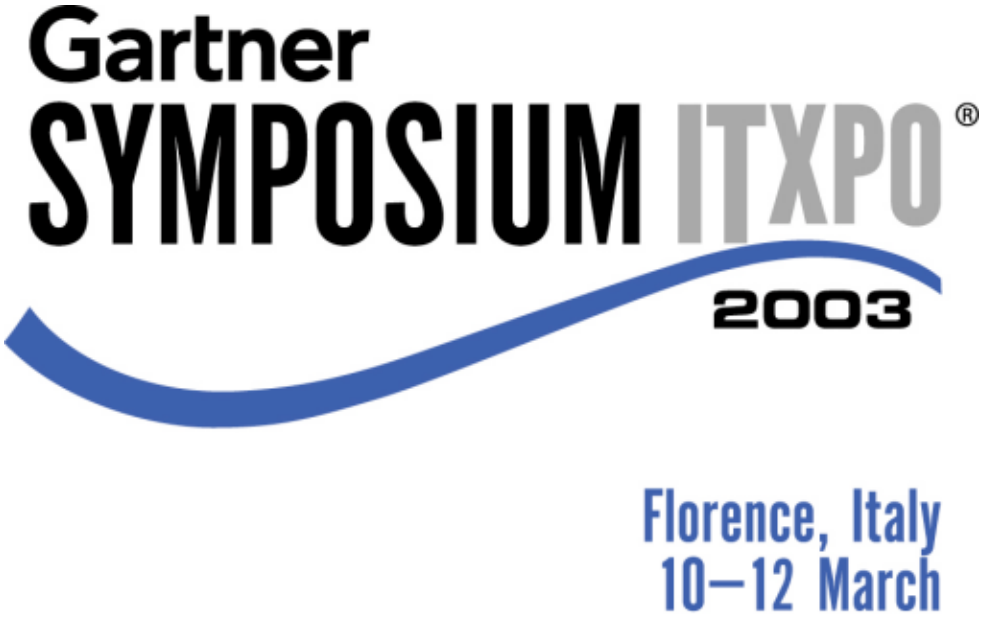
Report of the Digital Pearl Harbor Game



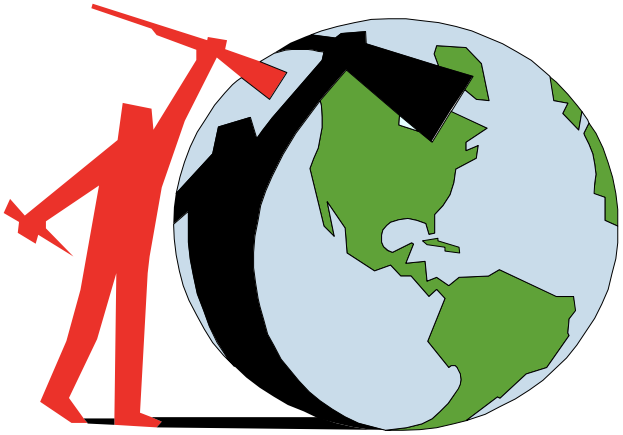
European Symposium

10–12 March 2003
Fortezza da Basso
Florence, Italy

French Caldwell

Strategic Imperative: Enterprises associated with global influence of the United States should take actions to minimize the risks or effects of terrorism and other attacks on people, production, logistics, distribution of operations and outsourced functions.

Terrorism in the Fourth Generation of Warfare



Global Base
- Religious-based ideology
- Affected by globalization

Cultural Targets
- Financial services
- National government
- Media and entertainment
- ...

