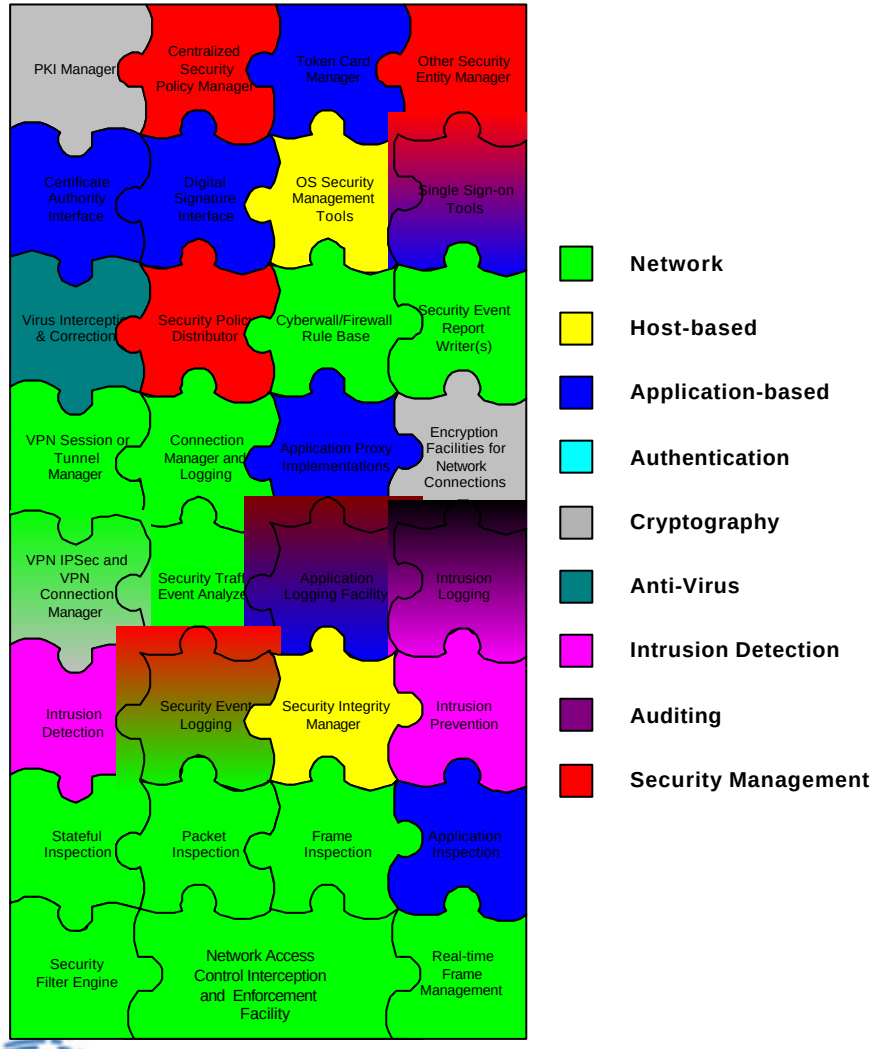
Cybersecurity From The Front Line

Dr. Bill Hancock, CISSP
Vice President, Security
Chief Security Officer
Cable & Wireless
bill.hancock@cw.com
+1-972-740-7347

