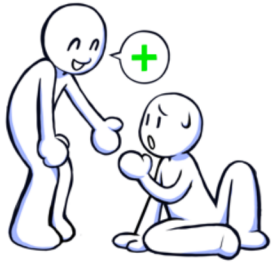
+1

Old Style Forensics Capability

+1 to station. A forensics tool for old style modems allows issues to be recognized on fifteen- to twenty-five year old hardware.

+1

Emergency Plan Upgraded



+1 to station. Facility's emergency plan has been upgraded to include the latest cyberinfrastructure attack potentials. When defense card played, cancels any vulnerabilities on this facility.

+1

Comprehensive Backup Plan

+1 to station. Also protects against ransomware.

2

Water Treatment Plant

For advanced play: this station is weak to phishing and vulnerable field device attacks. Add +3 to attack die rolls from those attacks.

2

Water Treatment Plant

For advanced play: this station is weak to alarm suppression attacks. Add +3 to attack die rolls from those attacks.

2

Water Treatment Plant

1

Lesser Water Station

1

Lesser Water Station

1

Lesser Water Station

For advanced play: this station is weak to brute force attacks. Add +3 to attack die rolls from those attacks.

-1

Vulnerable to Phishing

$1

Employees opened email and either clicked a link or opened an attachment sent from an attacker.

-1

Vulnerable to Phishing

$1

Employees opened email and either clicked a link or opened an attachment sent from an attacker.

-1

Field Devices Vulnerable

$1

Access gained via field devices. Many field devices such as transformers, circuit breakers, wind farms, etc. have a vulnerable technology like Bluetooth embedded that can't be turned off.

-2

Ransomware

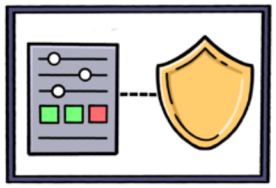
$4

Your business machines have been infected with ransomware and all the hackers care about is that you pay them.

-1

Control and Safety Implemented Together

$2



Control and safety features are implemented into the same hardware. Safety is now vulnerable.

-1

Alarm Suppression

$2

A local software misconfiguration or vulnerability is used to gain access and the alarm functionality of the system is suppressed.

Lateral Movement

$3

The last played vulnerability on this station moves to all stations directly connected to it if the vulnerability becomes an actual attack.

Output Fluctuates Through Brute Force I/O

-1 $3

Access gained and on/off commands were switched. Causes output to fluctuate unnaturally.

Offline

-2 $4

Station or substation offline and unusable for points the next turn.

Insignificant Target

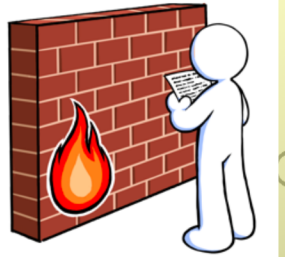
-1 $3

(Instant) -1! It was too insignificant to be a target and wasn't worth attacking, but attackers found it anyway.

Change Password

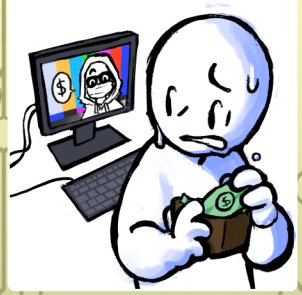
Make users choose a new and stronger password. Counters phishing and vulnerable field device vulnerabilities.

Firewall Log Review



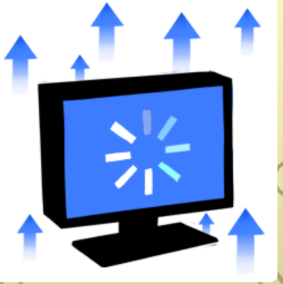
Firewall logs are reviewed and lateral movement discovered. Cancels Lateral movement card.

Pay Ransom



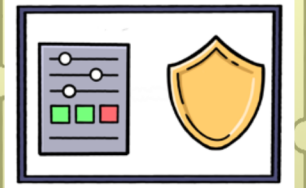
You pay the ransom. Roll d20 and if you get a 19 or 20 you get all your data back. If you get greater than a 10 you get some data back and take a -1 damage to your facility. Lose all points for the attack if you get a 10 or below.

