Greater Manchester | Greater Security | Greater Business

Cyber Foundry

Invest or Defend

Ben Goldsworthy, Jon Lomas & Zaffar Mughal
Presented at Play Secure 2022

European Union
European Regional
Development Fund

Lancaster University

MANCHESTER
1824
The University of Manchester

Manchester
Metropolitan
University

University of
Salford
MANCHESTER

Overview

1. Introductions
2. The problem
3. The workshop game
4. The online game

Greater Manchester | Greater Security | Greater Business

Cyber Foundry

Introductions

European Union
European Regional
Development Fund

Lancaster University

MANCHESTER
1824
The University of Manchester

Manchester
Metropolitan
University

University of
Salford
MANCHESTER

Introductions

European Union
European Regional Development Fund

School of Computing & Communications | Lancaster University

Secure Digitalisation

Greater Manchester | Greater Security | Greater Business

Cyber Foundry

Introductions

European Union
European Regional Development Fund

Ben Goldsworthy

- Lancaster University alumnus
- ...and emeritus
- Now an IT Consultant

- Email: me+playsecure@bengoldsworthy.net

Introductions

European Union
European Regional
Development Fund

Jon Lomas

- Business Support & Project Manager, Greater Manchester Cyber Foundry
- Email: j.lomas1@lancaster.ac.uk

Introductions

European Union
European Regional Development Fund

Zaffar Mughal

- Technical Manager, Greater Manchester Cyber Foundry
- Email: z.mughal1@lancaster.ac.uk

Greater Manchester Cyber Foundry

European Union
European Regional
Development Fund

- GMCF is a consortium of four Universities
- Enabled by £6m funding through ERDF
- Secure Digitalisation is delivered by LU
- Cyber innovation & growth programme
- Conferences, masterclasses, webinars
- Technical advice & briefing documents

Lancaster University

MANCHESTER
1824
The University of Manchester

Manchester Metropolitan University

University of Salford MANCHESTER

Greater Manchester | Greater Security | Greater Business

Cyber Foundry

Problem Specification

European Union
European Regional Development Fund

Lancaster University

MANCHESTER 1824
The University of Manchester

Manchester Metropolitan University

University of Salford MANCHESTER

The Problem – Invest or Defend

European Union
European Regional Development Fund

An interactive, fun, and alternative way to understand controls, risks, attacks and actors

Learning Objectives

European Union
European Regional
Development Fund

- Recognise key cyber security terms for common attacks
- Understand the 5 control areas of Cyber Essentials
- Analyse scenarios in which cyber attacks have occurred
- Apply knowledge of controls to scenarios
- Assess appropriate safeguards of critical infrastructure services

