**Cybersecurity and Infrastructure Card Game**

**Access Denied Full Play Instructions**

**Designer: Jessica D. Bayliss, Ph.D., Illustrator: Diego Barillas**

**Objective:** A fork of the resilience card game project for non-cybersecurity people. It's meant to help folks learn some basics about cybersecurity through learning attack and mitigation terms from the MITRE ATT&CK and MITRE ICS Matrices to help people become more productive when they participate in a scenario or wargame with cybersecurity components after.

**Player Narrative:**

You want to aid the facilities next door. Whenever your people notice a potential vulnerability in your neighbor’s facilities, you tell them about it. Sometimes you talk about the vulnerabilities because they’re interesting. Sometimes you point at them in amusement because they’ve gained a common vulnerability that people should have foreseen.

The other player does the same and points out vulnerabilities with your facilities.

Sometimes information about the vulnerabilities doesn’t get fixed in time or you don’t believe your neighbors and you’re attacked. The end goal is to mitigate as many found vulnerabilities for your facilities as possible with limited resources/people to check them out (represented by cards) while pointing out all the vulnerabilities you can find in other players’ facilities.

In real life winning means nobody gets attacked successfully, but in the game, whomever has the most points left in facilities and optimal connections wins.

**Educational Goals**

* Education, but not training
* Linking attacks to defense/mitigation
* Considering control system breaches (even below SCADA)
* Using information from real world events in cards:
  + 2000 Maroochy Water Services, Australia (water treatment)
  + 2016 Kyiv power grid cyber-attack (power)

**Acknowledgements**

This data was produced by Rochester Institute of Technology under United States Military Academy (USMA) Award Number W911NF-23-2-0036. USMA, as the Federal awarding agency, reserves a royalty-free, nonexclusive and irrevocable right to reproduce, publish, or otherwise use this data for Federal purposes, and to authorize others to do so in accordance with 2 CFR 200.315(b).

**Game Description**

* Number of players: 2
* Separate the water and power decks that come inside the same card case.
* Deck shuffling:
  + Shuffle all facilities per player into their own deck minus one 2pt starting facility. Place the rest of the deck face down.
  + Shuffle the rest of your deck and place cards face down in a separate pile from the facilities deck.
* Starting cards for each player:
  + Each player has a discard pile for cards from their own deck. The discard pile starts out empty.
  + Place one 2pt facility face up in front of yourself.
* Attackers are simulated by a d20 die roll. To get an online die look up the words: d20 roll.

**Ending the Game and Scoring**

Scores are tallied at the end of the last turn where either of the following occurs:

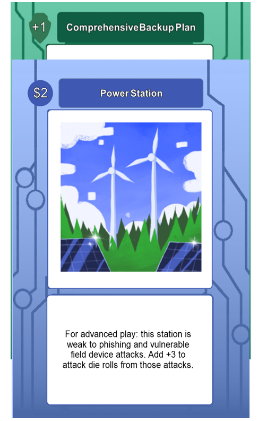
* One player runs out of cards
* One player loses their last facility

Score is tallied with the following:

* Remaining worth points in all facilities minus their negated points
* +1 for every facility that has the number of connections that are at a minimum or greater for the original point value of the facility

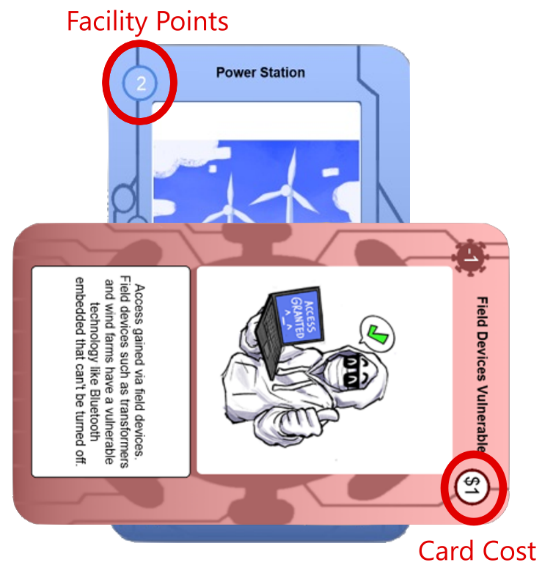
**Game Phases**

All players do each phase together and nobody starts the next phase before everybody has finished the current phase.

