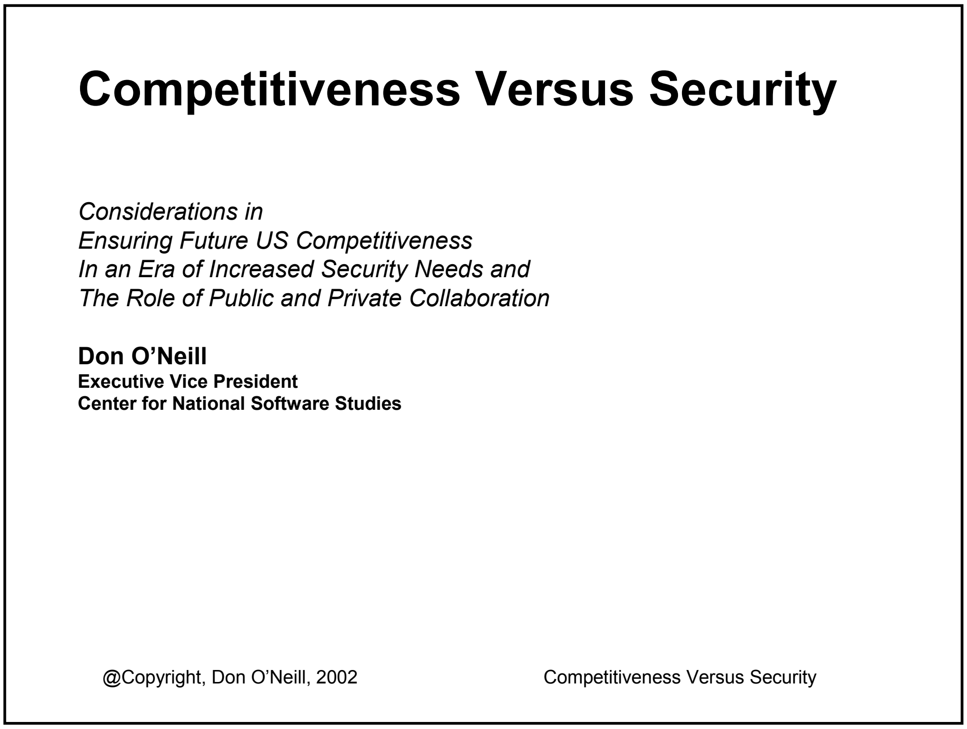
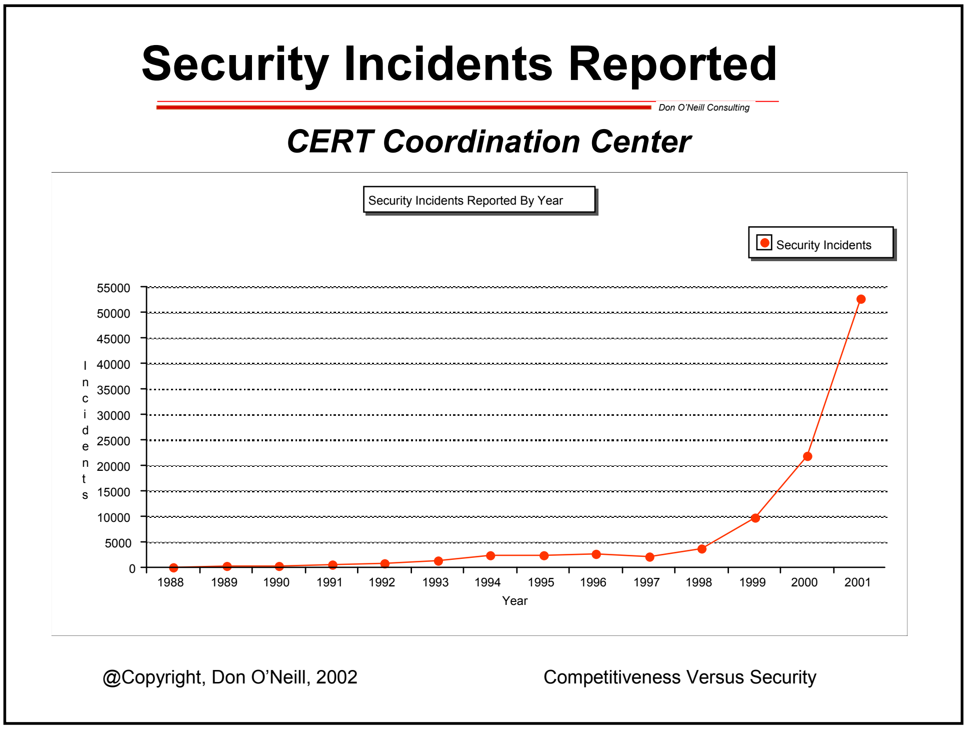


Competitiveness Versus Security

Considerations in
Ensuring Future US Competitiveness
In an Era of Increased Security Needs and
The Role of Public and Private Collaboration

Don O'Neill
Executive Vice President
Center for National Software Studies



Security Incidents Reported

Don O'Neill Consulting

CERT Coordination Center

Many Dimensions of Security

Spanning Boundaries

Threats, vulnerabilities, and readiness

Software architecture and trustworthiness

Best practices and certification of processes, people, and products

Private and public sectors and their tensions

Legislation and its unintended consequences

Government regulatory infrastructure

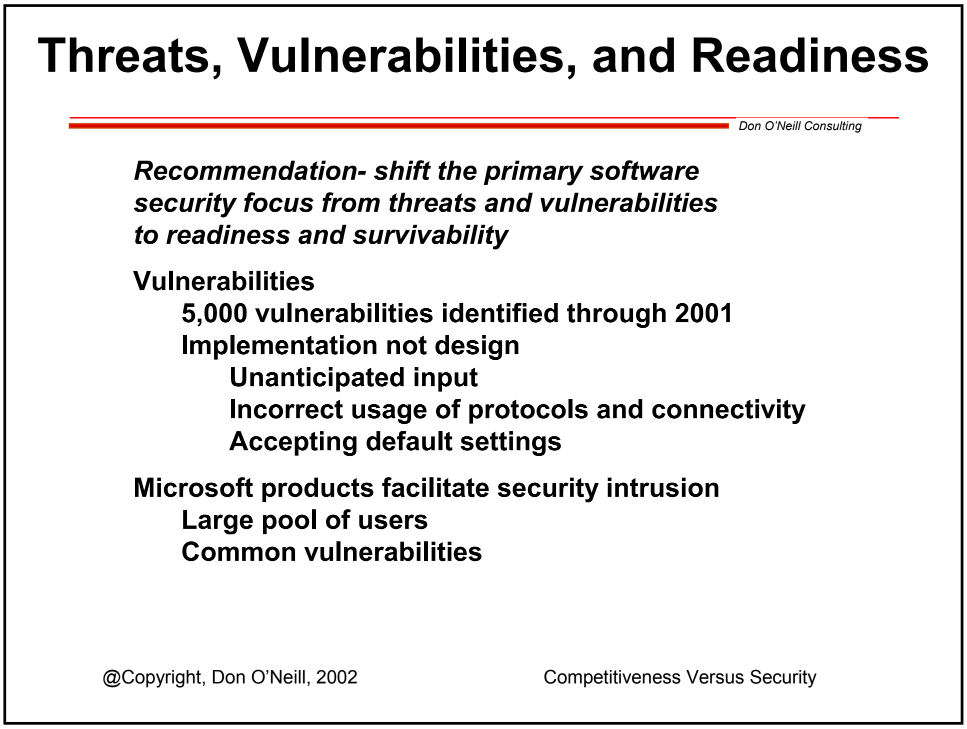
Lack of business incentive to promote security

