FISSEA Security Awareness, Training, & Education Contest

Entry Form

Name of submitter: DISA, SAIC, and Carney, Inc.

Organization: Carney, Inc.

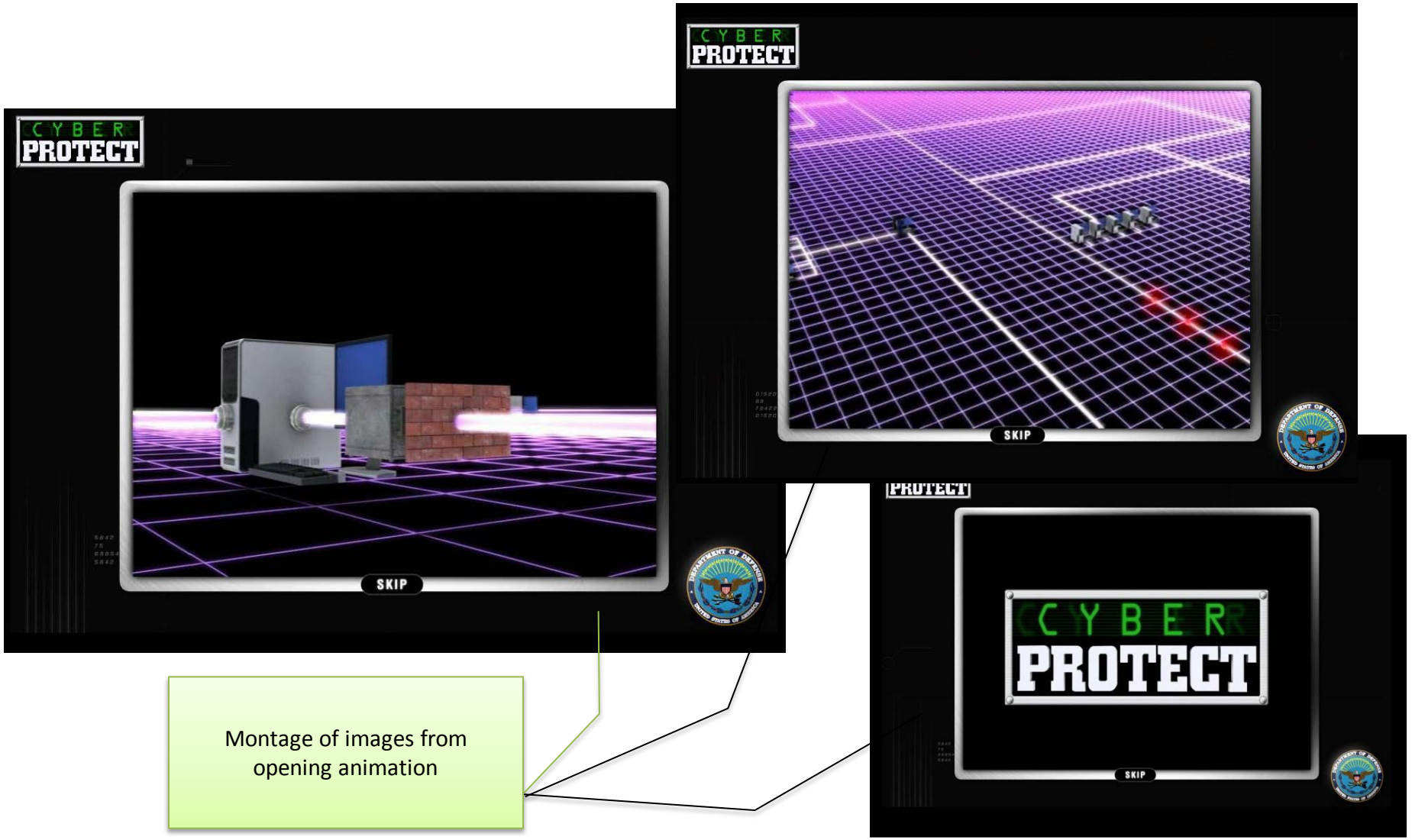
Type of Entry: Role-Based Training & Education > Interactive Scenario/Exercise

Title of Entry: CyberProtect, Interactive Training Exercise, Version 2.0

Description of Entry: Originally developed as a CD ROM application in 1999, CyberProtect version 2.0 encompasses the updated web based version of the gaming application offered in 2010.

