EXODUS

A CABLE & WIRELESS SERVICE

National Infrastructure Protection Issues

Dr. Bill Hancock, CISSP
Vice President, Security &
Chief Security Officer
bill.hancock@exodus.net

What is Protection in Cyberspace?

- Depends on who you talk to – everyone has an opinion and they vary dramatically
- Basic definition: stopping someone from taking something that is not theirs
- Sometimes, things are taken by force
- Who is hurt varies
  - Sometimes companies
  - Sometimes people
  - Sometimes - you

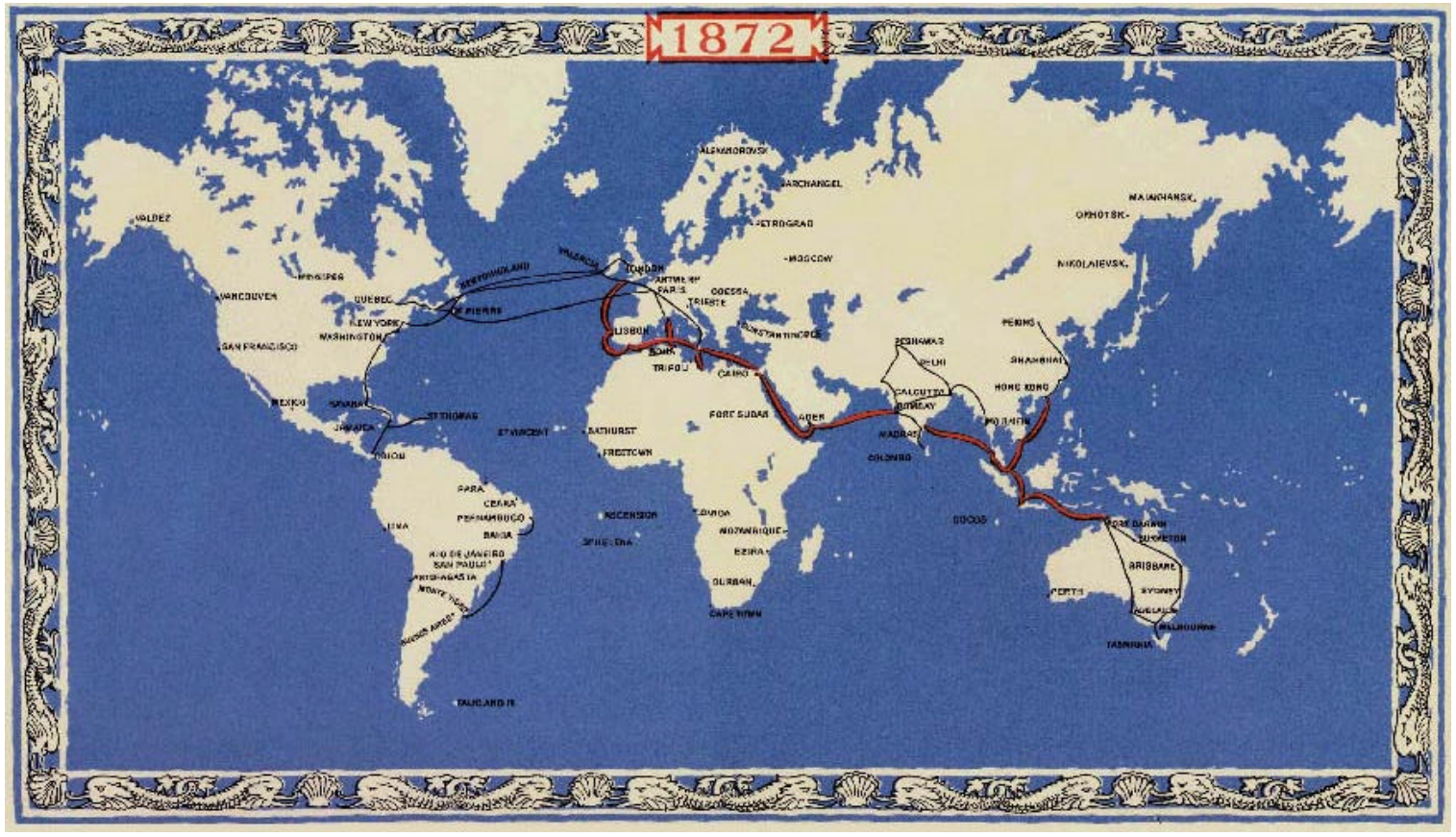
EXODUS
A CABLE & WIRELESS SERVICE

The Speaker's Perspective…

- Came from various large and small companies in networking and security over 30 year career
- Have designed or redesigned over 4000 networks, many in critical infrastructures (power, water, public safety)
- Have designed protocols, have patents, etc.
- Have been on several White House committees on critical infrastructure and Chair NRIC FG1B (cyber security)
- Currently responsible for security on the world's largest multinational IP network infrastructure:
  - **THE Internet backbone**
    - Bought from MCI in 1996/1997
      - 2.2m IP nodes active on network
      - Data, voice, video
  - World's largest hosting provider
    - 50% of top 100 web sites in the world
    - Hundreds of thousands of servers, millions of users
    - One of every three mouse clicks…
    - One of the largest operational security teams
    - Over 1000+ cyber attacks per month
  - **THE** telephone company in many countries (C&W)