Visible and High Impact
- Critical infrastructure
- Loss of life

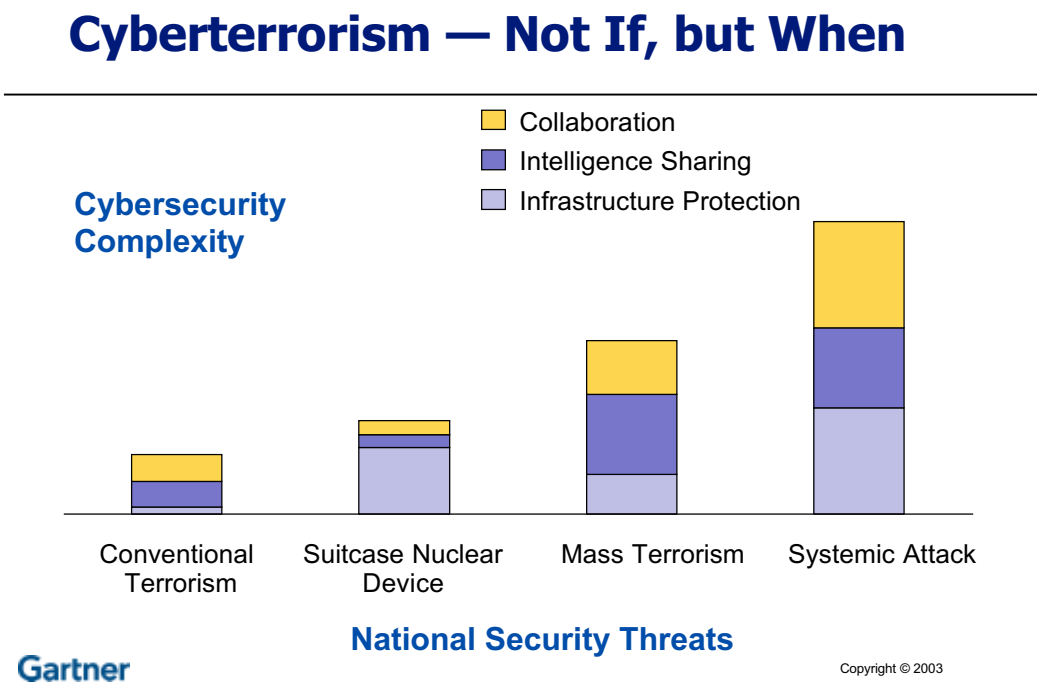
Gartner

Key Issue: How do enterprises need to prepare to face new regulatory constraints and risks when competing in the connected economy?

The fourth generation of warfare (4GW) is characterized by a blurring of the distinctions between war and peace, between military and civilian targets, and between the use of critical infrastructure as a target and as a weapon. Terrorism is not synonymous with 4GW; rather, it means that terrorism will become more systemic, focused on targets that appear detrimental to their base culture. They will look at the headquarters and critical facilities and Internet infrastructure that represent globalization, especially in financial services, national government, entertainment and media, defense and aerospace, petrochemical, large IT, and global consumer and hospitality brands. Anti-globalization groups' "cyberattacks" will also be a major problem for these industries, with a sort of synergy evolving between their cyberattacks and the physical and cyberattacks of terrorists.

Action Item: Operational contingency planning should include people, production, logistics, distribution of operations and outsourcing. No matter what the industry, enterprises in or near key locations for global industries should keep business continuity and disaster recovery plans fresh.

Strategic Planning Assumptions: For the next five years, each new wave of technology will make existing information-security measures obsolete, increasing security exposures in new and legacy environments (0.8 probability). By 2005, financially or ideologically motivated attacks will represent 30 percent of the total incidents and will represent 60 percent of the incident costs incurred by enterprises (0.6 probability).



Key Issue: How do enterprises need to prepare to face new regulatory constraints and risks when competing in the connected economy?

On 24 to 26 July 2002, Gartner and the U.S. Naval War College held a war game entitled "Digital Pearl Harbor" to determine the feasibility of cyberattacks crippling economic and national security infrastructure. Gamers designed attacks that, if executed successfully, would cause significant harm to four critical infrastructure areas: telecommunications, electrical power, the Internet and financial services. Gamers showed that attacks against isolated infrastructures, such as the control systems for electrical power distribution or telecommunications, were more difficult to effect, but at the same time may prove more difficult to detect. Attacks against IT networking and financial service systems that are connected to the Internet are easier to effect, but are also more readily thwarted by just taking reasonable security precautions. However, the scenarios that gamers developed were so extensively damaging as to suggest that the new terrain of cyberspace makes it impossible for enterprises alone to defend against cyberterrorism, and defense requires central coordination that links industries and governments.

Action Item: Get involved in industry consortia that are coordinating "cyberdefenses" for critical infrastructure protection. And, do the basics. Ninety percent of cyberattacks can be thwarted by good IT security practices.

Cyberterrorism Defined

1. The use of computers or computer networks to create terrorism in essence or effect through cyberspace, though not in actual form.
   Application — destroy or damage systems or networks that are critical to the functioning of a complex modern society in order to create a panicked or fearful response by people who are dependent upon the proper functioning of those systems.

2. The use of computers or computer networks to simulate terrorism in the mind, especially as a product of imagination.
   Applications — 1. Entertainment, to include media hype to build ratings on news programs. 2. Gain temporary strategic advantage over the political will of a people. Make people believe that a terrorist attack has occurred or will occur — e.g., Orson Welles' "War of the Worlds" scenario, but done by "a person or an organized group against people or property with the intention of intimidating or coercing societies or governments, often for ideological or political reasons."

