Critical Infrastructure Protection in the USA: Where are we after 8 years?

Jeffrey J. Carpenter, Technical Manager
jjc@cert.org
+1 412 268-5724
Agenda

• CERT/CC Overview
• The Last Ten Years
• ISACs
• Homeland Security
• Security Industry
• Business Motivators
• Conclusions
CERT/CC Focus

- Criminals
- Technologists
- Asset Holders

- intel
- military
- law enforcement
- Tech Staff
- National CSIRTs
- Financial Sector

CERT Coordination Center
The Last Ten Years
Critical Infrastructure Protection before 1997

National Security Telecommunications Advisory Committee (NSTAC)

QuickTime™ and a TIFF (LZW) decompressor are needed to see this picture.
ISACs

• Financial Services ISAC  
  – VeriSign
• Chemical Sector ISAC  
  – Chemical Transportation Emergency Center
• Emergency Management and Response ISAC  
  – U.S. Fire Administration, DHS
• Electricity Sector ISAC  
  – North American Electric Reliability Council
• Energy ISAC
• Food and Agriculture ISAC  
  – Food Marketing Institute
• Multi-State ISAC
• Telecommunications ISAC  
  – National Communications System (DHS)
• Real Estate ISAC  
  – The Real Estate Roundtable
• Surface Transportation ISAC  
  – EWA IIT; sponsored by American Association of Railroads and American Public Transportation Association
• Water ISAC  
  – Association of Metropolitan Water Agencies
• IT ISAC  
  – ISS
Homeland Security

- support for federal, state, local governments has made real progress
- critical infrastructure protection is a hard problem
- information sharing
  - PCI II
Security Industry Maturation

• MSSPs
• anti-virus updates
• vendor vulnerability handling
Motivators

- Healthcare Insurance Portability and Accountability Act (HIPAA)
- Sarbanes-Oxley
- Graham-Leach-Bliley
Business Problem

• we need to focus on the business case for security
  – demonstrate those investments bring operational benefits
  – often provides side benefits
    o attack prevention is also accident prevention
    o customer confidence
    o reliability
    o continuity of operations
Better understanding of the threat

- evidence of real threats
- how we know what vulnerabilities we need to worry about
- better information from law enforcement and intelligence agencies

- National Computer Security Survey (NCSS)
Conclusion

• Critical Infrastructure has been an issue for more than 25 years
• Operators have much better support from vendors and service providers
• Homeland Security is making progress; still has far to go
• We need to do a better job of building a business case
• We need a better understanding of the threat