INTERNET
SECURITY
ALLIANCE

Dave McCurdy
EIA President
& Executive Director
Internet Security Alliance

ANSI Annual Conference
October 1, 2003

The Internet Security Alliance

EIA
Electronic Industries Alliance
INTERNET SECURITY ALLIANCE
CERT
Coordination Center

The **Internet Security Alliance** is a collaborative effort between Carnegie Mellon University's ***Software Engineering Institute (SEI)*** and its ***CERT Coordination Center (CERT/CC)*** and the ***Electronic Industries Alliance (EIA)*,** a federation of trade associations with over 2,500 members.

INTERNET
SECURITY
ALLIANCE

Sponsors

AIG

CERIDIAN

CABLE & WIRELESS

ITT Industries
Engineered for life

Mellon

NAM
National Association
of Manufacturers

NORTHROP GRUMMAN

NASDAQ

NORSK TIPPING

NORTEL
NETWORKS

Raytheon

redsiren™
Security. Integrity. Trust.℠

Russell

SONY

SINTEF
Telecom and Informatics

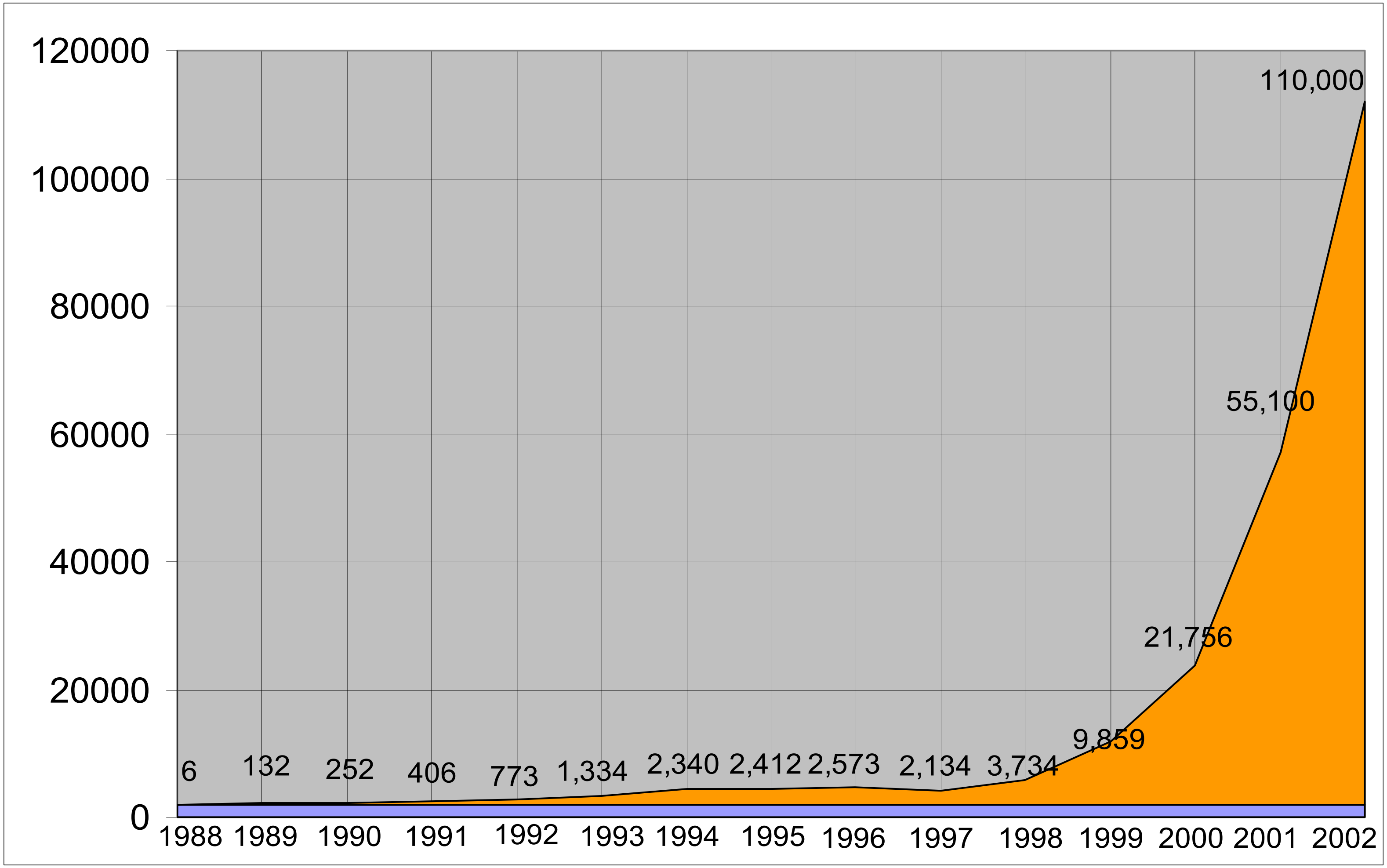
TATA

VISA

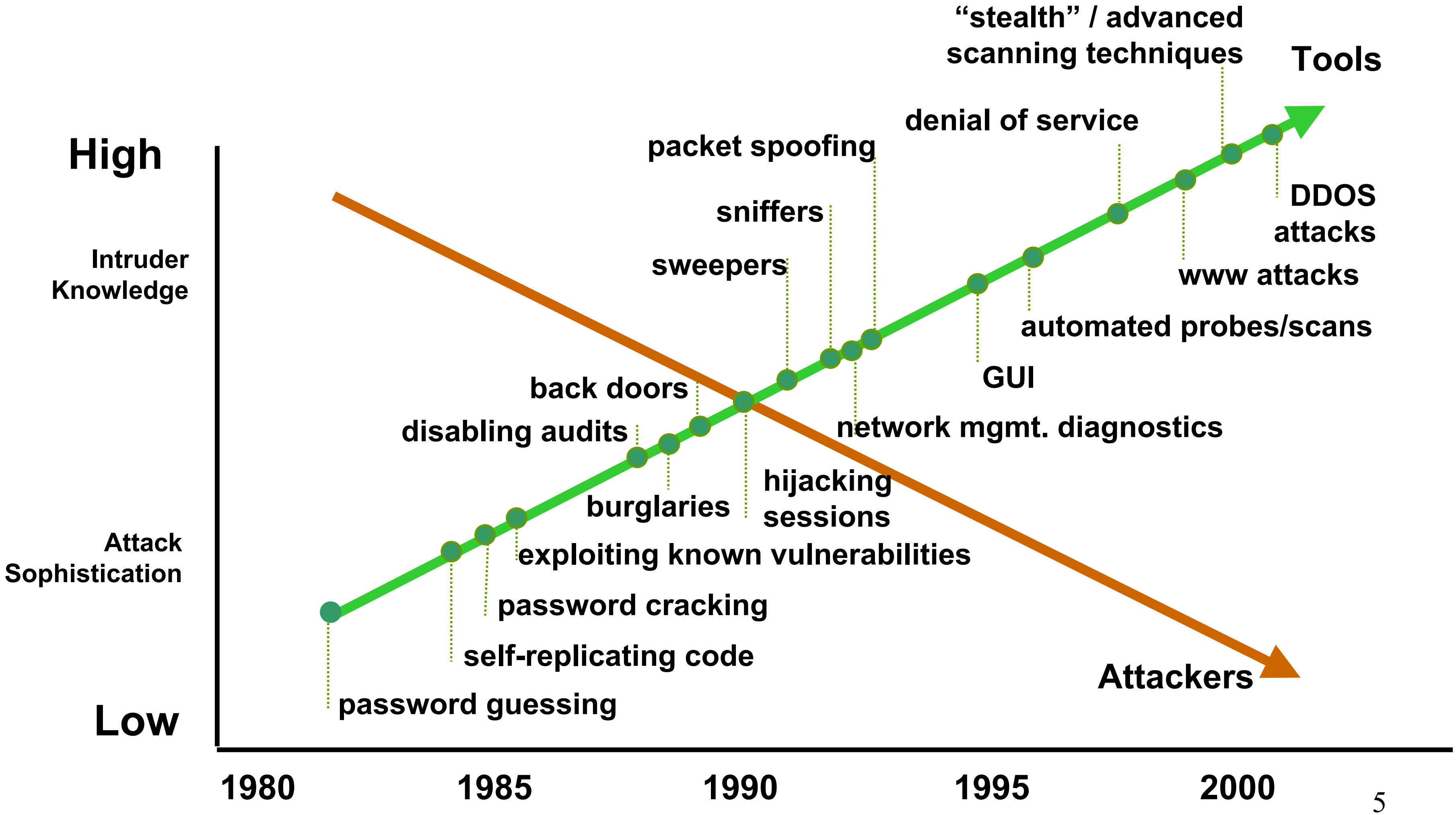
VeriSign®

verizon

Growth in Incidents Reported to the CERT/CC



Attack Sophistication v. Intruder Technical Knowledge



Financial Impacts of Attacks

- Klez virus:
  - Clean-up and lost productivity: $9 billion
- Code Red: 1 million computers affected
  - Clean-up and lost productivity: $2.6 billion
- Love Bug: 50 variants, 40 million computers affected
  - Clean-up and lost productivity: $8.8 billion
- Nimda
  - Clean-up and lost productivity: $1.2 billion
- Slammer
  - Clean-up and lost productivity: $1 billion +
  - Blaster & So Big combined clean-up and lost productivity estimate $2 billion