CABLE & WIRELESS

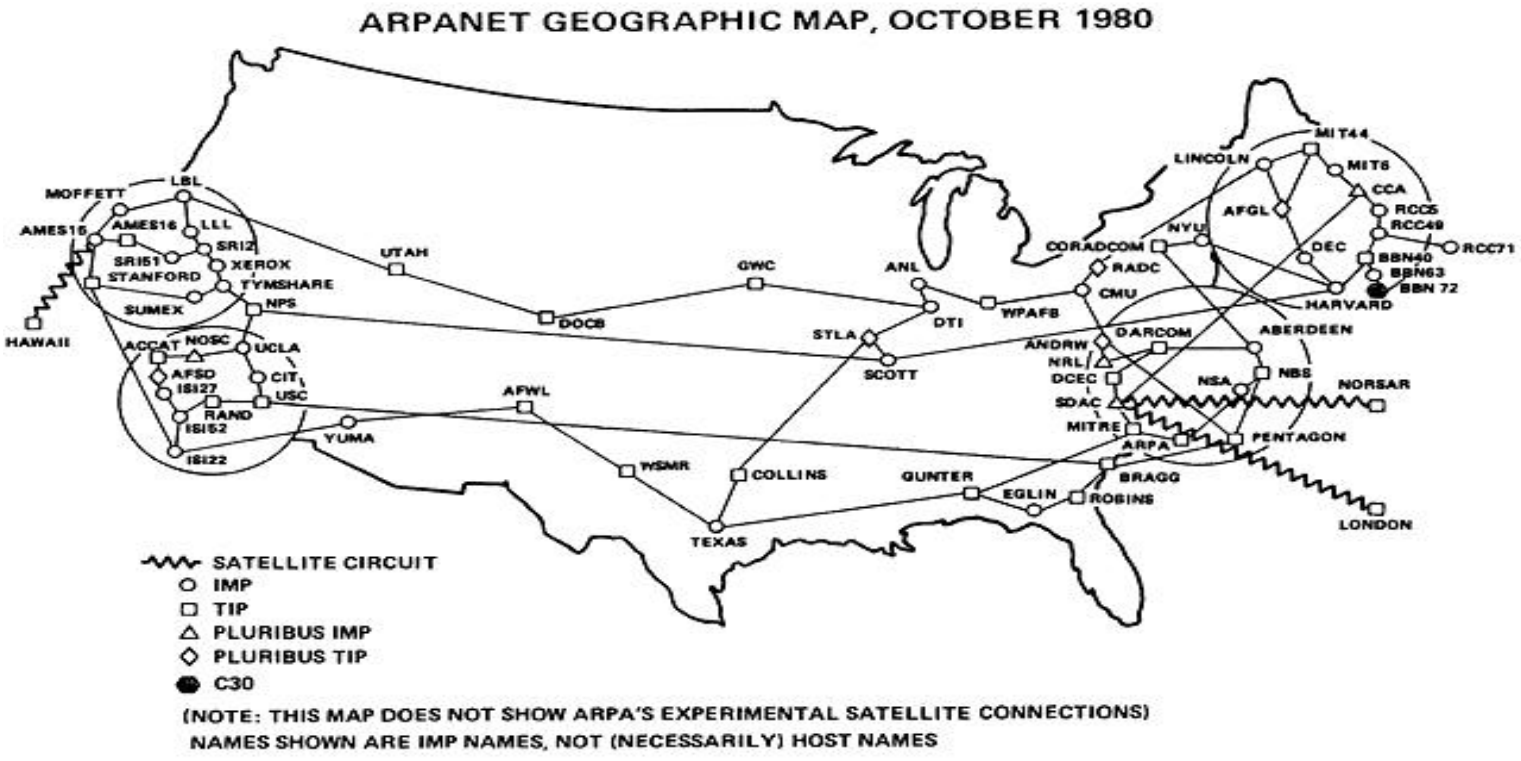
Security is Very Complex



- 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 from providers

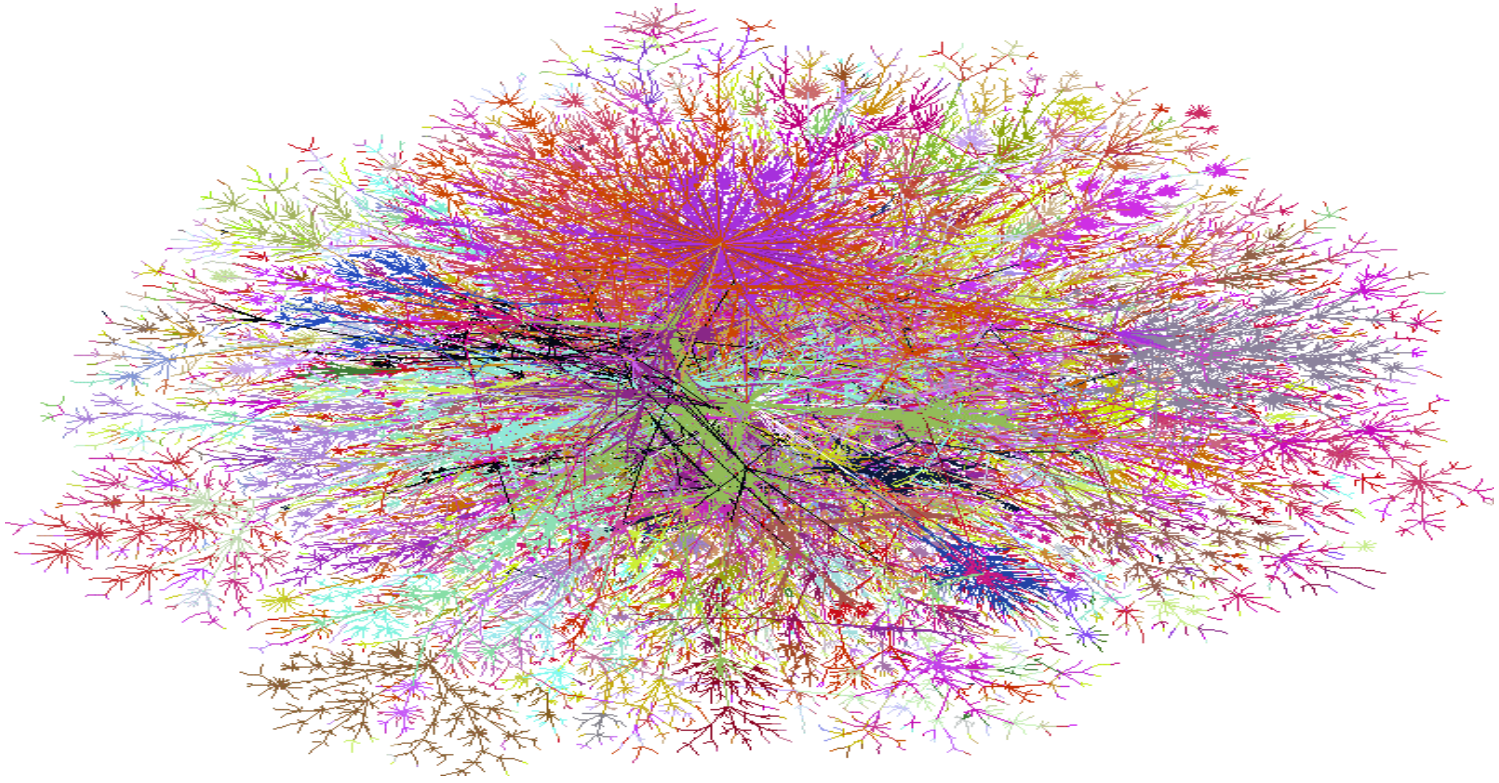
CABLE & WIRELESS

The Past



CABLE & WIRELESS

The Present

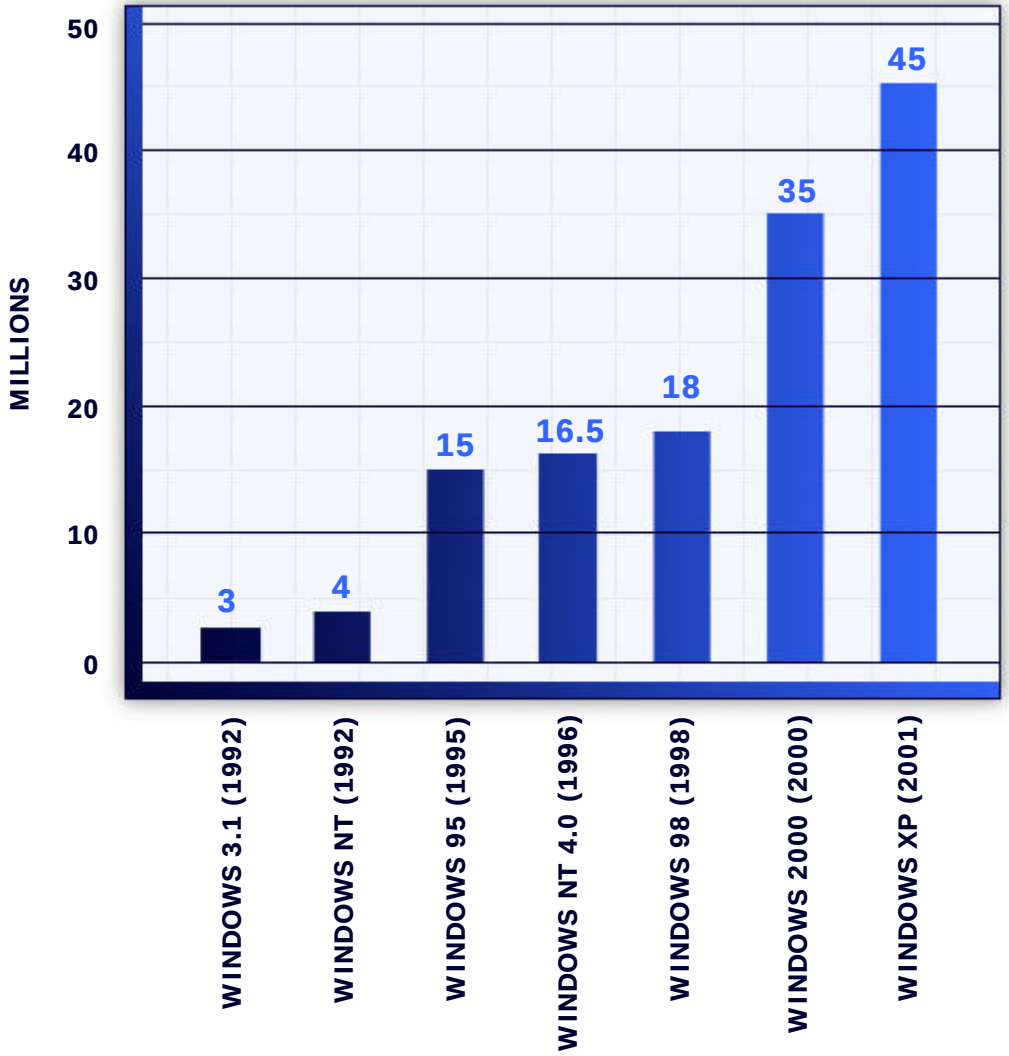


Source: http://cm.bell-labs.com/who/ches/map/gallery/index.html

CABLE & WIRELESS

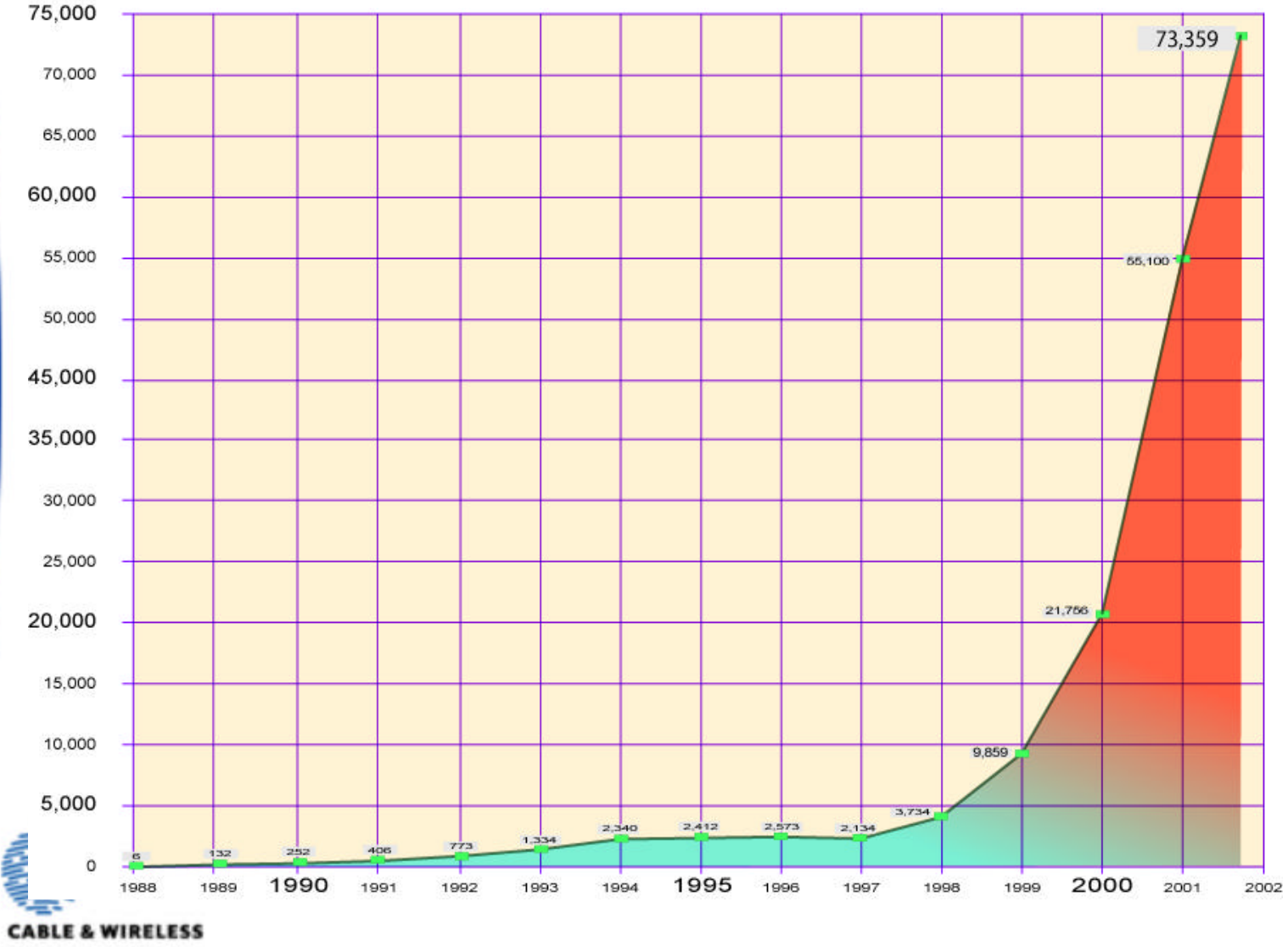
Software Is Too Complex

- **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**



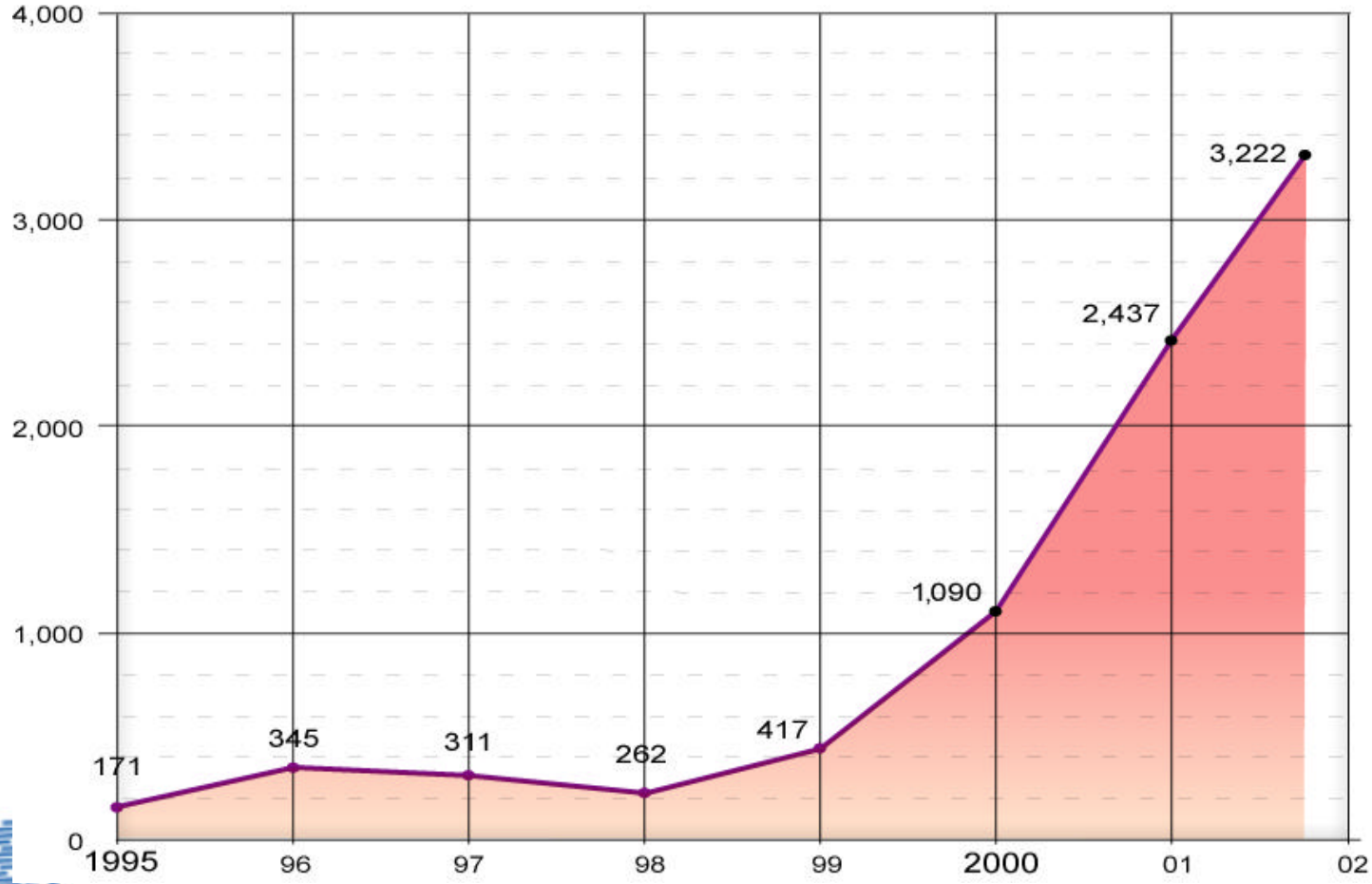
CABLE & WIRELESS

The Dilemma: Growth in Number of Incidents Reported to the CERT/CC



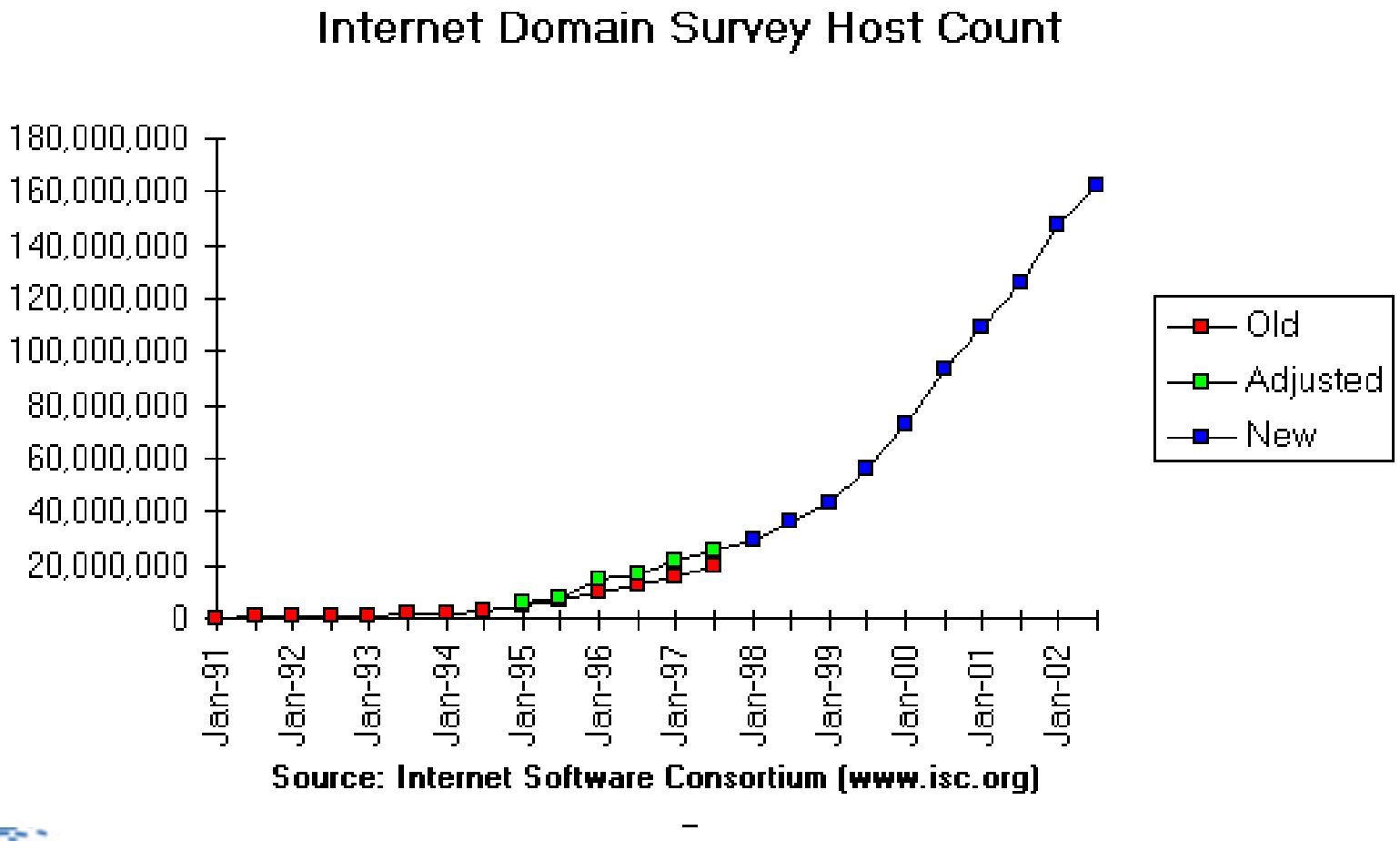
CABLE & WIRELESS

The Dilemma: Growth in Number of Vulnerabilities Reported to the CERT/CC



