INITIAL REVIEW OF THE DRAFT TECHNICAL PAPER ON SECURITY MEASUREMENT

The attached paper offers a good coverage of Security Measurement. The conceptual model for security that has been proposed addresses key management issues and its future use should lead to measurable concepts that are applicable across a wide range of types and scale of secure entity. Sector-specific guidance, along with considerations for physical security and cyber security, will be necessary in developing security measurement guidance.

With my new role as Director for Software Assurance in the Department of Homeland Security (DHS) National Cyber Security Division, I have an even greater interest in maturing security measurement. As such, I intend to be involved in further evolving this body. I will participate in the next PSM TWG meeting March 23-25, 2005 at Software Productivity Consortium (SPC) Herndon, Virginia.

Pete Baxter reviewed the paper, and noted that without specifically identifying the purpose, or the "user", of security, the framework and dimensions covered in the paper are useful, but don't ever get to answer the question "Why are we doing this?" For example, the security issues (and measures) for an acquirer are different than an integrator are different than a developer. Framing the question in terms of "Who are we going to secure?" would allow the framework and dimensions to be guided and assessed with respect to their use. Instead, the document tends to frame the discussion in terms of the technology and standards that are available. For example, the document points out why to use a maturity model, or why to use an IEEE standard for compliance, and it would be more useful if it included more about "Why am I doing this?" before a survey of existing work.

Many of the security points that are raised fall into at least two general categories: 1) security aspects we want to require or build into a system and 2) elements of operational monitoring that can ensure security and detect violations. The first topic really has to do with developing security requirements, allocating them (to contractors or software design/development for example) and then coming up with a technique to verify them. This is requirements management with aspects of system quality. The second topic is very closely aligned with operational and network monitoring. Essentially, we want to know what our systems are doing, and look for something that we have not seen before. (For example an intrusion, a sensor alert, an unsecured file, a high rate of rejects on a specific port, a mal-formed html request, ... other types of security alerts). In both of these cases, the framework of measurement (PSM, GQM or any other one) does not help forward the discussion about what we need to do to ensure security and then how we can measure it. The dynamic nature of security/threat detection is significantly different than the approach in PSM where we know specific information needs ahead of time - perhaps this is an area where PSM could be extended to better support security. The concept of "information need" could be generalized into something useful, but the decomposition into equations and base measures makes the information need a very specific/focussed entity. Security requires something that says "What looks unusual or different about my facility or network?" This is a different and will require the involvement of sector-specific experts and those with backgrounds in physical security and cyber security.

A discussion of organizational summary/roll-up does not seem to help bound the problem of securing systems or places or networks. From a security aspect, you can only secure an entire system. For example, the best/most secure code in the world is no good if the computer running it has no password and is left in a public library with the super user account already logged in. Security can only be assessed on a system level. Requirements for security can be allocated to subsystems, but the important message might more appropriately be that acquirers/developers/ users/operators cannot test or verify security on a unit/module/subsystem level - only at a system level. This should change how acquirers specify system tests and how suppliers conduct them internally.

RISK EXPOSURE AS AN ELEMENT OF BUSINESS CASE ANALYSIS AND RETURN OF INVESTMENT

From my perspective, security measurement needs to support "risk exposure" determination and decision making, especially relative to ROI. An organization has options for reducing risk exposure ranging from acquiring requisite assets/services to increasing insurance coverage (and insurance companies are evolving criteria to determine levels of client risk exposure).

How does an organization determine where best to focus security investments and quantifiably justify the investment to defend against those wanting to cut security budgets. Does a $5M investment in cyber security truly gain the requisite protections worth $5M?

That is the real relevance of your question: is the initial focus to develop measures that quantify how secure the current facility, system or network is? And, following this initial scope to determine measures of vulnerability? (From that logic above, if you secure your network, you are "ready" for the known threats but may be completely unprepared for the unknown ones.

This is the relevance of the 16 application practices in our Safety & Security Extensions for Integrated CMMs. We need measurement support for these. Threat identification, analysis, and mitigation, coupled with contingency operations (that include disaster recovery) are some of the practices that can benefit with more mature measurement. In turn, that could address how vulnerable are my products, networks, operations, etc. For instance, if we could develop safe and secure design guides (that specify, among other things, not using all features of the implementing languages, we could add to the criteria used to determine what components are trusted. I would hope that would influence development and acquisition decisions.

CYBERSECURITY SECTOR SPECIFIC CONSIDERATIONS

I agree that at some levels, security measurement must be sector/industry/business specific, even addressing differences between physical security and cyber security.

