Workshop routine

Before the game

1. **Build the game board** before everyone arrives (see image).
2. **Separate the cards** available to the team at the start (Firewall x 2, CCTV x 2, Security Training, Network Monitoring X 2, Antivirus, Asset Audit, Threat Assessment) from the cards available after the Asset Audit purchased (PC Encryption, DB Encryption, PC Upgrade, Server Upgrade, Controller Upgrade) and keep out of sight.
   N.B., there are corresponding lego pieces that represent each asset and each purchase card.

Starting the game

1. Welcome your new team members and ask them to complete the required **ethics paperwork** + **questionnaire**.
2. Ask if team are happy to have dialogue recorded – assure them that all participants and company will be anonymised in any research that occurs. **Start recording on the phone.**
3. Introduce yourself and ask each participant to introduce themselves.
4. **Explain overview of game:**
   - Participants have been asked to work together by an industrial company to help develop their cyber security strategy. Explain that you (the game master) are representing the board of directors.
   - The game boards represent a simple company with a power generation site and office site located in separate locations but connected via a standard internet connection.
5. **Explain assets on board (see cheat sheet as needed)**
6. **Explain round process:**
   - There are 4 rounds
   - The board provide £100k to invest in each round
   - Spare cash rolls over into future rounds
   - Each round represents 2 months
   - At the end of each round they will receive a summary of any attacks that may have occurred and impact on share price.
7. **Introduce the initial purchasing options available (see cheat sheet as needed)**
   - Emphasise that if Asset Audit or Threat Assessment purchased then information is provided right then and can help inform that round.
   - You can hint that using the asset audit will not only identify issues with the current system but may identify new potential solutions.

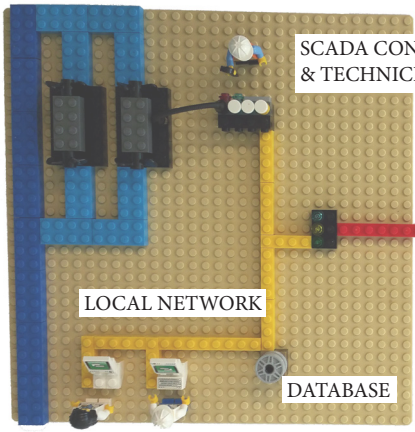
During the game

1. Remind team which round they are in and the amount of budget available
2. **Read out summary relating to investment choices (see cheat sheet)**
3. **Remember Asset Audit and Threat Analysis can be used mid-round**
4. **Summarise round:**
   - "So, that was round X and you purchased……."
   - **Add investments to website, scroll down and read out/summarise any incidents that occurred.** N.B. You don't need to read out the attack type
   - **Rinse and repeat as necessary**

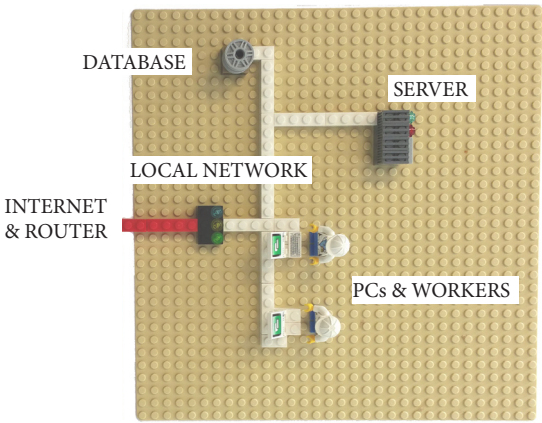
Ending the game

1. **Add optional nation state attack at end of game as you see fit**
2. **Review/Discuss the decisions made (see cheat sheet of 'better/perfect game scenarios')**

The plant



The office

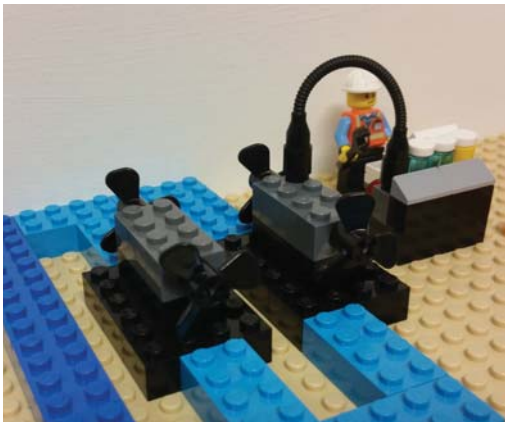


The assets on the board

Asset details

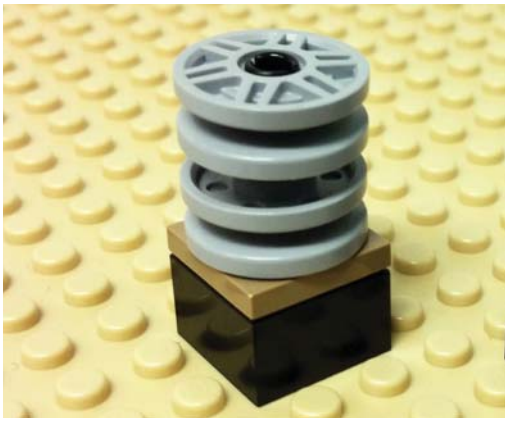
Turbines

The core physical process on which the entire business of the company relies. These turbines have been running for decades now, constantly producing electricity from the water stream. The turbines are under the constant observation and control of the SCADA **controller**.



