+1

Hire Cybersecurity Expert

+1 to station played on and can protect any station within a single connection. Goes away upon successful attack and nullifies a single attack OR can be used to nullify a lateral movement card on any station within its sphere of influence.

+1

Old Style Forensics Capability

+1 to station. A forensics tool for old style modems bought. Issues can now be ascertained on fifteen- to twenty-five year old hardware.

+1

Train employees

+1 to station. Train employees in ICS cybersecurity. IT and Industrial Control Systems (ICS) have different security needs.

+1

Emergency Plan Upgraded

+1 to station. Facility's emergency plan has been upgraded to include the latest cyberinfrastructure attack potentials.

+1

Comprehensive Backup Plan

+1 to station. Also protects against ransomware.

+1

Comprehensive Backup Plan

+1 to station. Also protects against ransomware.

3

Power Station

2

Power Substation

2

Power Substation

2

Power Substation

1

Lesser Power Substation

1

Lesser Power Substation

1

Lesser Power Substation

1

Lesser Power Substation

-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.

Vulnerable to Phishing

-1 $1

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

Field Devices Vulnerable

-1 $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.

Field Devices Vulnerable

-1 $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.

Ransomware

-2 $3

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

Ransomware

-2 $3

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

Virus Checking Software Installed

-1 $3

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.

Control and Safety Implemented Together

-1 $2

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

Alarm Suppression

-1 $2

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

Alarm Suppression

-1 $2

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

Service Modification Malware

-1 $2

Attackers use a service modification to load malware and gain access.

Functionality Not Separate

-1 $2

Your business and industrial control system networks aren't completely separate or your control safety systems are on the same hardware. Anything not separated can be attacked together.

Functionality Not Separate

-1 $2

Your business and industrial control system networks aren't completely separate or your control safety systems are on the same hardware. Anything not separated can be attacked together.

Lateral Movement

$3

Any vulnerabilities with this station move to all stations directly connected to it if the vulnerability becomes an actual attack.

Lateral Movement

$3

Any vulnerabilities with this station move to all stations directly connected to it if the vulnerability becomes an actual attack.

Lateral Movement

$3

Any vulnerabilities with this station move to all stations directly connected to it if the vulnerability becomes an actual attack.

Lateral Movement

$3

Any vulnerabilities with this station move to all stations directly connected to it if the vulnerability becomes an actual attack.

Offline

-2 $4

Station or substation offline. Something is wrong.

Offline

-2 $4

Station or substation offline. Something is wrong.

Offline

-2 $4

Station or substation offline. Something is wrong.

Offline

-2 $4

Station or substation offline. Something is wrong.

Output Fluctuates Through Brute Force I/O

-1 $3

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

Output Fluctuates Through Brute Force I/O

-1 $3

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

Compliance is Enough

-1 $3

(Instant) -1! Compliance does not equal complete security but your people believe it does. You drove a car with a valid driver's license at the proper speed limit. You still had an accident.

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.

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.

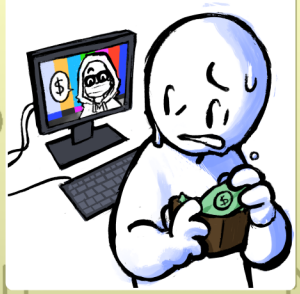
Firewall Log Review

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

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. Note that 80% of companies that pay the ransom are attacked a second time in the future.

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, Brute Force I/O, or Service Modification Malware. Failure means the attack happens.

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, Brute Force I/O, or Service Modification Malware. Failure means the attack happens.

Separate Functionality

Separate functionality to increase security. This can be business IT and Industrial Control System (ICS) functionality or even safety and control system hardware.

Separate Functionality

Separate functionality to increase security. This can be business IT and Industrial Control System (ICS) functionality or even safety and control system hardware.

Separate Functionality

Separate functionality to increase security. This can be business IT and Industrial Control System (ICS) functionality or even safety and control system hardware.

Repair Technician

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

Repair Technician

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

Repair Technician

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

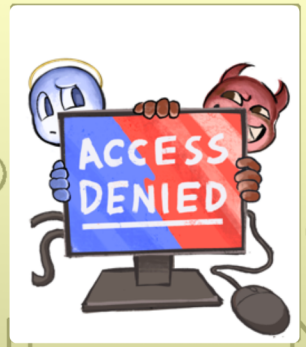
Run Analytics

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.

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.

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).

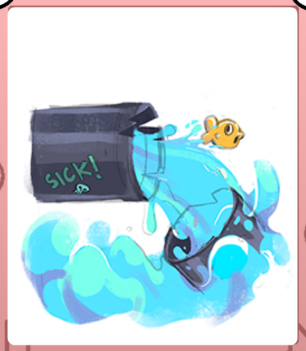
Physically Reset Devices

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



(Used on Water Only) Brute Force I/O attack sent false messages via radio network using a stolen machine 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.

Mechanical Breakdown

-2

$4

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

Hire Cybersecurity Expert

1

+1 to station played on and can protect any station within a single connection. Goes away after use and nullifies a single attack OR can be used to nullify a lateral movement card on any station within its sphere of influence.

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.

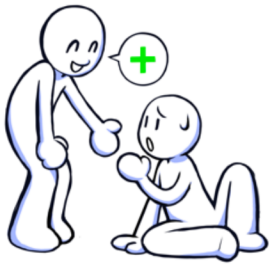
2

Train employees

+2 to station. Train employees in ICS cybersecurity. IT and Industrial Control Systems (ICS) have different security needs.