Gartner

Attack Factors

Key factors to consider with respect to the allocation of resources required to effect an attack are:

- ❑ The type of target
- ❑ The concentration of the target (that is, the cyber concentration — highly interconnected control systems would make a major attack feasible)
- ❑ Its importance.

Gartner

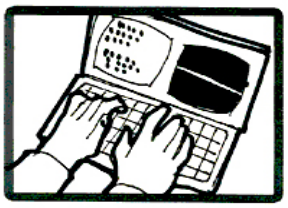
Internet Cell Digital Pearl Harbor

Headlines:

"Forces of Evil Hijack Internet, Use it Against U.S. as a Weapon of Mass Disruption"

Week of trillions in economic loss due to cyberterrorism continues, power and telecom blackouts, stock markets crippled, deleted or exposed corporate and government databases, media misinformation spread. Panic on Main Street, millions fear physical or biological attacks to follow, confidence in ineffective government shaken. Nowhere to run, nowhere to hide!

- **The DPH Internet cell decided against causing physical damage to the Internet and instead to use it as a launch platform for cyberattacks.**
- **Strategic objectives of fear, distrust and economic loss achieved.**



Gartner

Planning and Preparation for Internet Attacks

- Reconnaissance Group to Identify Vulnerable Sites
  - **Legitimate fronts**
- Seizing Control of the Internet
  - **Create overlay network**
- Disrupting Internet Operations
  - **Major systems, DOS, DNS, e-mail, router CA takeovers**
- Disabling the Internet
  - **Bugs, worms, Trojans, time bomb in ASICs**

Gartner

Cyberterrorist Modus Operandi

- To gain control and launch attacks:
  - Place highly technical operatives in legitimate businesses like software developers, Internet equipment suppliers and Internet-based businesses.
  - Identify legitimate Internet-attached enterprises with lax security.
  - Seize covert control of those enterprises
    - Peer-to-peer applications, “sleeper” viruses, worms, Trojans, logic and time bombs, password discovery.
  - Identify critical infrastructure providers and discover their internal networks.
  - Launch rotating cyberattacks as directed.
  - Avoid detection.

Copyright © 2003

Gartner

Financial Services Cell
Digital Pearl Harbor

Mission and Strategy

Systematic series of attacks on personal, corporate and financial markets to stall cash flow, disrupt credit facilities and degrade infrastructure in such a way to undermine confidence and create increasing complexity and cost of remediation.

Gartner

Financial Services Digital Pearl Harbor

	Cash Flow	Credit	Infrastructure
People	Bank Accounts	Credits Cards Ratings Loans	Investment Future
Industry	Sales and Receivables	Credit Facilities Bond Markets Ratings	Infrastructure (interconnecting systems)
Financial Markets	Settlements and Transactions	Credit Facilities	Depositories and Other Markets

Gartner

Financial Services Cell
Digital Pearl Harbor

Attack Scenario

Consumer Attack
- Holiday Weekend (Thanksgiving 2003)
- Bogus ACH Transactions

Corporate Attack
- Corrupt Backup Systems
- Time-Released Confusion

Gartner

Telecommunications Cell Digital Pearl Harbor

Network Attack Overview	Attack Type
• Signaling network	Cyber
• OSS	Cyber
• Outside plant	Low-Intensity
• Undersea cable	Low-Intensity
• Social engineering (insider) attacks	Both

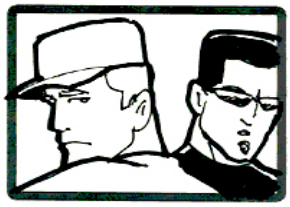
Skills/Technology Requirements

- Working knowledge of PSTN intricacies
- Ph.D. EE/CS
- Box/product-specific knowledge
- SS7 links/established CLEC
- Insider assistance (disgruntled employee)

Gartner

Results

- Resulting attack could serious damage — possibly even collapse the PSTN for a period of time
- Resource requirements very large
  - People
  - $$$
- Hard to keep quiet
- Limited attacks are possible, even easy
  - Cable vaults
  - Social engineering



Gartner

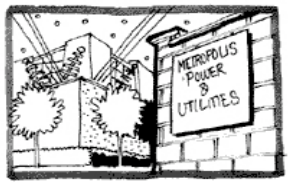
Electrical Power Grid Cell
Digital Pearl Harbor

FIGURE 3—SCADA SYSTEMS AT RISK

"A knowledgeable intruder, aided by publicly available 'hacker' tools, could issue false commands to a utilities energy management system (EMS), opening and closing relays, shutting down lines, and causing voltage oscillations and, potentially, cascading outages."