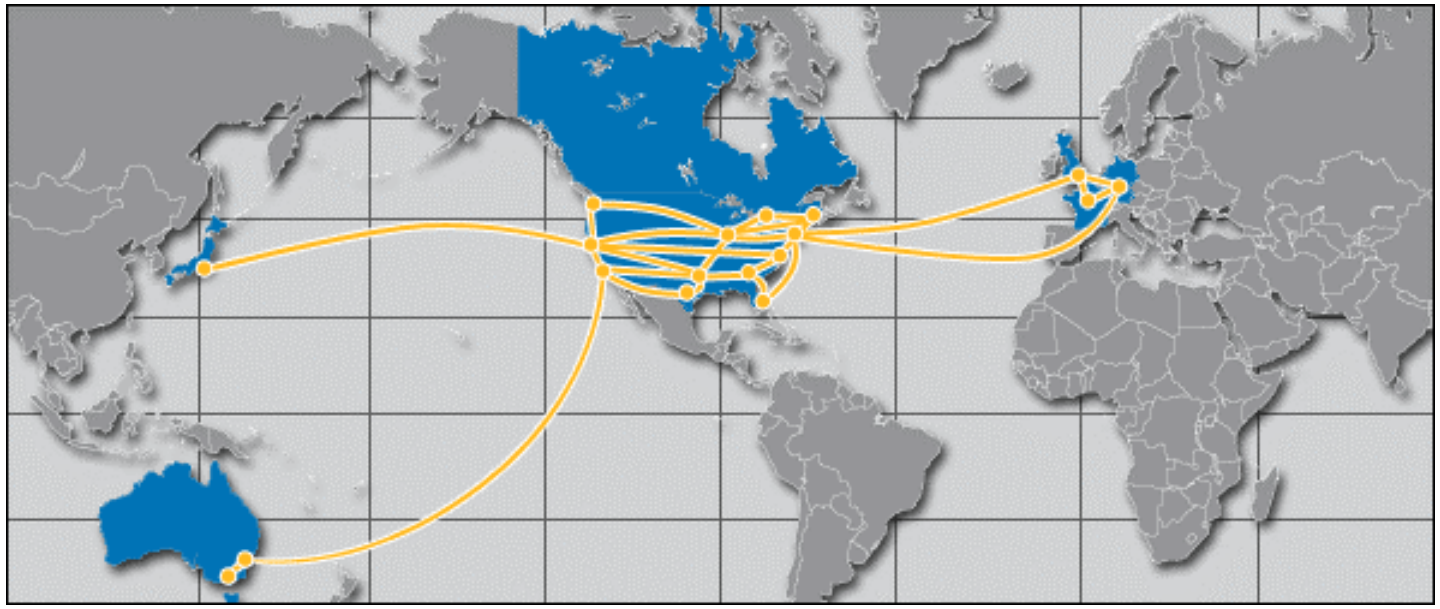
EXODUS
A CABLE & WIRELESS SERVICE

Eastern Telegraph Company



EXODUS
A CABLE & WIRELESS SERVICE

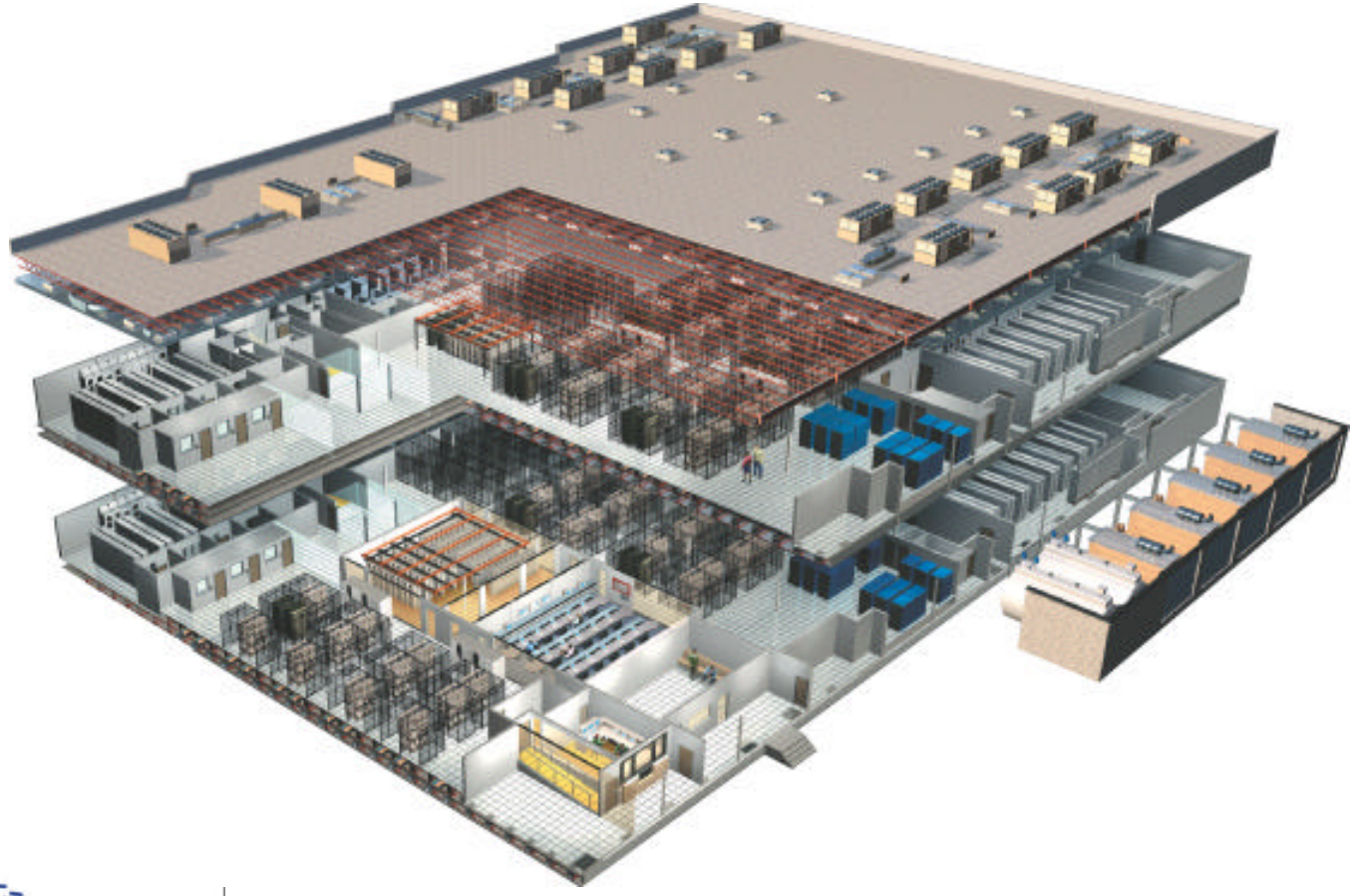
Global Infrastructure: The Cable and Wireless Internet Services (Exodus/CWIS) Network



