DECISIONS & DISRUPTIONS

Security Lancaster | Lancaster University

www.decisions-disruptions.org

DECISIONS & DISRUPTIONS

Overview

Decisions & Disruptions is a tabletop/ role-playing game about security in industrial control systems. ***D-D*** players are tasked with managing the security of a small utility company: they are given a budget that they can spend among different defensive options.

Decisions have to be made, taking into account a number of potential threats, known vulnerabilities of the infrastructure, past and ongoing cyber attacks, and of course budget limitations.

The game is to be played with 3 to 5 players plus a Game Master who directs the players, enforces rules and tells the game's narrative. A ***D-D*** session is expected to last up to 2 hours. The players need no preparation, and indeed, **players should not read the content of this rulebook**!

Partial information and the element of surprise are key elements of ***D-D.*** But if you, the reader, want to be a *Game Master*, then keep on reading: this is the reference manual that will guide you through the process of mastering ***D-D*** sessions.

Table of contents

How to Play

Before the game

Before playing ***D-D***, the Game Master (not the players!) gets familiar with the rules by reading this manual, and builds the game board as described in the ***Assets & Defences*** section.

Structure of a *D-D* session

D-D is a turn-based game, where each turn represents approximately 2 months in the ***D-D*** world. A complete ***D-D*** session lasts **4 turns**. Each turn follows the same structure:

- The Game Master describes the game situation to the players: the state of their infrastructure, known threats and ongoing attacks.

- The Game Master gives the players a budget (by default: 100,000 credits, or 100k) and presents a number of possible security investments such as firewall, antivirus or threat assessment.

- The players debate which defences are more appropriate and decide by consensus where to spend their budget.

- The Game Master tells the players about the consequences of their decisions: whether their defences deflect any attacks, and the effects of undefended attacks, such as data theft or equipment disruptions. In addition to technical consequences, the share price of the company can be affected by successful attacks. Then the next turn starts, with a fresh 100k budget plus any unspent money left from the previous turn.

The importance of a good narrative

D-D is a role-playing game, and as such, the immersion of players is an important success criteria. You, the Game Master, do not want your players to think that they are playing a game as if they were solving a riddle. Instead, players should think in terms of what they would do if the situation happened in real life: the decisions they take should be based on their common sense, experience, or gut instinct, not on trying to guess what is the content of the rule book.

To achieve a good immersive session, it is important that the Game Master tells a convincing story to the players. We provide a number of pre-written narratives that can

be read aloud to the players, describing the ***D-D*** world, the infrastructure they defend, the effect of attacks and defences. These are provided for inspiration: ideally, after having studied this rule book and the game's environment, the Game Master should be able to describe ***D-D***'s world and tell the game story in their own words. This will make the experience much more immersive for the players, and the Game Master will be able to better react to unexpected questions and decisions than if they were following the book.

It is perfectly fine to change any description or rule provided in this book! As the Game Master, you have complete control over the game, and any customisation is more than welcome.

Turn 1: how to start the session

At the start of the game, set up the game table: put the game board in the centre and dispose the first set of defence cards and figures beside it so that everyone can see them. This first set of defences includes (cf. the section on ***Assets & Defences***, for more details).

- ***2 Firewalls (plant and offices)***
- ***Anti-Virus***
- ***Security Training***
- ***Asset Audit***
- ***Threat Assessment***
- ***2 CCTV (plant and offices)***
- ***2 Network Monitoring (plant and offices)***

The other defence cards and figures (three *Upgrades* and two *Encryptions*) should stay hidden: the players should not know about these just yet. They will be unlocked later when they invest in an *Asset Audit*.

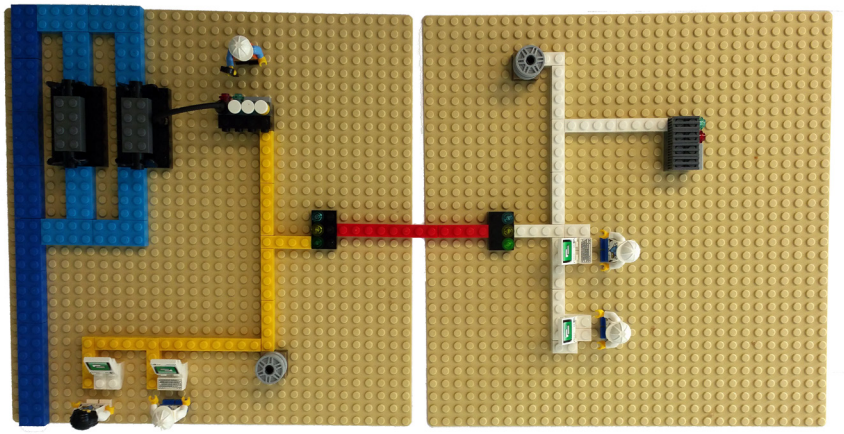


Image: Game board at beginning of game

Image: Cards available at the beginning of the game

Welcome address by the Board of Directors

You are now ready to start the game. You will be acting as the representative of the company's Board of Directors. Read the following text to the players, or if you feel confident enough, tell them a similar story in your own words:

"Congratulations! You have been appointed to be the team in charge of managing the security of this small company. I am representing the Board of Directors, from now on you will be reporting directly to me. Security is a very new concern for us, we don't understand much about it. But we also follow the news, and we have seen a growing number of security incidents in utility companies like ours. This is why you have been hired: you are our security experts, and we trust you to keep us safe and secure.

Your task is therefore to minimise the number of security incidents. As the Board of Directors, our task is to take care of the company's share price. We have high hopes in your ability to defend us against malicious attackers:

we wouldn't want the press to learn that we have been hacked, would we? Our share price would certainly be negatively affected. I will be giving you regular updates on how our stocks are doing. Hopefully, nothing will happen, and our shareholders and customers will be happy.

In this company we work on a 2-months financial cycle. I will therefore allocate your budget for the first cycle: 100,000 credits, or 100k. Use this money wisely. We have already identified a number of potential investments in defences, represented by these cards and figures. Since the money is limited, and there are a lot of options to choose from, you will have to prioritise the most important defences for this cycle, and delay less urgent investments to the next cycles. Any unspent money will carry over to the next cycle."

At this stage, ask the players whether they have any questions. We have compiled a number of frequently asked questions at the end of this section. When all questions have been answered, you can resume the narrative and show the players around their new company.