The interactive training exercise consists of an interactive practical challenge where players face real-world scenarios involving internal and external network security threats. The game begins with a fresh, unprotected Local Area Network (LAN) operating system. There are no defensive mechanisms in place such as firewalls, antivirus software, and redundant systems. It is up to the user to protect the network from malicious attacks by requisitioning and placing security tools within the network. Once installed, the system is tested for vulnerabilities, simulating real-life challenges faced by IT security professionals. The user's challenge is to balance the need for security with a finite budget for network tools using knowledge from training and personal experience. This lesson is available world-wide to the DoD community and public entities such as schools and universities.

The CyberProtect interactive training exercise begins with an animated depiction of information moving through an artistically rendered network. The animation immediately engages the user and sets up the exercise challenge, “The age of information is also the age of information security. Your challenge: protect your network. Successfully”. The opening scene is visually dynamic and includes upbeat background music to give the learner the feeling of entering a “Mission: Impossible” style game.



Montage of images from opening animation

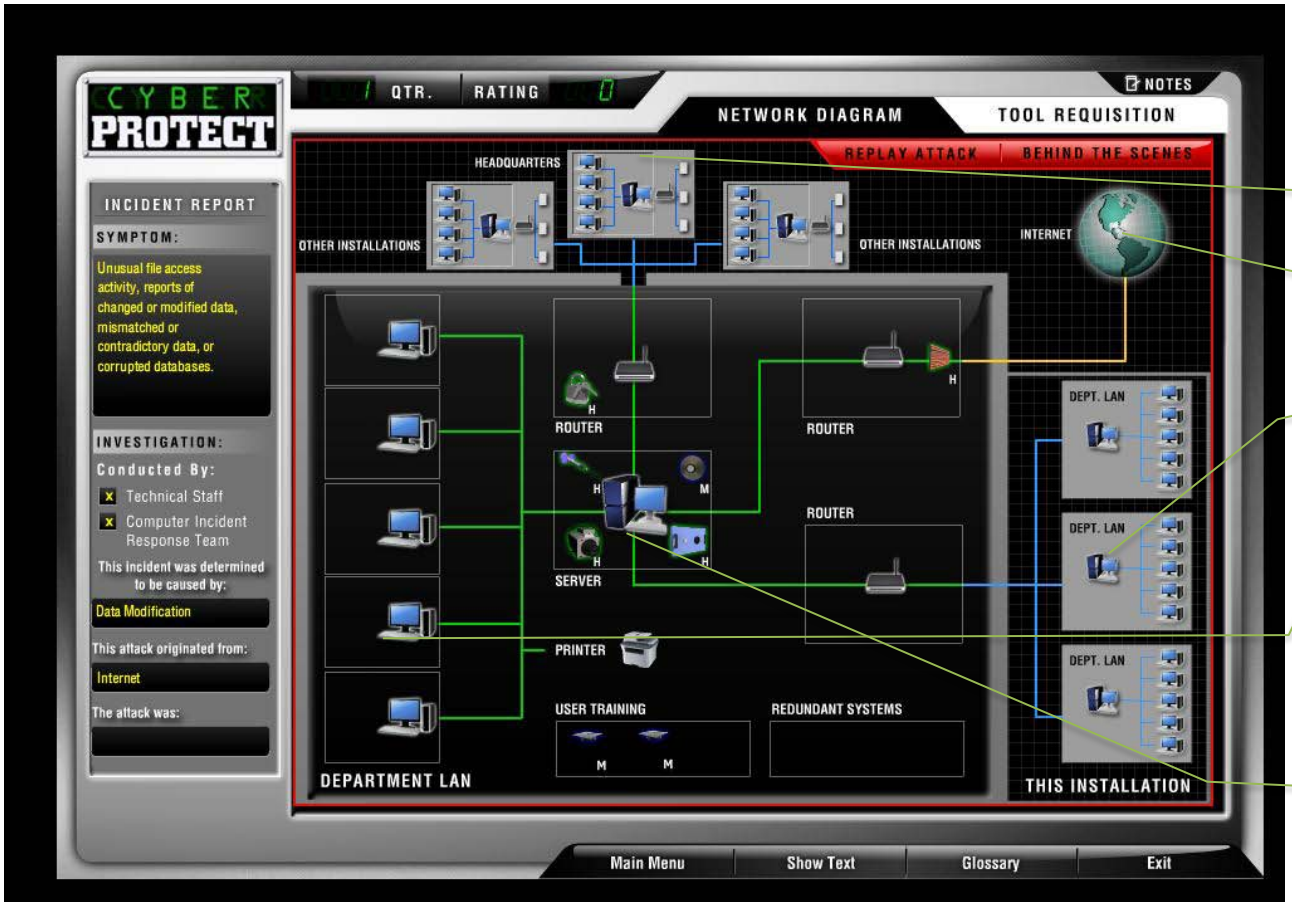
An overview section provides the learner with more detail surrounding the purpose of the exercise, available tools, and strategies for play. Learners are encouraged, but not required, to review educational information explaining the security tools at their disposal and potential security threats. This optional information brings new learners up to speed, gives learners with a moderate knowledge an opportunity to refresh their knowledge and allows experienced learners to forgo the background information and proceed straight to the exercise. A sample screen from the opening module appears below.