Greater Manchester | Greater Security | Greater Business

Cyber Foundry

The Workshop Game

European Union
European Regional
Development Fund

Lancaster University

MANCHESTER
1824
The University of Manchester

Manchester
Metropolitan
University

University of
Salford
MANCHESTER

The Workshop Game

European Union
European Regional Development Fund

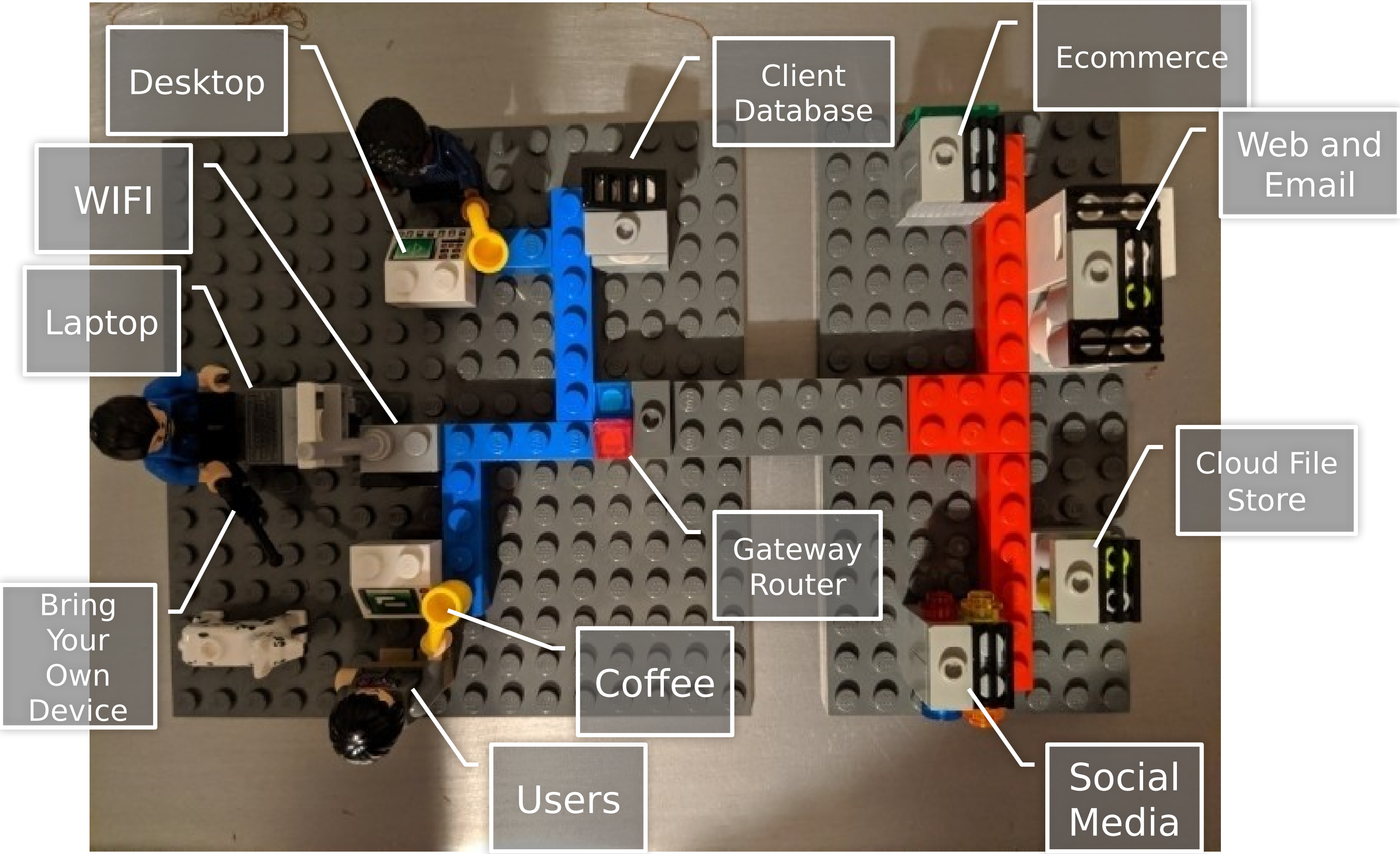
- Run in 4 cohorts between Mar 2019 and March 2020
- 43 participants across 43 organisations
- Objective: To encourage players to consider the opportunity costs involved in security investment decisions, and to teach them how to better assess likely return on investment