Controller

This SCADA controller monitors the turbines (e.g., water debit, generated power, temperature) and controls their electricity production at all times. Monitoring data is constantly being stored in the local **historian database**.



Network (plant)

This local network links together the **controller**, **historian database** and **PCs** used by technicians and engineers in the plant. The network is interfaced with the Internet via the plant's **router** that allows any traffic in both directions, from the Internet to the plant network and vice versa.

PCs (plant)

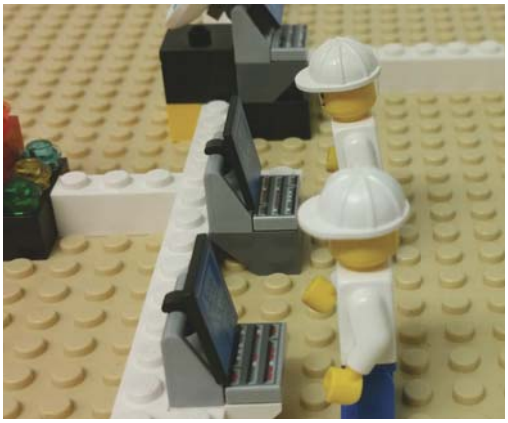
These PCs are used by plant employees to supervise and maintain the local infrastructure **controller**, **historian database** and for communication both internally (with the office) and externally (e.g., for organising maintenance with equipment vendors), mainly via email.

Historian database (plant)

This database receives a constant stream of monitoring data from the **controller**. At regular intervals (e.g., every few hours) the database is polled for aggregated analytics data by engineers in the **office**, for the purpose of long-term monitoring, productivity analysis, maintenance planning, etc.

Network (office)

This local network links together the company's **server** and **database** with **PCs** used by office employees. The network is interfaced with the Internet via the office's **router** that allows any traffic in both directions, from the Internet to the office network and vice versa.

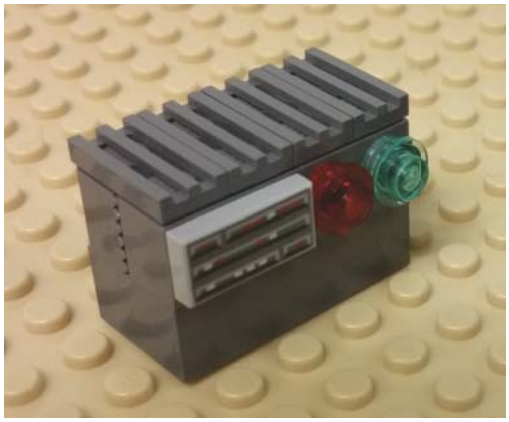


PCs (office)

These PCs are used by office employees for various purposes: technical administration of the company's infrastructure, contract management with clients, strategic analysis of long-term monitoring data generated on the plant site, management of human resources, internal and external communications (mainly via email), etc.

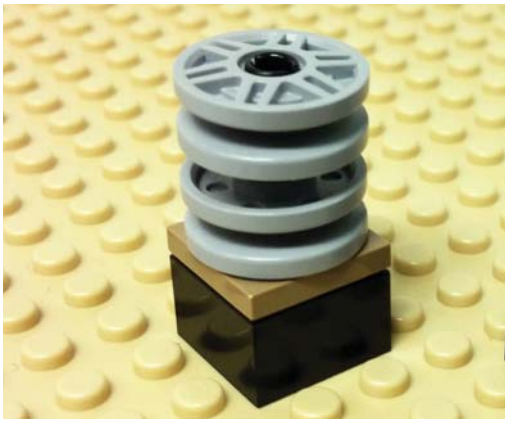
Server

The company's server runs important services: the email service all employees rely on to communicate internally and externally, the Human Resources management software, as well as the company's website used for advertisement and contracting purposes.

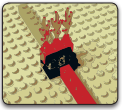


Database (office)

This database stores various types of sensitive data: client information and contracts, the company's email and website content, technical documentation on the entire infrastructure, personal details of all employees (e.g., payroll), strategic business plans for the company, etc.