Describing the game board

The game board is a physical representation of the infrastructure that the players are defending. We provide the following description as a reference, with important elements to point on the board highlighted in **red**:

"I will now walk you through our premises and show you around our infrastructure. First is the plant, or field site, which hosts power generators: you can see a river in blue at the back and two turbines driven by the stream. The turbines are controlled by a SCADA controller, maintained by this technician with the wrench, and connected to the local network in yellow. This local network also hosts a number of PCs for local engineers and technicians, and a database that stores monitoring values produced by the SCADA controller: water debit, power production, etc. The plant's network (in yellow) is connected to the Internet (in red) via this router.

The second site is the remote office, also connected to the Internet via its own router. The offices' local network (in white) also hosts a number of PCs for employees: managers, Human Resources, engineers,

analysts. The company runs its own email and web server, connected to a local database for storing emails, HR records, technical and financial data, etc."

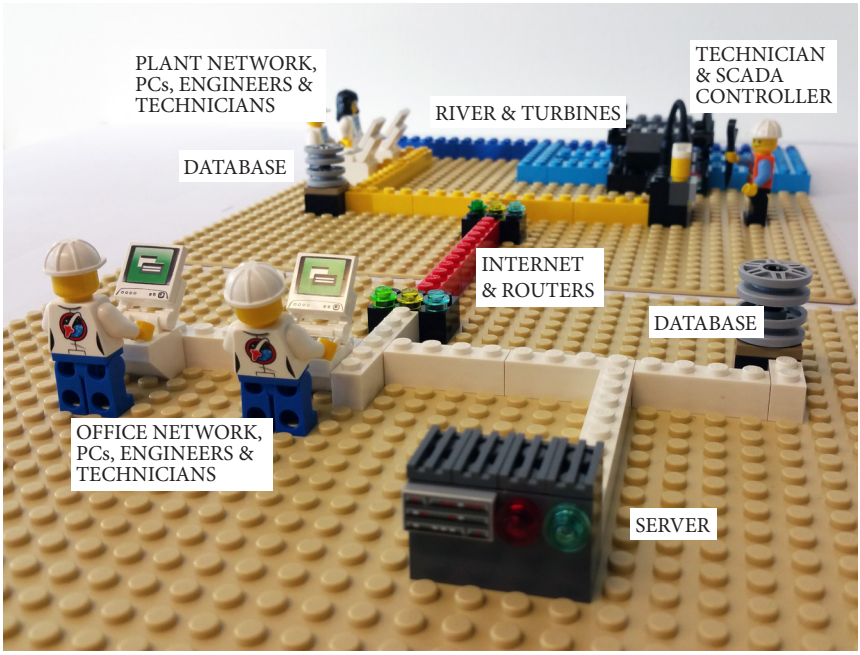


Image: Board components at the beginning of the game

Describing the defences

After showing the game board to the players and answering their questions, the Game Master should present them with available defences. Take the time to show the cards

one by one, read the description text on the cards and present the associated figures. Refer again to the ***Frequently Asked Questions*** section if need be.

Supervising player decisions

The players should be now ready to start making their first decisions and debate on what defences are the most appropriate. As the Game Master, you should try not to influence their discussions: you know about the attack scenario and which defences are indeed the most important. The players should be left ignorant of what will happen precisely, although investing in a threat assessment will give them precious clues regarding the threats they are facing.

Therefore, try to answer their questions in a neutral way and to not give indications regarding what would be a right or wrong decision. Making mistakes is a valid way of learning, and the final debriefing phase of the game will be the opportunity for them to understand what went wrong.

Some groups of players have a hard time making decisions and keep debating endlessly. A simple and neutral way of speeding things up is to organise a quick vote: ask each player

to mention the one defence they think is the most important, and to justify it briefly. Optionally, the player can also point out one defence that they think is not a priority. Such a voting exercise can help identify clear favourites among the defences, especially at the beginning of turn 1 when there are many options. Do not hesitate to organise several such voting rounds. The actual decision, however, should always follow player consensus: voting for important defences is simply a way to speed up the debates and eliminate unlikely candidates for an investment.

End of turn 1: deployment, attacks, consequences

Once the players have decided which defences to invest in, remove their cards from the table, and deploy the corresponding figures on the game board. The **Defences** section ***[Page 39]*** contains text descriptions of what happens when the defences are deployed in the infrastructure: read them to the players.

It is now time to run the attacks for turn 1. Refer to the **Attacks** section ***[Page 61]*** and describe to the players what happens during the two months following their investments. This (usually grim) phase ends the turn.

After turn 1: the game goes on

For the following turns, the players should already be familiar with the infrastructure and defences. They are, however, likely to be surprised by the attacks that happened at the end of the previous turn. Start again the process of debating which defences should be invested in, with a fresh budget plus any excess from the previous turn. In general, players take their decisions much more quickly after the first turn. They should be careful however: sticking to one's initial ideas is not always the optimal decision. Good players will be able to understand the threats behind the attacks and adapt their decisions accordingly.

Turn 4: how to end the session

At the end of the game, i.e. after turn 4, the Game Master reveals to the players the full range of attackers they were facing, which attacks they deflected successfully and which ones defeated their defences. This is the stage in which everyone reflects on their decisions and evaluate their cyber-defence strategies.

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.

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."*

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]****.*

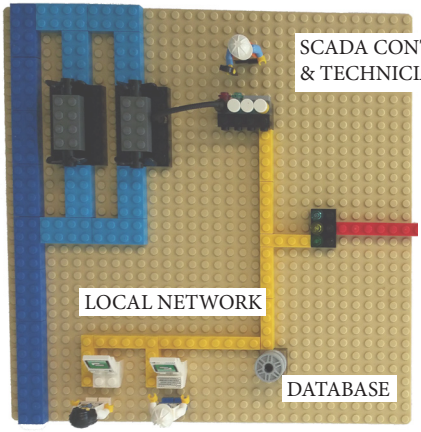
Q: What kind of access control do the routers enforce on traffic from the Internet to the office and plant networks? What is the visibility of assets on these networks (PCs, server, databases, controller) from the Internet?

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.