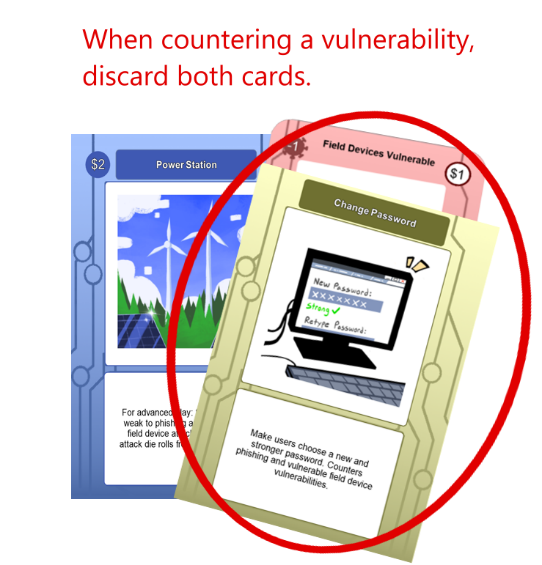
**Draw, Discard, and Discuss**: Draw until you have 5 cards in your hand. If one or more of the cards are discussion cards, then discuss the topic of the cards for five minutes. Redraw until you have 5 cards. Optionally, you may discard one to two cards into your discard pile and redraw until you get 5. The round always starts with 5 cards per player unless it’s the end of the game where somebody has run out of cards.

**Defense phase**: Lay down up to 1 card that gives defense to a station. This phase may be skipped if nobody has any cards to play.

**Vulnerability phase:**

Spend the number of points in facilities you own (not impacted by current “health” of facility, which is only used to subtract facilities from the game and calculate the end score) to let other players know the vulnerabilities you’ve discovered on their stations.

* Any players without vulnerabilities to play must wait for all other players to play their vulnerabilities before going into the Mitigation phase.
* More than one vulnerability can be played on a station (only 1 of any mitigation type though)
* Vulnerabilities are played face up to allow them to later be countered. The card is placed crosswise on top of a facility.
* Vulnerability cards have a red background.
* Purple instant negative cards should be played in this phase to allow for instant counters. Note: instant cards ARE NOT spread by the Lateral Movement card.
* DO NOT immediately mitigate vulnerabilities as they’re played. Waiting for the mitigation phase to counter ALL vulnerabilities except for instant cards means that you will be able to choose which cards to counter in cases where there are more vulnerabilities than mitigation cards to counter them.

**Mitigation phase:** Remove vulnerabilities from your stations by countering them with mitigation cards from your hand. Mitigation cards have a yellow background. Countered vulnerabilities go into the discard player of whomever played the cards. Mitigation cards go into your discard pile.

**Attack phase:**

* For the vulnerability cards that cannot be countered, roll a d20 to see if the vulnerability is attacked. Anything >10 is assumed to be a successful attack.
* For successful attacks, take off the points lost for that facility AND discard the vulnerability into the player’s discard pile for whomever played the card. Note: once a facility is <= 0 points it’s removed from play and those points are lost permanently. To indicate points taken off where the facility points remain >0 use a token (coins work) to indicate a facility has lost points.
* All vulnerabilities (including lateral movement) are left until either mitigated or the vulnerability is exploited. Lateral movement goes away when it is either mitigated OR used to do a lateral movement of any successful exploit once. If a card underneath lateral movement is mitigated, then the next vulnerability card under the mitigated card will be laterally moved OR if there is no existing vulnerability then the next vulnerability card played will be laterally moved.

**Facility phase**: Draw a new station from the facility card pile every turn until the facility card pile is empty. If you lose a facility, it is all right to place a new facility where the old one was located but you must place new connections as old connections are destroyed when facilities are lost.

**Connection phase**: Decide how to connect the new facility to your grid and note that the optimal number of connections at the end of the game (to score further points) is minimally the original worth point value of the facility. For example, a 2-point facility would need at minimum 2 connections for the connections to be worth a point at the end of the game. Facilities taken off the board lose their connection lines, but new connections may be forged with older facilities during a connection phase. Once a facility is set down and connected, it cannot be moved or reconnected in the future as connections may not be changed, but only added.

**Repeat from step 1** until one player runs out of cards OR one player loses all their facilities. Then tally the final score.

A group of people playing a board game

AI-generated content may be incorrect.

**Learning the Game and Suggested Alternate Rules**

**Learning:** Play the game as specified above without any special rules to learn the game. It helps to talk out loud while playing to incorporate the meanings of the cards and discuss cybersecurity with the other player(s).

**Speed game**:

Place all facilities at the very beginning of the game and allow for their full point usage in pointing out vulnerabilities and mitigating them.

OR

Allow for a full 5 card discard/draw at the beginning of each turn rather than the default 2 card maximum discard/draw allowance.

**More advanced strategic play:**

* A player can’t use a facility’s points in pointing out vulnerabilities if the facility is attached to nothing in the rest of the network. That facility will still count in points at the end of the game though and can still be attacked.
* Explain the best and worst ways to attack each network at the end of the game in a discussion between players.
* Use the advanced play weaknesses on facility cards (in their text)

**More advanced educational play:**

* Explain WHY or HOW you would protect or lose a facility beyond what the cards say. If there is a reason a card that ordinarily doesn’t counter a facility might in a specific situation, argue your case. Note: it helps to have a neutral referee if you’re going to do this.
* Explain different reasons a facility would be put offline outside of what the cards say.
* Have a new attack/defense in mind? Replace some of the cards with your new attack/defense (the game comes with the ability to do a pdf with cards OR make new digital cards) and make sure to explain it when players come across it. Both players can have fun coming up with the attacks they think would work the best along with mitigations to counter those attacks.