Gameplay Loop

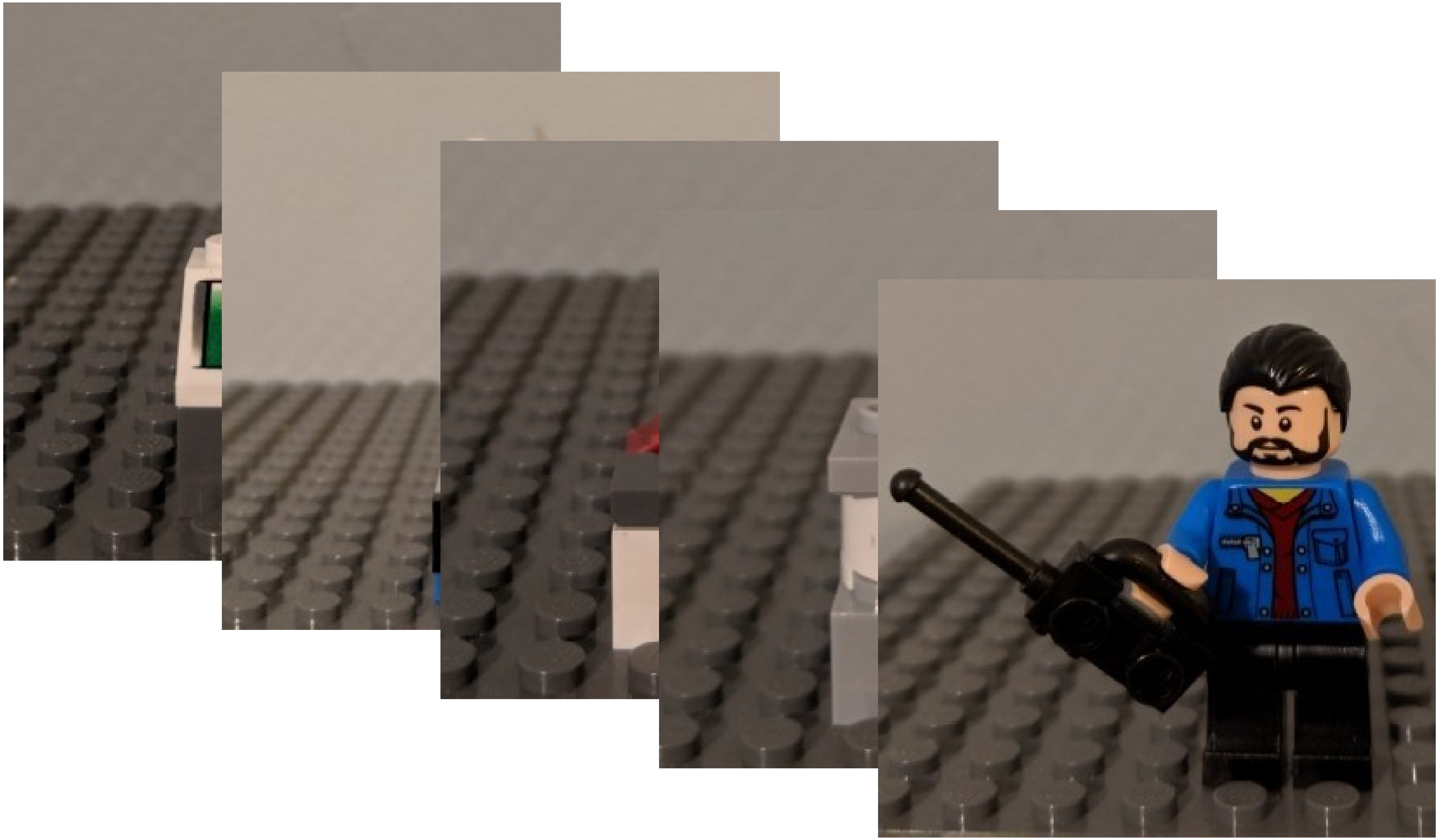
1. Each round, players are given a set amount of money which they can use to buy different cyber security controls
2. Each control costs a different amount and protects a different asset – players must explain where they are implementing the control and why
3. Any unspent funds are then added to the player’s balance
4. Cyber incidents are simulated, which may or may not succeed depending on which controls the player has implemented
5. Successful incidents have a cost, which comes off of the player’s balance
6. The goal is to have the highest balance at the end of the game

The Board

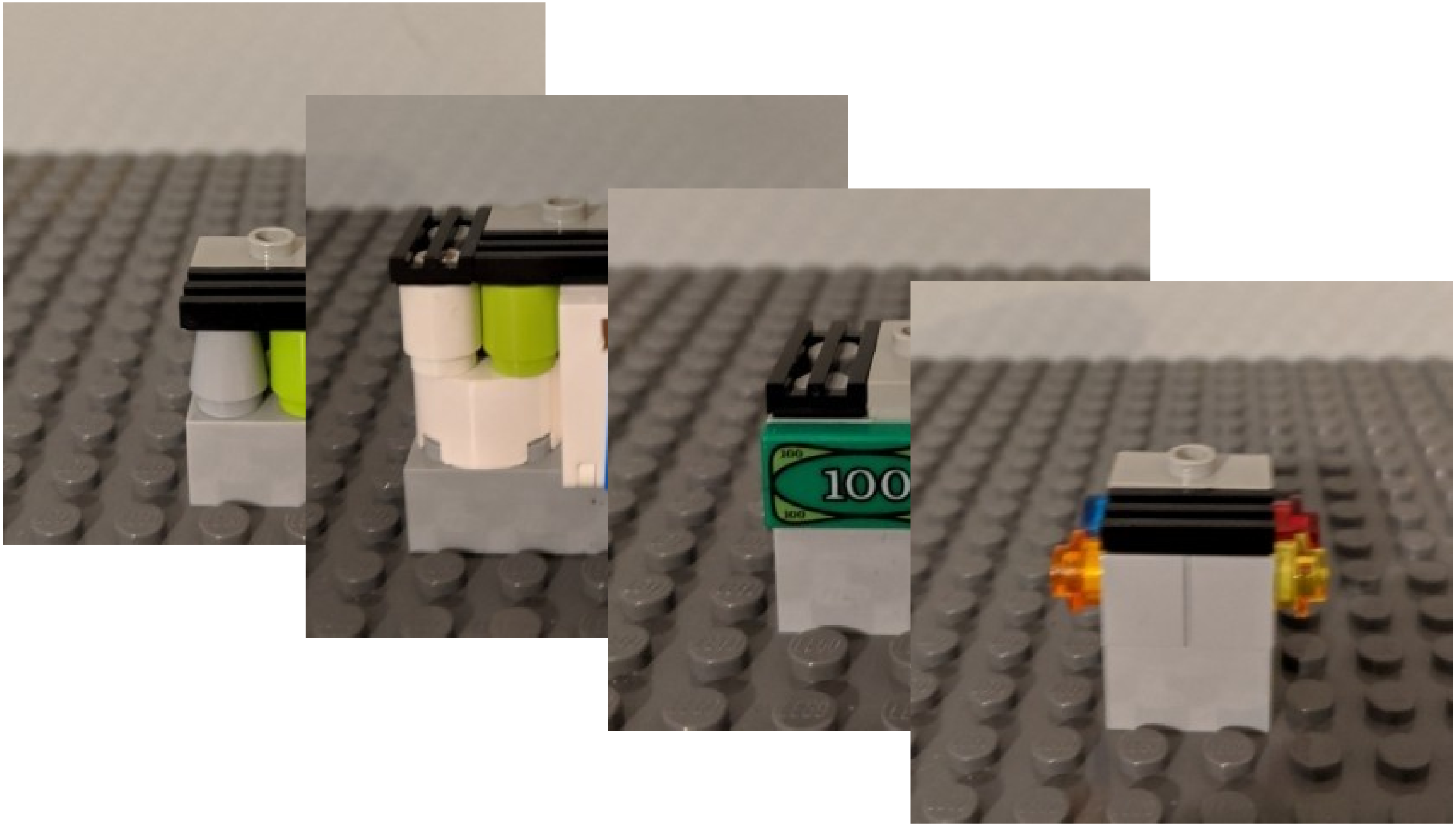
European Union
European Regional Development Fund