Threats, Vulnerabilities, and Readiness

Recommendation- shift the primary software security focus from threats and vulnerabilities to readiness and survivability

Threats

- **90% exploit known flaws; 60% are random; 40% are targeted, persistence unknown**
- **100% of enterprises are attacked; only 30% admit it**
- **70% of attacks are carried out by insiders**
- **17% of attacks attributed to industrial espionage and competitive intelligence**

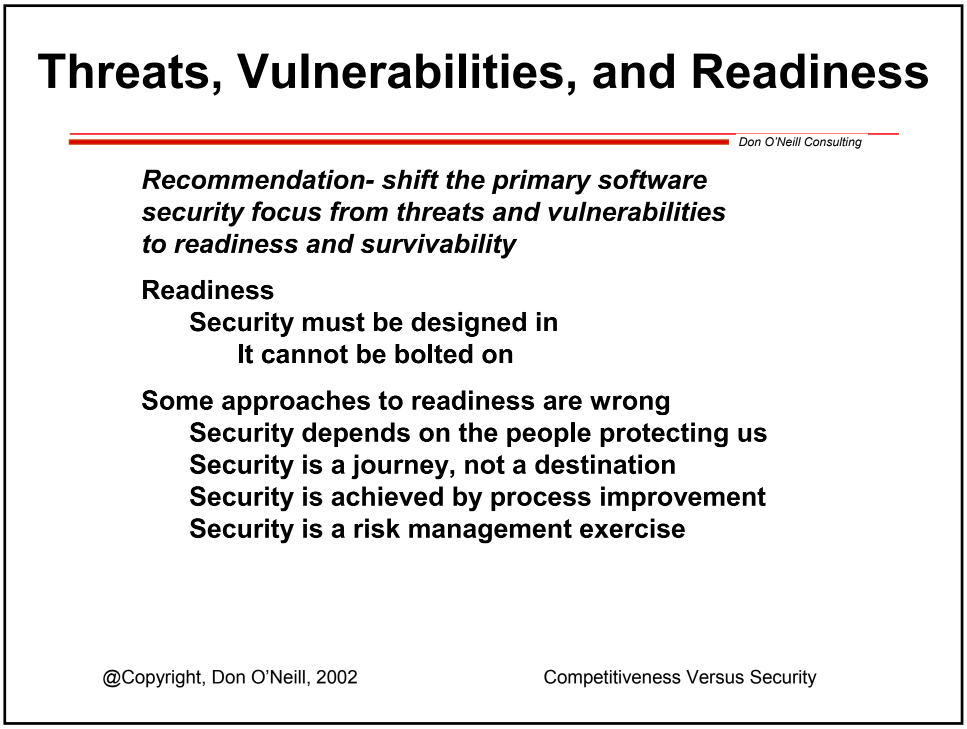


Threats, Vulnerabilities, and Readiness

Don O'Neill Consulting

Recommendation- shift the primary software security focus from threats and vulnerabilities to readiness and survivability

- Vulnerabilities
  - 5,000 vulnerabilities identified through 2001
  - Implementation not design
    - Unanticipated input
    - Incorrect usage of protocols and connectivity
    - Accepting default settings
- Microsoft products facilitate security intrusion
  - Large pool of users
  - Common vulnerabilities

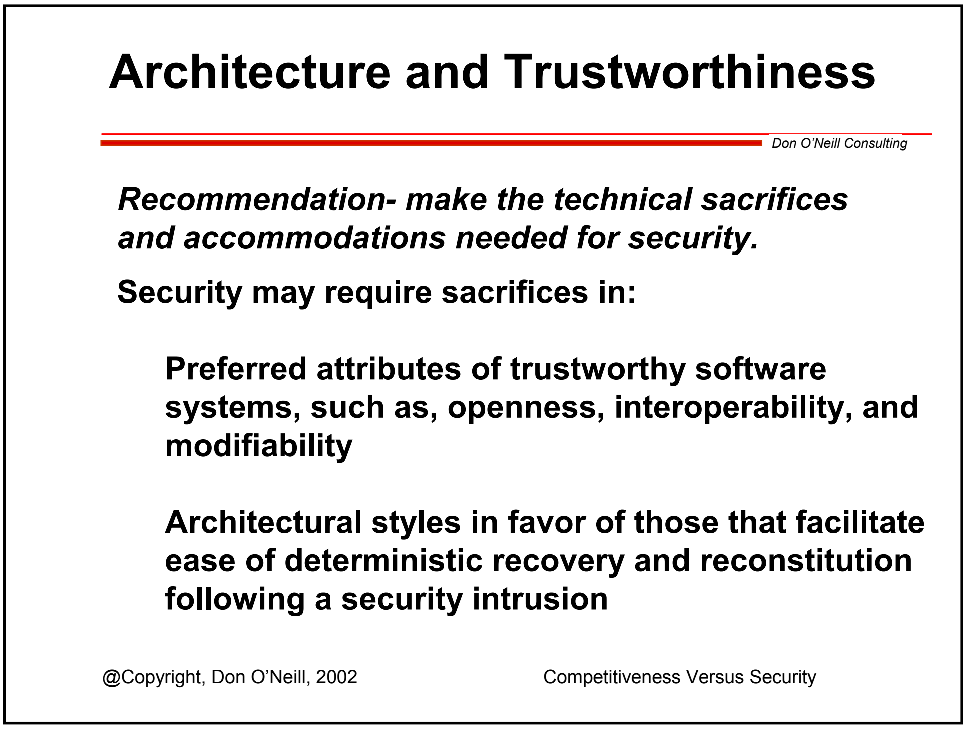


Threats, Vulnerabilities, and Readiness

Don O'Neill Consulting

Recommendation- shift the primary software security focus from threats and vulnerabilities to readiness and survivability

- Readiness
  - Security must be designed in
    - It cannot be bolted on
- Some approaches to readiness are wrong
  - Security depends on the people protecting us
  - Security is a journey, not a destination
  - Security is achieved by process improvement
  - Security is a risk management exercise



