Security for the Evolving Telecommunications Infrastructure

John Kimmins
Senior Director
(732) 758-2035
September 24, 1997
Objectives

• Current threat environment
• Network functional components
• Security issues
• Government & Industry response
Current Threat Environment

- Loose federations of intruders
- Domestic and international sources
- Insiders and outsiders
- New and old targets
- Some local outages
- New mindset - may create denials of service
Current threat environment

- Dial-ins, data communications connectivity and Internet access exploitations to get to critical components
- Basic and sophisticated techniques
- Mobile systems & wireless access used
Network Functional Components

- Local loop
- Switching
- Signaling
- Transmission facilities
- Operations
Functional Components: Criticality Assessment

- Impact on call/connection processing
- Cross component effects
- Number of users affected
- Operations impact
Major Security Issues
Examples

- Outsourcing of NE software development
- Outsourcing of network operations
- Vendor remote access
- Insertion of new technology NEs
- Open access to signaling/NEs/Operations
Evolution of Network Domains within Service Providers

- PSN
- Corporate DCNS
- ISP Systems & Support
- Internet
- New Technology
# Old/New technology Products: Evolution of Security Features

<table>
<thead>
<tr>
<th>Feature Req's as per Bellcore Requirements</th>
<th>Traditional Network Elements</th>
<th>New Technology Network Elements</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1990</td>
<td>Now</td>
</tr>
<tr>
<td>Individual Logins</td>
<td>M</td>
<td>H</td>
</tr>
<tr>
<td>Password Complexity</td>
<td>M</td>
<td>H</td>
</tr>
<tr>
<td>Password Aging &amp; User Updating</td>
<td>L</td>
<td>H</td>
</tr>
<tr>
<td>Warning Banner</td>
<td>N</td>
<td>H</td>
</tr>
<tr>
<td>Login Bypass Restriction</td>
<td>M</td>
<td>H</td>
</tr>
<tr>
<td>Embedded Operations Access</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>Protocol Access Restrictions</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>Security Alarms</td>
<td>H</td>
<td>H</td>
</tr>
<tr>
<td>Timeout</td>
<td>H</td>
<td>H</td>
</tr>
<tr>
<td>Resource Access Privilege</td>
<td>H</td>
<td>H</td>
</tr>
<tr>
<td>Security Log</td>
<td>M</td>
<td>H</td>
</tr>
<tr>
<td>Security Admin Facilities</td>
<td>H</td>
<td>H</td>
</tr>
<tr>
<td>EMS Security</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>NMS Security</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>Physical Security</td>
<td>H</td>
<td>M</td>
</tr>
</tbody>
</table>

**Note:**
EMS=Element Mgt.. System  
H=High  
L=Low  
M=Medium  
NA=Not Applicable  
NMS=Network Mgt.... System
Industry/Government Response Examples

- National Security Information Exchange
- President’s Commission on Critical Infrastructure Protection
- National Reliability & Interoperability Council
Industry Security Thrusts
Examples

- Enhancing signaling protocols
- Developing TMN security architecture
- Evolving security requirements
- Using user security tokens