As of end of Q4 ’01

EXODUS
A CABLE & WIRELESS SERVICE

Global Infrastructure:
CWIS Internet Data Centers



EXODUS
A CABLE & WIRELESS SERVICE

Clients Rely on Exodus/CWIS

Some Statistics…

- 43 Internet data centers globally deployed
- Dial-up POPs/NAPs in 170+ countries
- Over 4000 customers in IDCs alone
- One of the largest IP networks in the world growing at over 30% per year (or more)
- Operates the Tier 0 Internet Backbone
- The phone company in many countries
- Over 50m users per day traverse networks (peak in 2001 was 87m in one day)
- One of the largest operational cyber security teams in the world with some of the most skilled security practitioners in the world
- Participants in cyber security teams with governments in many countries of the world

EXODUS

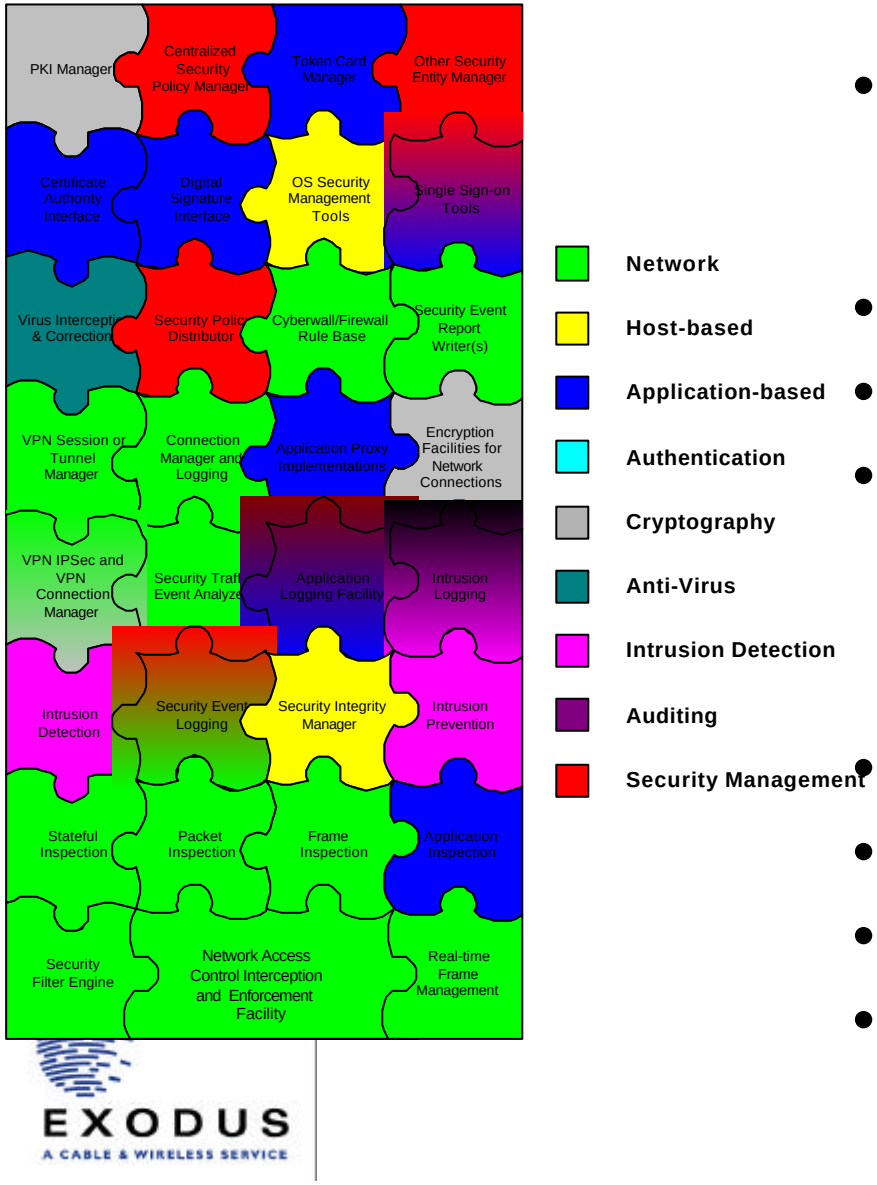
A CABLE & WIRELESS SERVICE

Critical Infrastructure Assessment Office (CIAO)

- Part of the U.S. National Critical Infrastructure Assessment Board (CIAB)
- Declared Exodus/CWIS a Type 1 CIAO in March, 2000
  - Outages determined to cause critical national harm to U.S. economy
- Works closely with Exodus/CWIS in many areas to help identify critical resources and work with government partnerships to share information and ideas to correct
- Now part of National Security Council, reporting to National Security Advisor (Dr. Condalezza Rice)