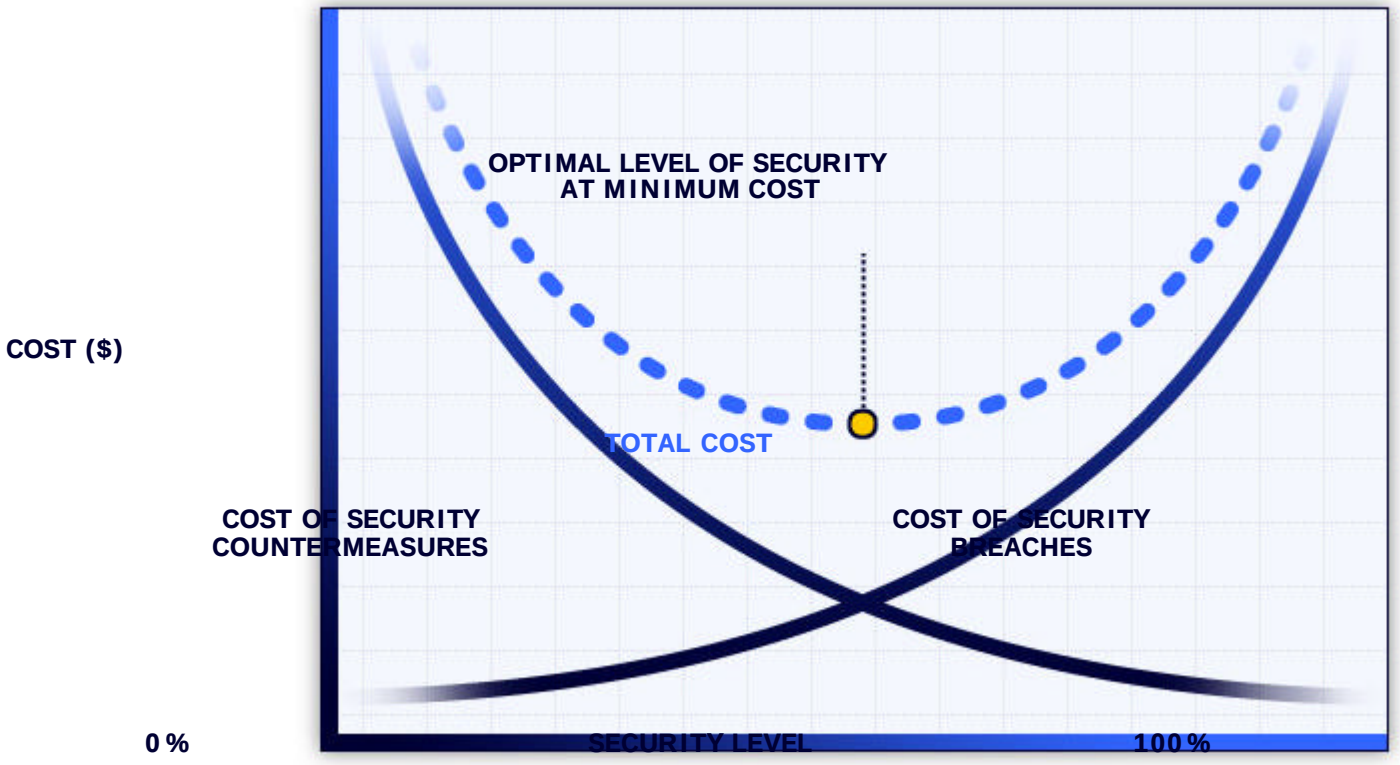
CABLE & WIRELESS

And Internet Continues to Increase in Size…

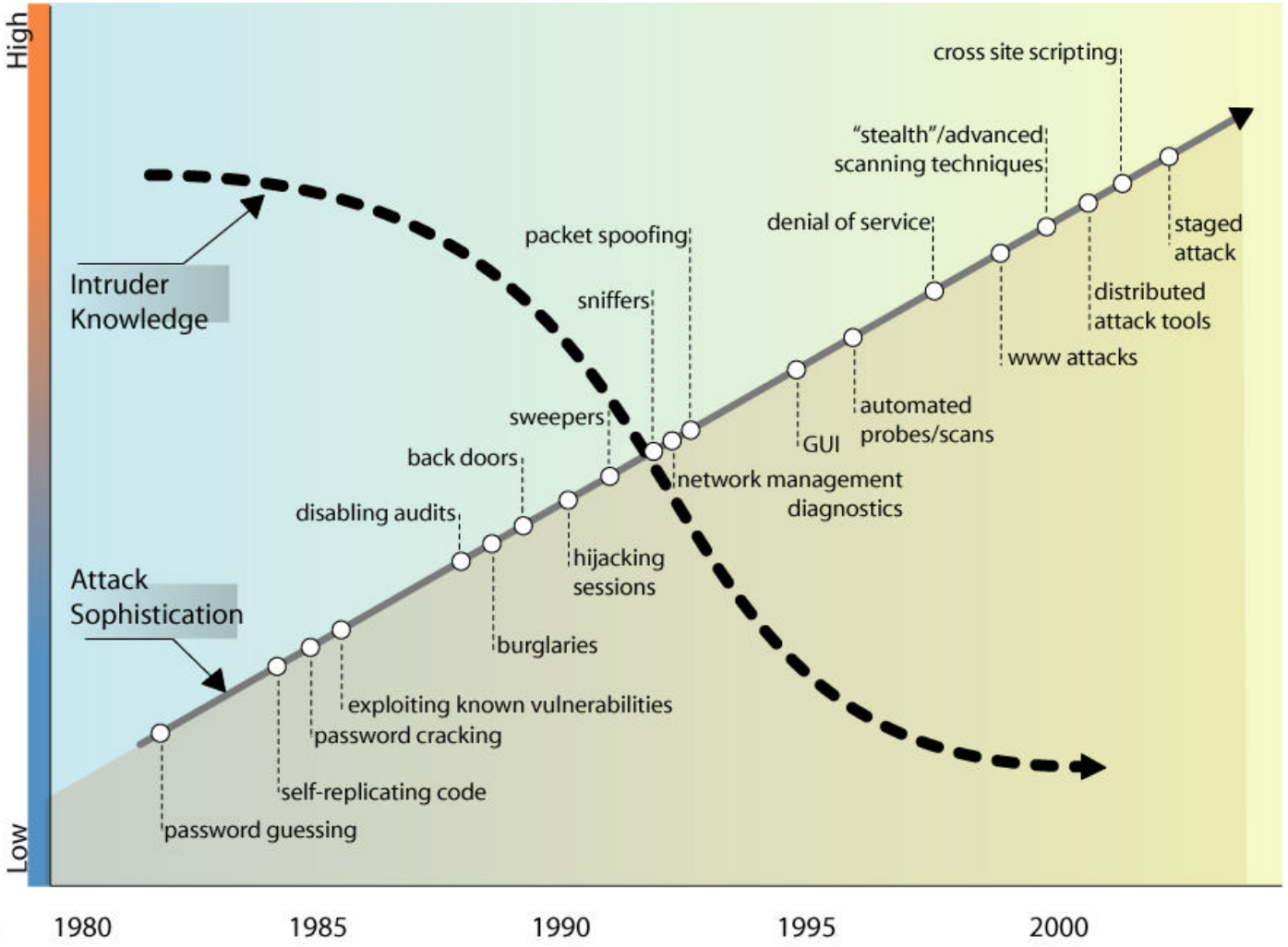


CABLE & WIRELESS

Security Must Make Business Sense to Be Adopted



As Systems Get Complex, Attackers are Less Mentally Sophisticated…



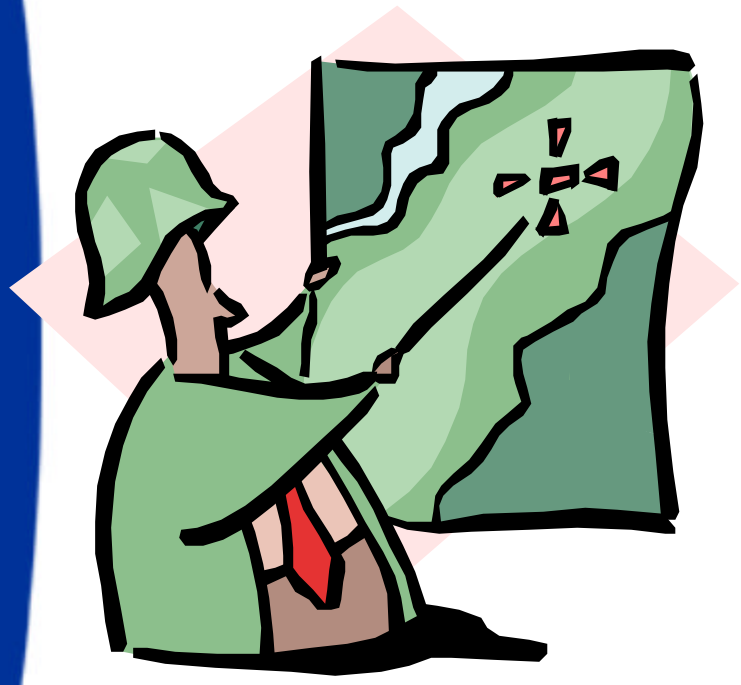
LOW

1980

CABLE & WIRELESS

CERT/CC

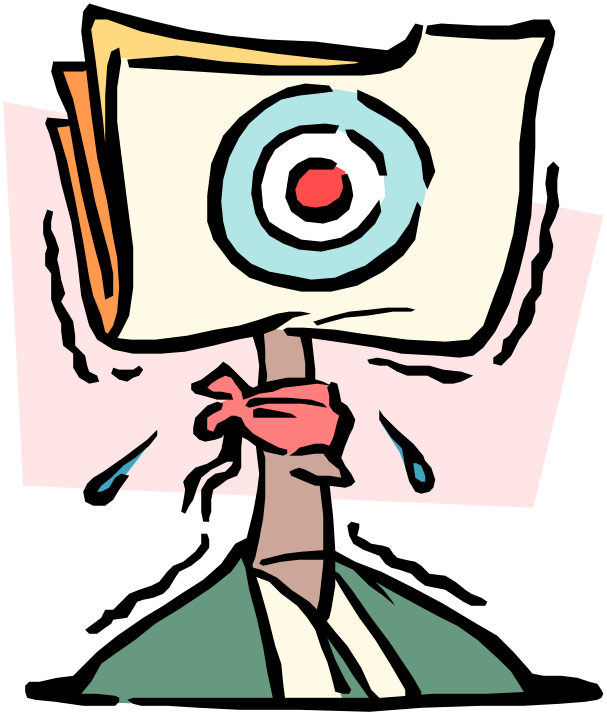
Classic Current IT Security Risks



- 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…

CABLE & WIRELESS

Upcoming Security Threats



- Geographic locations
  - China is major concern
  - Legislation in other countries
- New hacker methods and tools
- VoIP
- MPLS
- ASN.1 and derivatives
- Hacker “gangs”