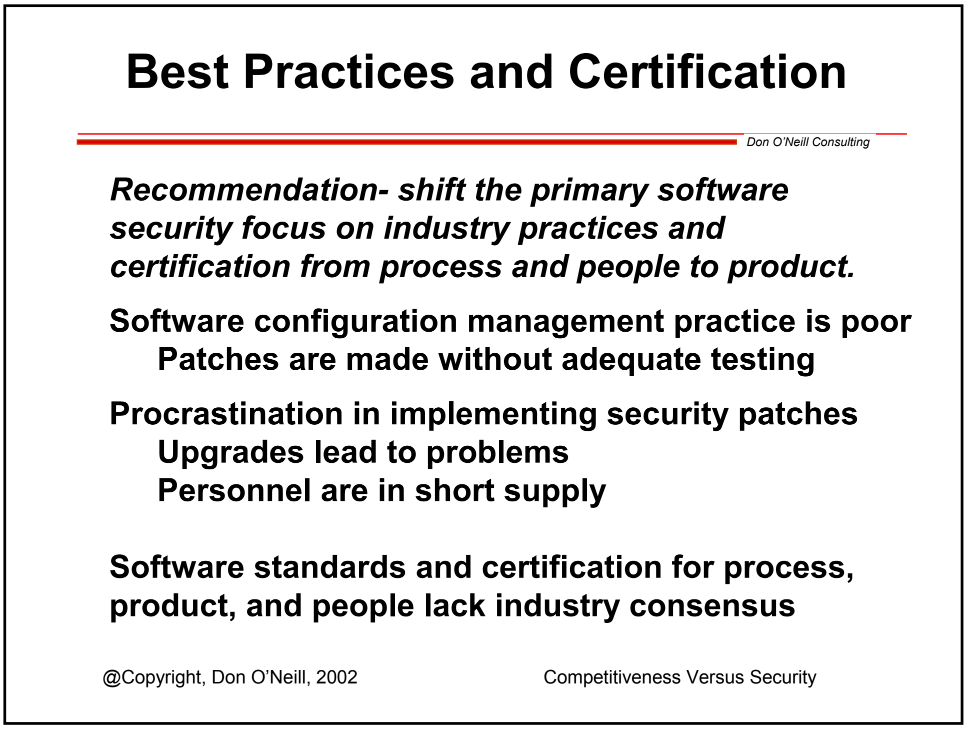
Architecture and Trustworthiness

Recommendation- make the technical sacrifices and accommodations needed for security.

Security may require sacrifices in:

- **Preferred attributes of trustworthy software systems, such as, openness, interoperability, and modifiability**

- **Architectural styles in favor of those that facilitate ease of deterministic recovery and reconstitution following a security intrusion**



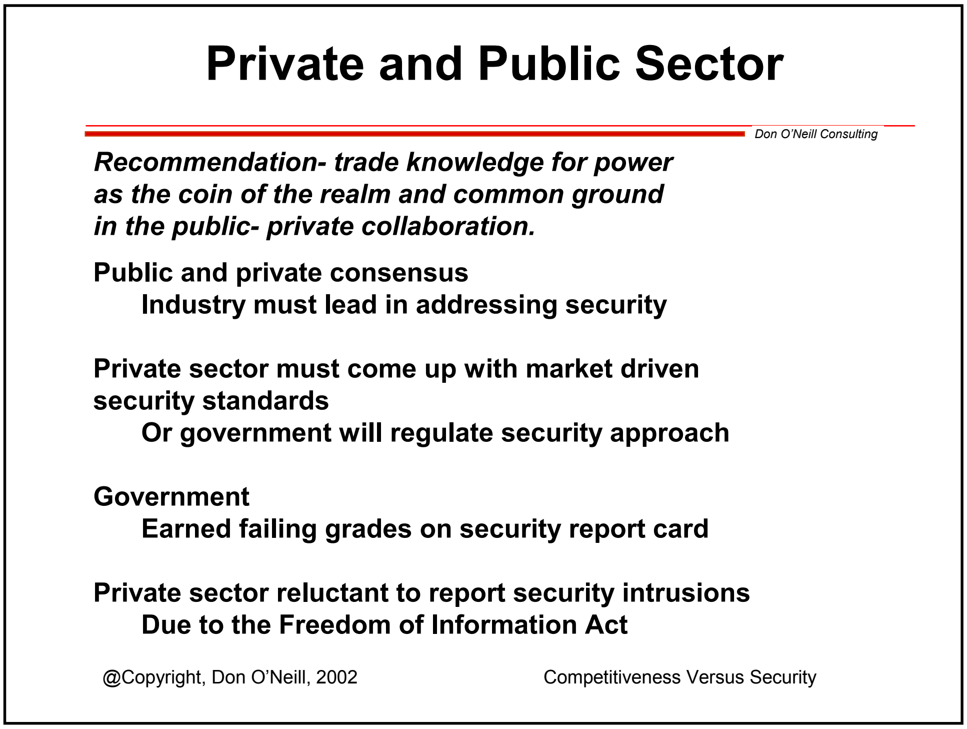
Best Practices and Certification

Recommendation- shift the primary software security focus on industry practices and certification from process and people to product.

Software configuration management practice is poor
- **Patches are made without adequate testing**

Procrastination in implementing security patches
- **Upgrades lead to problems**
- **Personnel are in short supply**

Software standards and certification for process, product, and people lack industry consensus



Private and Public Sector

Don O'Neill Consulting

Recommendation- trade knowledge for power as the coin of the realm and common ground in the public- private collaboration.

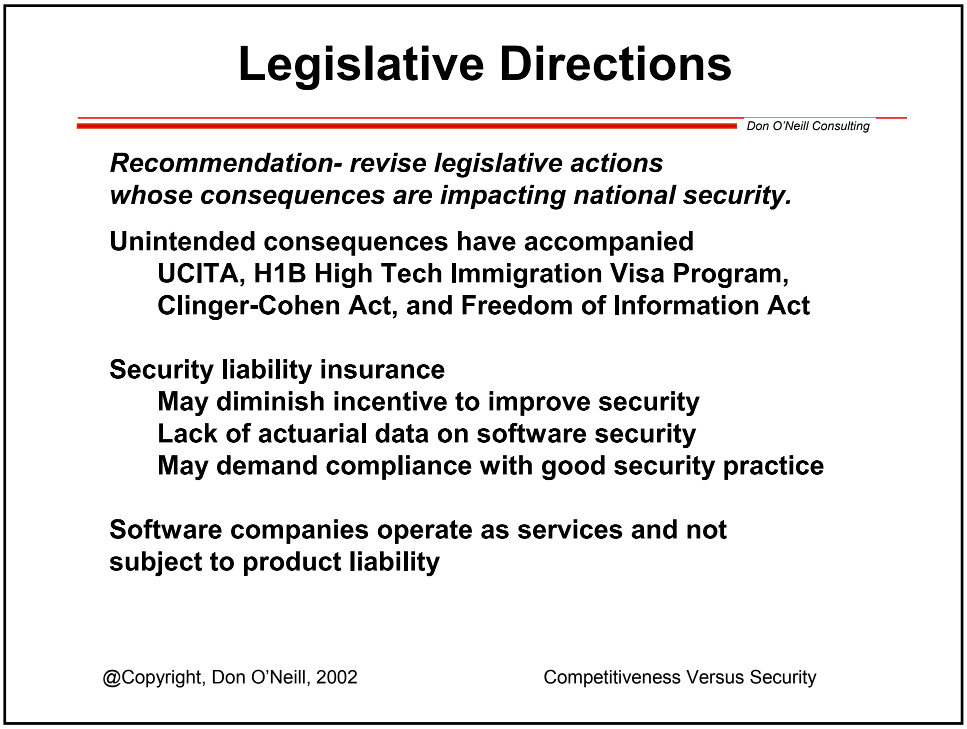
Public and private consensus
- **Industry must lead in addressing security**

Private sector must come up with market driven security standards
- **Or government will regulate security approach**

Government
- **Earned failing grades on security report card**

Private sector reluctant to report security intrusions
- **Due to the Freedom of Information Act**