EXODUS
A CABLE & WIRELESS SERVICE

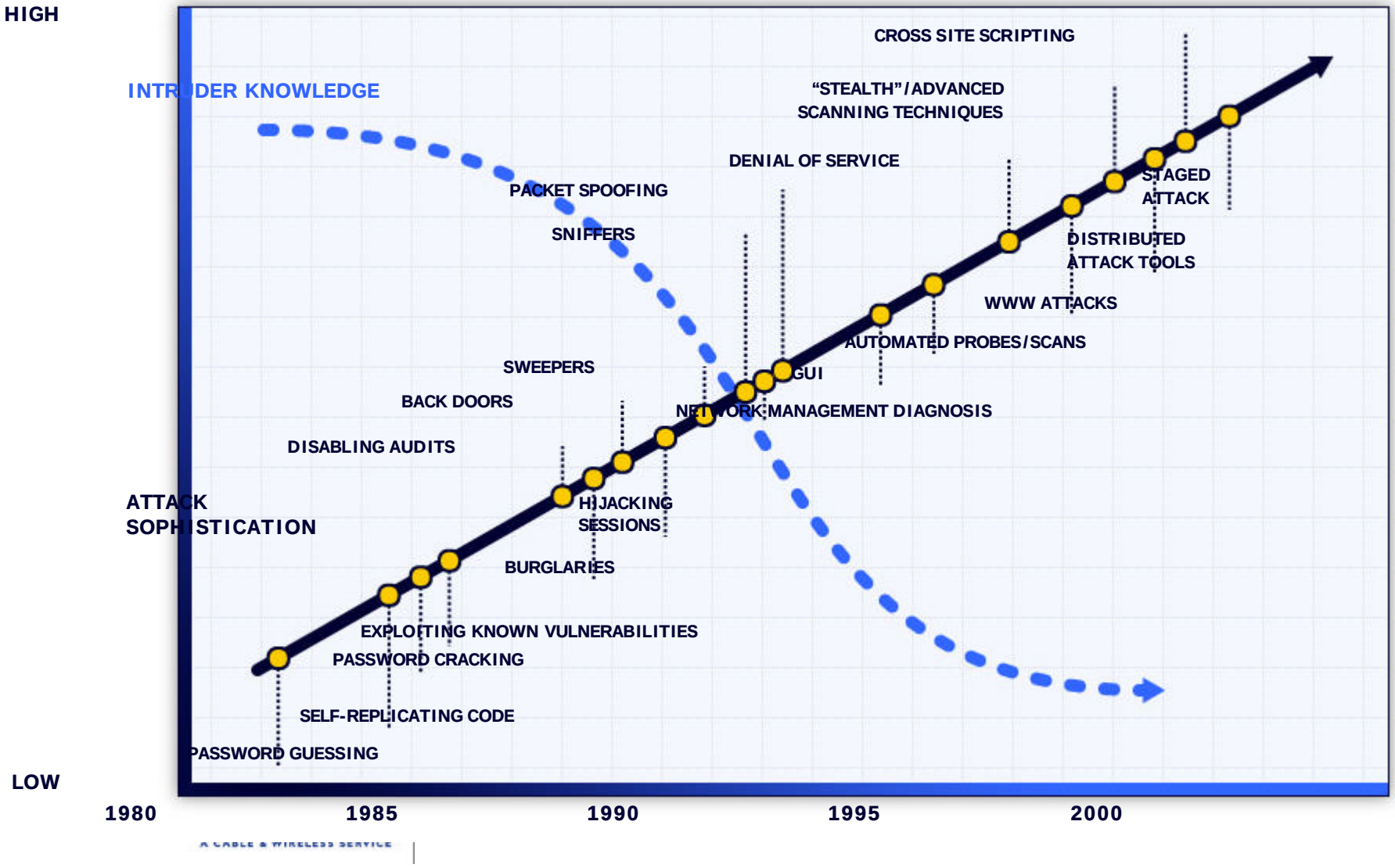
Security is Very Complex



- Security is currently where networking was 15 years ago
- Many parts & pieces
- Complex parts
- Lack of expertise in the industry (60% vacancy with no qualified personnel)
- No common GUIs
- Lack of standards
- Attacks are growing
- Customers require security for biz