- Complexity of application solutions make it easier to disrupt them (Active Directory, VoIP, etc.)
- Industrial espionage from competition
- Covert sampling
- Covert interception

CABLE & WIRELESS

Threats - Infrastructure

- Core (critical)
  - Routing infrastructure
  - DNS
  - Cryptographic key mgt.
  - PBX and voice methods
  - E-mail
- Essential
  - Financial systems
  - Access management to Exodus critical resources
  - Intellectual property protection methods
  - Privacy control methods
  - Internal firewalls and related management
  - HR systems

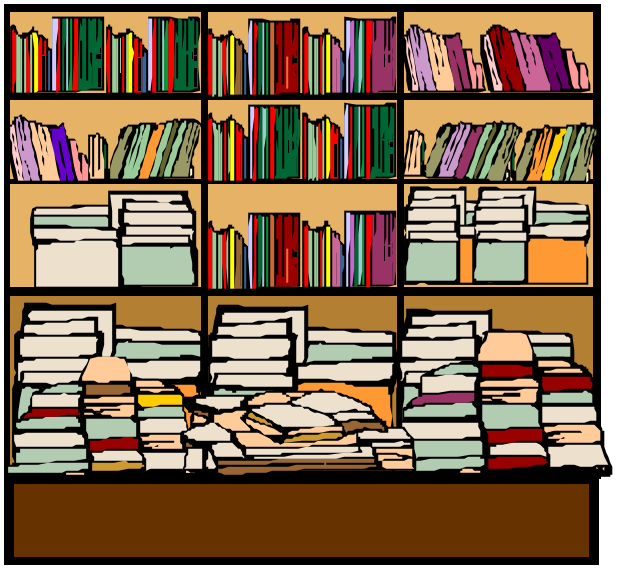
CABLE & WIRELESS

Routing Infrastructure

- No router-to-router authentication
  - Router table poisoning
  - Vector dissolution
