Purpose and audience of this paper

This proposal is a starting point put forward to the Open Group Security Forum’s membership to begin the discussion needed to reach a commitment on where we take the Enterprise vulnerability Initiative. Please review and send all your comments to the forum to assist the discussion. By the February meeting, we should have commit to our go-forward plan in this critical area.

I propose here a necessary although ambitious program: one we cannot do ourselves with our current membership, but one, with the help of new members, is achievable. First new activities we can do with the membership already in place include focusing on improving and expanding the proposed NIST standards government agencies will use to comply with FISMA. Industry’s contributing to these standards will make them more harmonized to the private sector’s best practices and so will enable the guidelines’ use within the private sector. The Open Group Security Forum can be a catalyst to create the opportunity for business and government to shape and reuse these guidelines, ensuring they are useful, effective, and economical.

Through these efforts the Security Forum can grow its membership, explore certification opportunities, and develop improved standards, processes, and tools to help IT users worldwide comply with their requirements to run secure, safe, and dependable IT services that support the vision of Boundaryless Information Flow.

Background:

Everyone who matters knows that the continuity of cyberspace is critical for western civilization. Everyone knows information systems businesses and the public rely upon are vulnerable to many threats. Some suspect a cyber disaster is only a matter of time.

Today system owners react to vulnerabilities. In short, the management process is

- A vulnerability is reported
- The technology owner (such as an OS vendor, application vendor, etc.) develops and releases a hot-fix to the vulnerability
- The system owner applies the fix, hopefully before the vulnerability is exploited and damage done

By its very design, this process has a built in vulnerability window that can be exploited. Where impacts of exploitation result in low to medium harm, this vulnerability management process has shown to be economically viable – it’s the de facto enterprise software systems EVM process standard worldwide.

When the impact of exploitation, however, is high, this process is insufficient. Historically, high severity systems rely upon time proven safety and dependability engineering principles for their trustworthyness. Securing Critical Information Infrastructure, whose impact of exploitation is very high, requires techniques that go beyond the simple reactive process the software industry has supported: techniques that proactively minimize vulnerability in addition to reacting to discovered vulnerabilities.
The Open Group Vulnerability Management Initiative seeks to develop the common body of knowledge needed to develop and operate highly reliable and trustworthy critical information systems using these two approaches. Applying the lessons learned from safety critical and dependability critical systems development is a good first step.

In the past industries that provided critical products and service have been regulated for security, safety and dependability. While these system attributes have been thought of as separate disciplines, they all have in common the notion of managing risk to acceptable levels commensurate with the public harm of vulnerability exploitation. As separate disciplines, safety, security, and dependability practitioners rarely interact. However, we believe that in the area of overall vulnerability management, they must interact. Business managers, customers, and the public hardly care why a mission critical service goes down; they care only that the service has gone down. Safety, dependability, and security should be looked at together, at an all-inclusive level: the vulnerability management level.

NIST, the organization responsible for setting security standards for US government systems, already recognizes the potential the Open Group Security Forum has for influencing the strategy for defending civilian systems covered under FISMA. NIST has asked the Security Forum to be more involved in reviewing and evaluating its upcoming guidelines and standards. These in turn can impact the private sector’s best practices through its recognition of NIST and the Security Forum’s due diligence in their creation.

Legislators and regulators increasingly are inserting themselves into the vulnerability management arena. USA-PATRIOT, Sarbanes-Oxley, Gramm-Leach-Bliley, and HIPAA legislation have passed, which govern how industry, especially critical industries, must manage their information and vulnerabilities to that information. Though on hold pending industry comment, Congressman Putnam proposed new legislation requiring all publicly traded companies to perform annual cybersecurity audits and make those results available to the public. While Congress isn’t yet satisfied with existing cybersecurity law, it seems open to an industry-led alternative “to get it right.” Through the EVMi, The Open Group can serve membership and public interests by contributing to this vital area.

Therefore, we propose an Vulnerability Management Initiative consistent with and supportive of The Open Group’s work in Boundryless Information Flow.