-- National Security Telecommunications Advisory Committee (NSTAC)

Source: "Electric Power Information Assurance Risk Assessment Report." *NSTAC Information Assurance Task Force* (March 1997)



Gartner

Source: NSTAC

Electrical Power Grid Cell
Digital Pearl Harbor

- Tower Destruction Plan
  - Identify targets
  - Surveillance of sites
  - Agree on target schedule
  - Identify placement of explosives on tower
  - Recruit bombing teams (within the U.S.)
  - Procure explosives and related equipment
  - Arrange logistics support (meals, lodging, transportation, cash)
  - Arrange/plan travel
  - Develop communication plan and procure equipment
  - Develop post-attack plans
  - Rehearse
  - Execute the plan

Gartner

Electrical Power Grid Cell Digital Pearl Harbor

- SCADA Disruption and Destruction Plan
  - Identify SCADA targets and operating systems
  - Surveillance of sites (support from telco group and Internet group)
  - Recruit SCADA D/D team from outside U.S.
  - Train engineers to operate the system
  - Agree on target schedule
  - Develop communication plan and procure equipment
  - Put “plant” in major industry association (SCADA Industry Group)
  - Develop post-attack plans
  - Finalize disruption and destruction nodal control points and sequence of attacks
  - Rehearse
  - Execute the plan

Gartner

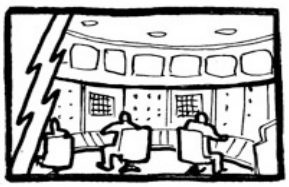
Has It Started?

Question: I am a post graduate in Electronics & Telecommunications Engineer from India. At present I am working as a Maintenance Engineer for computers and SCADA Systems for the Saudi Electricity company in Saudi Arabia. I have appeared for my interview under the independent immigrant category and, finally, the Visa Officer is asking me to arrange for job offers in Canada through some potential Canadian employers. Only then will my immigration visa be issued. Now I need a sponsor (a Canadian employer). How can I manage it? Can anyone assist me regarding this concern?

--------question on the Canadian immigration Web site.

Gartner

Life Imitates Art



FBI investigates biggest ever attack on internet

The Guardian **Thursday 24 October 2002**

The White House and the FBI announced a joint investigation last night into the biggest ever attack on the 13 computers that are the crucial basic components of the internet.

For at least an hour from 9.45pm British time on Monday, the internet's 13 "root server" computers - owned and operated by the US government, universities, private companies and other organizations around the world - were deluged with massive amounts of extra data, creating bottlenecks that prevented legitimate data from reaching its destination.

Seven of the servers were completely paralyzed and two failed intermittently.

"There is an investigation under way to determine who is responsible for the attacks," said Ari Fleischer, the president's spokesman. The FBI's national infrastructure protection center said it was "aware of the denial-of-service attack, and is addressing the matter".

Gartner

Top 10 List of Cybersecurity Mantras

1. If we only had more money!
2. Ninety percent of the problems would go away if only enterprises would follow basic security processes.
3. The markets will fix it.
4. Don't worry about the threat; just fix the vulnerabilities.
5. The business management needs to understand…
6. The CEO should sign for it.
7. You can't make the business case for cybersecurity.
8. The vendors need to fix it.
9. Focus on security awareness.
10. The users are stupid.

Gartner

CIP Cybersecurity Best Practices

- Do the basics. A well-designed infrastructure with firewalls and good internal security, as well as regularly patches vulnerabilities, will help significantly.
- Appoint someone internally as a "terrorist" and have the person infrequently attempt to break into your systems.
- Take a global view of security. Enterprises that have taken all necessary steps to secure their core operations in the United States could still be vulnerable offshore.
- Ensure the physical security of all backup tapes, especially while in transit.
- Strengthen background checks of new hires, consultants, contractors and third-party administrators.
- Review all insurance policies and consider the return on investment of clauses about the mitigation of cyberterrorism.
- Send out requests for information for pattern recognition software that can help rapidly detect aberrant activity (albeit after the fact).
- Avoid new technologies until they have been tested and found to include adequate security.
- Reconsider the security of disaster recovery and business continuity plans and operations.

Gartner

Bottom Line

- Follow IT security best practices, but prioritize
- Establish personnel reliability standards for critical systems operations and maintenance
- Focus on software quality
- Government — defensive early warning and intelligence

Gartner