Restart and Patch



System is restarted and patched. Roll a die to determine if the specialized ICS patch actually works for your facility. Failure is rolling a 1 or 2. Can fix Alarm Suppression, virus checking software installation, or Brute Force I/O. Failure means the attack happens.

Separate Functionality



Mitigates control and safety implemented together. Separate safety and control system hardware functionality to increase security.

Repair Technician

Send a repair technician to fix anything physical including brute force attacks, mechanical breakdowns, and offline facilities.

Run Analytics

Run analytics on user/system behavior to notice and then stop an outsider from accessing networks. Stops access from phishing and vulnerable field devices.

HALT

Cancels any card labeled as instant. Your organization was on the ball today.

Catch Rogue Employee

Catch previous employee sending false messages to radio network and causing them to dump sewage at a Hyatt Regency hotel . Fixes Brute Force I/O, sewage dump, or offline station and happened during 2000 Maroochy Water Services, Australian attack.

+1

Upgrade SCADA Access Authentication

+1 to station. Upgrade access authentication for SCADA (supervisory control and data acquisition) radio network so previous employees can no longer use it.

-2

Denial of Service Exploit Shutdown

$4

(Used on Power Only) Shutdown of power relay due to denial of service exploit for Siemens device vulnerability. Causes loss of station and operator life if power turned on before fixed. Fixable with Siemens Exploit patch or if it's the wrong IP.

-1

Power Fluctuation

$3

(Used on Power Only) Remote commands toggle circuit breakers in a rapid open-close-open pattern causing power fluctuations in a brute force I/O attack. Happened during 2016 Ukraine Power Grid Attack.

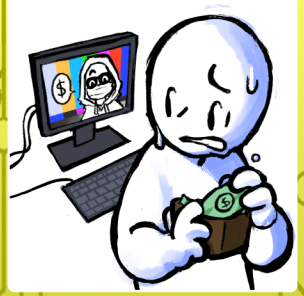
Rules

1. Discard a max of 2 cards, draw to have 5 cards.
2. Choose 1 defense card to play on a facility (if possible)
3. Sum Facilities worth and spend up to that amount to play vulnerabilities on your opponent. Choose to play any instant cards.
4. Play mitigation cards on any vulnerabilities you have. Discard both vulnerability and mitigation card to appropriate player's discard pile.
5. Roll for attacks on unmitigated vulnerabilities. >10 means attack is successful. Use counters to indicate harm to facility. Any total counts > facility+defense card worth total means facility has been lost and goes into the discard pile.
6. Draw a new station (if possible)
7. Add new connections between stations. Connections disappear when facilities are lost and may only be added (not changed).
8. Repeat from #1.
9. When you run out of cards OR a player loses all their facilities the game ends. Points are sum of facility worth + one point for every facility that has its number of connections >= the facility worth.

Emergency Action Plan

Discuss: How often does your company update their emergency action plan? Does it include cybersecurity threats? Could you potentially have both a natural disaster AND cybersecurity threat happen at the same time?

Ransomware



Discuss: Did you know that 92% of people who pay the ransom DO NOT get all their data back? Sometimes it's even sold. And 80% of the companies that pay will be attacked again for ransom in the future after having paid the first time. Do you have a comprehensive backup plan to protect yourself in the case of a ransomware attack?

+1

Comprehensive Backup Plan

+1 to station. Also protects against ransomware.

2

Power Station

For advanced play: this station is weak to phishing and vulnerable field device attacks. Add +3 to attack die rolls from those attacks.

2

Power Station

For advanced play: this station is weak to control and safety implemented together. Add +3 to attack die rolls from attacks that take advantage of them implemented together.

2

Power Station

1

Power Substation

1

Power Substation

1

Power Substation

For advanced play: this station is weak to alarm suppression attacks. Add +3 to attack die rolls from those attacks.

Loss of Defense

$3

(Instant) -1! Opponent lost some employees. Remove 1 defense card from an opponent.

-1

Vulnerable to Phishing

$1

Employees opened email and either clicked a link or opened an attachment sent from an attacker.

-1

Field Devices Vulnerable

$1

Access gained via field devices. Field devices such as transformers and wind farms have a vulnerable technology like Bluetooth embedded that can't be turned off.

