**Development**

CyberCIEGE software was created by United States Government employees at The Center for Information Systems Security Studies and Research (CISR) at the Naval Postgraduate School (NPS) and Rivermind, Inc. CyberCIEGE contains government work created by NPS employees and therefore those portions of CyberCIEGE are in the public domain and are not subject to copyright. All remaining work within CyberCIEGE is copyrighted by Rivermind and its use is subject to the copyright protection afforded to Rivermind.

CyberCIEGE offers opportunities to incorporate additional cyber security topics (e.g., mobile devices). If you have interest in sponsoring CyberCIEGE development, or custom scenario creation, please contact cyberciege@nps.edu.

**Information**

For more information regarding CyberCIEGE and a free demonstration download, visit our website at http://www.cisr.us/cyberciege. The game is available for unlimited use by the US Government and a no cost education license is available for educational institutions. To obtain a copy, send a request to: cyberciege@nps.edu.

The Scenario Development Tool (SDT) automates the syntax of the CyberCIEGE definition language and makes scenario development easy through the use of reusable libraries, forms, and pull down menus. The SDT is a great way for Information Assurance teachers to use CyberCIEGE to focus student attention on specific IA concepts.

CyberCIEGE scenarios can be developed for novice computer users all the way to sophisticated technical personnel. The content of the scenario depends only upon the goals and imagination of its developer.

The Scenario Development Tool (SDT) automates the syntax of the CyberCIEGE definition language and makes scenario development easy through the use of reusable libraries, forms, and pull down menus. The SDT is a great way for Information Assurance teachers to use CyberCIEGE to focus student attention on specific IA concepts.
Each CyberCIEGE scenario includes a set of users whose productive work makes money for the enterprise. Users have goals that must be met for the users to remain productive and happy. Players are responsible for providing the resources and environment needed by users to reach their goals. Users have different amounts of trust, which may lead to insider attacks.

Players may hire and fire IT and security staff to help maintain systems and keep the physical premises secure.

In its interactive environment, CyberCIEGE covers the significant aspects of network management and defense. Players purchase and configure workstations, servers, operating systems, applications, and network devices. They make trade-offs and prioritization decisions as they struggle to maintain a balance between budget, productivity, security, and user goals. Each phase may require increasingly sophisticated defenses, including firewalls, anti-virus, VPNs, biometric scanners, smart cards, and cross domain solutions. Players can watch the consequences of their choices, while money is spent, and defenses are built.

Risk Management

Game Characters

CyberCIEGE enhances information assurance education and training through the use of network management and defense scenarios. Players advance through a series of challenges that illustrate the importance of planning and decision making in a dynamic environment. Each phase may require increasingly sophisticated defenses, including firewalls, anti-virus, VPNs, biometric scanners, smart cards, and cross domain solutions. Players can watch the consequences of their choices, while money is spent, and defenses are built.

Can you keep the network alive?