EXODUS
A CABLE & WIRELESS SERVICE

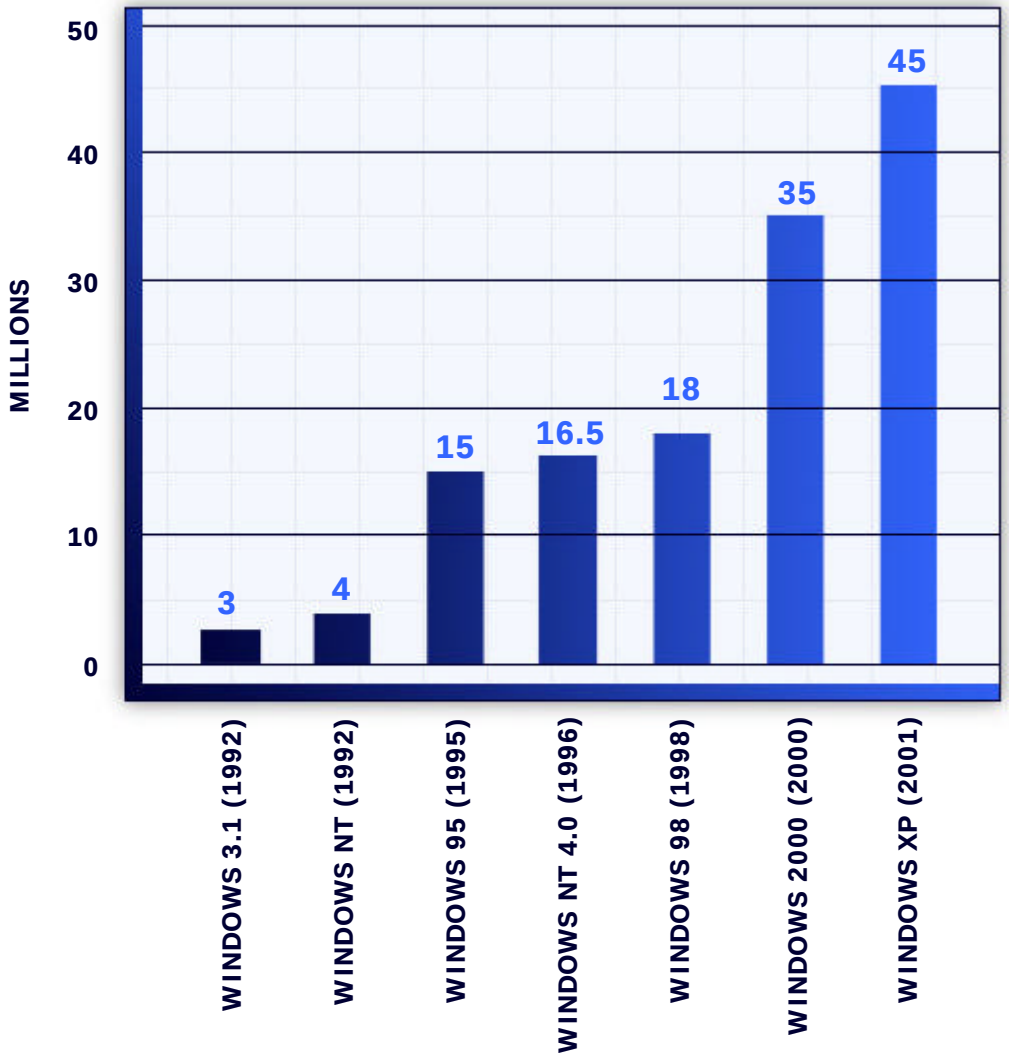
As Systems Get Complex, Attackers are Less Sophisticated…



Software Is Too Complex

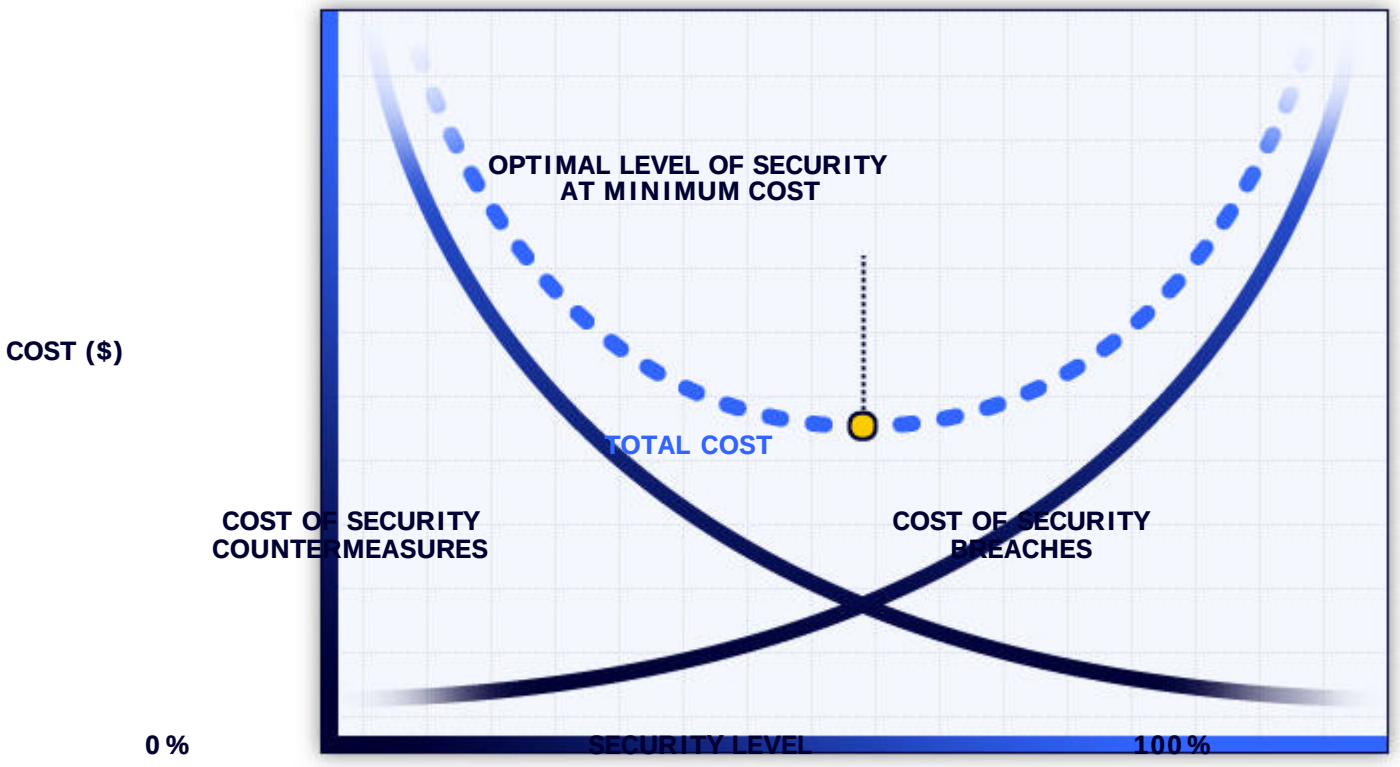
Sources of Complexity:

- Applications and operating systems
- Data mixed with programs
- New Internet services
  - XML, SOAP, VoIP
- Complex Web sites
- Always-on connections
- IP stacks in cell phones, PDAs, gaming consoles, refrigerators, thermostats



EXODUS
A CABLE & WIRELESS SERVICE

Security Must Make Business Sense to Be Adopted



Some Reality on Infrastructure Security in the Private Sector

- **Statistics show that post 9/11/01, security sales have NOT increased due to heightened awareness of security threats**
- **Corporate management will NOT spend money on security and reliability issues unless:**
  - **There is a REAL operational requirement**
  - **There is a legal requirement**
  - **There is the threat of bad public relations or press**
  - **There is some perceived Return on Investment (ROI)**
  - **There are government incentives to do so**
- **Most critical infrastructure networks continue to be vulnerable to a wide range of attacks**

EXODUS
A CABLE & WIRELESS SERVICE

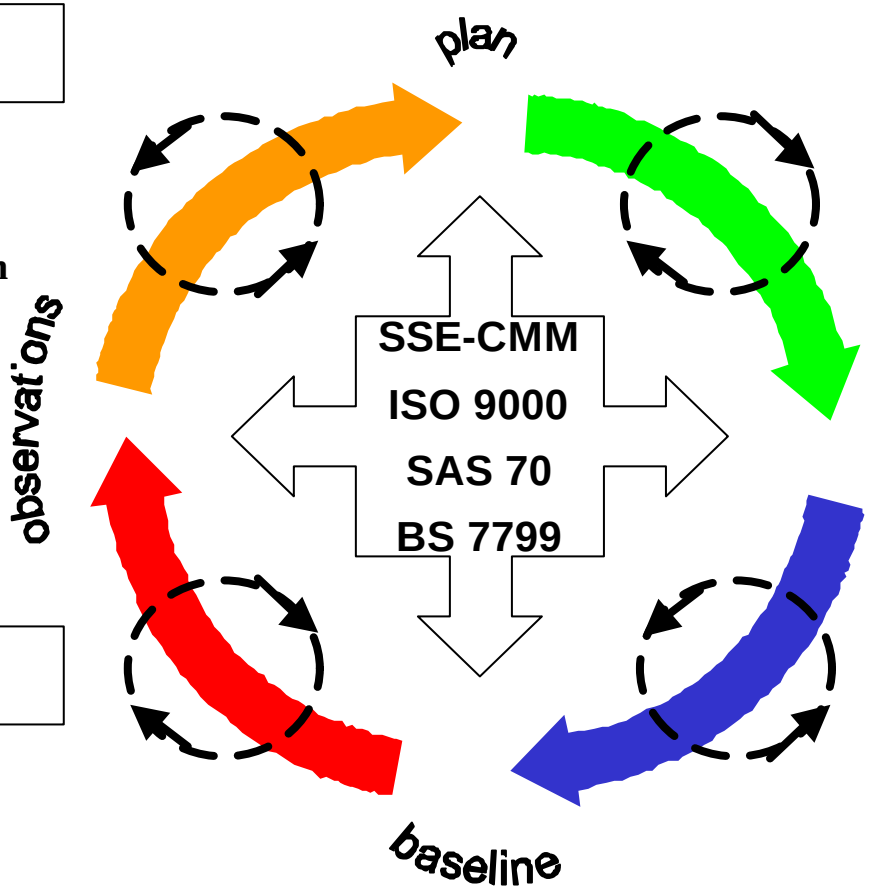
Security Lifecycle Solutions

Assess

Requirements Analysis
Risk Assessment
Product/Service Evaluation
Trade-Off Study
Compliance Verification
Architecture Review
Application Testing

Design

Secure Architecture and Code Design
Business Continuity/Disaster Recovery Planning
PKI Solutions
Policy and Procedures
Site Evaluation



Monitor

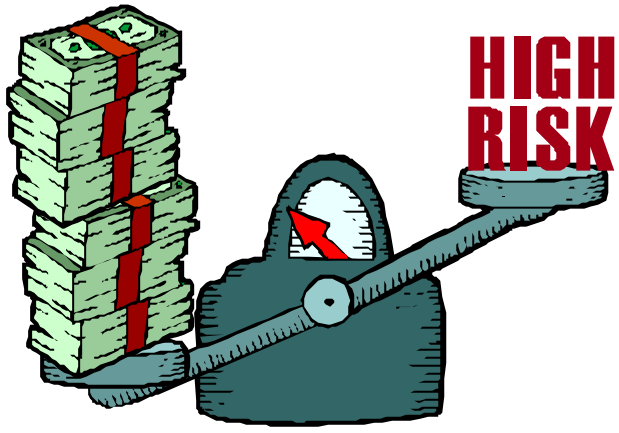
Incident Response and Recovery
Vulnerability Scans
Penetration Testing
Alert Monitoring
Log Analysis
System Audit
Integrity Monitoring

EXODUS
& WIRELESS SERVICE

Implement

Training
Firewall/IDS Configuration
VPN
OS Hardening
Roles & Responsibility Integration

Why are Security Risks Increasing?