Office Assets

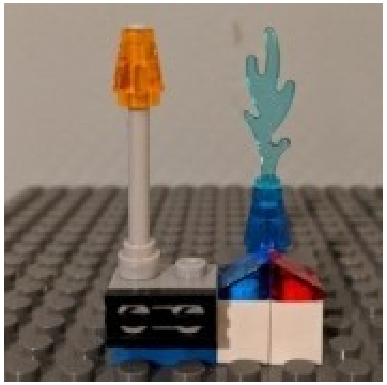


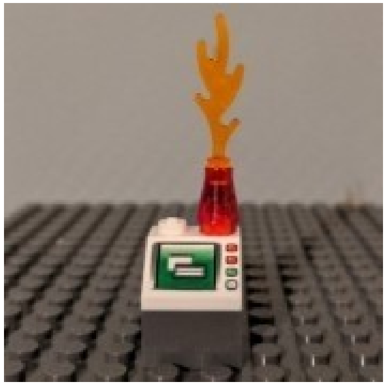
Internet Assets

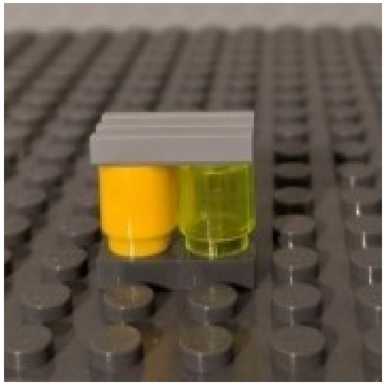


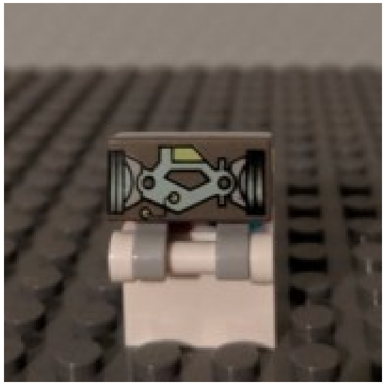
Impementing Controls

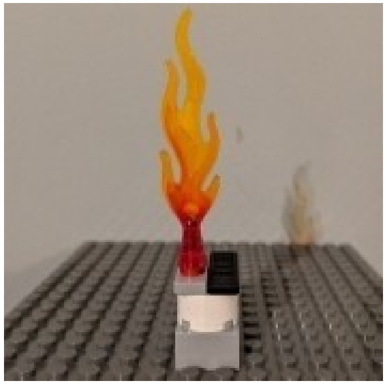
Controls - Technical











Firewalls

Protect devices by setting up rules about what network traffic can go in and out of the device.