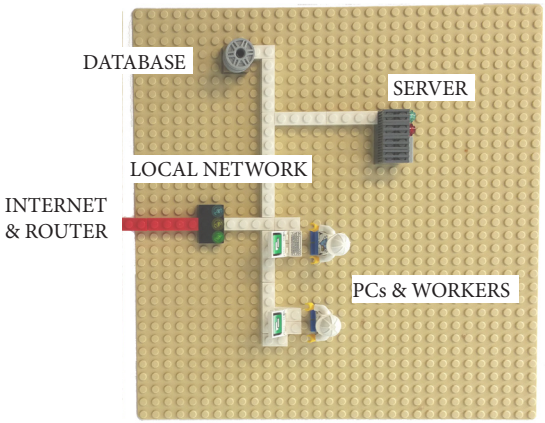
Assets & Defences

The Game Board (Assets)

The plant



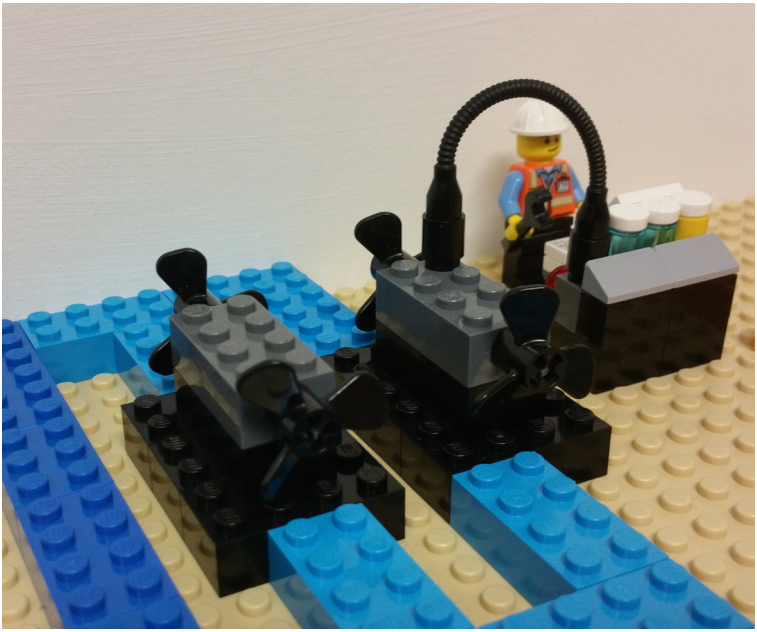
The office



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**.



Network (plant)

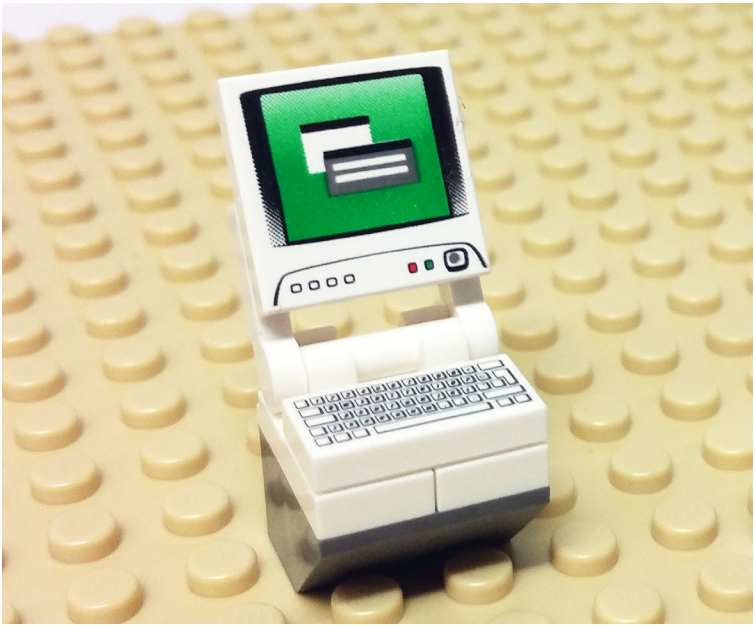
This local network links together the **controller**, **historian database** and **PCs** used by technicians and engineers in the plant. The network is interfaced with the Internet via the plant's **router** that allows any traffic in both directions, from the Internet to the plant network and vice versa.

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.**

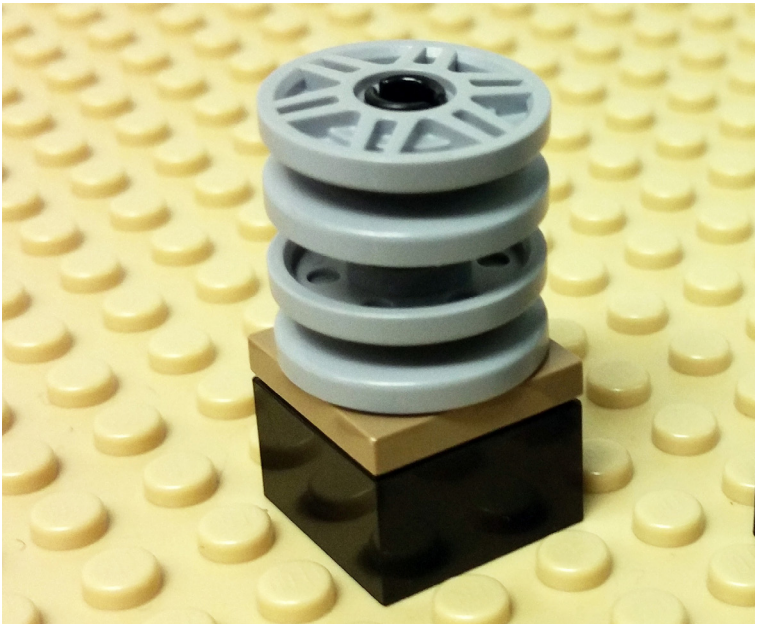
PCs (plant)

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.