  - Hop count disruption
  - Path inaccuracies
  - Immediate effect
  - Redundancy has no effect on repair/recovery
- Edge routers/switches do not use strong access authentication methods
- No company-wide internal network IDS/monitoring
- No internal network security monitoring for anomalies or stress methods
- No effective flooding defense or monitoring

CABLE & WIRELESS

Generic DNS Security Assessment



- Grossly inadequate security methods against attacks (DNS weakness)
- No distributed method for attack segmentation recovery
- Geographic distribution inadequate and easy to kill due to replication
- Zone replication allows poisoning of DNS dbms
- DNS servers around the company do not implement solid security architecture

CABLE & WIRELESS

Mobile Technology Security

- **Most customer mobile technology when removed from the internal network or premises is WIDE OPEN to data theft, intrusion, AML, etc.**
  - **Laptops (no FW, IDS, VPN, virus killers, email crypto, file crypto, theft prevention/management, cyber tracking, remote data destruct, remote logging, AML cleaning, etc., etc., etc.**
  - **Palm Pilots, etc, - no security**
  - **3G and data cells – no security**
  - **No operational security over wireless methods**

CABLE & WIRELESS

Hyperpatching

- The need to quickly patch vulnerabilities is becoming a major security pain point
  - As of June 2002, Microsoft alone had issued 30 patches for 40 security vulnerabilities since the beginning of 2002