The narrator, Mark, gives an animated tutorial on the game interface

If the learners opt to take advantage of all of the learning materials at their disposal, they can access “Mark’s Notes”. Here they learn their goal is to maintain an operational readiness rating of at least 90%, the definition of a readiness rating, and a description what to expect when their LAN is attacked. Learners can always come back to review key information at any point during play if a question comes to mind.

Mark’s notes contain useful information to prepare for the next attack

Once learners feel confident with their level of knowledge, they begin the game. A grid style network diagram introduces them to their department's LAN, taking into consideration the flow of information both internally within their department and externally to other departments on the installation, exterior installations such as Headquarters, and connections to the internet.



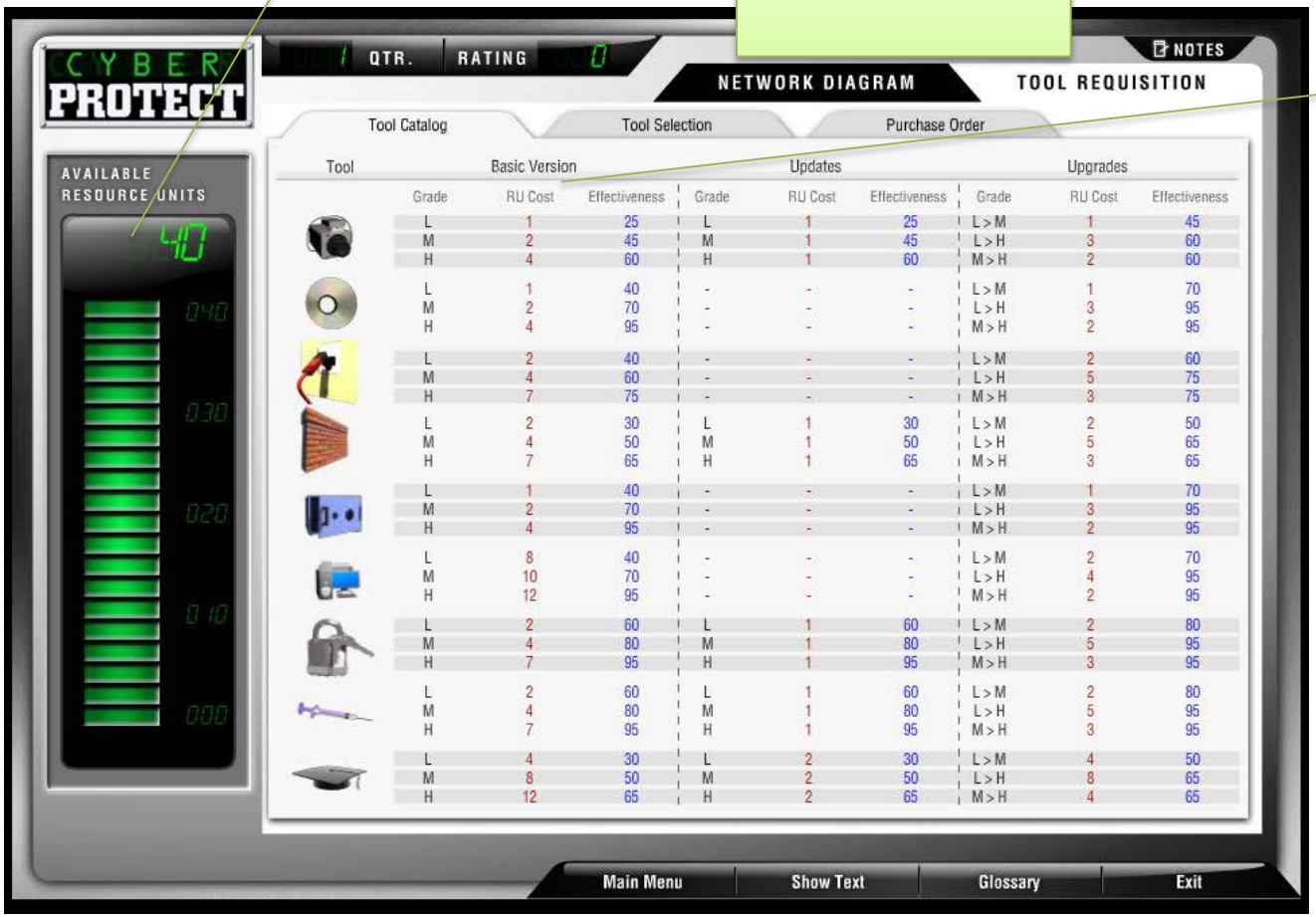
System attacks can come from any direction, internal or external

