

NCOIC™

LOCKHEED MARTIN

The State of Cyber Security 2011

LtGen (ret) Charlie Croom
Chair, NCOIC Executive Council
Vice President, Cyber Security Solutions, Lockheed Martin

Approved for Public Release
Distribution Unlimited
NCOIC-NCW-CC20110125

NCOIC is a Unique Organization

NCOIC exists to facilitate the global realization of Network Centric Operations/Net Enabled Capability. We seek to enable interoperability across joint, interagency, intergovernmental, and multinational industrial and commercial operations.

- Global Organization
- Voice of industry
- Cadre of technical experts
- Dedicated to interoperability
- Advisory Council of senior advisors who help prioritize our work in a non-competitive environment



In the photo: BrigGen Dieter Dammjacob (DEU AF)-J3 NATO Supreme Headquarters, Allied Powers Europe; Lt.Col. Danut Tiganus-CIS Directorate, EU Military Staff; Dr. Tom Buckman-NC3A Chief Architect; Gen Harald Kujat,-German AF (Ret.) former Chief of Staff of German Armed Forces & head of NATO Military Committee, Marcel Staicu-European Defense Agency NEC Project Officer .

NCOIC Members

80+ Member Organizations including leading IT and Aerospace & Defense companies, government organizations, non-governmental organizations and academic institutions

Members from 18 Countries

Advisors from 26 key stakeholders from Australia, EDA, France, Germany, Italy, NATO, The Netherlands, Sweden, UK and US



Working Group collaboration



Technical Council



Terry Morgan honors outgoing Advisory Council Chair, Keith Hall



Executive and Advisory Council joint meeting

Relationships

■ Government

- Australia Defence Organization (ADO)
- Eurocontrol
- European Defence Agency
- National Geospatial Intelligence Agency
- NATO
 - ACT
 - NC3A
 - NCSA
- Netherlands Command & Control Centre of Excellence
- Sweden Civil Aviation Authority (LFV)
- Sweden Defence Materiel Administration (FMV)
- US Defense Information Systems Agency (DISA)
- US Department of Homeland Security (DHS)
- US Federal Aviation Administration (FAA)
- US Joint Forces Command (JFCOM)
- US NAVAIR
- US SPAWAR
- OSD(NII)

■ Organizational

- Australia Defence Information & Electronic Systems Association (ADIESA)
- NATO Industry Advisory Group (NIAG)
- OASIS
- Open Geospatial Consortium
- World Wide Consortium for the Grid (W2COG)



2008 IDGA Award:
Outstanding Contribution
to the Advancement
of Network Centric Warfare

Current State of Cyber Security




- Trends
- Shifting Dimensions of the Global Threat?
- Facts About Intrusions
- How Serious Is The Threat?
- What is the Strategy?
- Are We Ready?
- A Way Ahead

Where Do We Have Consensus?

Trends

- 
- Social Networking
 - Mobile Devices
 - Non-Computing Devices (printers, networked TV)
 - Personal Electronic Devices in Office
 - Wiki Leak-like occurrences
 - Privacy concerns
 - Cloud computing
 - Malware creation
 - “Hacktivism” (cyber protests)
 - Social Engineering

- 
- Company investment
 - Maturing cyber security processes
 - Personal background checks
 - Portable device security standards/procedures
 - Compliance testing
 - Employee security awareness training
 - Authentication based on use risk classification
 - Centralized security information management process

• PWC 2011 Global State of Information Security Survey[®]

Networks Become Borderless, There Is No Perimeter

Shifting Dimensions of the Global Threat

Has the Threat Fundamentally Changed in 2011?



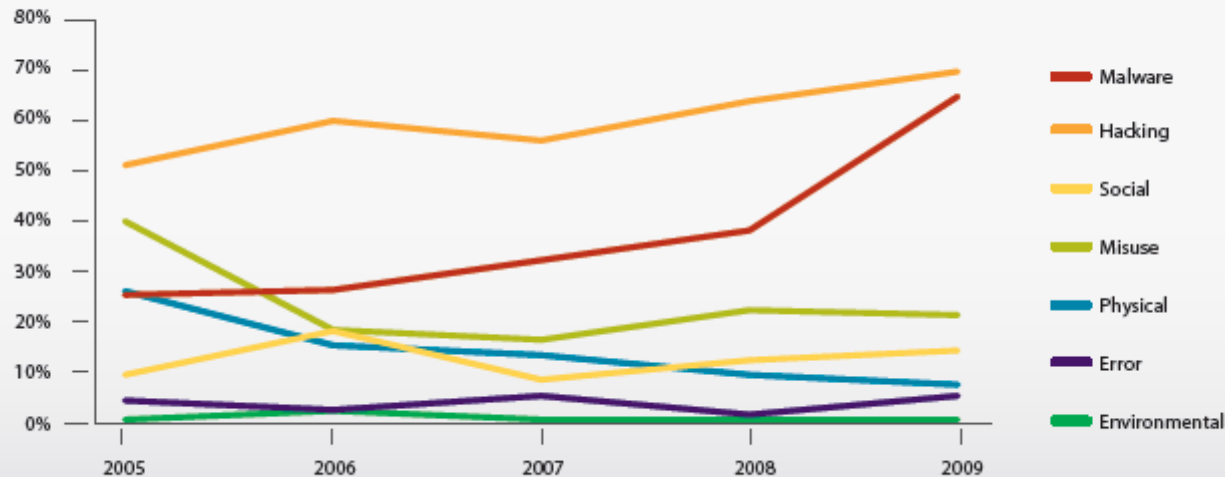
Event	Why it's significant
CISCO (Counterfeit Equipment)	CISCO Product Integrity Damaged...\$145M seized by FBI
Buckshot Yankee (Malicious Flashdrive)	DOD Classified and UnClassified Systems Compromised
Google	Publicly Identified An Intrusion, Asked for Government Help
Stuxnet	High Level Of Sophistication and Target Specific
Wiki Leaks	Insider Threat, Activists Empowered

