

# AndyPurdy.com

## PRESENTATION EXCERPTS

### **Addressing National Cyber Risk Public-Private Partnership is the Cornerstone**

#### **GovTech 2008**

Hosted by the State Information Technology Agency (SITA), South Africa

Durban, South Africa

July 28, 2008, 8:30 am South Africa Time (2:30 am EST)

Cyber risk must be addressed with a keen understanding of the fact that there is a wide dispersion of ownership and control of cyberspace among government and the private sector. The interdependency between government and the critical infrastructure within and horizontally across the sectors within each nation, requires a new approach to addressing cyber risk, one that relies on an organized and resourced public-private partnership, rather than simply government leadership. This partnership should be focused on:

- assessing and mitigating cyber risk,
- enhancing the nation's preparedness to respond to, and recover from, malicious, man-made and natural cyber hazards, and
- reducing the frequency and impact of malicious cyber activity and cybercrime.

This collaboration and the information sharing that is an important component and requirement of it, requires engagement with other nations -- governments and private entities -- and CERTs (Computer Emergency Response Team) in the region and globally.

The experience of governments and private entities in dealing with malicious cyber activity, physical attacks, and natural disasters compels action by governments to ensure that physical and cyber risk is understood and addressed by key stakeholders. One lesson from the terrorist attacks against the United States on September 11, 2001, is that nations should not wait until they have specific information of an impending threat or attack to take protective action. Rather, they should engage in a risk management approach -- based on threat, that is, the intent and capability of malicious actors, and the existing vulnerabilities, and consequences if the vulnerabilities are exploited - to drive priorities for resource allocation and action.

Such a risk approach requires that the key stakeholders - the owners, operators, users, and producers—participate in this process. Because of the importance of the private sector to the risk associated with IT and communications infrastructures and systems, government should seek the involvement of representatives of the key entities in the assessment and mitigation of risk, and building a coordinated capability to detect and respond to significant cyber incidents. The entities that own and operate and depend on the critical infrastructure should actively seek to participate in this process on an ongoing basis. Although a key element of this process has to be information sharing—often in situations where trust is critical-- the private sector role is so important that it should be as a true partner, not just the source or recipient of information. Among the key sectors of a nation's economy that should be actively encouraged to participate in the planning, implementation, and operational stages of building and administering a national CERT, are Information Technology, telecommunications, finance, and power.

To build and maintain an effective national CERT requires a collaboration by key stakeholders in

government and the private sector who form a community of interest about the importance of maintaining the cyber (IT and telecommunications) infrastructure on which government and the critical infrastructure of a nation have come to depend, and will depend on increasingly as economies mature and grow. The national CERT should provide value to the government and private sector throughout the nation, by facilitating a common situational awareness about threats and vulnerabilities, a shared capability to analyze and assess the seriousness of cyber incidents as they develop, and a framework for coordinated efforts to respond to, and recover from, the most serious cyber incidents.

An effective national CERT requires a regularized multi-directional flow of incident and analysis information from key entities and government and the private sector, and from regional and global international partners. The information sharing capability requires an agreed-upon system for alerts and warnings so that protective and restorative action can be taken quickly to mitigate damage and expedite recovery.

This collaboration needs to identify current capabilities and requirements of government and the critical infrastructure, and of potential regional or global partners. There are a number of models for national CERTS that can be drawn on to create or improve a national CERT. A national CERT can be based in and run by the government, by academia, or a coalition between government and the private sector. Because of the importance of information sharing and collaboration, it is particularly valuable to leverage the existing CERT-like capabilities that exist in government, academia, or private companies. By using the "business case" that drives and funds these efforts, a partnership among current and planned efforts can save resources and build on existing skill sets, technologies, and information sharing mechanisms. An effective CERT requires serious and dynamic collaboration and information sharing.

Part of the process of building an effective national CERT should include active outreach to the key organizations in government and the private sector that have an interest and dependency on the cyber and communications infrastructure. The coalition should be broad-based to facilitate its effectiveness and secure necessary resources and information. In the United States, individual sectors - like IT, Communications, and Finance, among others - have formed Information Sharing and Analysis Centers (ISACs) to facilitate the exchange of cyber incident and analysis information, and to build communications mechanisms to respond effectively to incidents. An effective national CERT needs robust information coming in from and between government and the private sector, trusted sharing of analysis of the data, and a partnership mentality with government and the private sector for coordination of alerts, as well as for responding to cyber incidents and recovering from disruptions. This national collaboration should be complemented by similar engagement with global and regional organizations internationally, as well as with key government and private entities outside the boundaries of the nation, because of the inherently international nature of cyberspace.

It is vitally important to the future of cyberspace, and all who depend on it within government and the private sector, that the existing international collaboration and information sharing among national CERTS and key players in the IT and communications infrastructure be significantly enhanced. Just as it is critical within a nation, it is also essential internationally that international organizations, governments, and global companies build and operate at least an informal collaboration framework to assess and mitigate risk and enhance resiliency; build an international capability for detection, analysis, watch and warning, and response and recovery; and build a capability to collect and share information about the most significant malicious actors in cyberspace, those who enable them, and the black markets in malicious cyber tools for exploitation. The call for greater international coordination of collaboration and information sharing regarding cyber risk and preparedness is not a criticism of the activity that has developed to date; rather, it reflects the reality that the seriousness of the current global threat warrants a corresponding level of international engagement.

One necessary component of addressing cyber risk and enhancing a nation's preparedness, is to build a collaboration between law enforcement, others in government, and the private sector to dynamically assess the state of malicious activity and cyber crime affecting the nation, and work in

a coordinated fashion to reduce the frequency and magnitude of that malicious activity impacting or emanating from within the country. The national CERT, to warn potential victims of malicious cyber activity and generally educate organizations and individual users on how to reduce risk, should lead, or at least facilitate, a national awareness campaign about safe online practices.

In summary, the public-private collaboration to address national cyber risk should identify requirements for the national CERT and its engagement and partnership with government and the private sector, prepare a plan to build the CERT, seek necessary resources and support from within and outside the country, and lead the implementation of the plan. The CERT should publish regular updates on the progress toward effectiveness and the status of cyber risk, and promote outreach and awareness to help users reduce their risk. To more appropriately and adequately address the cyber risk, necessary preparedness requirements, and the scourge of malicious cyber activity, it is also incumbent on the global community to enhance collaboration and information sharing if the benefits of cyberspace are to continue to improve and spread to more citizens of the world.

*Andy Purdy is currently President of DRA Enterprises, Inc. in Bethesda, Maryland, USA ([www.andypurdy.com](http://www.andypurdy.com)), is a member of the Executive Advisory Board of BigFix, Inc. of Emeryville, California, and a partner in the law firm of Allenbaugh Samini, LLP ([www.alsalaw.com](http://www.alsalaw.com)). He is also co-founder of the International Cyber Center at George Mason University. Purdy served as a member of the White House staff in 2002-2003 that helped to draft the U.S. National Strategy to Secure Cyberspace released by President Bush in February 2003. He worked at the Department of Homeland Security from 2003 to 2006, the last two as Acting Director of the National Cyber Security Division/US-CERT.*