- Denial of the problem
- Improperly designed infrastructure of existing systems, apps, networks, etc.
- Acceleration of new technologies with no security capabilities
- Lack of proper threat assessment for assets and development of protective measures for same
- No legislative impetus
- Improper recognition of risks by senior management

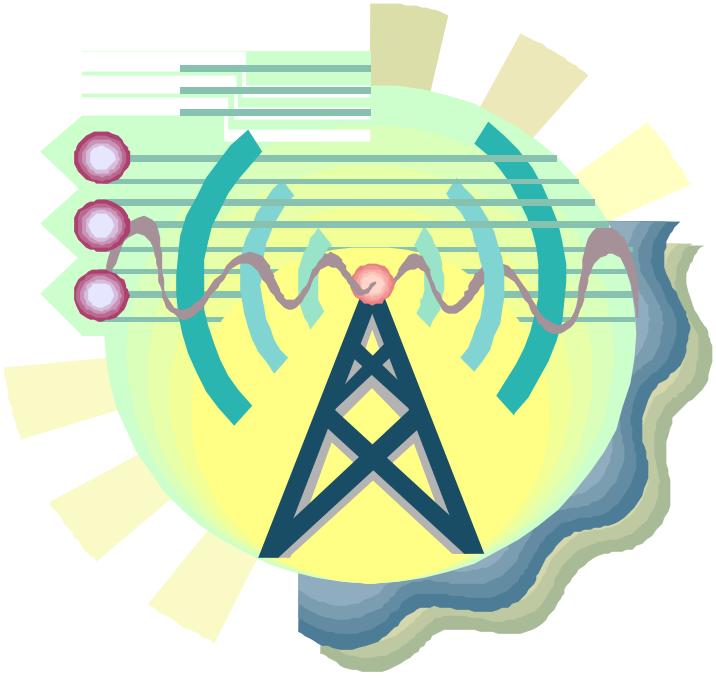
EXODUS
A CABLE & WIRELESS SERVICE

Classic Current IT Risks

- DNS attacks
- DDoS, DoS, etc.
- Virii, worms, etc.
- Spoofs and redirects
- Social engineering
- Router table attacks
- OS holes, bugs
- Application code problems
- Insider attacks
- Others…

EXODUS
A CABLE & WIRELESS SERVICE

Example: Wireless LANs



- **85% of all WLANs have no WEP enabled**
- **WLANs with WEP and/or VPN solutions do not stop:**
  - **DoS and DDoS**
  - **Off-WLAN sniffinga**
  - **Session hijacks**
  - **DNS spoofing**
  - **Redirection attacks**
  - **Etc., etc., etc…**

EXODUS
A CABLE & WIRELESS SERVICE

Common Uses for Wireless Today

- **Wireless Voice**
  - Cellular (CDMA, GSM, TDMA, CDMA-One)
  - Multifunction (2.5G, 3G)
  - Residential 900MHz
  - Family channel comms (walkie-talkies)
  - Lightware line-of-sight)Rockwell)
- **Wireless Data**
  - CDPD cellular packet data) & proprietary
  - Paging and text messaging
  - 2.5G and 3G
  - IEEE 802.11x (wi-fi)
  - IEEE 802.15 (Bluetooth)
- **Video**
  - 802.11x, 3G
  - T.120 and H.323 adapted
- **Multifunction**
  - Satellite (narrow and wideband)
  - Local loop replacement technologies
  - Embedded technologies (cars, aircraft, etc.)
  - Microwave (power companies)
  - Lightware relay (laser)

EXODUS
A CABLE & WIRELESS SERVICE

Wireless Security Methods

- **Voice**
  - By and large – wide open (scanning systems)
  - Digital: encryption methods (if enabled)
  - Frequency hopping and spread spectrum
- **Video**
  - DES encoding optional
  - Some proprietary (e.g. phase encoding)
  - Typically disabled - too hard to manage & expensive
- **Data**
  - 802.11x WEP 64 or 128 bit encryption
    - Disabled on 85% of all installations
    - Remaining WLANs typically have default password
    - Several “pedestrian” methods to crack WEP
    - Includes a system authentication method that is managed by a passphrase that is typically disabled
  - Proprietary methods at Layer 2
  - Some cellular data use Secure Sockets Layer (SSL)
  - Mostly difficult to implement and manage, so companies turn encryption and authentication OFF

EXODUS
A CABLE & WIRELESS SERVICE

Problems with Wireless Security

- **Missing core security technologies to be truly secure (all are add-on facilities):**
  - **Firewall facilities**
  - **Content filtering**
  - **Application security controls and proxies**
  - **System hardware authentication**
  - **Strong user authentication**
  - **Encryption key management facilities**
  - **Cryptography management and controls**
  - **Event logging and alert management**
  - **Network and host intrusion detection facilities**
  - **End-to-end security connectivity options (VPN, etc)**
  - **Security policy management facilities**
  - **Content integrity facilities**
  - **Etc…**

EXODUS
A CABLE & WIRELESS SERVICE

Critical Infrastructure Not Only Has Design Flaws, but Bugs…

- **It is uniformly agreed in industry and research that critical infrastructures have flaws:**
  - **Outdated, archaic or flawed design for critical networks such as power, water and others**
  - **Lack of standards**
  - **Lack of international cooperation**
  - **Lack of knowledge on dependency of technologies**

- **Critical Infrastructure extends to those technologies used to define the building blocks of critical networks and systems:**
  - ***Abstract Syntax Notation . 1 (ASN.1)***

EXODUS
A CABLE & WIRELESS SERVICE

The Discovery of the ASN.1 Bug

Approximately 10 months ago, a Finnish research project discovered serious security vulnerabilities in the Simple Network Management Protocol (SNMP) v1

- **SNMP is used in practically every network component for monitoring and management purposes. It is also used in most systems**
- **Any vulnerability is very bad news**
- **Known effects are the ability to crash a network device, like a switch or a router, with relatively simple methods and little or no information about the configuration of the device**
- **Most people and companies think the SNMP problem is isolated to SNMP only – and it is NOT**

EXODUS

A CABLE & WIRELESS SERVICE

The Bug gets worse…

- **Cisco Systems is one of the few initial vendors that was told of the SNMPv1 vulnerability by the Finns at onset**
  - **In the reparation attempts, they and other companies discovered that the problem is congenital to the base encoding language, ASN.1 (X.680/ISO 8824-1…4)**

- **ASN.1 Basic Encoding Rules (BER) allegedly has a congenital flaw that can allow execution of code on systems which have ASN.1 encoded components, protocols or applications**

EXODUS

A CABLE & WIRELESS SERVICE

What Components use ASN.1?