In an effort to mitigate cyber threats, the World Bank has worked with the international financial sector to develop e-security processes and procedures that are described in "Electronic Security: Risk Mitigation in the Financial Transactions". It indicates ISO 17799 (one of the input standards for our Safety and Security Extensions to CMMI and iCMM) is the most widely utilized security standard for information systems. However, it also indicates ISO 17799 was written with the 90's cyber-space environment in mind, it has become outdated and deficient given the growth in outsourcing, wireless usage, applications, blended threats and the organized and dynamic approach to hacking that various criminal syndicates have taken in recent years. The attached checklist aims to ask those questions that all to often have been ignored. Thus, defense in depth, specifically through an implementation of Layered Security, is essential to achieving the desired goals. These are applicable to our software assurance efforts; so we should consider how these might be used in evolving security measurement and evaluating the capabilities of suppliers and those providing IT services and in assessing security vulnerabilities in IT operations.

The thirteen layers of e-security described in The World Bank publication cover both the hardware and software pertaining to network infrastructures. Comprised of often binary criteria, these 13 layers comprise a matrix, which manages the externalities associated with open architecture environments.
1. Risk Management-A broad based framework for managing assets and relevant risks to those assets.
2. Policy Management- A program should control Bank policy and procedural guidelines vis-à-vis employee computer usage.
3. Cyber-Intelligence- Experienced threat and technical intelligence analysis regarding threats, vulnerabilities, incidents, and countermeasure should provide timely and customized reporting to prevent a security incident before it occurs.
4. Access Controls/Authentication-Establish the legitimacy of a node or user before allowing access to requested information. The first line of defense is access controls; these can be divided in to passwords, tokens, biometrics, and public key infrastructure (PKI).
5. Firewalls-Create a system or combination of systems that enforces a boundary between two or more networks.
6. Active content filtering-At the browser level, it is prudent to filter all material that is not appropriate for the workplace or that is contrary to established workplace policies.
7. Intrusion detection system (IDS)-This is a system dedicated to the detection of break-ins or break-in attempts, either manually or via software expert systems that operate on logs or other information available on the network. Approaches to monitoring vary widely, depending on the types of attacks that the system is expected to defend against, the origins of the attacks, the types of assets, and the level of concern for various types of threats.
8. Virus scanners-Worms, Trojans, and viruses are methods for deploying an attack. Virus scanners hunt malicious codes, but require frequent updating and monitoring.
9. Encryption-Encryption algorithms are used to protect information while it is in transit or whenever it is exposed to theft of the storage device (e.g. removable backup media or notebook computer).
10. Vulnerability testing-Vulnerability testing entails obtaining knowledge of vulnerabilities that exist on a computer system or network and using that knowledge to gain access to resources on the computer or network while bypassing normal authentication barriers.
11. Systems administration-This should be complete with a list of administrative failures that typically exist within financial institutions and corporations and a list of best practices.
12. Incident response plan (IRP)-This is the primary document used by a corporation to define how it will identify, respond to, correct, and recover from a computer security incident. The main necessity is to have an IRP and to test it periodically.
13. Wireless Security- This section covers the risks associated with GSM, GPS and the 802.11 standards.

The World Bank Technology Risk Checklist is designed to provide Chief Information Security Officers (CISO), Chief Technology Officers (CTO), Chief Financial Officers (CFO), Directors, Risk Managers and Systems Administrators

with a way of measuring and validating the level of security within a particular organization. The CISO plays a key role in this initiative by overseeing the entire gamut of processes, procedures, and technologies pertaining to an institution's IT infrastructure.

Such sector-specific checklists may prove useful in developing security measurement guidance.

There is growing need for mature security measurement, and recent concerns in cyber security have raised the need for better measurement. US Congressional interest has been recently documented in the December 2004 "Cybersecurity For the Homeland" Report of the Activities and Findings by the Chairman and Ranking Member on the Subcommittee on Cybersecurity, Science, and Research & Development, in the US House of Representatives Select Committee on Homeland Security. There are many relevant articles on improving cybersecurity at https://www.csialliance.org/news/inthenews/.

QUESTIONS AND CONSIDERATIONS FOR EVOLVING SECURITY MEASUREMENT

How might security measurement be best addressed within standards? In addition to linking this with PSM and ISO 15939, how might this be addressed by standards managed by NIST and/or IEEE Software and Systems Engineering Standards Committee EXCOM? I participate in the IEEE CS S2ESC EXCOM, chaired by Paul Croll. The next face-to-face meeting of the S2ESC EXCOM will be held at the SEI Arlington VA offices from 28 February through 2 March, 2005. That should be a good opportunity to address safety and security measurement relative to IEEE standards, in addition to the ISO standards. My intent is to also involve NIST, and I will fund NIST via a software assurance task in support of their other security efforts.

I would like to help accelerate the progress on developing the security/safety measurement body of work, specifically directed at addressing the questions in the draft white paper in the "Conclusion" the noted concerns related the achieved integrated security performance of an entity to the total security costs incurred. At the next level of decomposition, you indicate we can ask the following basic questions (that I suggest need further elaboration:

1. What is the capability/competence of the resources deployed on security? (this should address operations, acquisition/procurement, and development -- how would this be objectively evaluated/appraised, and how can it be linked, as appropriate, to safety?)