2 Factor Auth

Protects a service by ensuring that two methods are used to prove you are a legitimate user

Anti-Malware

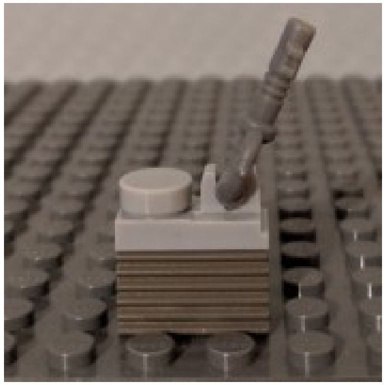
Installed on devices and is able to detect malicious software if it is known about

Controls - Policy

European Union
European Regional Development Fund

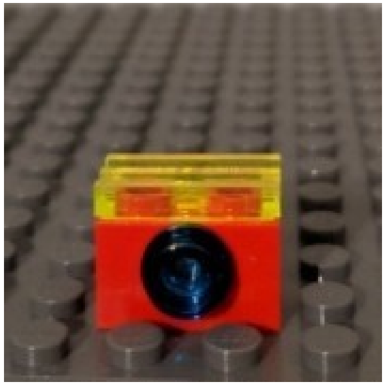
BYOD Policy

Sets up specific policies on the use of personal devices and what control the business has over the device



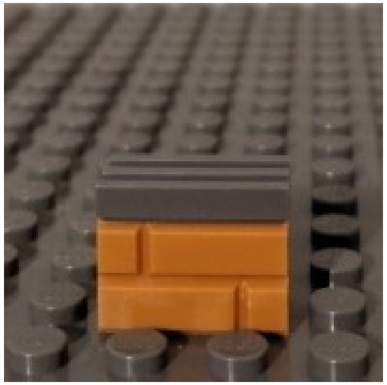
Password and Account Policy

Enforces the use & management of strong passwords alongside making sure only



Patching Policy

Makes sure all devices, operating systems and applications are up to date with the latest software and



Device Hardening

Makes sure all devices have a strong security configuration

Controls - Organisational

European Union
European Regional
Development Fund

Asset and Threat Audit

Assesses your network for security issues and provides threat intelligence on who might

User Training

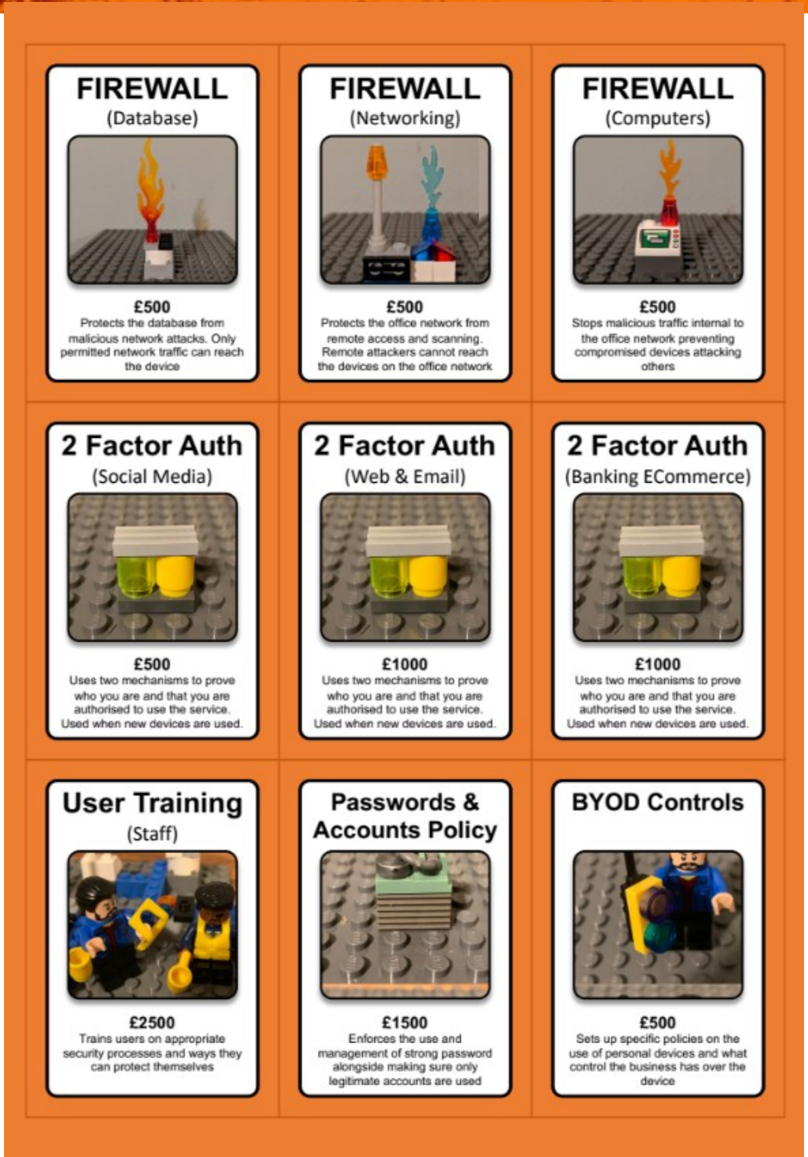
Trains users on appropriate security processes and ways they can protect themselves