- Protocol exploits such as SNMP will accelerate and require additional patching and fixes
- Customers should stop with “old think” change control and start considering using hyperpatching and mass roll-out systems (push technology) to start solving hyperpatching problems

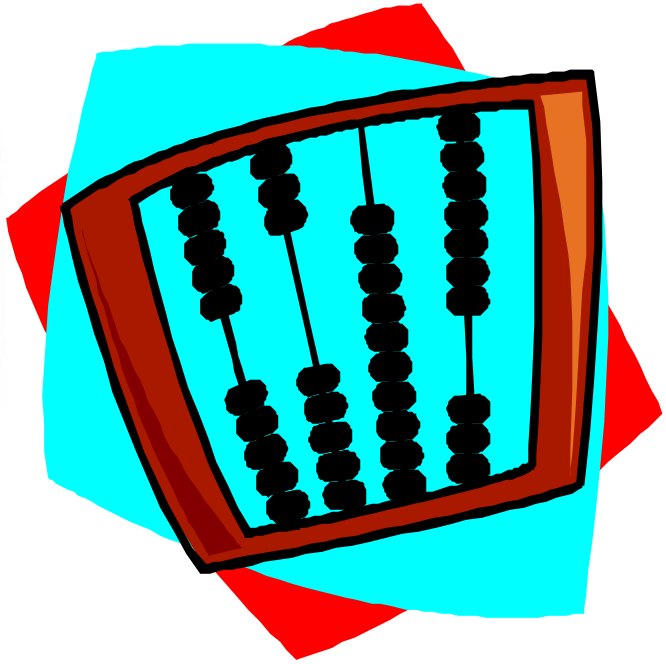
CABLE & WIRELESS

Employee Extortion

- At least 5 different extortion methodologies have appeared that affect employee web surfers
- Latest one involves persons who surf known child pornography web sites or hit on chat rooms on the subject
  - A link is e-mailed to the person and they threatened with being turned over to officials and employers unless they pay to keep the information about their surfing habits secret
- This is a growing business…