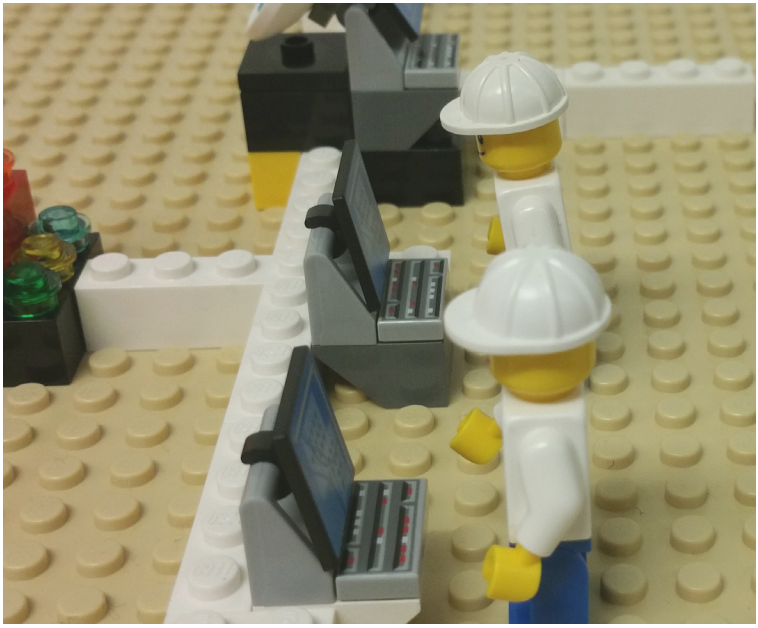
Historian database (plant)

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.



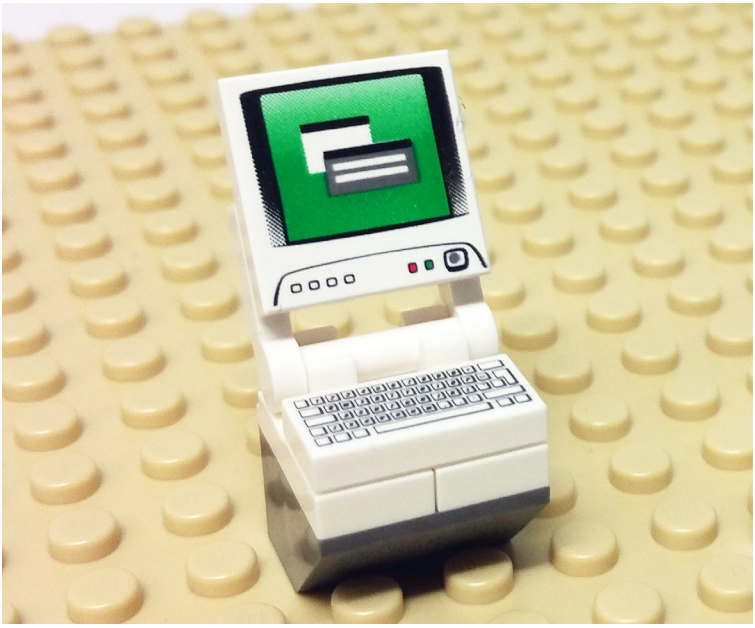
Network (office)

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.



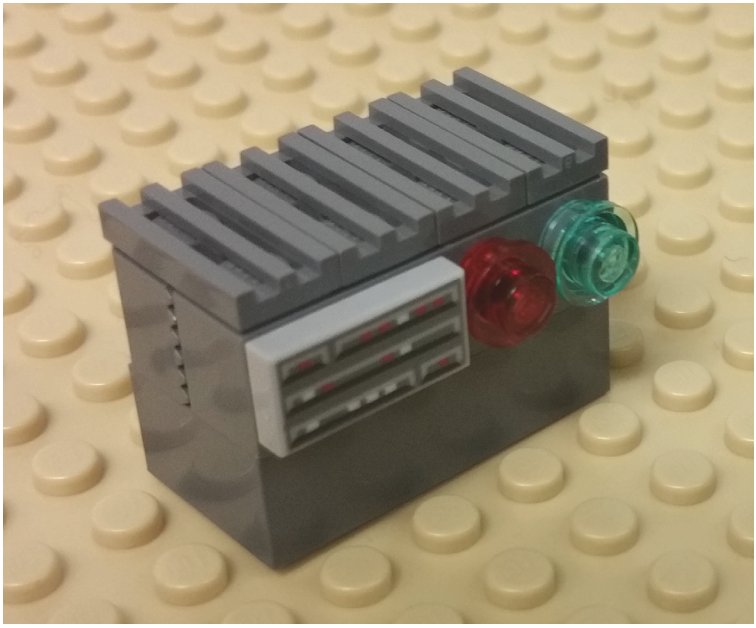
PCs (office)

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.



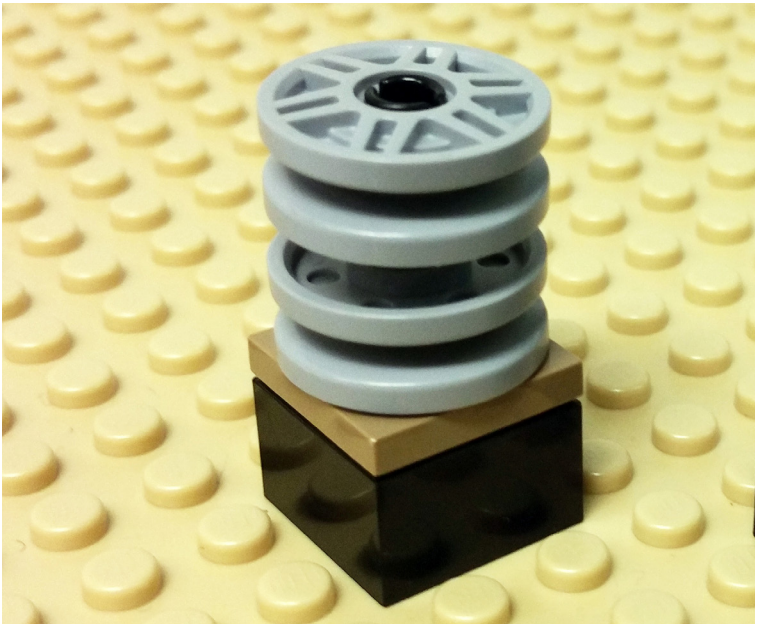
Server

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.



Defences

Defences are represented by cards with an associated lego figure. Each card displays information such as: *Defence name; Defence cost; A short description.*

In this section, we provide additional information for the Game Master (**players should not have direct access to these!**):

- Additional descriptions, providing the Game Master with background content to answer questions by the players.

- A description of what happens when the defence is deployed in the infrastructure, to be read to the players after they buy the defence.

- A description of the defence's effect when it stops an attack, to be read when the attack is countered (**not when describing the defence to the players!**).