Defensive equipment bolsters security

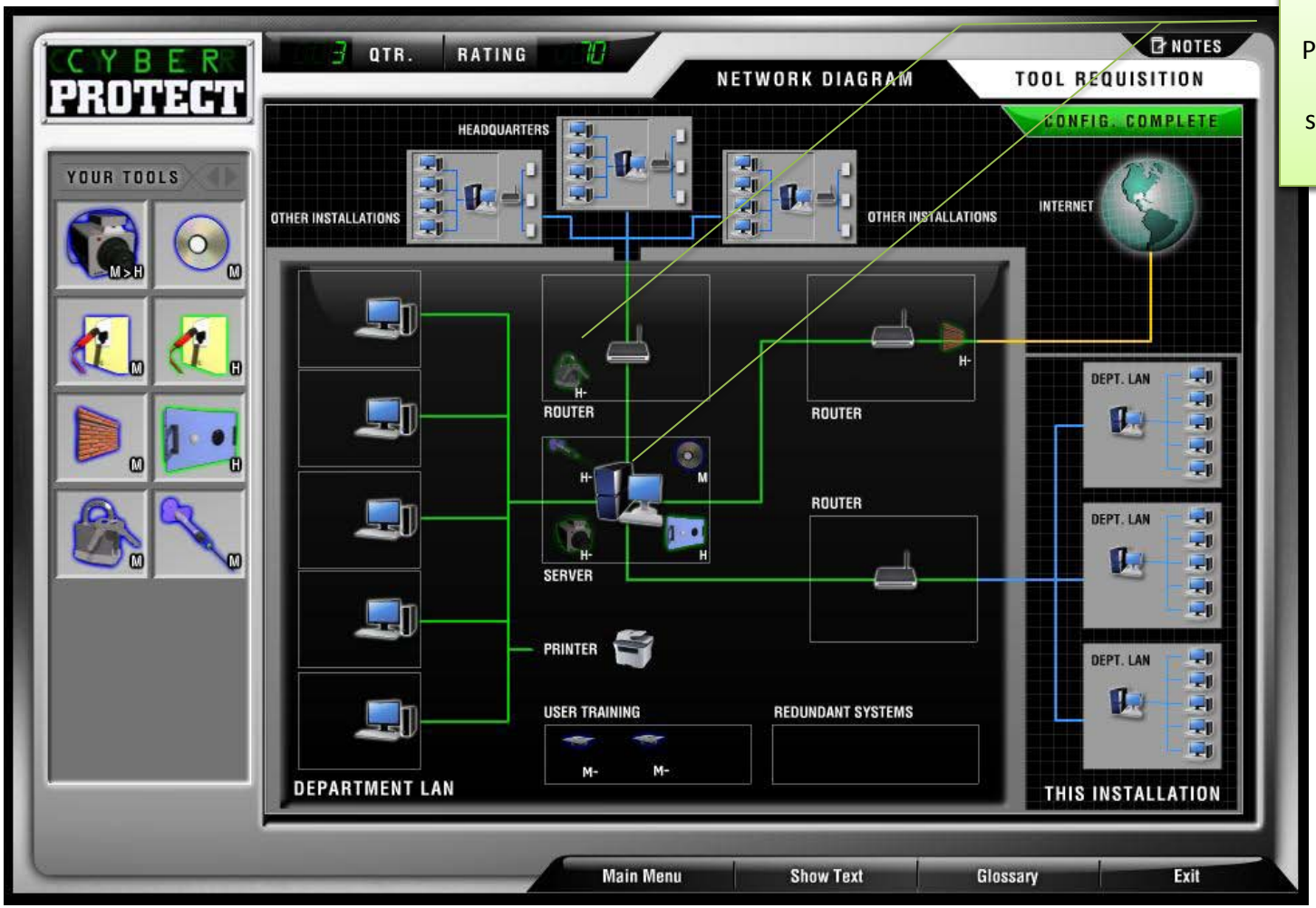
In order to protect their new LAN, learners must purchase the appropriate tools, such as firewalls, anti-virus software, and intrusion detection devices. As in all real-world scenarios, this game takes into consideration the budget constraints the learner will face on the job. Each tool comes in a variety of grades from low to high with appropriate price points to match. The game is played over the course of four quarters with an estimated annual budget of 100 requisition units. To begin, the learner is only provided with the first quarter budget of 40 requisition units. It is up to the learner to apply the funds carefully to achieve maximum protection.

Budget Tracker

Weigh cost and effectiveness of the different defensive equipment



After purchasing the desired tools, the learner returns to the network diagram and deploys those tools on the desired systems. No tool is returnable, so learners are cautioned to only buy what they need.



Purchased tools are added to the servers and routers

Once the tools are placed appropriately, the learner selects the **Configuration Complete** button to begin play. The attacks begin.

A warning display alerts the learner to a specific attack scenario. If the appropriate tools are in place, the attack is rendered unsuccessful.