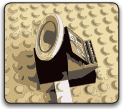
FIREWALL
(plant)



Firewall (plant) : 30k

A software and hardware solution that monitors and filters unauthorised traffic coming from the Internet to the plant network

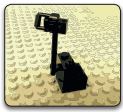
NETWORK MONITORING



Network Monitoring (plant) : 50k

This big, shiny piece of bleeding-edge technology is quite expensive but also very effective

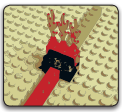
CCTV
(plant)



CCTV Surveillance : 50k

Surveillance camera and alarms that will automatically warn security guards of an intrusion

FIREWALL
(office)



Firewall (office) : 30k

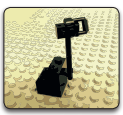
A software and hardware solution that monitors and filters unauthorised traffic coming from the Internet to the office network

NETWORK MONITORING

Network Monitoring (office) : 50k

This big, shiny piece of bleeding-edge technology is quite expensive but also very effective

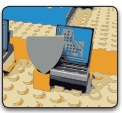
CCTV
(office)



CCTV Surveillance : 50k

Surveillance camera and alarms that will automatically warn security guards of an intrusion

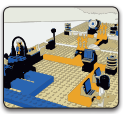
ANTIVIRUS
(plant & office)



Antivirus : 30k

A recent, decent professional anti-virus from a reputable provider

ASSET AUDIT



Asset Audit : 30k

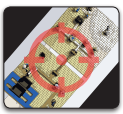
The entire infrastructure is thoroughly assessed for vulnerabilities

SECURITY TRAINING

Security Training : 30k

A quick yet thorough one-day formation on security essentials for all employees

THREAT ASSESSMENT



Threat Assessment : 20k

Reveals existing threats to the company, the attack vectors they use, and the possible effects of their attacks

Investments Cheatsheet

Firewall (offices or plant) – 30k

"An engineer from a famous networking company comes to the office with a big box. They spend a day with the network administrator installing the firewall, configuring access rules and making sure that everything runs smoothly."

CCTV (offices or plant) – 30k

"Cameras are installed at strategic points all around the plant: entrance, control room, turbine room, etc. Everything is linked to a central monitoring console where security guards monitor the offices 24/7."

Antivirus – 30k

"Two engineers come to both sites and spend a day installing the antivirus on all PCs, configuring it and making sure all employees understand its purpose and react properly in case of an alert."

Security Training – 30k

"A team of professional trainers organise a one-day seminar for all employees and teach them essential security hygiene: Do not click on random links while browsing the Web. Do not open email attachments from unknown sources. Do not bring personal thumb drives to work, especially when you do not know where they come from! Here is how to design a secure, easy to remember password. And do not put it on a sticky note on your monitor! Etc."

Network Monitoring (Offices or Plant) – 50k

"The office/plant network administrator is extremely excited: they have got a brand new shiny toy to play with! The vendor sends one of their engineers to help with the installation, and the network administrator spends a few more days fine-tuning precise filtering rules and alert conditions. Soon, nothing that happens on the office network can escape their vigilance."

Threat Assessment – 20k

"*A consultant does a threat analysis on the company and identifies three different threat actors...*

- ***Script kiddies** have low computer skills: they only use tools built by others and their attack repertoire is limited to simple, known techniques, such as scanning an infrastructure for known vulnerabilities, spreading malware found on the Internet via poorly-written email, or running small Denial of Service attacks with experimental tools. They are motivated by the "fun" aspect of hacking more than anything else. Due to the number of such low-skilled attackers and the wide availability of their techniques, their attacks are expected to be targeting the company's infrastructure at all times. They are probably already at work as we speak!*

- ***Organised crime** attackers have high skills and clear motivations: they will use advanced attack techniques, such as sophisticated phishing email, Remote Access Tools (RATs) and bespoke malware, in order to steal sensitive data or disrupt a target in subtle ways. Unlike script kiddies who hit indiscriminately all systems that they can reach, such advanced attackers choose specific, valuable targets, which makes their attacks less likely. However, the probability of facing them cannot be underestimated: it would be surprising if at least one of them did not take interest in the company at some point in time.*

- ***Nation state** attackers work on behalf of hostile remote interests. They use bleeding-edge tools and techniques that even organised criminals do not have access to, in order to conduct espionage and cyber*

warfare. Should one of them target the company, which is extremely unlikely, there is very little that one could do to resist them."