What is the capability of this supplier? What are their process capabilities? What are the attributes of a secure product? What are the artifacts of the processes that provide evidence of a secure product? (cf QA methods)

What is the capability of the demand side? Capability of specifying needs? What are my needs, constraints, trades?

What is the capability of the adjudicator role? Prioritization of security threats. Tell me the product limitations and the product devlpt process limitations.

COTS product suppliers: threat modeling? Crashing/ suitability for use?
Differences between certification lab processes: how to develop commonality? 'Gold standard' tool sets for standard contexts? Require products to be tested against a reference checker/ suite of tools. (safe & secure subset of languages …) Added to that, will be the reqmts of the demand-side specific context.

Resources deployed on security: HW, SW, people?

Configuration of resources to deliver security? Risk reduction/ ROSI?

Supplier delivering a capability .. mix of these three.

TASK: Guidance about how to prioritize security needs, using the R7 radar diagram. 'Stack' of different diagrams for different requirements; average mission. Bridging demand-side need with supply-side specs. What decision did the adjudicator make? Develop rigor / methods for this role.

Trade between development time investment and operational costs? Models that help with devlpt time investment choices, trades? Hence acq by specs rather than performance in DoD.

TASK: Supplier-side: system model to guide me about process / product improvement priorities that will enable me to meet security performance targets.

Identification of lower-level measures for security – i.e. of lower level components/ process elements… and how the roll up into higher level indicators. Ref: JHU study. DoD IA Metrics study (700 metrics etc) Map DoD study to higher level indicators. Will support development of draft PSM guidance materials.

Cost of non-conformance ..

TASK: Set of reasonable measures, indicative of security .. (to whom?) Qualitative arguments, conventional wisdom etc. Purpose: supports trade with downstream operational costs. For decision-makers, in the absence of eng-type measures, a qualitative indicator helps with choice. Some scoring 1 – 5, indicative of 'security rating' of the product/ services. Built from checklists, existence of security actions.
Fitness criteria at milestones. Born secure. Scoring a system at the point of transition to operations.
Ref: Net-centric Operations & Warfare Reference Model. (where are the security functions placed? Must be specified.)
Performance reference models associated with this…
Model is comprehensive, but complex and hard to comprehend….

User changes to a system from the originally delivered system. Execute-only components.

2. Are security actions based on known best practice and in compliance with applicable standards and legal requirements? (from a US industry perspective, this should also address security requirements derived from compliance with Sarbanes-Oxley.)

Among the drivers of the checklists in above indicator concept.
Banking Industry technology security BITS, checklists.
World Bank Technology Risk Check List.
HIPAA Health Insurance Portability Act, further checklist inputs.

3.How is the security risk being managed?
How is safety risk being managed? (and specifically, how does measurably improved security contribute to managing safety risk and privacy risks?)
Venn diagram to differentiate between different risks, and overlaps. Also other risks. In, out, criteria.
Different variants of security risk (privacy, integrity etc). Task for adjudicator.

4. What is the assurance evidence that defines our degree of confidence in likely future security performance? (what of this could be used as indicators for future security performance? How should the PSM "Security Measurement" WhitePaper v1.0 30-Nov-04 be revised to target specific user needs?)

Where is the reference point? Where's the ground reference point? Standards, criteria.

5. What is the achieved performance of our systems in terms of managing threats, vulnerabilities, responding to events and recovering from & controlling damage? (what level of decomposition is needed to address software assurance, information assurance, cybersecurity, etc.?) R7 model.

Again, ground?

Devolution of a service: emergent

Evolution: emergent of properties/ performances.

Mixed analog/digital.

Consistent with the recommendations for future work (listed in the paper), I will explore the possibility of co-sponsoring with UK MOD (if necessary via task order funded by DoD and/or DHS via PSM):

1. Development of example measurement specifications based on particular security/safety practices/standards, and particular technologies (e.g. software development, CC security functional components, etc.);

Ref: the 16 practices identified in the Safe Sec AAs. Open to development.
Based on standards. But when connected to a user; context-specific issues arise. Voluntary or regulated adaptation?

Need experimentation: enables demonstration of value to users.

Common Criteria: practical use is the difficulty. E.g. protection profiles could be specified to be difficult to meet. But an expressive way to characterize security needs. Who should be responsible for writing this?

2. Development of practical guidance on how to develop security/safety measures in support of management decision-making;

Template example:
PSM – generic situation: decisions to be made, indicators reqd, example data, analytics. Plus guidance for tailoring to the context-specific.

But in security: there is a minimum, common set of decisions, and sets of indicators, data that support this.
Figure of merit for security.

Raise the floor – do not need sophisticated measures ….

Example: how is confidentiality achieved: what mechanisms achieve this?

Sample responses to the relevant questions, with scenarios for how the answers could provide the indicators management needs in making decisions regarding security/safety. Ref: Jack Lenihan report.

3. Pilot/test proposals in conjunction with security/safety specialists and standards organizations (test measurement proposals and improve by means of project trials);

Eventually … standards, curriculum..