Initially the players have access to the following defences only:

- 2x **Firewall** (plant and office)
- **Antivirus**

- **Security Training**
- **Asset Audit**
- **Threat Assessment**
- 2x **CCTV** (plant and office)
- 2x **Network Monitoring** (plant and office)

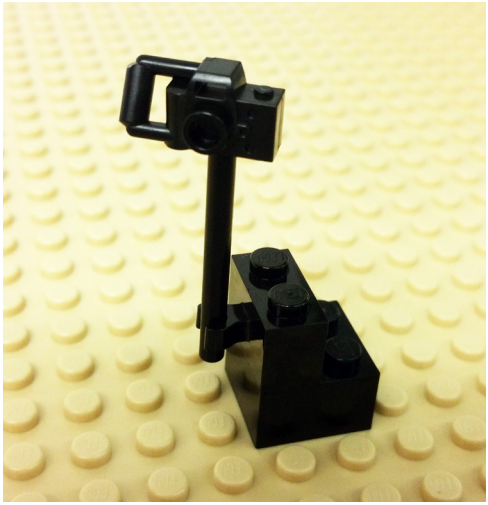
Additional defences (3x **Upgrade** and 2x **Encryption**) are made available to the players when they invest into the **Asset Audit**.

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.*

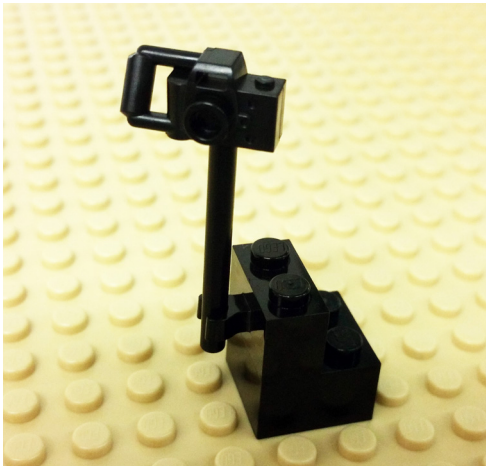


CCTV Surveillance (Plant) – 50k

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.*



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.

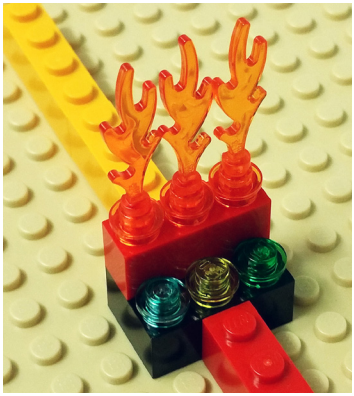
Firewall (Plant) – 30k

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.*

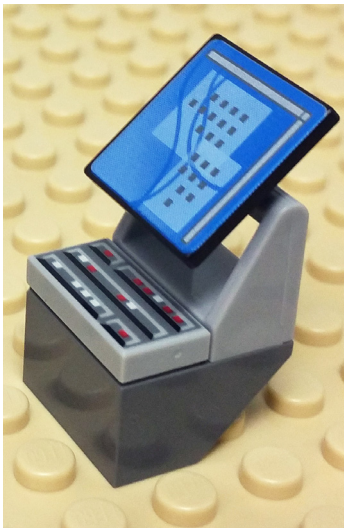


PC Upgrade – 30k

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.*

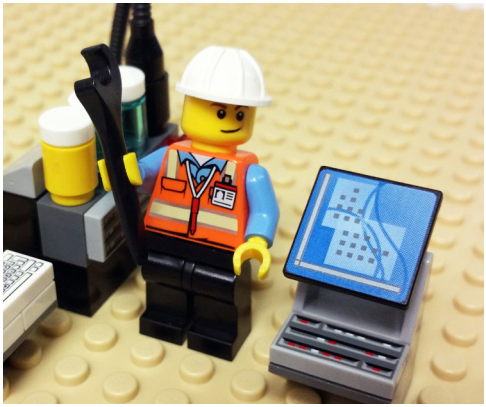
This defence also has a potential silent effect: it prevents the **Remote control database plant** attack from an APT attacker on the plant network on turn 2. In case the players have deployed a Network Monitor for the plant during that turn, the logs will show unsuccessful attempts at accessing an old,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

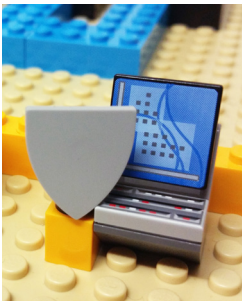
Counters Phishing offices (trojan), Disruption PC offices, Infected thumb drive office and Remote control PC (use the appropriate event among the following options):

Upon opening an attachment from an unknown sender...

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

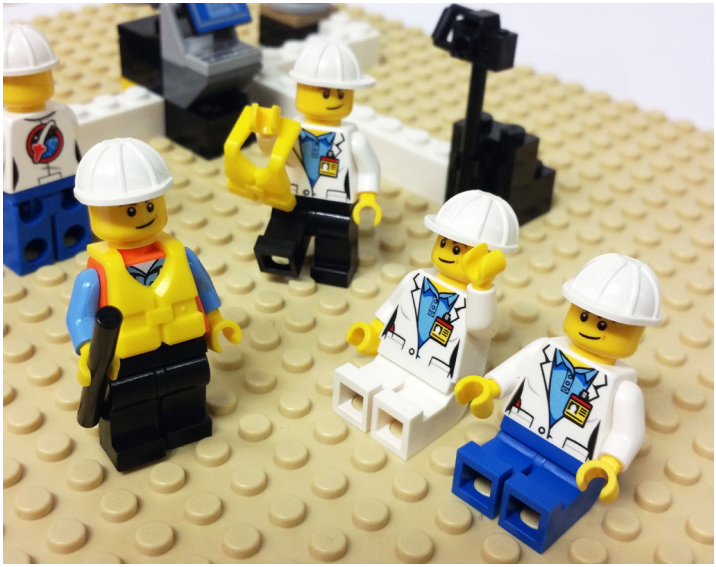
One day, seemingly out of nowhere...