Asset Audit – 30k

"A team of external experts comes and spends an entire day on each site, scanning your networks and asking questions to your system administrators. They come back with a number of findings:

- *An unsecured, undocumented Wi-Fi network was found in the plant. After some investigation, this was set up years ago by an engineer, who is now retired. They needed to install a set of additional debit sensors on the water stream, and an open Wi- Fi network was a cheap and simple solution compared to deploying a complicated set of cables. The Wi-Fi network was never documented and eventually forgotten. It has now been secured with a strong password.*

- *The company PCs run an old, insecure operating system long past its end of life. They can be upgraded to a recent, secure, supported operating system via the **PC Upgrade**. The server's and database's operating systems and software are also outdated and suffer from known vulnerabilities. These can be patched via a **Server Upgrade**.*

- *The controller's firmware has never been updated since its deployment, twenty years ago. It is vulnerable to very simple exploits. A **Controller Upgrade** will patch known vulnerabilities.*

- *The company has never encrypted any data – everything is stored in the clear. **PC Encryption** will encrypt the content of all Personal Computers (e.g., technical documentation used by engineers). **Database Encryption** will encrypt the content of the two databases (controller monitoring data on the plant's historian database, email, HR records, client contracts and other sensitive data on the office database).*

THE FOLLOWING ARE UNLOCKED BY THE ASSET AUDIT

PC Upgrade – 30k

"The week after the update is difficult: users complain that they are lost, they do not recognise the icons, they prefer the old system, and so on. After a few days, however, everyone gets used to the new environment, and soon enough the old PCs are no more than a fond memory."

Server upgrade – 30k

"The webmaster and system administrators take down the server and databases for a day, in order to deploy the new software, port the existing data and applications, and restart everything. Soon enough, everything is back up and running."

Controller upgrade – 30k

"Updating the controller takes three full days: one day to stop the whole process, one day to install the new firmware, and one day to restart everything and do all mandatory safety check. The cost of this defence also covers the business losses due to the three days downtime."

PC Encryption – 20k

"The system administrators take a few days to review all PCs in use in the company and equip them with an up-to-date encryption suite. All data stored on Personal Computers is now encrypted with a strong cypher which makes it unreadable to whoever does not have the corresponding decryption key. (Replace PC's light gray base with a dark gray base)"

Database Encryption – 20k

"The database administrators take the office database and the plant's historian down for a few hours. When they are restarted, all their content is now encrypted with a strong cypher which makes it unreadable to whoever does not have the corresponding decryption key. (Replace database light gray wheels / disks with a dark gray ones)"

Investments (in more detail)

CCTV Surveillance (Offices)– 50k
A set of surveillance cameras and alarms that will automatically warn security guards of an intrusion in the offices.

Deployment : *Cameras are installed at strategic points all around the offices: entrance, corridors, server room, etc. Everything is linked to a central monitoring console where security guards monitor the offices 24/7.*

Counters On-site Infiltration (Offices): *An intruder is detected entering the offices and trying to open some doors. The moment the security guard comes and asks them what they are doing, they run away.*

41

CCTV Surveillance (Plant) – 50k
A set of surveillance cameras and alarms that will automatically warn security guards of an intrusion in the field site.

Deployment : *Cameras are installed at strategic points all around the plant: entrance, control room, turbine room, etc. Everything is linked to a central monitoring console where security guards monitor the offices 24/7.*

Counters On-site Infiltration (Plant): *An intruder is detected entering the plant perimeter and trying to access the buildings. The moment the security guard comes and asks them what they are doing, they run away.*

42

Firewall (Office) – 30k
A software and hardware solution that monitors and filters unauthorised traffic coming from the Internet to the office network.

Deployment : *An engineer from a famous networking company comes to the office with a big box. They spend a day with the network administrator, installing the firewall, configuring access rules and making sure that everything is running smoothly.*

Counters Network Scan (Offices): *The firewall intercepts a number of scanning attempts from all over the world. Apparently, there are people out there very interested in knowing more about your server.*

Counters DoS (Offices): *A sudden surge of traffic is detected: a number of machines from all around the world are trying to flood your web server with requests. Fortunately, your network administrator can quickly update the filtering rules of the offices firewall, and the attack does not cause much disruption.*

43

Firewall (Plant) – 30k
A software and hardware solution that monitors and filters unauthorised traffic coming from the Internet to the plant network.

Deployment : *An engineer from a famous networking company comes to the plant with a big box. They spend a day with the network administrator, installing the firewall, configuring access rules and making sure that everything is running smoothly.*

Counters Network Scan (Plant) : *The firewall intercepts a number of scanning attempts from all over the world. Apparently, there are people out there very interested in knowing more about your infrastructure.*

Counters Remote Control Controller: *Upon looking at detailed firewall logs, your plant network administrator discovers that an overseas machine tried to query the remote administration port of your SCADA controller. Fortunately, the firewall's rules denied access to the attacker.*

44

PC Upgrade – 30k

A brand new, up-to-date OS and software suite for all personal computers (offices and plant), including continuous support and security patches.

Deployment : *The week after the update is difficult: users complain that they are lost, they do not recognise the icons, they prefer the old system, and so on. After a few days, however, everyone gets used to the new environment, and soon enough the old PCs are no more than a fond memory.*

Counters : This defence has no direct visible effect for the players: it silently prevents malware sent via phishing emails from infecting the PCs (*Phishing offices (trojan) attack*) and freezing them (*Disruption PCs offices* attack).