CABLE & WIRELESS

Cryptographic Key Management



- None at most sites
- What is available is all manual
- Changing keys on some technologies takes MONTHS (e.g. TACACS+)
- Keys are weak in some areas and easily broken
- No “jamming” defenses for key exchange methods
- Little internal knowledge on key mgt and cryptographic methods

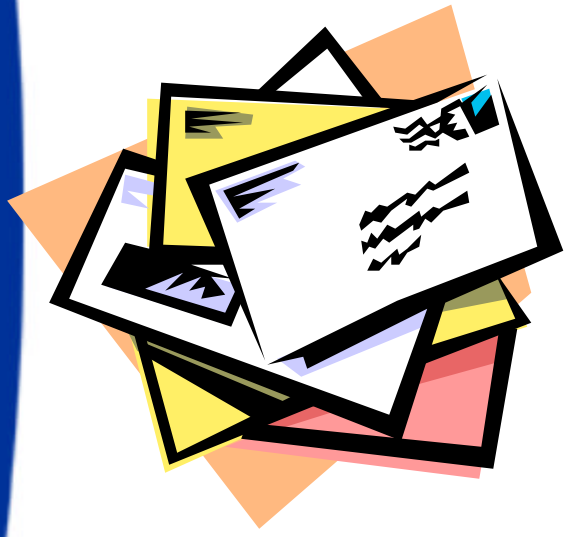
CABLE & WIRELESS

PBX and Voice Methods

- No assessment of toll fraud and PBX misuse at most sites
- Cell phones used continually for sensitive conversations
- No conference call monitoring for illicit connections or listening
- No videoconferencing security methods
- No voicemail protection or auditing efforts trans company
- Easy to social engineer PBX access and re-direction

CABLE & WIRELESS

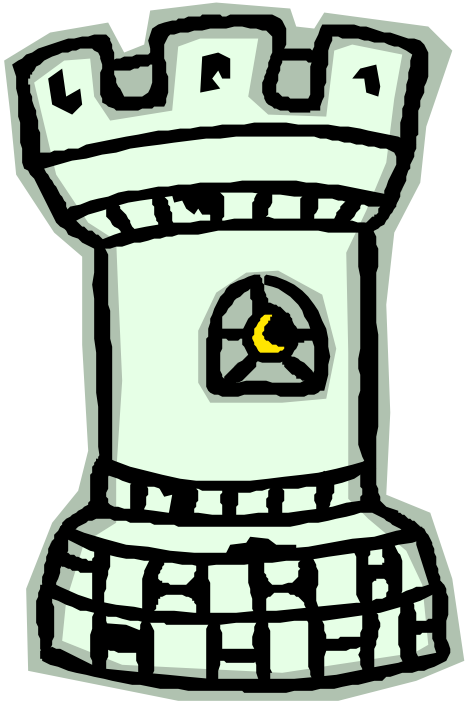
E-Mail Security Issues



- Employees in trusted positions reading e-mail (happens at most customer sites)
- E-mail security methods take a long time to implement
- Lack of use of encryption methods for confidential e-mail
- Lack of keyserver for cryptographic methods (this is due to power)
- Newly devised security methods not implemented yet
- Use of active directory and LDAP in future a major concern
- Wireless e-mail a concern
- No filters for SPAM
- No keyword filter searching methods for potential IP “leakage”
- Ex employees retain access information for their and other accounts

CABLE & WIRELESS

Essential Internal Services



- Financial systems
- Console management systems
- Access management to critical resources
- Intellectual property protection methods
- Privacy control methods
- Internal firewalls and related management
- HR systems
- Others…

CABLE & WIRELESS

Wireless

- Continues to be a problem
- Mostly due to lack of implementation of controls
- War driving is easy to do for most sites and to get on most networks
  - Illegal connection to a wireless network violates FCC regs
- Need intrusion detection for wireless to detect who is associated to the LAN and doesn't belong
- Best short-term solution are peer-to-peer VPNs (desktop, site-to-site, etc.)
- New threats with upcoming 3G products

CABLE & WIRELESS

Data Retention

- BIG push for data retention in many parts of the world
- With retention comes liabilities for retained information
- U.S. has no specific retention laws except in specific financial and healthcare areas
- EU and Asian countries recently enacted serious retention laws

CABLE & WIRELESS

Other Security Needs

- Strategic plans
- Tactical plans
- Customer education
- Travel security
- Site surveys/audits
- Internal auditing by competent companies
- Manpower
- Executive security education
- Tactical response
- Intellectual property protection
- Legal staff infosec security education (serious problem)
- Remote office security

CABLE & WIRELESS

Blended Attacks

- **Biological and Cyber**
  - **Bio infection and DDoS against infrastructure**
- **Multiphasic Cyber Attack**
  - **DDoS against routers, DNS poisoning attacks and defacement attacks at the same time**
- **Sympathetic hacking group attacks**
- **Upstream infrastructure attack**
  - **IXC disruption**
  - **Power grid disruption**
  - **Peering point disruption**
  - **Supply-chain vendor disruption**

CABLE & WIRELESS

Summary

Dr. Bill Hancock, CISSP
Vice President, Security
Chief Security Officer
Cable & Wireless
bill.hancock@cw.com
+1-972-740-7347

CABLE & WIRELESS