... 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.*



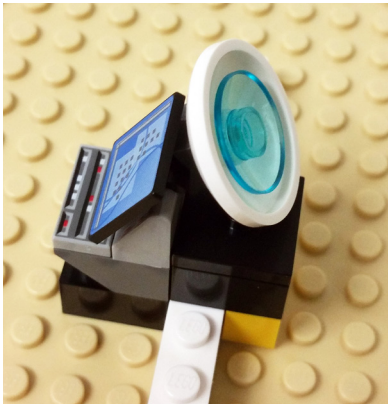
Counters Phishing offices (trojan) and Infected thumb drive offices (use the appropriate events in the following text): *Upon receiving an email with an attachment from an unknown source / finding a thumb drive in the parking lot, an employee reports it directly to you (the players). Upon close inspection, 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.*



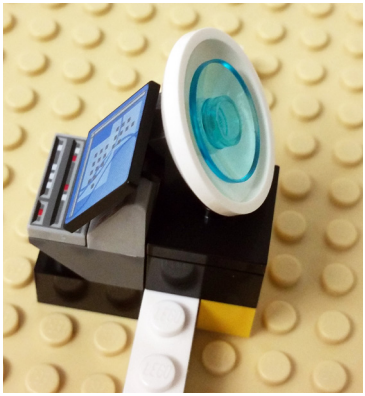
Counters Remote Control attacks on the server and office PCs (use the appropriate variation among the following): *One day, the office's network administrator comes to talk to you: they have detected suspicious activity on the office network. The server / a PC seems to be communicating at regular intervals 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.*

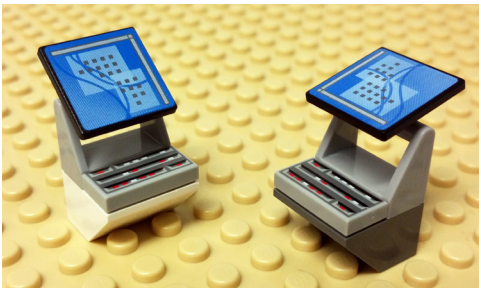
Counters Data Exfiltration attacks on the historian database: *One day, the office's network administrator comes to talk to you: they have detected a suspicious data stream originating from the historian database and going to an unknown address on the Internet, located in a foreign country. Upon closer 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.

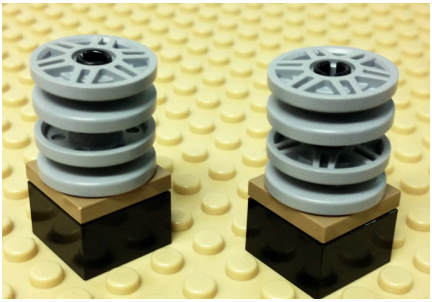


Database Encryption – 20k

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.

Attackers & Attacks

Overview

This section presents the attack scenarios happening during a ***D-D*** session. There are three types of attackers:

- **script kiddies**
- **organised criminals**
- **item nation states**

The following sections present each attacker and the attack techniques they use. All attacks are summarised in the attack table ***[Page 83]***. All attacks follow a linear progression: each attack runs until the players invest in a defence that counters it, at which point the attack comes to an end. Depending on the attack, the defence, and the turn in which the countermeasure is deployed, the players may or may not learn that they have successfully deflected an attack, as described next. The Game Master should also refer to the defence descriptions ***[Page 39 onwards]*** in order to inform the players of the effects of their investments.

Script kiddie attacks

These attacks represent low-skill, common security threats faced by any system connected to the Internet. Script kiddies have no precise goal other than hacking whatever they can, and their simple attacks are repeated every turn (except for turn 1 in the case of the DoSing, hacking and malware kiddie). The attack scenarios feature five such attackers.

Scanning kiddie

This attacker simply scans the Internet, looking for vulnerable systems. The scans may come from all around the world and target both the offices and the plant, every turn of the game.

Attack effect : Scans have no direct negative impact on the target infrastructure, yet they are often a preliminary reconnaissance phase to an actual attack, such as a Denial of Service (DoS) or hacking a vulnerable system, represented by the following two attackers.

Countermeasures : As soon as a **firewall** is deployed, the corresponding network (office or plant) is protected against scans, and the players will know about it. Even

several turns after the firewalls have been deployed, it is always helpful to remind the players that scanning attacks continue and that their firewall(s) keep protecting their infrastructure.

DoSing Kiddie

This attacker floods the office network with traffic generated by hundreds of infected ***bots****.*

Attack effect : The office network is out of order, no one can connect to the Internet, and the local database and server crash. As no employee can work properly for several days, the share price takes a small dip.

Countermeasures : A **firewall** deployed on the office network counters the DoS attack, as it can be configured to deflect traffic from unknown sources.

Hacking Kiddie

This attacker exploits a simple, public vulnerability in the company's web server to get access to it during turn 2. During turn 3, emails stored on the database are exfiltrated.

Attack effect : At the end of turn 3, the players receive a snarky email written in an approximate language and taunting the company for their poor security. Soon after,

the company's emails are published on the Internet, and the press learns about the breach. The company's share price takes a small dip.

Countermeasures : **Upgrading** the server on turns 1 or 2 stops the attack altogether. **Encrypting** the database on turn 3 or before prevents the attacker from doing anything with the data they stole. In case a **network monitor** is deployed on the office network on turn 3, the players detect the suspicious data stream from their database to the attacker, their network administrator is able to detect the infiltration and remove the attacker's access just in time.

Phishing Kiddie

Every turn, this attacker sends viruses they found on the Internet to random email addresses, including the company's employees.

Attack effect : Upon opening the malicious attachment, a malicious program (Remote Access Tool, or "RAT") is installed on the victim's PC and gives access to the attacker. There is no direct visible effect of infection, however, the attacker will use the RAT to disrupt office PCs later on (cf. *malware kiddie*).

Countermeasures : A **security training** prevents employees from opening the malicious attachment, and they report the attack to the players. An **antivirus** stops the malicious RAT from infecting the victim's PC and raises a warning, also alerting the players. Alternatively, **upgraded PCs** are not vulnerable to the RAT, and the attack fails silently.

Malware Kiddie

This attacker exploits RATs already infecting office PCs after a successful phishing attack during the previous round (cf. phishing kiddie attack). The attacker deploys a cryptolocker that encrypts the victim's hard drive.

Attack effect : The players receive a threatening email asking for a 10k ransom in exchange of the decryption key. Employees signal that their machines have stopped functioning and display bizarre messages, similar to the ransom email. The board of directors strictly forbids the players from paying the ransom. The lost data is never recovered, and the infected machines have to be replaced. The company's share price suffers lightly from the disruption.

Countermeasures : Counters to the initial phishing phase (**security training**, **antivirus**, **PC upgrade**) stop the initial infection. In case the defences are deployed in the round right after the infection (e.g., there is a successful phishing on turn 1 but the players invest in a **security training** during turn 2), the attack is also stopped: an **antivirus** detects the malicious ransomware, a **PC upgrade** prevents it from functioning, or **trained** employees realise that they have been phished and turn their machine in for decontamination, just in time.