In case the players have invested in an Antivirus or a Security Training, then they become aware of the existence of the malware and whether or not it infected or disrupted its target.

Server Upgrade – 30k

A brand new, up-to-date OS, web server and database management system, including continuous support and security patches.

Deployment : *The webmaster and system administrators take down the server and databases for a day, in order to deploy the new software, port the existing data and applications, and restart everything. Soon enough, everything is back up and running.*

Counters Remote control server: *The logs of the server show that someone on the Internet tried to use an SQL injection to compromise the server. This would have affected the old version of the software, by fortunately, the vulnerability has been patched.*

This defence also has a potential silent effect: it prevents the **Remote control database plant** attack from an APT attacker on the plant network on turn 2. In case the players have deployed a Network Monitor for the plant during that turn, the logs will show unsuccessful attempts at accessing an old, vulnerable remote control utility on the database, now patched.

Controller Upgrade – 30k

An update to the firmware of the SCADA controller.

Deployment : *Updating the controller takes three full days: one day to stop the whole process, one day to install the new firmware, and one day to restart everything and do all mandatory safety check. The cost of this defence also covers the business losses due to the three days downtime.*

Counters : This defence silently counters the **Remote control Controller** and **Disruption Controller** attacks. In case the players have deployed a **Network Monitor** in the field site network, the Network Monitor shows in its logs failed attempts at accessing an old, insecure remote access facility that has been disabled in the new version of the firmware.

Antivirus – 30k

A recent, decent professional antivirus from a reputable provider, good enough to stop common malware. Support and continuous updates are included in the price.

Deployment : *Two engineers come to both sites and spend a day installing the antivirus on all PCs, configuring it and making sure all employees understand its purpose and react properly in case of an alert.*

Counters Phishing offices (trojan), Disruption PC offices, Infected thumb drive office and Remote control PC (use the appropriate event among the following options):

Upon opening an attachment from an unknown sender...

Upon plugging in a thumb drive found in the parking lot...

One day, seemingly out of nowhere...

... the antivirus fires an alert and announces that a malicious program has been stopped from running on the computer. Upon closer inspection, it was indeed a common piece of malware the antivirus stopped just in time: disaster averted!

Security Training – 30k
A quick yet thorough one-day formation on security essentials for all employees.

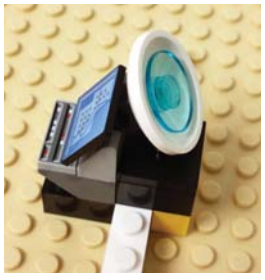
Deployment : *A team of professional trainers organise a one-day seminar for all employees and teach them essential security hygiene: Do not click on random links while browsing the Web. Do not open email attachments from unknown sources. Do not bring personal thumb drives to work, especially when you do not know where they come from! Here is how to design a secure, easy to remember password. And do not put it on a sticky note on your monitor! Etc.*

Counters Phishing offices (trojan) and Infected thumb drive offices (use the appropriate events in the following text): *Upon receiving an email with an attachment from an unknown source / finding a thumb drive in the parking lot, an employee reports it directly to you (the players). Upon close inspection, the attachment / thumb drive did indeed contain malware. Good thing the employee knew better than opening it themselves!*

Counters Phishing office credentials : *Your system administrator comes one day with an interesting screen capture: someone has sent them a very realistic email, forged using the company's logo, and containing a link to a fake login page. The attacker could have stolen server access credentials, fortunately, the administrator knew better than opening it!*

Network Monitoring (Offices) – 50k
A sophisticated piece of hardware and software that will record everything that is going on in the office network: web browsing, email, remote access, etc. An advanced detection system will signal any suspicious activity: malware signatures on the network, unexpected remote access, data being exfiltrated, etc. This big, shiny piece of bleeding-edge technology is quite expensive but also very effective: it will indeed detect any kind of attack going on in the office network and allow immediate measure to be taken, such as isolating infected machines, blocking unauthorised traffic, and showing exactly what is going on.

Deployment : *The office network administrator is extremely excited: they have got a brand new shiny toy to play with! The vendor sends one of their engineers to help with the installation, and the network administrator spends a few more days fine-tuning precise filtering rules and alert conditions. Soon, nothing that happens on the office network can escape their vigilance.*



Counters Remote Control attacks on the server and office PCs (use the appropriate variation among the following): *One day, the office's network administrator comes to talk to you: they have detected suspicious activity on the office network. The server / a PC seems to be communicating at regular intervals with an unknown machine on the Internet, located in a foreign country. Upon closer investigation, the server / PC was compromised and remotely operated: the administrator makes sure that the link to the attacker's machine is shut down and any malware on the infected target is removed.*