Suspicious activity on the network warns the learner that an attack is underway

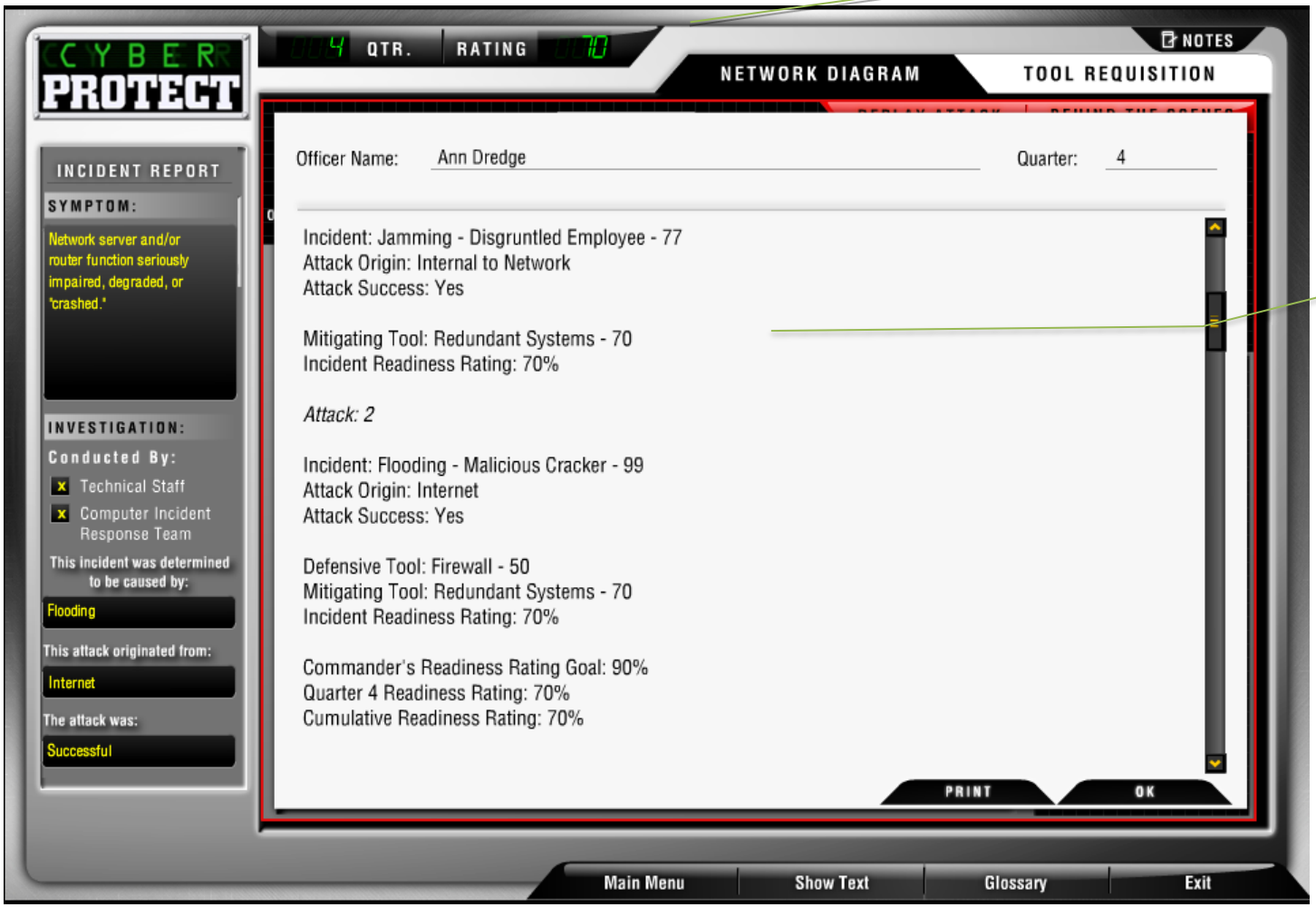
The learner receives more detailed information regarding the attack via “Behind the Scenes” feedback that explains the type of person behind the threat and potential motives. Scenarios range from corporate espionage to hackers tricking befuddled users into transmitting a virus. Every care is taken to assure the plausibility of the attack.

There are many types of threats, both malicious and unintentional

The game concludes after the learner has completed all four quarters. A final operational readiness report outlines the learner's performance and compares it to the goal of achieving a target 90% readiness rating.

A quarterly breakdown provides an outline of each attack, the results, and the individual rating applied to each scenario, allowing the learner to pinpoint areas for improvement.

The engaging and instructive game motivates learners to play again and again until they achieve the target readiness ratings for each quarter.



Final Score

Cumulative Operational Readiness Report