Organised crime attacks

These attacks are carried out by professionals with clear goals: stealing valuable data, or disrupting sensitive infrastructure. Unlike script kiddies, these criminals are skilled attackers following sophisticated schemes typical of Advanced Persistent Threats (APT): reconnaissance and penetration (turn 1), lateral movement in the infrastructure (turn 2), exfiltration / disruption (turn 3), exploitation (turn 4). In total, four such APT will be attacking the players, each focusing on a different target.

APT PC Offices

This attack attempts to steal sensitive data from employee PCs:

- Turn 1: An infected thumb drive is left in the company's parking lot near the offices. An employee picks it up, plugs it into their computer, and unwillingly installs a Remote Access Tool (RAT).

- Turn 2: The infected machine is used by the attacker to gain access to other machines on the office network and identify sensitive data on them.

- Turn 3: The attacker exfiltrates sensitive emails and technical data from the infected PCs to a remote location on the Internet. At the end of the turn, the data is sold on Dark Web marketplaces for a few bitcoins.

- Turn 4: If the attack is still running at this point, all sorts of unimportant data are exfiltrated from infected machines and published on the Internet, as a show of force from the attackers.

Attack effect : If the attack is still active at the end of turn 3, the press learns about the data leak and the company's share price plummets. If the attack is still not stopped at the end of turn 4, the company is forced to shut down its entire infrastructure for sanitisation.

Countermeasures : The attack can be countered in different ways, and the players do not suffer any consequences (bad press, depreciated share price) if they manage to stop it at turn 3 or before.

- Turn 1: An employee with a **security training** will be suspicious of the infected thumb drive and not plug it in. An **antivirus** will detect and stop the RAT.

- Turn 2-3: An **antivirus** installed on turn 2 will detect and stop the RAT installed during turn 1. A **network monitor** in the office will detect the RAT and flag the machine for sanitisation.

- Turn 3: In addition to **antivirus** and **network monitoring**, **encrypting** the PCs prevent the APT from accessing any sensitive data.

- Turn 4: A late **antivirus**, **office network monitor**} or **PC encryption** will prevent the attack from shutting down the company completely, however, most of the damage has already been done.

APT Server

This attack attempts to exfiltrate sensitive data from the server and office database:

- Turn 1: A spear phishing email is sent to the office network administrator, crafted with the company logo and containing a link to a fake login page. The administrator opens it and gives away their access credentials to the server.

- Turn 2: The attackers, now silently in control of the server, identify the office's database as a valuable target and gain access to it.

- Turn 3: Sensitive data (email, HR records, client contracts, banking details, etc.) is exfiltrated from the database to a server in a remote country. At the end of the turn, the data is sold on Dark Web marketplaces for a few bitcoins.

- Turn 4: If the attack is still running at this point, the attackers use a cryptolocker to lock down the content of the office database. As all activity has to be stopped in the office, since no one can work without access to the database, a chilling email is sent to the players, asking for a 500k ransom.

Attack effect : If the attack is still active at the end of turn 3, the press learns about the data leak and the company's share price plummets. If the attack is still not stopped at the end of turn 4, the board of directors refuses to pay any ransom, and the company, having lost one of its core assets, is forced to shut down.

Countermeasures : The attack can be countered in different ways, and the players do not suffer any consequences (bad press, depreciated share price) if they manage to stop it at turn 3 or before.

- Turn 1: A network administrator with **security training** will not fall for the spear fishing email, they will instead report it to the players.

- Turn 2-4: **Network monitoring** in the office will detect a suspicious connection between the server and a remote address, prompting the administrator to change access credentials and check the server for malware.

- Turn 3-4: **Encrypting the database** prevents the attackers from reading its content.

APT Plant Database

This attack attempts to exfiltrate sensitive data from the plant's historian database:

- Turn 1: Local attackers find an open Wi-Fi network in the plant (cf. description of the **asset audit** results for an explanation) and infiltrate the plant network.

- Turn 2: The attackers identify the plant's historian database and use a vulnerable remote management utility to gain access to it.

- Turn 3: The attackers exfiltrate the content of the historian database to a remote location and attempt to sell it to the company's competition.

- Turn 4: If the attack is still running at this point, the attackers corrupt the content of the historian database.

Attack effect : If the attack is still active at the end of turn 3, one of the competitors alerts the players that their data has been stolen, and shortly after, the story leaks to the press. The company's share price plummets. If the attack is still active at the end of turn 4, the company's share price takes another dive, as the corruption of the historian database slows down all activities significantly for a few days.

Countermeasures : The attack can be countered in different ways, and the players do not suffer any consequences (bad press, depreciated share price) if they manage to stop it at turn 3 or before.

- Turn 1: An **asset audit** reveals the insecure Wi-Fi network in the plant and secures it, preventing the attackers from infiltrating the plant network (players do not learn about the attack).

- Turn 2: A **server upgrade** patches the vulnerable remote management utility and prevents the attackers from gaining access to the historian database. Since the attack fails silently, the players do not learn about it.

- Turn 2-3: **Network monitoring** in the plant network detects suspicious activity around the historian and prompts the system administrator to shut down the vulnerable management utility. In this case, the players learn about the attack.

- Turn 3: If, on turn 3, the historian database is **encrypted**, the attackers cannot decypher its content and give up on the attack.

- Turn 4: Two defences can prevent the attackers from corrupting the database: **network monitoring** in the plant reveals the attackers and allows the network administrator to remove their access just in time, while **database encryption** prevents the attackers from reading / writing database records.

APT Controller

This attack attempts to disrupt the plant's SCADA controller with a malicious firmware update:

- Turn 1: Attackers scan the plant network from the Internet (similar to a scanning kiddie attack) and identify the vulnerable controller.

- Turn 2: The attackers exploit a vulnerable remote access utility to gain control of the controller.

- Turn 3: The attackers update the controller's firmware with a malicious patch that disrupts the functioning of the turbine. At the end of the turn, a partial failure lightly damages the turbine, and the attackers send a ransom request (500k) to the company.

- Turn 4: If the attack is still running at the end of turn 4, the attackers blow up the turbine in a spectacular, destructive incident.

Attack effect : If the attack is still active at the end of turn 3, the turbine is slightly damaged and requires several days of maintenance. The company's share price

plummets. If the attack is still active at the end of turn 4, the board of directors refuses to pay the ransom, and the company, having lost one of its core assets, is forced to shut down.