Lesson: lack of vigilance in a changing landscape increases risk

What Was The Cost Of Being Insecure \$\$\$\$

Facts About Intrusions

Figure 16. Threat action categories over time by percent of breaches (Verizon cases)



Verizon 2010 Data Breach Investigation Report

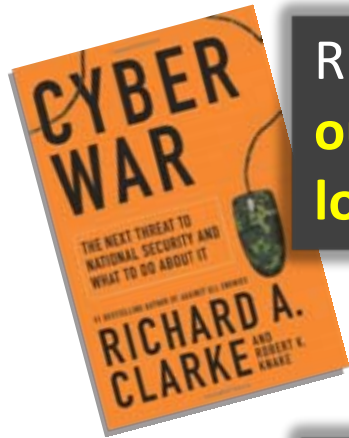
WHO IS BEHIND DATA BREACHES?

- 48% were caused by insiders
- 11% implicated business partners

WHAT COMMONALITIES EXIST?

- 85% of attacks were not considered highly difficult
- 61% were discovered by a third party
- 86% of victims had evidence of the breach in their log files
- 96% of breaches were avoidable through simple or intermediate controls

Is It This Serious?






Richard Clarke: **a vision in which thousands die; cities run out of food; the world's finance system collapses and looters take to the streets.**

“In all wars America has fought, no nation has ever done this kind of damage to our cities. But a sophisticated cyber war attack by one of several nation-states could do that today, **in 15 minutes**, without a single terrorist or soldier ever appearing in this country.”

National Post, Peter Goodspeed, 23 Oct 2010

Why Haven't We Been Attacked?

Differing Points of View on Cyber Threat

Theme	Strategy	Approach	Common?
Admiral McConnell  "We are at War, and we are losing"	<ul style="list-style-type: none"> Military 	<ul style="list-style-type: none"> Offensive Tactics 	<ul style="list-style-type: none"> Partnership Secure the Critical Infrastructure (power, telco, financial, etc)
Howard Schmidt  "US vulnerability to cyber attack is exaggerated"	<ul style="list-style-type: none"> Private Industry 	<ul style="list-style-type: none"> Industry enablement Economic incentives Military in supporting role 	
Secretary Napolitano  "cyberspace is fundamentally a civilian space"	<ul style="list-style-type: none"> Civilian 	<ul style="list-style-type: none"> Public / Private Partnership Regulation International 	

Fix the Lexicon, We are talking past each other!

Strategy: What is it?

Is it Important?

Player	Strategy Options	Expected Position
Government	<ul style="list-style-type: none">• Best practices or regulation?• R&D Manhattan project?• Economic Incentives?• Critical Infrastructure Protection?• Procurement drivers?	<ul style="list-style-type: none">• Regulation and Mandated Standards• Data breach reporting• Public/Private Partnership• Awareness Campaign
Military	<p>How to use cyber weapons?</p> <ul style="list-style-type: none">• Release authority?• Are all targets justified?• Threshold for war?• Kinetic/cyber mix?	<ul style="list-style-type: none">• Late to strategy• Organizing• Clarifying roles/missions• Increase training
Industry	<ul style="list-style-type: none">• What's the business case?• Public/private partnership	<ul style="list-style-type: none">• Against regulation• Need better intelligence• Economic incentives

Are We Ready?



Who is in charge?

What is the plan?

Clear Roles and Responsibilities?

Is Government Shifting Resources to Face the Threat?

Is Industry Shifting Resources? (do they have the business case)

**Cyber Command Declares Full Operational Capability...
but lacks funding, talent, processes, technology.
Command's components greatest need: situational awareness**

A Way Ahead

Player	Way Ahead
Government <ul style="list-style-type: none">• Strong leadership• Proactive policy• Limited regulation	<ul style="list-style-type: none">• Leadership & clear roles/responsibilities• Research & Development Leadership• Empower the ISPs• Secure the power grid• International agreement to eliminate Botnets• Security Incentives
Military <ul style="list-style-type: none">• Serve as the model• Pilot the technology• Quiet partner• Win wars	<ul style="list-style-type: none">• Implement basics well - automatic• Create synergies between intelligence and operations<ul style="list-style-type: none">– Access to data: what is happening on network (shared/collaborated)– Better intel on intruder (shared and collaborated)– Develop ability to rapidly change techniques, tactics, procedures
Industry <ul style="list-style-type: none">• Build to open standards• Interoperability• Research and development• Promote education	<ul style="list-style-type: none">• Implement open standards, build to interoperate• Build trusted Hardware and Secure the code• Autonomous security and always on systems• Education• Information sharing, open source cyber intelligence

The State of Cyber Security 2011

Thank you

Charlie Croom



BACKUP

Lockheed Martin – who we are



- University of Maryland Cyber Center supporter
- Leading provider of IT to the Federal Government
- 133,000 employees worldwide
- NexGen Cyber Innovation & Technology Center
- Security Intelligence Center for Network Defense
- Cyber Security Range
- Lockheed Martin Cyber Security Alliance
- Our solutions: *integrative, proactive, resilient*

Leading through partnership & innovation