Security and Emergency Management** 5(1).

Barton, Bryan, Dennis Carlton, Oliver Ziehm (2007) **Identity Management in the 21st Century: Balancing Safety, Security and Liberty in a Global Environment.** Bethesda: IBM Institute for Business Value.

Bayes, Thomas (1764). "An Essay Towards Solving a Problem in the Doctrine of Chances." **Philosophical Transactions of the Royal Society of London.**

Bisbal, Jesus, Deidre Lawless, Bing Wu and Jane Grimson (1999). "Legacy Information Systems: Issues and Directions." **IEEE Software** 16(5): 103-111.

Braman, Sandra (2006). **Change of State : Information, Policy, and Power.** Cambridge: MIT Press.

Bramhall, Pete, Marit Hansen, Kai Rannenberg and Thomas Roessler (2007). "User-Centric Identity Management: New Trends in Standardization and Regulation." **IEEE Security & Privacy** 5(4): 81-87.

Branscomb, Anne Wells (1994). **Who Owns Information? From Privacy to Public Access.** New York: Basic.

Brin, David (1998). **The Transparent Society : Will Technology Force Us to Choose between Privacy and Freedom?** New York: Perseus.

Buchanan, James M. (1968). **The Demand and Supply of Public Goods.** Chicago: Rand McNally & Company.

Burton, James G. (1993). **The Pentagon Wars: Reformers Challenge the Old Guard.** Annapolis MD: Naval Institute Press.

Cabinet Office of the United Kingdom (2007). **Security in a Global Hub: Establishing the Uk's New Border Arrangements.** London.

Cavoukian, Ann (2002). T**he Privacy Payoff: How Successful Businesses Build Customer Trust** New York: McGraw Hill.

Cavoukian, Ann and Don Tapscott (1996). **Who Knows: Safeguarding Your Privacy in a Networked World.** New York: McGraw Hill.

Chamberlain, Todd (2007). "Systems Dynamics Model of Al-Qa'ida and United States "Competition"." **Journal of Homeland Security and Emergency Management** 4(3).

Chew, Elizabeth, Alicia Clay, Joan Hash, Nadya Bartol and Anthony Brown (2006). **Guide for Developing Performance Metrics for Information Security: Recommendations of the National Institute of Standards and Technology:** NIST Special Publication 800-80.

Chirillo, John and Scott Blaul (2003). **Implementing Biometric Security** New York: Wiley.

Coleman, Kevin (2005). "Enterprise Performance Management in Homeland Security." **Directions** (July 14).

Cranor, Lorrie Faith and Joseph Reagle (1998). Designing a Social Protocol: Lessons Learned from the Platform for Privacy Preferences Project. **Telephony, the Internet, and the Media: Selected Papers from the 1997 Telecommunications Policy Research Conference.** MacKie-Mason, Jeffrey K. and David Waterman, Eds. Mahwah NJ: Erlbaum. 215-232.

Davis, Darren W. and Brian D. Silver (2004). "Civil Liberties Vs. Security: Public Opinion in the Context of Terrorist Attacks on America." **American Journal of Political Science** 48(1): 28-46.

Downs, Anthony (1972). "Up and Down with Ecology: The Issue Attention Cycle." **Public Interest** 28: 38-50.

Easton, David. (1953). **The Political System.** New York: Knopf.

Etzioni, Amitai (1999). **The Limits of Privacy.** New York: Basic Books.

Etzioni, Amitai (2004). **How Patriotic Is the Patriot Act? Freedom Versus Security in the Age of Terrorism.** New York: Routledge.

European Commission Directorate-General Joint Research Centre (2005). **Biometrics at the Frontiers: Assessing the Impact on Society.** Seville, Spain: European Commission.

Gandy Jr., Oscar H. (1989). "The Surveillance Society: Information Technology and Bureacratic Social Control." **Journal of Communication** 39(3): 61-76.

Gandy Jr., Oscar H. (1993). **The Panoptic Sort: A Political Economy of Personal Information.** Boulder CO: Westview Press.

Greenfield, Harry (2000). "Surrogate Demand: A Note on Demand Theory." **Challenge** (November).

