



Protecting our digital shores
Dec 7, 2011

Finding Disruptive Technologies to enhance the Cyber Environment

Peter Szczepankiewicz - IBM

Eric Ziegast – Internet Systems Consortium

Brian Foster – McAfee

Tom Byrnes - Threat Stop



Overview / Background

(discussion items)

A disruptive technology is an innovation that helps create a new market and value network, and eventually goes on to disrupt an existing market and value network (over a few years or decades), displacing an earlier technology there. The term is used in business and technology literature to describe innovations that improve a product or service in ways that the market does not expect, typically first by designing for a different set of consumers in the new market and later by lowering prices in the existing market *(wiki)*

Why pursue?

“ By having a logical framework for understanding CyberSecurity, and the major domains it represents, enterprises can implement their Cyber strategies and develop specific plans tailored for each domain. The challenge is far broader than simply addressing one issue such as securing mobile devices or securing cloud computing environments, so by ensuring the CyberSecurity strategy and logical framework addresses all of these inter-related trends, business leaders can be confident of a comprehensive approach...”

(from Unisys Disruptive Technology & Trend Point of View Whitepaper Series)

Overview / Background

(discussion items)

“Key focus areas should include governance, risk and compliance, users (identity assurance regardless of location or device type), data (sensitive data protection no matter where it resides), applications (application security modernization), infrastructure (securing the “borderless” enterprise including cloud computing) and assets (cyber supply chain). ...

There is no single answer for success, but by working across public- and private sector partnerships and by advancing security measures particularly with regard to mission-critical systems, processes and applications that are connected into cyberspace, businesses will be able to work towards a future environment that is both open and secure and prosperous....”

Major factors

(some of them... maybe)

Increasing Sophistication of CyberCrime

Cloud Computing

Rise of Mobile Devices & Applications

(The *consumerization of IT effect*)

Leakage of Sensitive Data (DLP...)

Increasing Regulatory Environment

THEN there is also...

Governance

Risk / Compliance

Identity / Access assurance

Application security

Supply chain security

ET AL.....

**Is there a 'magic bullet'
that we all secretly hope for**

OR

**Will it really take ALL of us doing
common things in similar ways?**

So where MIGHT we look?

Establish a logical framework for CyberSecurity

Re-visit plans related to Governance, Risk and Compliance

Manage User Identities and entitlements in a comprehensive, integrated approach - Centralized Identity and Access Management

Take a coordinated approach to Sensitive Data Protection

Incorporate CyberSecurity enhancements as an integral part of Application Modernization initiatives

Re-assess the integrity of your Cyber Supply (Value) Chain

Take advantage of the built-in capabilities of today's next generation devices to better secure mobile users, devices and applications

So what REALLY matters / makes a difference???