Won’t Advanced Technology Protect Us?

“Installing a network security device is not a substitute for a constant focus and keeping our defenses up to date… There is no special technology that can make an enterprise completely secure.”

– *National Plan to Secure Cyberspace, 2/14/03*

Step 1 Invest in Cyber Security

- US Government increasing spending 64% for cyber security.

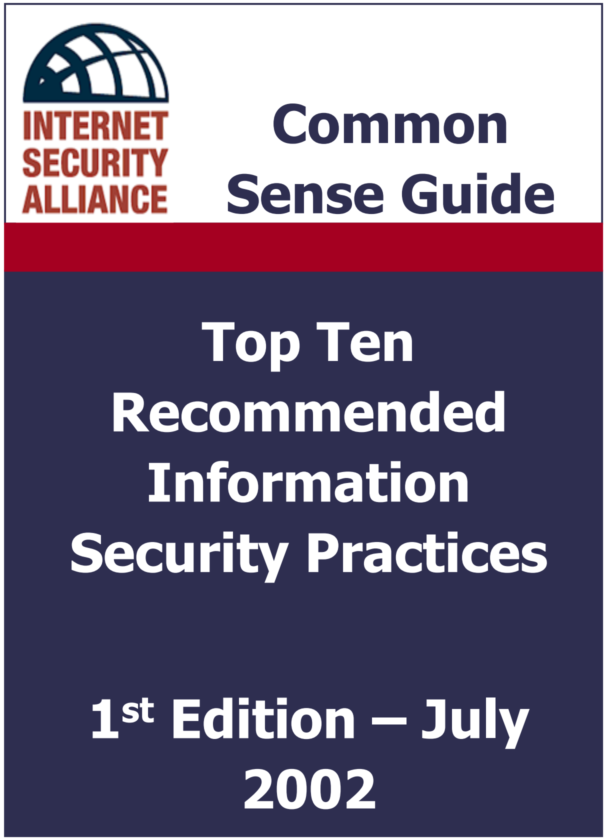
*****

For business there is a 21% ROI for early incorporation of security

- CSO Magazine 12/02

Step 2. Adopt and Implement Best Practices

- Cited in US National Draft Strategy to Protect Cyber Space (September 2002)
- Endorsed by TechNet for CEO Security Initiative (April 2003)
- Endorsed US India Business Council (April 2003)