Halman, Loek, Ronald Inglehart, Jaime Diez-Medrano, Ruud Luijkx, Alejandro Moreno and Miguel Basanez (2008). **Changing Values and Beliefs in 85 Countires.** Leiden: Brill.

Hardin, Garrett (1968). "The Tragedy of the Commons." **Science** 162: 1243-1248.

Haveman, Jon D., Howard J. Shatz and Ernesto A. Vilchis (2005). "U.S. Port Security Policy after 9/11: Overview and Evaluation." **Journal of Homeland Security and Emergency Management** 2(4): 1.

Heritage Foundation (2005). "Reforming the Department of Homeland Security." **WebMemo** #706

Hess, Howard M. (2005). "Aligning Technology and Business: Applying Patterns for Legacy Transformation." **IBM Systems Journal** (March).

Home Office and Foreign and Commonwealth Office of the United Kingdom (2007). **Managing Global Migration: A Strategy to Build Stronger International Alliances to Manage Migration.** London.

Home Office of the United Kingdom (2006). **Strategic Action Plan for the National Identity Scheme: Safeguarding Your Identity.** London.

Howard, Russell D., James Forest and Joanne Moore, Eds. (2005). **Homeland Security and Terrorism** New York: McGraw-Hill.

Krueger, Alan B. (2007). **What Makes a Terrorist: Economics and the Roots of Terrorism.** Princeton: Princeton University Press.

Levinthal, Daniel (1988). **"A Survey of Agency Models of Organizations."** Journal of Economic Behavior & Organization 9: 153-185.

Linzer, Dafna (2008). In New York, a Turf War in the Battle against Terrorism. **The Washington Post.** Washington: A1.

Lowson, Robert H. (2002). **Strategic Operations Management: The New Competitive Advantage.** New York: Routledge.

Mitnick, Kevin D. (2003). **The Art of Deception: Controlling the Human Element of Security.** New York: Wiley.

Moore, Jr., Barrington (1984). P**rivacy: Studies in Social Cultural History.** Armonk, NY: M. E. Sharpe.

Morris, Paul V., Ed. (2005). **Border Security or Insecurity.** New York: Novinka.

Mueller, John (2006). **Overblown: How Politicians and the Terrorism Industry Inflate National Security Threats, and Why We Believe Them.** New York: Free Press.

Nanavati, Samir, Michael Thieme and Raj Nanavati (2002). **Biometrics: Identity Verification in a Networked World.** New York: Wiley Computer Publishing.

National Research Council (2003). **Who Goes There?: Authentication through the Lens of Privacy.** Washington, DC: National Academy Press.

National Science and Technology Council (2006). **The National Biometrics Challenge.** Washington DC.

National Science and Technology Council (2006). **Privacy and Biometrics: Building a Conceptual Foundation.** Washington DC.

OECD (2002). **OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.** Paris, France: OECD Publications.

Ostrom, Elinor (1990). **Governing the Commons: The Evolution of Institutions for Collective Action.** New York: Cambridge University Press.

Ott, Attiat F. and Richard J. Cebula, Eds. **(2006). The Elgar Companion to Public Economics: Empirical Public Economics.** London: Elgar.

Ramsey, Todd, Ed. (2004). **On Demand Government: Continuing the E-Goverment Journey.** Lewisville TX: MC Press.

Ritti, R. R. and Fred H. Gouldner (1969). "Professional Pluralism in an Industrial Organization." **Management Science** 16(Dec): B233-B246.

Samuelson, Paul A. (1954). "The Pure Theory of Public Expenditure." **Review of Economics and Statistics** XXXVI(November): 387-89.

Samuelson, Paul A. (1955). "Diagrammatic Exposition of a Theory of Public Expenditure." **Review of Economics and Statistics** XXXVII(November): 350-56.

Scandanamis, Nicolas, Frantzis Sigalas and Sofoklis Stratakis (2007). "Rival Freedoms in Terms of Security: The Case of Data Protection and the Criterion of Connexity." **CEPS Challenge Program Research Paper No. 7**.

Schneier, Bruce (2006). **Beyond Fear: Thinking Sensibly About Security in an Uncertain World.** New York: Springer.