Counters Data Exfiltration attacks on the server, office database and office PCs (use the appropriate variation in the following): *One day, the office's network administrator comes to talk to you: they have detected a suspicious data stream originating from the server / the database / a PC and going to an unknown address on the Internet, located in a foreign country. Upon closer investigation, it was a data exfiltration attack: the administrator makes sure that the link to the attacker's machine is shut down and any malware on the infected target is removed.*

Network Monitoring (Plant) – 50k
A sophisticated piece of hardware and software that will record everything that is going on in the plant network: web browsing, email, remote access, etc. An advanced detection system will signal any suspicious activity: malware signatures on the network, unexpected remote access, data being exfiltrated, etc. This big, shiny piece of bleeding-edge technology is quite expensive but also very effective: it will indeed detect any kind of attack going on in the plant network and allow immediate measure to be taken, such as isolating infected machines, blocking unauthorised traffic, and showing exactly what is going on.

Deployment : *The plant network administrator is extremely excited: they have got a brand new shiny toy to play with! The vendor sends one of their engineers to help with the installation, and the network administrator spends a few more days fine-tuning precise filtering rules and alert conditions. Soon, nothing that happens on the plant network can escape their vigilance.*

Counters Remote Control attacks on the plant's historian database: *One day, the office's network administrator comes to talk to you: they have detected suspicious activity on the plant network. The historian database seems to be communicating at regular intervals with an unknown machine on the Internet, located in a foreign country. Upon closer investigation, the historian was compromised and remotely operated: the administrator makes sure that the link to the attacker's machine is shut down and any malware on the historian is removed.*

Counters Data Exfiltration attacks on the historian database: *One day, the office's network administrator comes to talk to you: they have detected a suspicious data stream originating from the historian database and going to an unknown address on the Internet, located in a foreign country. Upon closer investigation, it was a data exfiltration attack: the administrator makes sure that the link to the attacker's machine is shut down and any malware on the infected historian is removed.*

PC Encryption – 20k
Military-grade, proven encryption mechanism for the hard drives of all PCs (plant and office), protecting technical documentation, client information, and other sensitive data from being stolen.

Deployment : *The system administrators take a few days to review all PCs in use in the company and equip them with an up-to-date encryption suite. All data stored on Personal Computers is now encrypted with a strong cypher which makes it unreadable to whoever does not have the corresponding decryption key.* (Replace PC's light gray base with a dark gray base)

Counters : Silently counters **Data Exfiltration** attacks on PCs – the data stolen by the attackers is unreadable and cannot be exploited. Players do not learn about this, unless they detect the data exfiltration attack via a network monitor: in that case, the players should know that it is unlikely that the attacker will be able to exploit the data they stole.

Database Encryption – 20k
Military-grade, proven encryption mechanism for the hard drives of the two databases (plant and office), protecting the technical data, email, client information, HR records, and other sensitive data from being stolen.

Deployment : *The database administrators take the office database and the plant's historian down for a few hours. When they are restarted, all their content is now encrypted with a strong cypher which makes it unreadable to whoever does not have the corresponding decryption key.* (Replace database light gray wheels / disks with a dark gray ones)

Counters : Silently counters **Data Exfiltration** attacks on the server and databases – the data stolen by the attackers is unreadable and cannot be exploited. Players do not learn about this, unless they detect the data exfiltration attack via a network monitor: in that case, the players should know that it is unlikely that the attacker will be able to exploit the data they stole.

Asset Audit – 30k

The entire infrastructure is thoroughly assessed for vulnerabilities, in order to identify systems with known security holes and propose potential solutions (i.e. new defence cards are unlocked). Note: if players choose to invest in an Asset Audit, the result of the audit is given to them straight away, before the end of the turn, and new defences are unlocked. The players can then decide how to spend the rest of their budget given the new options.

Deployment : *A team of external experts comes and spends an entire day on each site, scanning your networks and asking questions to your system administrators. They come back with a number of findings:*

- An unsecured, undocumented Wi-Fi network was found in the plant. After some investigation, this was set up years ago by an engineer, who is now retired. They needed to install a set of additional debit sensors on the water stream, and an open Wi-Fi network was a cheap and simple solution compared to deploying a complicated set of cables. The Wi-Fi network was never documented and eventually forgotten. It has now been secured with a strong password.

- ll company PCs run an old, insecure operating system long past its end of life. They can be upgraded to a recent, secure, supported operating system via the **PC Upgrade**.
- The server's and database's operating systems and software are also outdated and suffer from known vulnerabilities. These can be patched via a **Server Upgrade**.
- The controller's firmware has never been updated since its deployment, twenty years ago. It is vulnerable to very simple exploits. A **Controller Upgrade** will patch known vulnerabilities.
- The company has never encrypted any data – everything is stored in the clear. **PC Encryption** will encrypt the content of all Personal Computers (e.g., technical documentation used by engineers). **Database Encryption** will encrypt the content of the two databases (controller monitoring data on the plant's historian database, email, HR records, client contracts and other sensitive data on the office database).