INTERNET SECURITY ALLIANCE

Common Sense Guide

Top Ten Recommended Information Security Practices

1st Edition – July 2002

Common Sense Guide Top Ten Practice Topics

- Practice #1: General Management
- Practice #2: Policy
- Practice #3: Risk Management
- Practice #4: Security Architecture & Design
- Practice #5: User Issues
- Practice #6: System & Network Management
- Practice #7: Authentication & Authorization
- Practice #8: Monitor & Audit
- Practice #9: Physical Security
- Practice #10: Continuity Planning & Disaster Recovery

Step 3. Risk Mitigation/Cyber Insurance

"Until recently, traditional property insurance may have provided some coverage for virus-related exposures, but as of January 2002, the majority of insurers eliminated it as well."

CSO Magazine

"The insurance industry has a pivotal role to play, particularly by developing cyber insurance policies."

Paul B. Kurtz, Senior Director for National Security

Are you covered? Should you be covered?

- Many policies no longer cover cyber

INTERNET
SECURITY
ALLIANCE

ISAlliance Cyber-Insurance Program

- Free cyber check-up provided by AIG for members
- Market incentive for increased security practices
- 10% discount for ISAlliance members
- Additional 5% discount for implementing ISAlliance Best Practices (July 2002)
- Discounts more than offset sponsorship dues
- Audit program to be announced soon

INTERNET
SECURITY
ALLIANCE

Step 4 Join ISAlliance

Join and participate in a cyber-security information sharing organization

INTERNET SECURITY ALLIANCE

Benefits

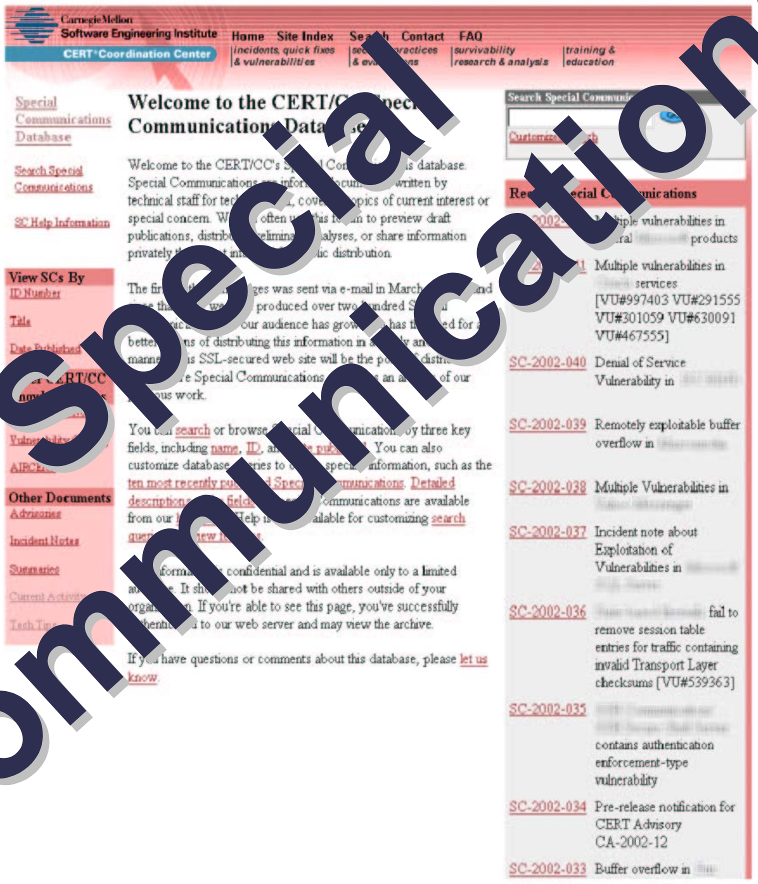
- Share critical information across industries and across national borders
- Provide secure setting to work on common problems
- Provide economic incentive programs
- Develop model industry programs
- Give policy makers an alternative to regulatory models