-2

Ransomware

$4

Your business machines have been infected with ransomware and all the hackers care about is that you pay them.

-1

Virus Checking Software Installed

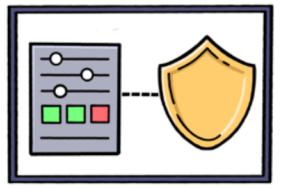
$2

Somebody installed virus checking software that causes a denial of service attack of up to 6 minutes on the industrial control system because it interrupts real-time operations. The Denial of Service self attack was unintended.

-1

Control and Safety Implemented Together

$2



Control and safety features are implemented into the same hardware. Safety is now vulnerable.

-1

Alarm Suppression

$2

A local software misconfiguration or vulnerability is used to gain access and the alarm functionality of the system is suppressed.

Lateral Movement

$3

The last played vulnerability on this station moves to all stations directly connected to it if the vulnerability becomes an actual attack.

Offline

-2

$4

If a station survives this attack it will be offline and unusable for points the next turn.

Output Fluctuates Through Brute Force I/O

-1

$3

Access gained and on/off commands were switched. Causes output to fluctuate unnaturally.

Authentication Provides Confidentiality

-1

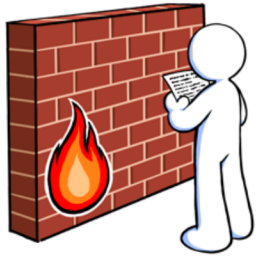
$3

(Instant) -1! Access and privacy are two separate things. You were logged in but your data was still stolen over that unencrypted wi-fi.

Change Password

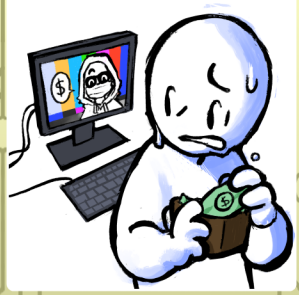
Make users choose a new and stronger password. Counters phishing and vulnerable field device vulnerabilities.

Firewall Log Review



Firewall logs are reviewed and lateral movement discovered. Cancels Lateral movement card.

Pay Ransom

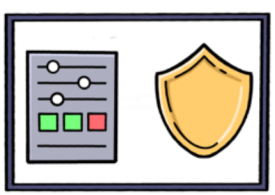


You pay the ransom. Roll dice and if you get a 19 or 20 you get all your data back. If you get greater than a 10 you get some data back and take a -1 damage to your facility. Lose all points for the attack if you get a 10 or below.

Restart and Patch

System is restarted and patched. Roll a die to determine if the specialized ICS patch actually works for your facility. Failure is rolling a 1 or 2. Can fix Alarm Suppression, virus checking software installation, or Brute Force I/O. Failure means the attack happens.

Separate Functionality



Mitigates control and safety implemented together. Separate safety and control system hardware functionality to increase security.

Repair Technician

Send a repair technician to fix anything physical including brute force attacks, mechanical breakdowns, and offline facilities.

Run Analytics

Run analytics on user/system behavior to notice and then stop an outsider from accessing networks. Stops access from phishing and vulnerable field devices.

HALT

Cancels any instant action. Somebody was on the ball today.

Wrong IP

Attacker uses the wrong IP for a relay switch open command and nothing happens. Fixes Brute Force I/O and happened during 2016 Ukraine Power Grid Attack.

Patch Siemens Relay Exploit

+1

+1 to station. Patch Siemens mechanical relay exploit (stops any relay issues on that station).

Physically Reset Devices

Physically reset devices in a facility. Used for Brute Force I/O and Stations that are not working. Can only be used on stations with the Siemens mechancial relay exploit patched or else station explodes (-5 pt) and life is lost.

Sewage Dumped

-1

$3

(Water Only Vuln) Brute Force I/O attack sends false messages via radio network to disable alarm reporting and corrupt a water pump system to run incorrectly. Can't be played on a station with upgraded SCADA access authentication.

-2

Mechanical Breakdown

$4

(Water Only Vuln) Pump sewerage station stopped through mechanical error when equipment fails after being used incorrectly due to cyber attacks. Fixed through repair.