Competitiveness Versus Security



Legislative Directions

Don O'Neill Consulting

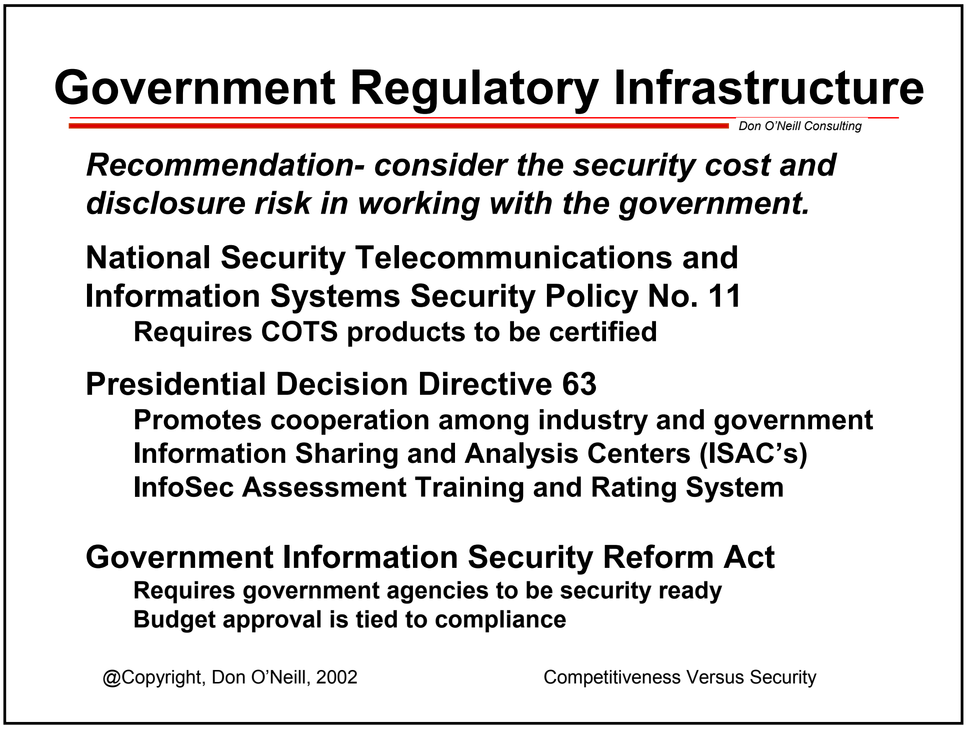
Recommendation- revise legislative actions whose consequences are impacting national security.

Unintended consequences have accompanied
- **UCITA, H1B High Tech Immigration Visa Program, Clinger-Cohen Act, and Freedom of Information Act**

Security liability insurance
- **May diminish incentive to improve security**
- **Lack of actuarial data on software security**
- **May demand compliance with good security practice**

Software companies operate as services and not subject to product liability

Competitiveness Versus Security



Government Regulatory Infrastructure

Recommendation- consider the security cost and disclosure risk in working with the government.

National Security Telecommunications and Information Systems Security Policy No. 11

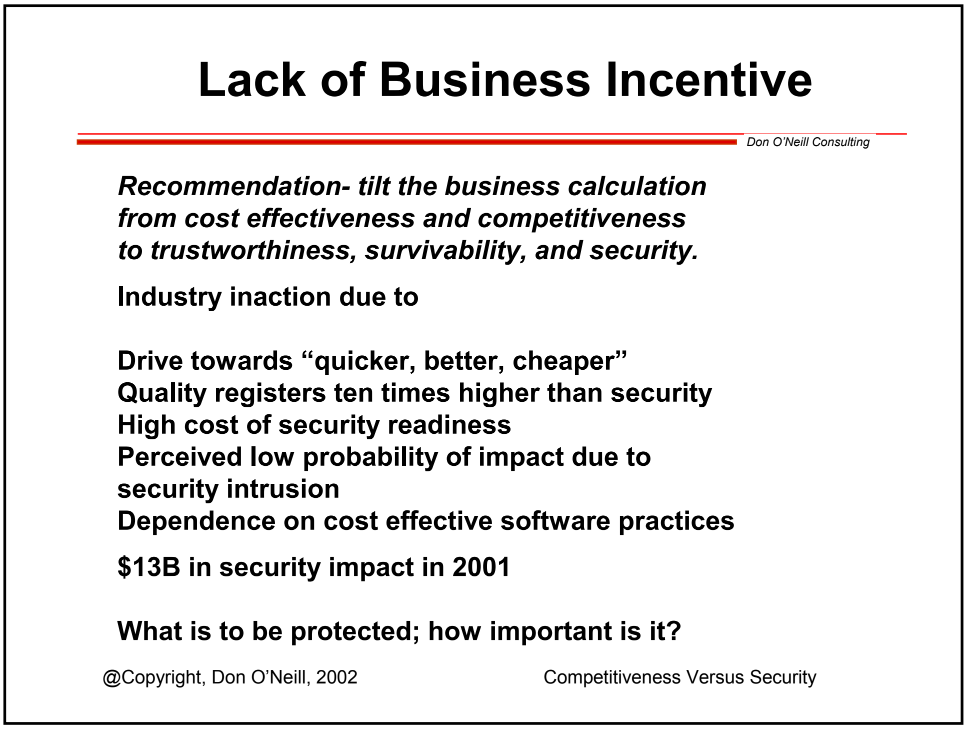
- **Requires COTS products to be certified**

Presidential Decision Directive 63

- **Promotes cooperation among industry and government**
- **Information Sharing and Analysis Centers (ISAC's)**
- **InfoSec Assessment Training and Rating System**

Government Information Security Reform Act

- **Requires government agencies to be security ready**
- **Budget approval is tied to compliance**



Lack of Business Incentive

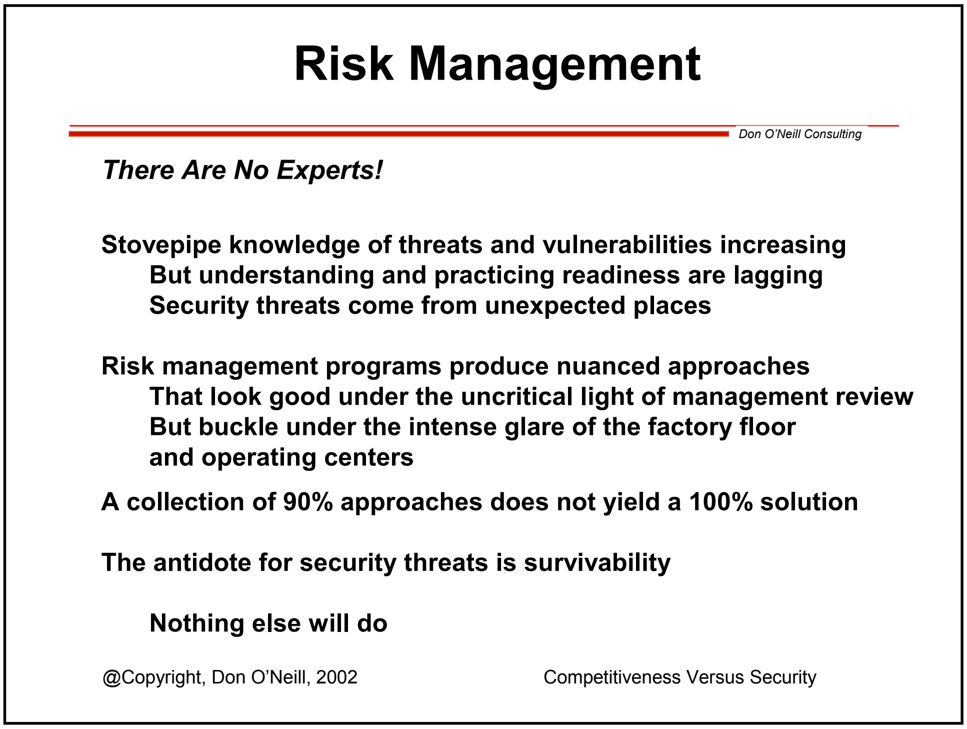
Recommendation- tilt the business calculation from cost effectiveness and competitiveness to trustworthiness, survivability, and security.