CERT Knowledgebase Examples

CERT Coordination Center

Special Communications

Figure 3: Special Communications index page



Carnegie Mellon
Software Engineering Institute
CERT® Coordination Center
Home
Site Index
Sea[illegible]h
Contact
FAQ
incidents, quick fixes & vulnerabilities
sec[illegible] practices & eva[illegible]ns
survivability research & analysis
training & education

Special Communications Database
Search Special Communications
SC Help Information
View SCs By
ID Number
Title
Date Published
[illegible] CERT/CC [illegible]
Vulne[illegible]
AIRCE[illegible]
Other Documents
Advisories
Incident Notes
Summaries
Current Activity
Tech Tips

Welcome to the CERT/C[illegible] Communication[illegible] Data[illegible]e

Welcome to the CERT/CC's S[illegible] Con[illegible] is database. Special Communications [illegible] written by technical staff for tec[illegible], cove[illegible] topics of current interest or special concern. W[illegible] often u[illegible] this fo[illegible]m to preview draft publications, distrib[illegible] relimina[illegible] alyses, or share information privately [illegible] int[illegible] lic distribution.

The fir[illegible] ges was sent via e-mail in March [illegible] and [illegible] tha[illegible] we[illegible] produced over two hundred S[illegible] [illegible] our audience has grow[illegible] has t[illegible] ed for a bette[illegible] ns of distributing this information in a[illegible] y an[illegible] manne[illegible] is SSL-secured web site will be the po[illegible] f distri[illegible] [illegible] re Special Communications [illegible] s an a[illegible] of our [illegible] ous work.

You [illegible] search or browse S[illegible] cial C[illegible] unication[illegible] by three key fields, including name, ID, a[illegible] te pub[illegible]. You can also customize database [illegible] eries to [illegible] speci[illegible] information, such as the ten most recently pu[illegible] d Speci[illegible] mmunications. Detailed description[illegible] e fields [illegible] ommunications are available from our [illegible] Help is [illegible] ailable for customizing search queri[illegible] iew [illegible].

[illegible] forma[illegible] confidential and is available only to a limited au[illegible] e. It sh[illegible] not be shared with others outside of your orga[illegible] n. If you're able to see this page, you've successfully [illegible] thenti[illegible] d to our web server and may view the archive.

If y[illegible] have questions or comments about this database, please let us know.

Re[illegible] ecial C[illegible] unications

[illegible] 2002-[illegible]	M[illegible] ltiple vulnerabilities in [illegible] ral [redacted] products
[illegible] 2[illegible] 1	Multiple vulnerabilities in [redacted] services [VU#997403 VU#291555 VU#301059 VU#630091 VU#467555]
SC-2002-040	Denial of Service Vulnerability in [redacted]
SC-2002-039	Remotely exploitable buffer overflow in [redacted]
SC-2002-038	Multiple Vulnerabilities in [redacted]
SC-2002-037	Incident note about Exploitation of Vulnerabilities in [redacted]
SC-2002-036	[redacted] fail to remove session table entries for traffic containing invalid Transport Layer checksums [VU#539363]
SC-2002-035	[redacted] contains authentication enforcement-type vulnerability
SC-2002-034	Pre-release notification for CERT Advisory CA-2002-12
SC-2002-033	Buffer overflow in [redacted]

Benefits of Information Sharing Organizations

- May lessen the likelihood of attack

> *"Organizations that share information about computer break ins are less attractive targets for malicious attackers." – NYT 2003*

- Participants in information sharing have the ability to better prepare for attacks

Benefits of Information Sharing Organizations/Examples

- SNMP vulnerability
  - CERT notified Alliance members Oct. 2001
  - Publicly disclosed Feb. 2002
- Slammer worm
  - CERT notified Alliance members May 2002
  - Worm exploited Jan. 2003

INTERNET
SECURITY
ALLIANCE

Internet Security Alliance

2500 Wilson Boulevard
Arlington, Virginia 22201

www.isalliance.org

Phone: 703.907.7090

Fax: 703.907.7903