Counters : If the Asset Audit is bought during turn one, the discovery of the insecure Wi-Fi network silently counters the **Unsecured Wi-Fi Infiltration** attack: unbeknownst to the players, an attacker is prevented from infiltrating the plant network at the end of turn 1.

Threat Assessment – 20k

Reveals existing threats to the company, the attack vectors they use, and the possible effects of their attacks. Note: if players choose to invest in a Threat Assessment, the result of the assessment is given to them straight away, before the end of the turn. The players can then decide how to spend the rest of their budget given the new intelligence they received.

Deployment : *A consultant does a threat analysis on the company and identifies three different threat actors...*

- **Script kiddies** have low computer skills: they only use tools built by others and their attack repertoire is limited to simple, known techniques, such as scanning an infrastructure for known vulnerabilities, spreading malware found on the Internet via poorly-written email, or running small Denial of Service attacks with experimental tools. They are motivated by the "fun" aspect of hacking more than anything else. Due to the number of such low-skilled attackers and the wide availability of their techniques, their attacks are expected to be targeting the company's infrastructure at all times. They are probably already at work as we speak!

- **Organised crime** attackers have high skills and clear motivations: they will use advanced attack techniques, such as sophisticated phishing email, Remote Access Tools (RATs) and bespoke malware, in order to steal sensitive data or disrupt a target in subtle ways. Unlike script kiddies who hit indiscriminately all systems that they can reach, such advanced attackers choose specific, valuable targets, which makes their attacks less likely. However, the probability of facing them cannot be underestimated: it would be surprising if at least one of them did not take interest in the company at some point in time.
- **Nation state** attackers work on behalf of hostile remote interests. They use bleeding-edge tools and techniques that even organised criminals do not have access to, in order to conduct espionage and cyber warfare. Should one of them target the company, which is extremely unlikely, there is very little that one could do to resist them.

Counters : This defence does not counter any attack.

FAQs

Frequently Asked Questions (by the players)

Players will often ask questions as the Game Master describes the board and defences, but also later during the game. We have compiled the most frequent ones here. Some of these can be answered directly by the Game Master, while others will require the players to first invest in an ***Asset Audit*** (see ***Defences*** section ***[Page 39]***). In case an unexpected question comes, the Game Master must make up their own answer. Providing answers that are both realistic and consistent is important for players to immerse in the world of ***D-D***, think in terms of what they would do in real life and forget that they are actually playing a game.

Q: Where are these sites situated?

A: The field site is somewhere in a mountainous area of the country. The offices occupy one floor of a corporate building somewhere in a city centre, a few dozen miles from the field site.

Q: How many employees does the company have?

A: The company has a few dozen employees: around 20 working in the field site, and a few more working in the offices. The company is an independent branch of a larger, national utility, which explains why they have their own clients, IT infrastructure, management, etc.

Q: How old is the company? The infrastructure?

A: The company has been running for a few decades already. The water canal and the turbines have not changed since the early days. The IT infrastructure has not been updated in years. For more details (OS versions, controller firmware, server software, known vulnerabilities), invest in an Asset Audit!

Q: What are the current cyber-security defences?

A: The company has been taking cyber-security into account only very recently. You (the players) are the very first to implement any sort of security provisions. You can therefore expect to build from the ground up. For instance: there are no firewalls, no antivirus, no security updates for the software and operating systems.

DECISIONS & DISRUPTIONS

Q: Is there any communication between the two sites?

A: Employees from both sites communicate constantly via the email server, which is publicly visible on the Internet. Other than that, monitoring data is pulled every day from the plant's database to the offices for strategic analysis, e.g., how much are we producing, what is the performance of the generators, etc. This is used to make predictions about the future, for maintenance planning, and to decide strategic investments such as equipment replacements. There is no direct control of the generators from the offices: the plant's controller is the only one that can stop the physical process in case of an emergency.

Q: What if we don't spend all our budget?

A: Any money left will carry over to the next turn. For instance, if there is 20k left at the end of this turn, then the budget for the next turn will be 120k.

Q: Can we have more budget?

*A: This is a classic: almost every group will ask for a larger budget. It is important to reply to this query in-game, as the board of directors, and **not** as the Game Master. A typical way of handling this situation is to ask the players to make a case justifying why they want a larger budget. Then, the board of directors grants or refuses this extra budget, for instance, based on their (potentially flawed) perception of the threats on the company. An easy way of dismissing the query is to use stonewalling along the lines of: "The board of directors has taken your demand into careful consideration. Given that you have been doing an excellent job so far (for instance, there have been no detected attacks) they fully trust you to carry your mission within the limits of your current allocated budget."*

Rulebook

Q: What OS / firmware / software runs on the PCs? Server? Database? Controller?
Q: Are there known vulnerabilities in the infrastructure?
Q: Can we update the PCs? Server? Database? Controller?
Q: Is anything encrypted? Can we encrypt it?