1

Emergency Plan Upgraded



+1 to station. Facility's emergency plan has been upgraded to include the latest cyberinfrastructure attack potentials.

1

Comprehensive Backup Plan

+1 to station. Also protects against ransomware.

1

Comprehensive Backup Plan

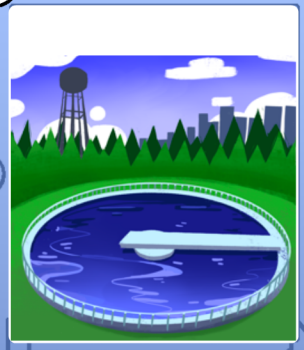
+1 to station. Also protects against ransomware.

2

Water Treatment Plant

2

Water Treatment Plant



2

Water Treatment Plant

2

Water Treatment Plant

1

Lesser Water Station

1

Lesser Water Station

1

Lesser Water Station

1

Lesser Water Station

-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

Vulnerable to Phishing

$1

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

Field Devices Vulnerable

-1 $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.

Field Devices Vulnerable

-1 $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.

Ransomware

-2 $3

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

Ransomware

-2 $3

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

Virus Checking Software Installed

-1 $3

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. This was unintended.

Control and Safety Implemented Together

-1 $2

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

Alarm Suppression

-1 $2

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

Alarm Suppression

-1 $2

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

Service Modification Malware

-1 $2

Attackers use a service modification to load malware and gain access.

Functionality Not Separate

-1 $2

Your business and industrial control system networks aren't completely separate or your control safety systems are on the same hardware. Anything not separated can be attacked together.

Functionality Not Separate

-1 $2

Your business and industrial control system networks aren't completely separate or your control safety systems are on the same hardware. Anything not separated can be attacked together.

Lateral Movement

$3

Any vulnerabilities with this station move to all stations directly connected to it if the vulnerability becomes an actual attack.

Lateral Movement

$3

Any vulnerabilities with this station move to all stations directly connected to it if the vulnerability becomes an actual attack.

Lateral Movement

$3

Any vulnerabilities with this station move to all stations directly connected to it if the vulnerability becomes an actual attack.

Offline

-2 $4

Station or substation offline. Something is wrong.

Offline

-2 $4

Station or substation offline. Something is wrong.

Offline

-2

$4

Station or substation offline. Something is wrong.

Offline

-2

$4

Station or substation offline. Something is wrong.

Output Fluctuates Through Brute Force I/O

-1

$3

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

Output Fluctuates Through Brute Force I/O

-1

$3

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

IT and ICS Security are the Same

-1

$3

(Instant) -1! They're different! IT business security prioritizes confidentiality and ICS security prioritizes safety, integrity, and availability. ICS devices are also commonly real time systems that may be up to 25-years old.

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

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

Change Password

Maker 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.

Firewall Log Review

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

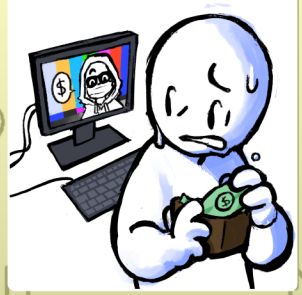
Firewall Log Review

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

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. Note that 80% of companies that pay the ransom are attacked a second time in the future.

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, Brute Force I/O, or Service Modification Malware. Failure means the attack happens.

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, Brute Force I/O, or Service Modification Malware. Failure means the attack happens.

Separate Functionality

Separate functionality to increase security. This can be business IT and Industrial Control System (ICS) functionality or even safety and control system hardware.

Separate Functionality

Separate functionality to increase security. This can be business IT and Industrial Control System (ICS) functionality or even safety and control system hardware.

Separate Functionality

Separate functionality to increase security. This can be business IT and Industrial Control System (ICS) functionality or even safety and control system hardware.

Repair Technician

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

Repair Technician

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

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.

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.

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.

Upgrade SCADA Access Authentication

1

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

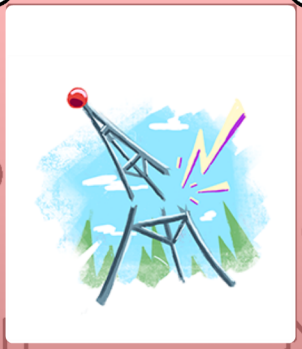
Upgrade Control System

Upgrade control system and information integrity to not accept outside/false messages that could be sent by attackers. Stops Brute Force I/O Attacks and Alarm Suppression.

Denial of Service Exploit Shutdown

-2

$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.

Power Fluctuation

-1

$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.

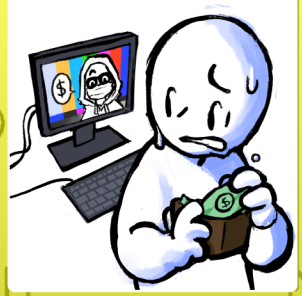
Emergency Action Plan

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?

Emergency Action Plan

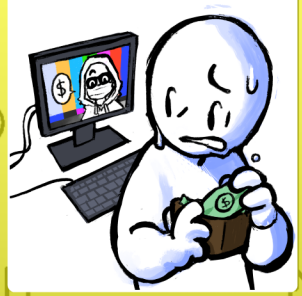
Discuss: How often does your company update their emergency action plan? Does it include cybersecurity threats? Could you potentially have both a natural disaster AND cybersecurity threat happen at the same time?

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?

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?