Industry inaction due to

Drive towards "quicker, better, cheaper"
Quality registers ten times higher than security
High cost of security readiness
Perceived low probability of impact due to security intrusion
Dependence on cost effective software practices

$13B in security impact in 2001

What is to be protected; how important is it?



Risk Management

Don O'Neill Consulting

There Are No Experts!

Stovepipe knowledge of threats and vulnerabilities increasing
But understanding and practicing readiness are lagging
Security threats come from unexpected places

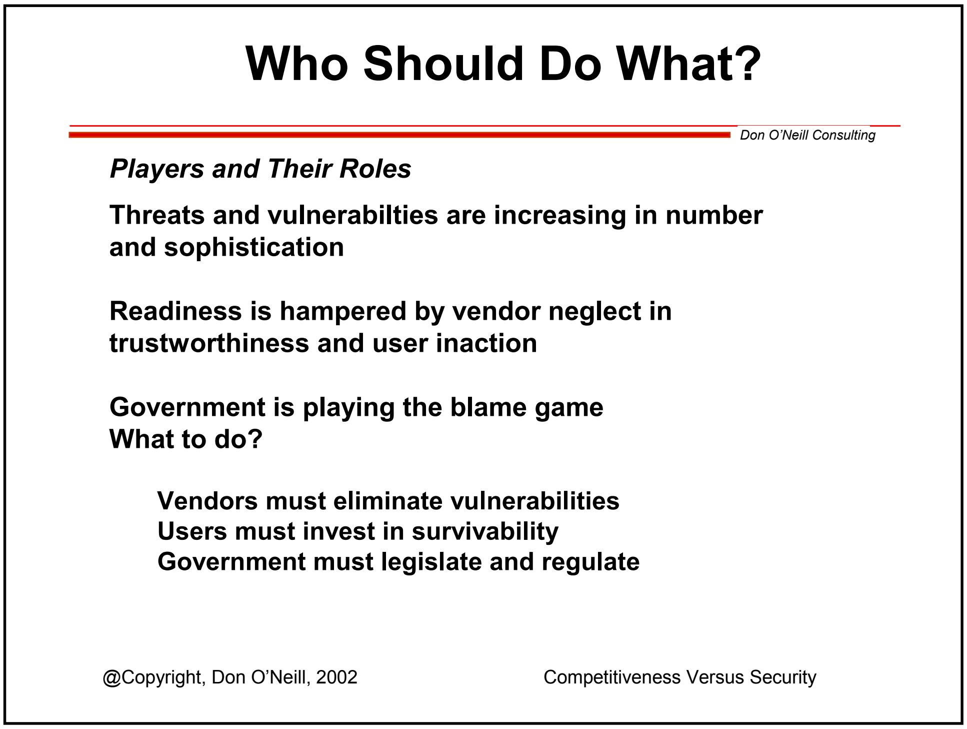
Risk management programs produce nuanced approaches
That look good under the uncritical light of management review
But buckle under the intense glare of the factory floor
and operating centers

A collection of 90% approaches does not yield a 100% solution

The antidote for security threats is survivability

Nothing else will do

Competitiveness Versus Security



Who Should Do What?

Don O'Neill Consulting

Players and Their Roles

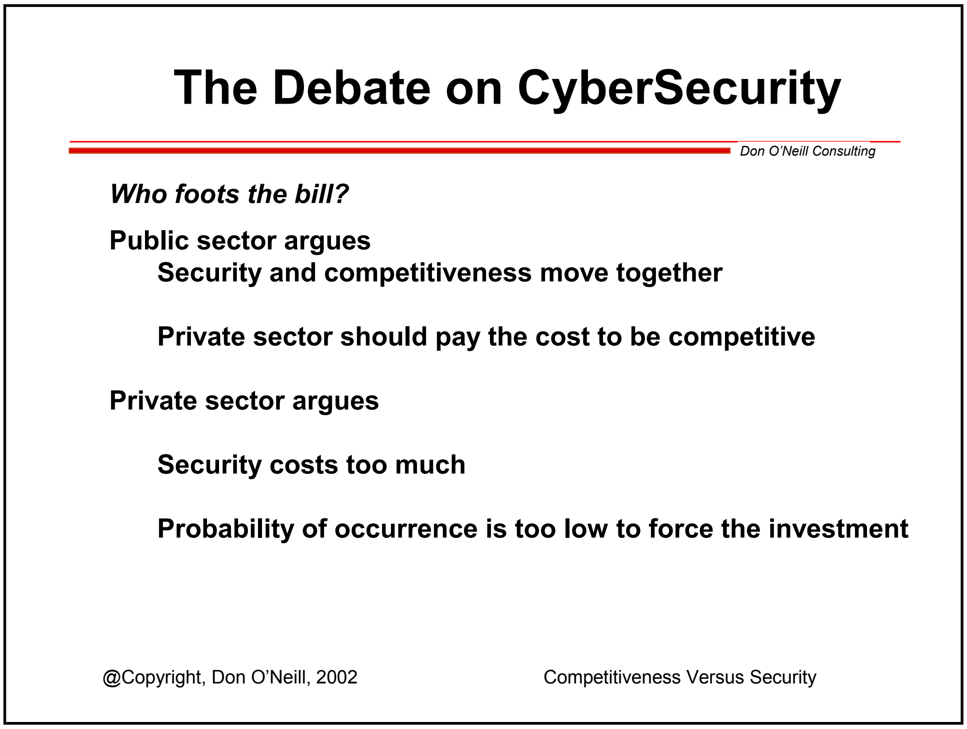
Threats and vulnerabilties are increasing in number and sophistication

Readiness is hampered by vendor neglect in trustworthiness and user inaction

Government is playing the blame game
What to do?