*A: All these require the players to first invest in an Asset Audit for the Game Master to provide answers. New defences will be unlocked that will allow the players to defend the vulnerabilities the Audit revealed, cf. Defences section **[Page 39]**.*

Q: What kind of access control do the routers enforce on traffic from the Internet to the office and plant networks? What is the visibility of assets on these networks (PCs, server, databases, controller) from the Internet?

A: The routers do not filter any traffic and make every asset on the plant and office networks visible and accessible from the Internet. This arguably insecure configuration was chosen years ago to make it easy for monitoring data generated on the plant site by the controller and stored on the plant's historian database to be accessed from the offices for analysis purposes. Investing in a firewall for either the plant or the office router will implement proper access control rules for the corresponding network: the visibility and access to all assets on that network will be restricted to trusted sources only. For instance, upon installing the plant firewall, only analyst PCs on the office site will be able to see and access the plant's historian database, and the other assets on the plant network (PCs, controller) will not be visible from outside the plant network any more. Similarly, upon installing the office firewall, only the server (web and email) will be accessible from the Internet and the other assets (PCs, database) will be hidden.

Attack table

The attack table sums up the different attacks faced by the players during the game. For each round, the attack stage for each attack is shown, and possible countermeasures are listed. The way to use the attack table efficiently as a Game Master is the following:

- Before the game, make a paper copy of the attack table: photocopy the rulebook, or print the page in the pdf soft copy. **Do not show it to the players!**

- At the end of each turn, read the corresponding column in the table. Based on the player investments during this turn, identify which attacks have been countered: circle the attack stage and scratch the whole attack line, as the attack has now come to an end.

- For each circled attack stage, assess whether you need to tell the players about the attack they just countered, based on the attack description provided in this section and the corresponding defence description.

- Remember that once an attack has met its counteremeasure, it comes to an end: the following stages of the attack will not happen, hence the reason why the entire line has been scratched.

- During the following rounds, scratched attacks lines have already been stopped by the players: focus only on the unscratched, still ongoing attack lines.

(See overleaf for Attack Table)

Attack table

Attacker	Round 1	Round 2	Round 3	Round 4
Scanning Kiddie	Scan offices × Firewall offices	Scan offices × Firewall offices	Scan offices × Firewall offices	Scan offices × Firewall offices
DoSing Kiddie		DoS offices × Firewall offices	DoS offices × Firewall offices	DoS offices × Firewall offices
Hacking Kiddie		Remote control server offices × Server patch	Data exfiltration server offices × Network monitoring offices × Encryption DB	Data exfiltration server offices × Network monitoring offices × Encryption DB
Phishing Kiddie	Phishing offices (trojan) × Training × Antivirus × Patches PCs	Disruption PC offices × Antivirus × Patches PCs	Disruption PC offices × Antivirus × Patches PCs	Disruption PC offices × Antivirus × Patches PCs
Mafia APT PC Offices	Infected USB offices × Training × Anti-virus PC	Remote Control PC offices × Anti-virus PC × Network monitoring offices	Data exfiltration PC offices × Anti-virus PC × Encryption PCs × Network monitoring offices	Data exfiltration PC offices × Anti-virus PC × Encryption PCs × Network monitoring offices
Mafia APT Server Offices	Phishing offices (credentials) × Training	Remote Control Server offices × Network monitoring offices	Data exfiltration DB offices × Network monitoring offices × Encryption DB	Data exfiltration DB offices × Network monitoring offices × Encryption DB
Mafia APT Server Plant	Vulnerable Wi-Fi plant × Asset Audit	Remote Control DB plant × Patch server × Network monitoring plant	Data exfiltration DB plant × Network monitoring plant × Encryption DB	Data exfiltration DB plant × Network monitoring plant × Encryption DB
Mafia Disruption Controller	Scan plant × Firewall plant	Remote control Controller × Patch controller × Firewall plant	Disruption controller × Patch controller	Disruption controller × Patch controller
Nation State Intelligence	Physical intrusion plant × CCTV plant	Remote control DB plant (0day) × Network monitoring plant	Data exfiltration DB plant × Network monitoring plant	Data exfiltration DB plant × Network monitoring plant
Nation State Disruption	Physical intrusion plant × CCTV plant	Remote control controller (0day)		Disruption controller

The perfect game

Round 1

- Asset audit
- Security training
- Office firewall

Round 2

- Plant firewall
- Patch servers
- Encrypt Databases
- Antivirus

Round 3

- Encrypt PCs
- Patch controller
- Network monitor office

Round 4

- Patch PCs
- Network monitoring plant