**Opportunity**

The Open Group working with other standards organizations have the opportunity for:

- Establishing a common set of best practices for managing vulnerabilities in enterprise systems
- Establishing a mechanism for measuring vulnerability
- Adapting practices of the dependability and safety community to the security problem in novel ways
- Learn from academic, industry, and other leaders about state of the art vulnerability management techniques and approaches. Work with leading researchers to establish a research agenda that meets industry needs
- Identify and establish technical standards that enable vulnerability management data interchange and interoperability.
- Reduce the cost of vulnerability management through improved products and automated VM tool/market development
Proposal:

The Open Group EVMi will consist of the following:

The Managers Guide to Enterprise Vulnerability Management

- This book is consistent with our program of developing useful guidance to business managers, however I suggest that we use it as also as a roadmap document for ourselves, describing our vision of the multiple facets of vulnerability management and the projects The Open Group will undertake.

- The book would include The Open Group Security Forum’s view of the vulnerability management problem in as large a context as we can handle from the CEO down to the practitioner, across the business performance, risk management, and compliance

Projects in the Manager’s guide (or deliverables) need to include:

- Vulnerability Assessment / Measurement
  - American Security Consortium’s Risk Preparedness Index? As enhanced by The Open Group Security Forum?
  - Review and incorporate NIST’s 800-53, other guidelines in this area
  - Feedback and support harmonization

- Compilation of VM Best Practices to include
  - Operational: A guide such as this the I3C requested as the best thing the Open Group SF could produce for vertical industries. If we were to analyze all the practices we know about (NIST, ISO, ISSA, others) as a general cross-industry baseline, we could then look at how we’d customize that base for vertical industries, perhaps then spinning off customization to other industry groups.
  - Systems Development Life Cycle such the work Dr. Robinson presented at the last meeting. We could develop an OG standard, linked to the architecture work of how vulnerability managed systems should be architected and managed throughout development.
  - Systems Architecture that includes how systems gracefully react to exploitation, optimizing their performance of critical functions perhaps at the expense of those less critical functions.
  - Vulnerability management methodology (as presented by NIST for FISMA regulated agencies, for example)

- Compilation and categorization of vendor products
  - Would our members benefit from a guide listing vendor products, what they do? Would we benefit from a book/guide/white paper describing how the vendor community views vulnerability management? This is one way to attract vendor members into the SF, giving them a way to make their product visible, discuss the technical deficiencies, and position their products.

- Standards Development
I believe that as we get into the technical understanding of VM products, we will discover areas where information interoperability/exchange is required to enable complete VM solutions built from vendor component products. Interoperable open systems thinking applied to solving the VM problem

- Regulatory Compliance Guidance
  - Given that we now understand assessment, best practices, standards, etc., can we give technical guidance in complying with regulations? Should we?

- Certifications
  - Would it make sense to develop certifications of products and processes that automate elements of the VM process? For example, would an OpenGroup Certified vulnerability scanner that fed results into the RPI be a good idea to enable an enterprise to assess its own RPI in certain areas independent of an auditor? Would results from “certified tools” be of sufficient quality to pass some parts of regulatory inspections? If so, there’s a business case for certifications of vulnerability management tools.

Building the Team and Making Progress

We know that this is an ambitious program. We know we don’t have the membership team in place to do it all. Our mission then is three fold

- Recruit and add new members to the Security Forum who are attracted to the EVMi.
- Bring in speakers who will help educate the membership in area we don’t understand well. Find and share material that builds the expertise of the membership group.
- Rely upon other industry expert groups to contribute as much of the total solution as possible. The Security Forum will reuse best of breed practices, standards, technology, and approaches. The Security Forum will only work on those items that haven’t been done before.

We have other opportunities to build the team and visibility of the initiative. Creative options include:

- Work with research institutions to create research projects to do work we don’t have the resources for. In turn share and expose the work researchers are doing in this area to our membership for support.
- Recruit executive sponsorship for product development companies to support the EVMi, particularly the work NIST is doing. The NIST work certainly will impact product requirements. Product developers should want to get in on the ground floor to understand their government customers’ guidelines and standards. Working with the Security Forum, these vendors can share their expert knowledge with the standards setter, to the benefit of all.
- Recruit executive sponsorship of major IT customers, particularly the critical infrastructure companies, to work with the EVMi. These customers directly or indirectly may be affected by the NIST guidelines. By working with the Security
Forum now, global IT security architects can share their knowledge to shape future standards they may have to live with in some way.

This proposal is just the beginning and will benefit from robust discussion and refinement. I ask you all to openly engage this discussion in a way that converges to a committed EVMi program we all will actively support.

Regards,

Mike Jerbic
Chair, Open Group Security Forum