- Most protocols at most layers
- Practically ALL network devices and network applications
- Vector-structure applications
  - LDAP
  - OpenSSL
  - Many, many others
- ASN.1 is used in voice, video and data protocols and applications
- Earliest implementations in early 1980's, many still used in today's technologies

ASN.1 and Architecture

Very high level definitional code

```
Order-for-stock ::= SEQUENCE
{order-no INTEGER,
name-address BranchIdentification,
details SEQUENCE OF
SEQUENCE
{item OBJECT IDENTIFIER,
cases INTEGER},
urgency ENUMERATED
{tomorrow(0),
three-day(1),
week(2)} DEFAULT week,
authenticator Security-Type}
```

ASN.1 CrossCompiler or Implementor Tool

Re-usable Object Code

Dynamic interpretive or static executable program code

EXODUS
A CABLE & WIRELESS SERVICE

What Can Happen?

- **Cable and Wireless security research teams have found the following:**
  - **For a specific protocol, the same exploit will react differently and unpredictably on various implementations of the same protocol:**
    - **SNMP**
    - **LDAP**
    - **HTTP**
  - **With some ASN.1 embedded implementors, arbitrary binary code can be executed (trojan horse)**
  - **Some exploits tested transcend protocol types and implementation and are ASN.1 implementor specific**
  - **Vendor supplied patches are version specific and do not necessarily fix an ASN.1 embedded flaw in future versions of the code if the same ASN.1 implementor methodolology is used on the future version**

EXODUS

A CABLE & WIRELESS SERVICE

How Easy is it to Crash/Reset a Device?

- Depends on the ASN.1 implementation of the component and what other protection is in place
- By and large, it is pretty easy:
  - Cisco switches (CatOS) can be crashed with a malformed SNMP packet
  - Cisco routers (IOS) can be crashed but requires knowledge of the SNMP community string
  - Nokia IPSO can be root-accessed with the same buffer overflow attack against the OBID field as the Cisco components

EXODUS
A CABLE & WIRELESS SERVICE

What is the Economic Impact?

- **Estimated to be much greater than costs incurred in Y2K reparations**
  - **More equipment affected**
  - **Repairs must be done much faster and more than once**
  - **More equipment in inventory than when Y2K repairs were needed**
  - **More testing required due to complexity of configurations**
  - **Hacker attacks will cause periodic outages and cost the company revenue to discover and repair**

EXODUS
A CABLE & WIRELESS SERVICE

Rapid Change Management is Crucial to Success with ASN.1

- Current C&W assessment is over 75 known protocols are affected – and growing
- Rapid changes and deployment of updates is a critical success factor
  - Examples
    - Cisco changes to 2154 routers: 2-5-02 until 4-14-02
    - 2100 Nokia firewalls: 10 hours on 2-10-02
- Costing of ASN.1 will cause management tradeoffs between making networks more orbust or just paying for the updates to existing networks so they continue to run

EXODUS

A CABLE & WIRELESS SERVICE

Other Protection Problems

- Privacy
- Family
- Personal assets
- Relationships
- The Standard Stuff
  - Telecom infrastructure
  - Internet infrastructure
  - Intellectual Property
- Etc…

EXODUS
A CABLE & WIRELESS SERVICE

Intelligence and Information Sharing During Critical Events

- One of the biggest problems in cyber security
- Trust is a major factor and major problem
- Need to share critical information that may violate privacy laws or intellectual property
- May reveal collection methods, which is usually very sensitive to any entity
- Example:
  - May 2001 Hackers Union of China Global attacks
  - Sympathetic attacks from Brazil and Bulgaria
  - Force-multiplier worms from “zombies”
- U.S. initiatives
  - ISACs
  - Infragard (FBI + private companies)

EXODUS
A CABLE & WIRELESS SERVICE

Efforts Underway in the U.S.

- National Reliability and Interoperability Council (NRIC VI) FCC advisory focus groups (Homeland Security)
- National Security Telecommunications Advisory Council (NSTAC)
- National Security Council Office of Cybersecurity ISP Working Groups
- Internet Security Alliance (ISA)
  - ISA = EIA + CERT + Industry Companies
  - Internet Security Foundation (Europe)
- National Communication System (NCS) Emergency Assistance Group

EXODUS
A CABLE & WIRELESS SERVICE

Some Lessons Learned …So Far

- Lack of standards means that companies and governments will do what they have to do to solve their problems in a non-uniform way
- Costs always come first and companies resist security costs in favor of minimal or no security if they can do so
- Companies implement security features when required by regulations or public pressure (press)
- Governments (U.S.) are starting to try to put together best practices, but not necessarily critical practices
- Some critical infrastructures are so complex and so large that re-design and re-deployment is the only solution (and also impractical)
- Making critical infrastructures work securely is not as much an intellectual challenge as much as it is a financial and political challenge: we KNOW HOW; whether we can afford it is a different problem

EXODUS
A CABLE & WIRELESS SERVICE

EXODUS

A CABLE & WIRELESS SERVICE

Dr. Bill Hancock, CISSP
Vice President, Security
& Chief Security Officer
Email: bill.hancock@exodus.net
Web: www.exodus.net/drbill
Phone: 972-740-7347