Incident Plan

Puts in place a plan in case a security event happens reduces the harm of an security attack

Control Cards

European Union
European Regional
Development Fund



FIREWALL
(Database)
£500
Protects the database from malicious network attacks. Only permitted network traffic can reach the device

FIREWALL
(Networking)
£500
Protects the office network from remote access and scanning. Remote attackers cannot reach the devices on the office network

FIREWALL
(Computers)
£500
Stops malicious traffic internal to the office network preventing compromised devices attacking others

2 Factor Auth
(Social Media)
£500
Uses two mechanisms to prove who you are and that you are authorised to use the service. Used when new devices are used.

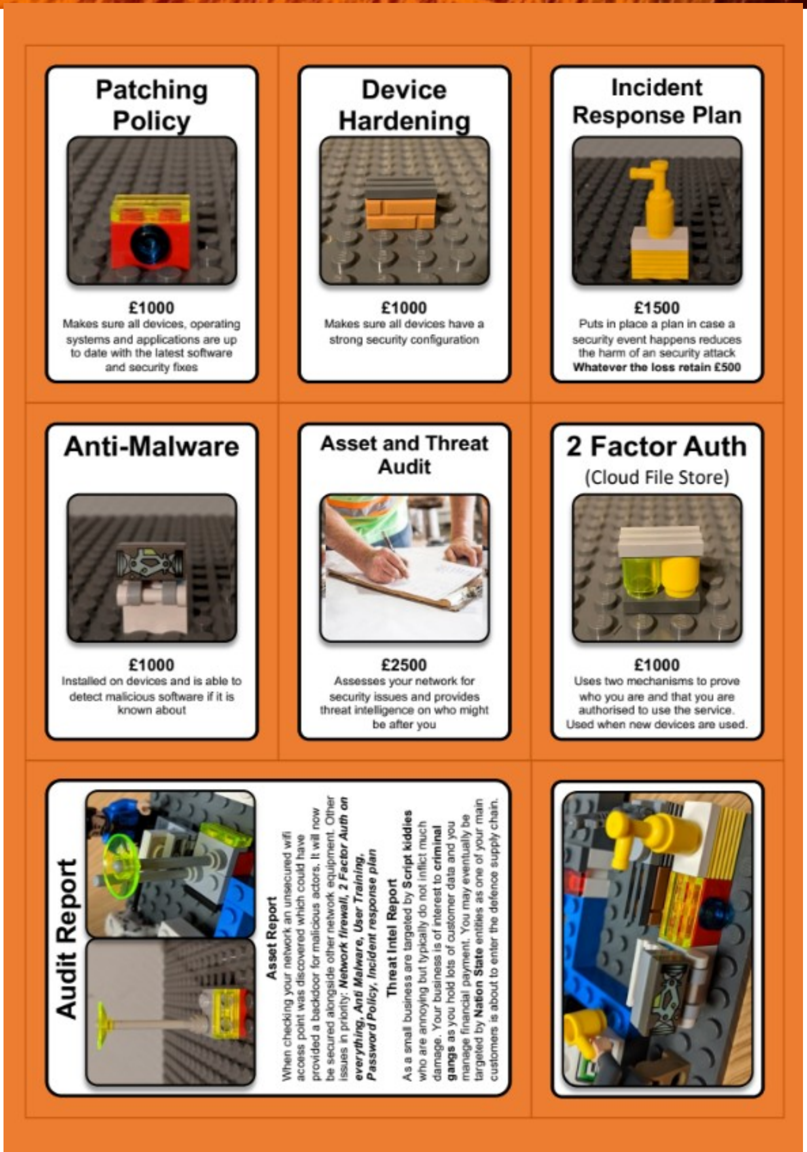
2 Factor Auth
(Web & Email)
£1000
Uses two mechanisms to prove who you are and that you are authorised to use the service. Used when new devices are used.