Vendors must eliminate vulnerabilities
Users must invest in survivability
Government must legislate and regulate

Competitiveness Versus Security



The Debate on CyberSecurity

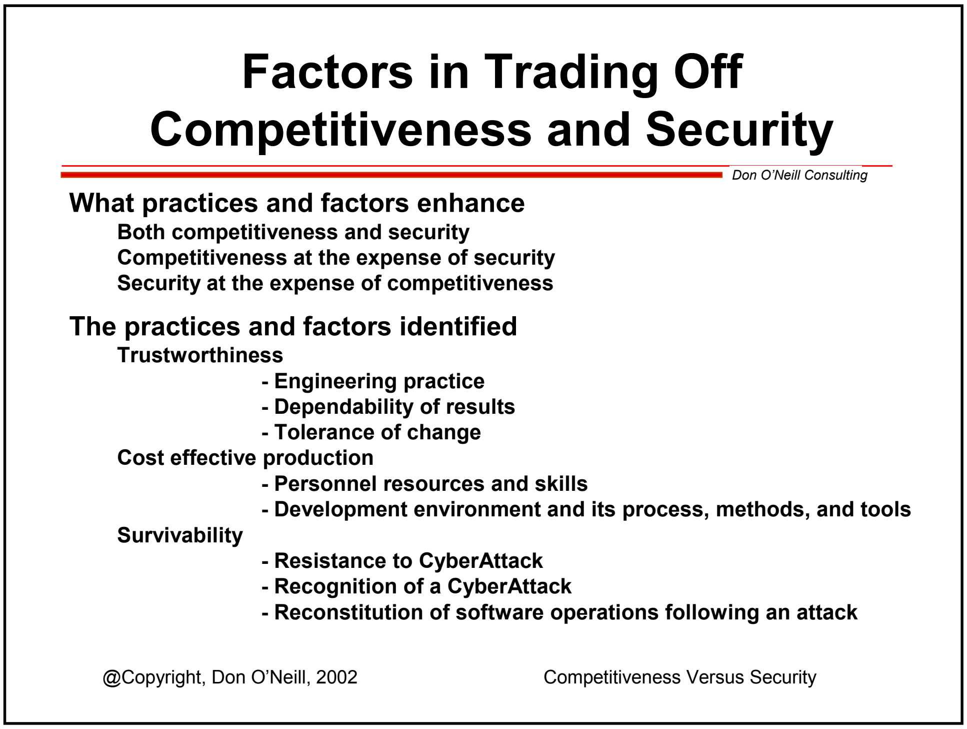
Who foots the bill?

Public sector argues

- **Security and competitiveness move together**
- **Private sector should pay the cost to be competitive**

Private sector argues

- **Security costs too much**
- **Probability of occurrence is too low to force the investment**



Factors in Trading Off Competitiveness and Security

What practices and factors enhance

- **Both competitiveness and security**
- **Competitiveness at the expense of security**
- **Security at the expense of competitiveness**

The practices and factors identified

- **Trustworthiness**
  - **Engineering practice**
  - **Dependability of results**
  - **Tolerance of change**
- **Cost effective production**
  - **Personnel resources and skills**
  - **Development environment and its process, methods, and tools**
- **Survivability**
  - **Resistance to CyberAttack**
  - **Recognition of a CyberAttack**
  - **Reconstitution of software operations following an attack**

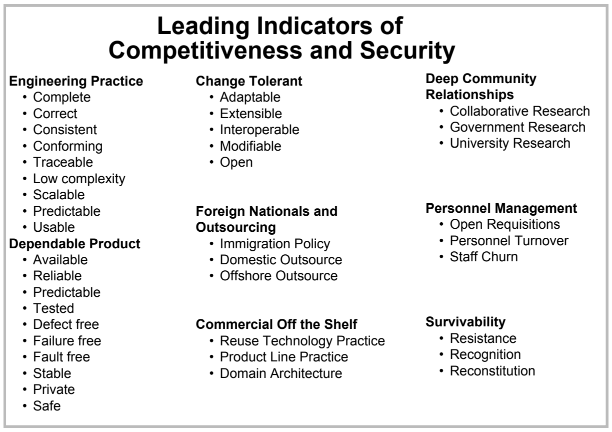
Competitiveness Versus Security

Impacting Factors

Factors	Competitiveness	Security
Engineering Practice	+	+
Dependable Product	+	+
Change Tolerance	+	- [Ease of Change]
Cost Effectiveness	+	- [Foreign Nationals, COTS]
Deep Community Rel.	+	- [Collaborative Research]
Personnel Management	- [Personnel Turnover]	- [Personnel Turnover]
Survivability	- [Resist, Recognize, Reconstitute]	+

Figure 3: Trade Off Factors

Leading Indicators of Competitiveness and Security



Leading Indicators of Competitiveness and Security

Engineering Practice
- Complete
- Correct
- Consistent
- Conforming
- Traceable
- Low complexity
- Scalable
- Predictable
- Usable

Dependable Product
- Available
- Reliable
- Predictable
- Tested
- Defect free
- Failure free
- Fault free
- Stable
- Private
- Safe

Change Tolerant
- Adaptable
- Extensible
- Interoperable
- Modifiable
- Open

Foreign Nationals and Outsourcing
- Immigration Policy
- Domestic Outsource
- Offshore Outsource

Commercial Off the Shelf
- Reuse Technology Practice
- Product Line Practice
- Domain Architecture

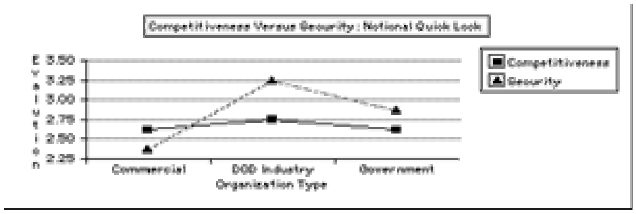
Deep Community Relationships
- Collaborative Research
- Government Research
- University Research

Personnel Management
- Open Requisitions
- Personnel Turnover
- Staff Churn

Survivability
- Resistance
- Recognition
- Reconstitution

Competitiveness Versus Security

Notional Quick Look



Practice	Commercial	DOD Industry	Government
Engineering Practice	1	3	2
Dependable Product	2	3	1
Ease of Change	2	3	1
Foreign Nationals	4	2	3
Commercial Products	4	2	2
Collaborative Research	2	4	3
Personnel Management	4	3	2
Survivability	2	4	1

competitiveness=(engineering+dependable+change+foreign+cots+research+(6-personnel)+(6-survivability))/8
security=(engineering+dependable+(6-change)+(6-foreign)+(6-cots)+(6-research)+(6-personnel)+survivability)/8

What Findings Are Suggested?

Rebalance Cost Effectiveness Tactics

- Downplay emphasis on "better, quicker, cheaper"
- Reverse usage of foreign nationals
- Reconsider commercial off the shelf usage

Strengthen Industry Capacity

- Promote trustworthiness in software systems
- Counter CyberSecurity threat with Survivability

Revisit Legislative Directions

- UCITA
- H1B High Tech Immigration Visa Program
- Clinger-Cohen Act
- Freedom of Information Act

Software Survivability

Forge a shared vision on the nature of the threat, vulnerabilities, and readiness

Realistic Assumptions

Threats continuously evolve

Vulnerabilities are large and growing

Critical assets are under continuous attack by insiders and outsiders

Attacks are targeted, persistent, directed at both system and application, and adaptive