Countermeasures : The attack can be countered in different ways, and the players do not suffer any consequences (damaged turbine, depreciated share price) if they manage to stop it at turn 3 or before.

- Turn 1-2: Deploying a **firewall** on the plant network stops the initial scan and prevents the attackers from accessing the controller.

- Turn 2-3: **Upgrading** the controller removes the vulnerable utility used by the attackers to gain control of the controller.

- Turn 4: **Upgrading** the controller on turn 4 removes the attackers' access and saves it from complete destruction.

Nation state attacks

Nation state attacks represent the highest threat level. These attacks are optional, as they are more difficult to defend against than organised crime attacks. It is up to the Game Master to choose whether or not they wish to mention these attacks to the players. As a rule of thumb: when players have already suffered from several attacks, it is unnecessary to add yet another defeat to their game session; but if the players have successfully defended all script kiddie and organised crime attacks, then the nation state attacks become a way for the Game Master to remind them that perfect security can never be achieved, as it all depends on the level of resource of their opponents. We give here two examples of nation state attacks.

State intelligence

This attack attempts to steal the content of the historian database in the plant:

- Turn 1: A spy infiltrates the plant and dissimulates a malicious device, with satellite remote access, connected to the plant network.

- Turn 2: The attacker exploits a zero-day vulnerability to gain control of the historian database.

- Turn 3 and 4: The attacker exfiltrates the content of the database via the satellite link.

Attack effect : The attack is completely silent, as no ransom or disruption alerts the players. The content of their historian database ends up in the hands of a hostile remote power. Unless the players counter the attack (see below) the only way they can learn about it is at the end of the game, during the debriefing with the Game Master.

Countermeasures : There is only one way the players can counter this attack: a **CCTV** deployed in the plant during turn 1 detects the spy's intrusion (and in that case, the players must have skipped a number of essential turn 1 investments). Otherwise, a **network monitor** deployed in the plant during turns 2 to 4 detects suspicious network traffic around the historian database. This tells the players that someone has infiltrated their network. However, they cannot patch the database (as no fix exists against the zero-day used by the attacker), they cannot shut it down either as it is

essential to the plant's functioning, and they cannot find the malicious device dissimulated on the local network. As there is no visible harmful consequences to this activity, they will have to live with the idea that something is going on that they cannot help.

State disruption

This attack attempts to take control of the plant's SCADA controller and disrupt its operations:

- Turn 1: A spy infiltrates the plant and installs a malicious bug on the SCADA controller. The bug can be triggered remotely, via a wireless link, to disrupt the controller.

- Turn 2-3: The bug sits silently on the controller, doing nothing.

- Turn 4: The attackers trigger the bug, destroying the turbines and damaging the controller.

Attack effect : The attack, made in the context of a global cyber warfare operation, destroys the core asset of the company.

Countermeasures : The only possible counter to this attack is again deploying **CCTV** in the plant at turn 1, intercepting the spy's intrusion. Again, in that case, the players must have skipped a number of essential turn 1 investments: they will suffer from a number of other attacks, and mentioning this particular nation state attack at the end of the game is not necessary.

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

CONTENTS

Models built of LEGO® bricks and components. LEGO® is a trademark of the LEGO Group of companies.

Base
Large square base boards X2

River / Turbines
Dark blue brick 2x4 – X8
Light blue brick 2x4 – X8
Black brick 2x4 – X8
Grey brick with attachments – X2
Black propellers – X4

Plant Network
Yellow brick 1x4 – X10
Lego person with helmet – X2

Office Network
White brick 1x4 – X7
White brick 1x2 – X3
Lego person with hair – X2

Internet
Red brick 1x4 – X3 (may vary)
Black brick 2x3 – X2
Transparent coloured lights X6

PCs & Encryption
White keyboard tiles – X4
White screen tiles – X4
White sloping brick 2x4 – X4
White screen attachment – X4
White 1x2 with grabber – X8
Grey sloping brick 2x4 – X4

PC Upgrade
Grey keyboard tiles – X4
Grey screen tiles – X4
Grey screen attachment – X4

Servers
Grey brick 2x4 – X1
Black brick 2x4 – X1
Grey brick double sided 1x4 – X1
Black brick double sided 1x4 – X1
Grey keyboard tile – X1
Transparent coloured lights – X2
Grey grill bricks ¬– X4
Black grill bricks – X4
Grey corrugated brick 1x2 – X2
Black corrugated brick 1x2 – X2

Databases
Black brick 2x2 – X2
Black brick with single attachment 2x2 – X2
Grey wheels – X4
Black wheels – X4
Black middle attachment – X2

Firewalls
Flames – X6
Transparent lights with attachment – X6
Red brick 1x3 – X2
Red Bag 10 Label: Antivirus
Shields – X4
Tapered black stands – X4

Network Monitoring 1
Black brick 2x2 – X2
Yellow brick 1x2 – X1
Grey sloping brick 2x4 – X1
Grey screen attachment – X1
Grey screen tile – X1
Grey keyboard tile – X1
Grey 1x1 with grabber – X1
White dish – X1
Blue transparent dish – X1
Black brick with single attachment 2x2 – X1

Network Monitoring 2
Black brick 2x2 – X2
Yellow brick 1x2 – X1
Grey sloping brick 2x4 – X1
Grey screen attachment – X1
Grey screen tile – X1
Grey keyboard tile – X1
Grey 1x1 with grabber – X1
White dish – X1
Blue transparent dish – X1
Black brick with single attachment 2x2 – X1

Security Training
Yellow life vest – X4

Controller & Upgrade
Lego person with helmet and orange torso – X1
Spanner – X1
Grey keyboard tile – X2
Grey screen tile – X1
Grey screen attachment – X1
Grey sloping brick 2x4 – X1
White keyboard tile – X1
White screen tile – X1
White sloping brick 2x4 – X1
White screen attachment – X1
White 1x2 with grabber – X2
Black brick 2x4 – X1 (may vary)
Grey brick double sided 1x4 – X1
Black brick double sided 1x4 – X1
Transparent barrel lights – X3
White caps – X3
Transparent lights – X2
Black barrel – X2
Flexible joiner – X1

CCTV
Black brick 2x2 – X2
Black brick with grabber 1x2 – X2
Black stick X2
Black camera X2

Notes

www.decisions-disruptions.org