2 Factor Auth
(Banking ECommerce)
£1000
Uses two mechanisms to prove who you are and that you are authorised to use the service. Used when new devices are used.

User Training
(Staff)
£2500
Trains users on appropriate security processes and ways they can protect themselves

Passwords & Accounts Policy
£1500
Enforces the use and management of strong password alongside making sure only legitimate accounts are used

BYOD Controls
£500
Sets up specific policies on the use of personal devices and what control the business has over the device



Patching Policy
£1000
Makes sure all devices, operating systems and applications are up to date with the latest software and security fixes

Device Hardening
£1000
Makes sure all devices have a strong security configuration

Incident Response Plan
£1500
Puts in place a plan in case a security event happens reduces the harm of an security attack
Whatever the loss retain £500

Anti-Malware
£1000
Installed on devices and is able to detect malicious software if it is known about

Asset and Threat Audit
£2500
Assesses your network for security issues and provides threat intelligence on who might be after you

2 Factor Auth
(Cloud File Store)
£1000
Uses two mechanisms to prove who you are and that you are authorised to use the service. Used when new devices are used.

Audit Report

Asset Report
When checking your network an unsecured wifi access point was discovered which could have provided a backdoor for malicious actors. It will now be secured alongside other network equipment. Other issues in priority: ***Network firewall, 2 Factor Auth on everything, Anti Malware, User Training, Password Policy, Incident response plan***

Threat Intel Report
As a small business are targeted by **Script kiddies** who are annoying but typically do not inflict much damage. Your business is of interest to **criminal gangs** as you hold lots of customer data and you manage financial payment. You may eventually be targeted by **Nation State** entities as one of your main customers is about to enter the defence supply chain.

Example Round 1 - Buy

European Union
European Regional Development Fund

Round & CapEx	Cyber Investment	Cyber Items Bought	Why	Banked	Loss (Total Loss)
1 £2500	£500	- Network Firewalls			
2 £3000	£				
3 £3000	£				

Example Round 1 - Reason

European Union
European Regional
Development Fund

Round & CapEx	Cyber Investment	Cyber Items Bought	Why	Banked	Loss (Total Loss)
1 £2500	£500	• Network Firewalls	To protect the main office network from everything on the internet		
2 £3000	£				
3 £3000	£				

Example Round 1 - Bank

European Union
European Regional Development Fund

Round & CapEx	Cyber Investment	Cyber Items Bought	Why	Banked	Loss (Total Loss)
1 **£2500**	£500	• Network Firewalls	To protect the main office network from everything on the internet	£2000	
2 **£3000**	£				
3 **£3000**	£				

Example Round 1 - Attack

European Union
European Regional
Development Fund

Round & CapEx	Cyber Investment	Cyber Items Bought	Why	Banked	Loss (Total Loss)
1 **£2500**	£500	- Network Firewalls	To protect the main office network from everything on the internet	£2000	£1000 **£1000**
2 **£3000**	£				
3 **£3000**	£				

Example Round 1 - Update

European Union
European Regional
Development Fund

Round & CapEx	Cyber Investment	Cyber Items Bought	Why	Banked	Loss (Total Loss)
1 **£2500**	£500	- Network Firewalls	To protect the main office network from everything on the internet	£2000	£1000 **£1000**
2 **£3000**	£			£1100	
3 **£3000**	£				

Example Round 2 - Buy

European Union
European Regional Development Fund

Round & CapEx	Cyber Investment	Cyber Items Bought	Why	Banked	Loss (Total Loss)
1 **£2500**	£500	• Network Firewalls	To protect the main office network from everything on the internet	£2000	£1000 **£1000**
2 **£3000**	£1000	• External Penetration Testing		£1000	
3					

Example Round 2 - Reason

Round & CapEx	Cyber Investment	Cyber Items Bought	Why	Banked	Loss (Total Loss)
1 **£2500**	£500	- Network Firewalls	To protect the main office network from everything on the internet	£2000	£1000 **£1000**
2 **£3000**	£1000	- External Penetration Testing	To find out our weaknesses	£1000	
3					

Example Round 2 - Bank

European Union
European Regional
Development Fund

Round & CapEx	Cyber Investment	Cyber Items Bought	Why	Banked	Loss (Total Loss)
1 **£2500**	£500	• Network Firewalls	To protect the main office network from everything on the internet	£2000	£1000 **£1000**
2 **£3000**	£1000	• External Penetration Testing	To find out our weaknesses	£1000 £2000	
3					