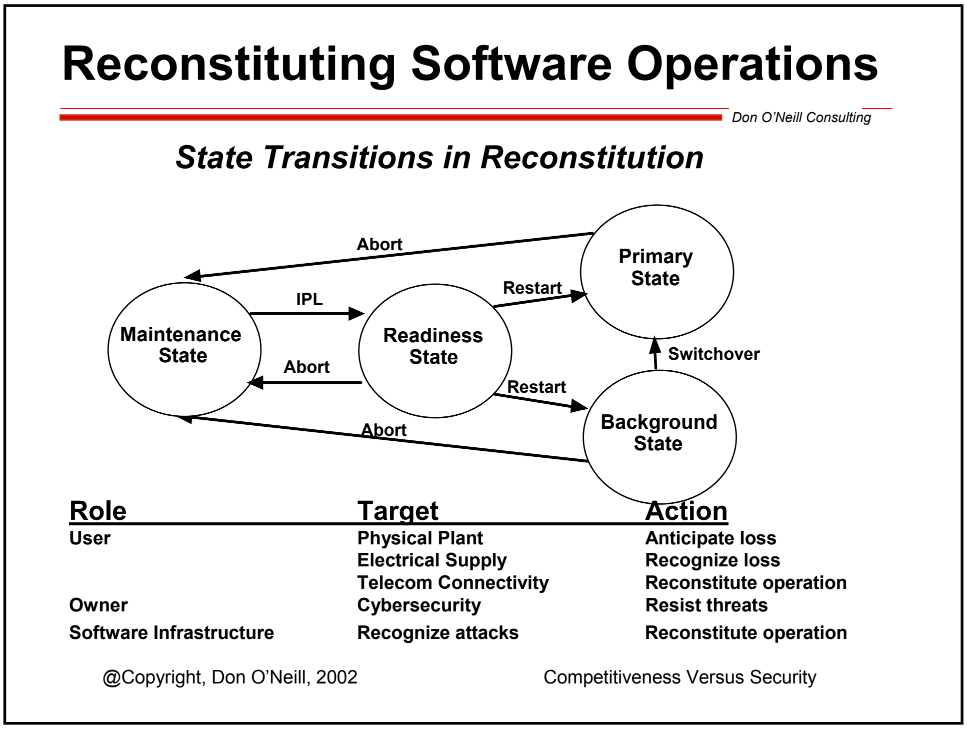
Threats and vulnerabilties are outside the control of the enterprise and not fully knowable

Survivability strategies must be independent of threats and vulnerabilities

Survivability Model

Cybersecurity Survivability Model

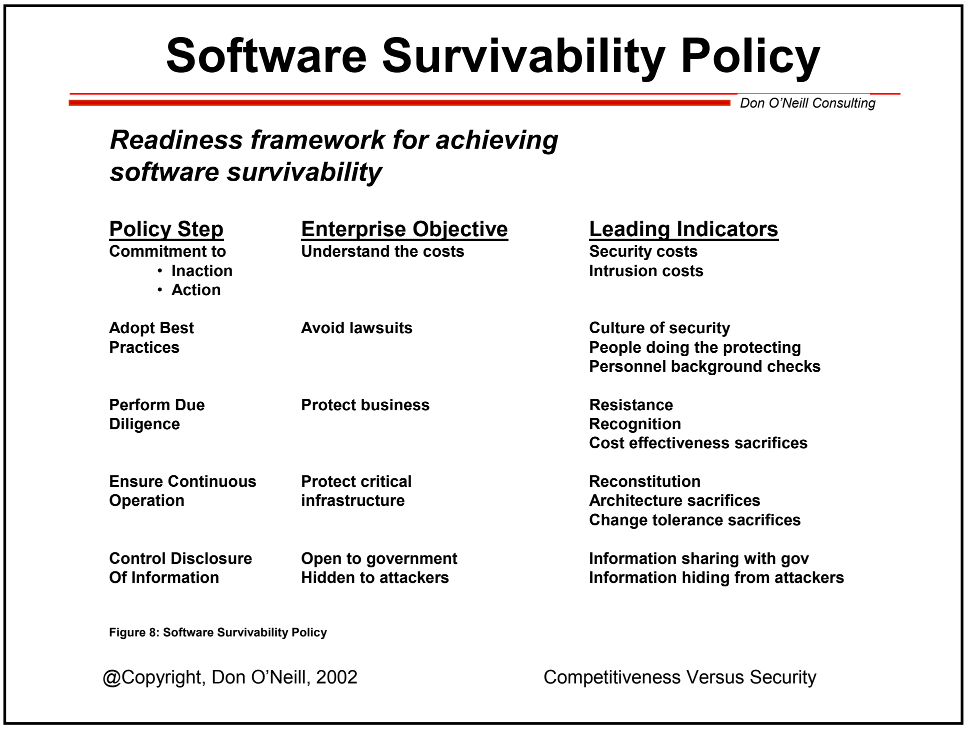
	Function	Form	Fit
Resistance • **Bulletproof**	-User authorization -Access Control -Encryption -Firewalls -Proxy servers	-Dispersion of data -Diversification of systems -Rules of construction -State data isolation -Systematic programming -Disciplined data	-50% loading -Predictable response -No memory leaks -Rate Monotonic scheduling -Time line vs. event driven
Recognition • **Detect**	-Cyber forensics -Normal operation monitoring -Backup operation -Shadow operation -Fully redundant operation -Voting	-Intrusion usage patterns -Virus scans -Internal integrity checking -Secure state data monitor -Exception handlers	-Monitor memory management -Time line predictability -Watch-dog timer
Reconstitution • **Restore** • **Continue**	-Restore data and programs -Minimum essential function -Alternative services -Disaster recovery	-Full system state architecture -Minimum essential function -Isolation of damage	-Full system predictability -Reduced volume -Conserve time and memory



Reconstituting Software Operations

State Transitions in Reconstitution

Role	Target	Action
User	Physical Plant	Anticipate loss
	Electrical Supply	Recognize loss
	Telecom Connectivity	Reconstitute operation
Owner	Cybersecurity	Resist threats
Software Infrastructure	Recognize attacks	Reconstitute operation



Software Survivability Policy

Readiness framework for achieving software survivability

Policy Step	Enterprise Objective	Leading Indicators
Commitment to • Inaction • Action	Understand the costs	Security costs Intrusion costs
Adopt Best Practices	Avoid lawsuits	Culture of security People doing the protecting Personnel background checks
Perform Due Diligence	Protect business	Resistance Recognition Cost effectiveness sacrifices
Ensure Continuous Operation	Protect critical infrastructure	Reconstitution Architecture sacrifices Change tolerance sacrifices
Control Disclosure Of Information	Open to government Hidden to attackers	Information sharing with gov Information hiding from attackers

Figure 8: Software Survivability Policy

Security Best Practices

Information Security Alliance

General Management
Policy
Risk Management
Security Architecture & Design
User Issues
System & Network Management
Authentication & Authorization
Monitor & Audit
Physical Security
Continuity Planning & Disaster Recovery

Security Training Curriculum

Certified Information System Security Professional (CISSP) by (ISC)2

Access Control System
Application and System Security
Business Continuity Planning
Disaster Recovery Planning
Cryptography
Law, Investigations, and Ethics
Operations Security
Physical Security
Security Architecture
Security Management Practice
Telecommunication and Network Security

Conclusion

Government and Industry Responsibilities

While government cannot make us safe
It can tilt the business calculation towards security

Industry software products make us vulnerable
So it must make the sacrifices needed to achieve security