Schneier, Bruce and David Banisar, Eds. (1997). **The Electronic Privacy Papers.** New York: John Wiley & Sons.

Seacord, Robert C., Daniel Plakosh and Grace A. Lewis (2003). **Modernizing Legacy Systems: Software Technologies, Engineering Processes, and Business Practices.** Reading MA: Addison-Wesley.

Shenk, David (1998). **Data Smog : Surviving the Information Glut.** New York: Harper.

Slone, Skip (2004). **Identity Management.** San Francisco: The Open Group.

Smelser, Neil J. (2007). **The Faces of Terrorism: Social and Psychological Dimensions.** Princeton: Princeton University Press.

Smith, Robert Ellis (1993). **Our Vanishing Privacy.** Port Townsend WA: Loompanics.

Stigler, Stephen M. (1982). "Thomas Bayes's Bayesian Inference." **Journal of the Royal Statistical Society** A145(2): 250-258.

Stigler, Stephen M. (1984). "Who Discovered Bayes's Theorem?" **The American Statistician** 37: 290-296.

Swanson, Marianne, Nadya Bartol, John Sabato, Joan Hash and Laurie Graffo (2003). **Security Metrics Guide for Information Technology Systems:** NIST Special Publication 800-55.

Thomas, Robert J. (1994). **What Machines Can't Do: Politics and Technology in the Industrial Enterprise.** Berkeley: University of California Press.

Torpey, John (2000). **The Invention of the Passport: Surveillance, Citizenship and the State.** New York: Cambrdige University Press.

Trubow, George (1989). **Watching the Watchers: The Coordination of Federal Privacy Policy**, The John Marshall Law School.

Tversky, Amos and Daniel Kahneman (1981). "The Framing of Decisions and the Psychology of Choice." **Science** 211: 453-458.

U.S. House of Representatives Committee on Homeland Security Majority Staff (2007). "The State of Homeland Security."

Westin, Alan F. (1967). **Privacy and Freedom.** New York: Atheneum.

Westpfahl, Brad (2004). Safety and Security. **On Demand Government: Continuing the E-Goverment Journey.** Ramsey, Todd, Ed. Lewisville TX: MC Press. 99-112.

White, Jonathan R. (2003). **Defending the Homeland: Domestic Intelligence, Law Enforcement, and Security.** New York: Wadsworth.

White, Lynn (1966). **Medieval Technology and Social Change.** New York: Oxford Univeristy Press.

White House (2007). **Homeland Security Presidential Directive/HSPD-20.** Washington D.C.

Wicklein, John (1981). **Electronic Nightmare.** New York: Viking Press.

Willis, Henry H., Andrew R. Morral, Terrence K. Kelly and Jamison Jo Medby (2005). **Estimating Terrorism Risk.** Santa Monica CA: RAND.

Yildirim, Julide, Selami Sezgin and Nadir Öcal (2006). The Demand for Military Spending in Middle Eastern Countries and Turkey. **The Elgar Companion to Public Economics: Empirical Public Economics.** Ott, Attiat F. and Richard J. Cebula, Eds. London: Elgar. 195-213.

Zureik, Elia and Mark B. Salter, Eds. (2005). **Global Surveillance and Policing: Borders, Security, Identity.** New York: Willan.

W. Russell Neuman, Ph.D., is the John Derby Evans Professor of Media Technology in Communication Studies and Research Professor at the Institute for Social Research, University of Michigan. He recently returned from serving as a Senior Policy Analyst in the White House Office of Science and Technology Policy working in the areas of information technology, broadband policy and technologies for border security. His recent books include The Gordian Knot: Political Gridlock on the Information Highway (MIT Press, 1997), and Affective Intelligence (University of Chicago Press, 2000). Dr. Neuman taught at the University of Pennsylvania where he directed the Information and Society Program of the Annenberg Public Policy Center. He also taught at Harvard and Yale and was one of the founding faculty of the MIT Media Laboratory. His Ph.D. is from the University of California, Berkeley and his undergraduate degree is from Cornell University.

IBM Coperation
Route 100
Somers, NY 10589
U.S.A.
Produced in the United States of America
October 2008