References

Issue Summary

http://members.aol.com/ONeillDon2/issue-summary.html

Technical Report

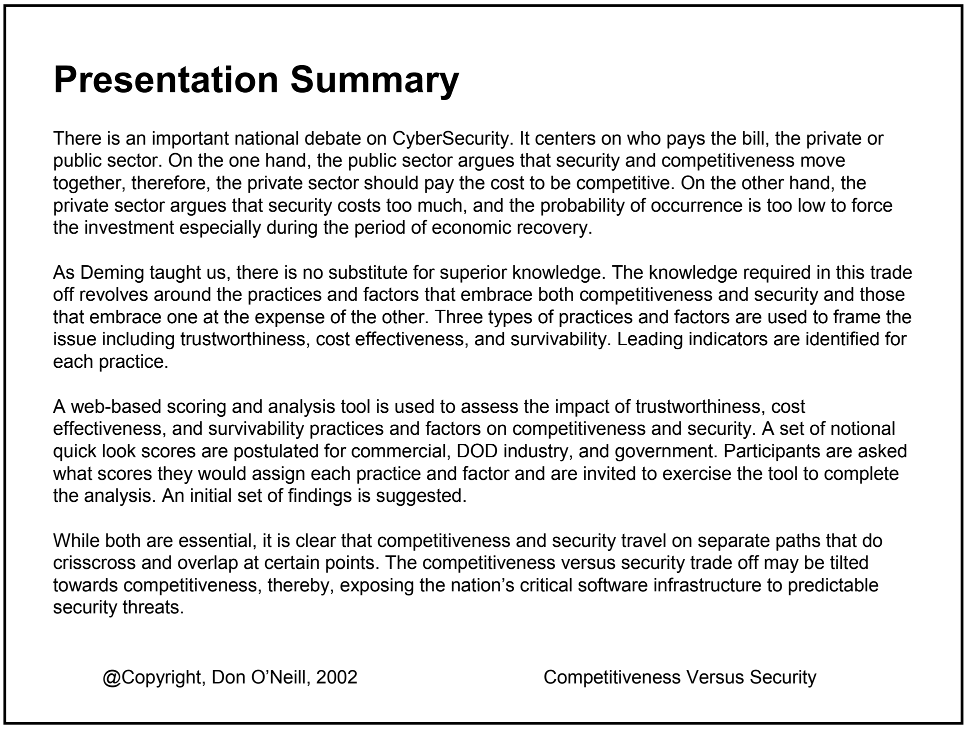
http://members.aol.com/ONeillDon2/comp-sec-paper.html

Factor Scoring and Impact Analysis Tool

http://members.aol.com/ONeillDon2/comp-sec_frames.html

Send email

ONeillDon@aol.com



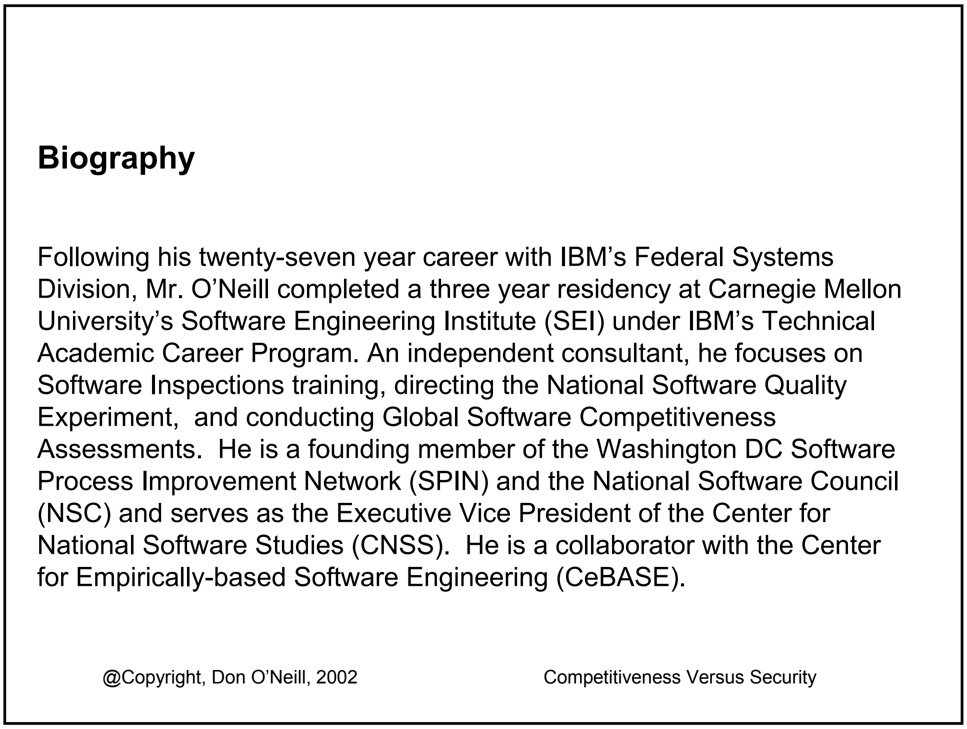
Presentation Summary

There is an important national debate on CyberSecurity. It centers on who pays the bill, the private or public sector. On the one hand, the public sector argues that security and competitiveness move together, therefore, the private sector should pay the cost to be competitive. On the other hand, the private sector argues that security costs too much, and the probability of occurrence is too low to force the investment especially during the period of economic recovery.

As Deming taught us, there is no substitute for superior knowledge. The knowledge required in this trade off revolves around the practices and factors that embrace both competitiveness and security and those that embrace one at the expense of the other. Three types of practices and factors are used to frame the issue including trustworthiness, cost effectiveness, and survivability. Leading indicators are identified for each practice.

A web-based scoring and analysis tool is used to assess the impact of trustworthiness, cost effectiveness, and survivability practices and factors on competitiveness and security. A set of notional quick look scores are postulated for commercial, DOD industry, and government. Participants are asked what scores they would assign each practice and factor and are invited to exercise the tool to complete the analysis. An initial set of findings is suggested.

While both are essential, it is clear that competitiveness and security travel on separate paths that do crisscross and overlap at certain points. The competitiveness versus security trade off may be tilted towards competitiveness, thereby, exposing the nation’s critical software infrastructure to predictable security threats.



Biography

Following his twenty-seven year career with IBM’s Federal Systems Division, Mr. O’Neill completed a three year residency at Carnegie Mellon University’s Software Engineering Institute (SEI) under IBM’s Technical Academic Career Program. An independent consultant, he focuses on Software Inspections training, directing the National Software Quality Experiment, and conducting Global Software Competitiveness Assessments. He is a founding member of the Washington DC Software Process Improvement Network (SPIN) and the National Software Council (NSC) and serves as the Executive Vice President of the Center for National Software Studies (CNSS). He is a collaborator with the Center for Empirically-based Software Engineering (CeBASE).

Mission of CNSS

The Center for National Software Studies (CNSS) is a public policy research organization established as a non-profit 501(c)(3) status. The CNSS is a private corporation governed by a board of directors and accepts funding through contributions and grants. With a mission to elevate software to the national agenda, the CNSS is set up to provide objective expertise, studies, and recommendations on national software issues. The software issues of national importance identified by the CNSS include:

Software Value to US Economic Competitiveness
Software System Trustworthiness
Research and Development Funding
Software Workforce Issues
Maintaining Security and Privacy in Electronic Commerce
Protecting Intellectual Property and Preventing Piracy

Currently in Phase I, the CNSS startup operation is a web-based eCenter intended to prove its viability and value as a national resource. Background information is available in the CNSS Prospectus & Strategic Plan and the CNSS web page at http://www.CNsoftware.org.