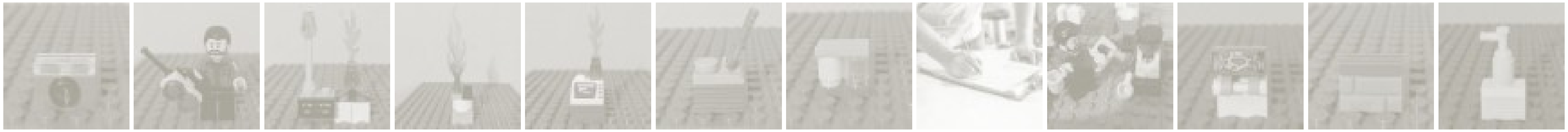
Example Round 2 - Attack

European Union
European Regional
Development Fund

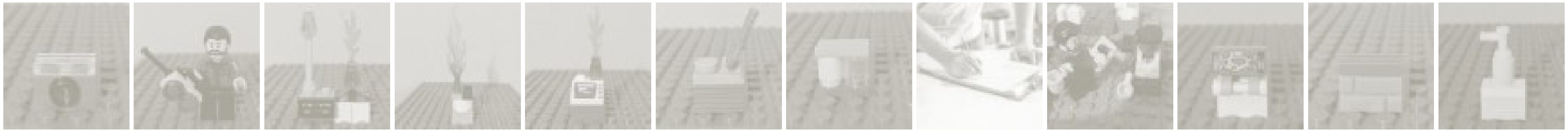
Round & CapEx	Cyber Investment	Cyber Items Bought	Why	Banked	Loss (Total Loss)
1 **£2500**	£500	• Network Firewalls	To protect the main office network from everything on the internet	£2000	£1000 **£1000**
2 **£3000**	£1000	• External Penetration Testing	To find out our weaknesses	£1000 £2000	£2000 **£1500**
3					

Game Progression

European Union
European Regional
Development Fund



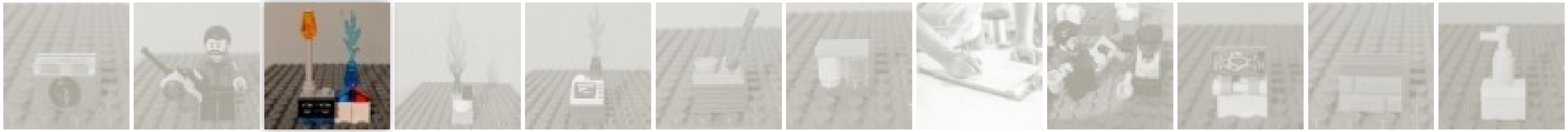
Round 1 – Buy and Decide



Round 1 – Scanning

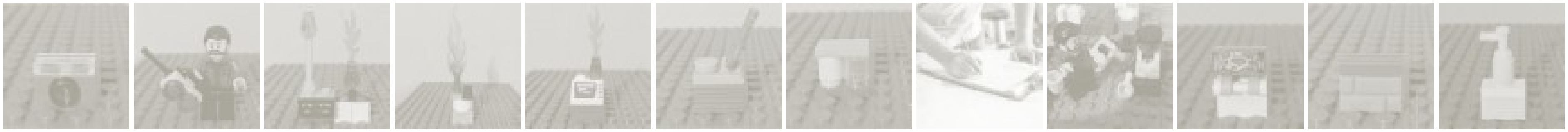
Script Kiddies

- They are scanning your network to find vulnerabilities
- No real impact but you don’t know what they will do next



Round 2 – Buy and Decide

European Union
European Regional
Development Fund

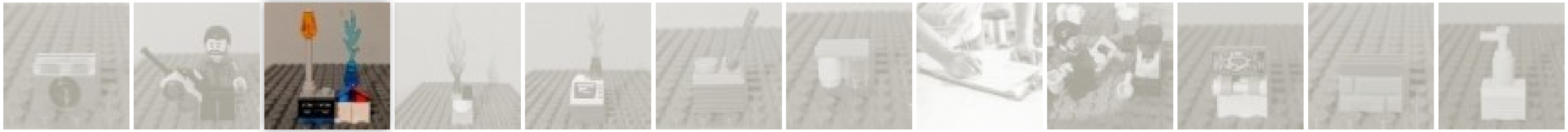


Round 2 – Denial of Service

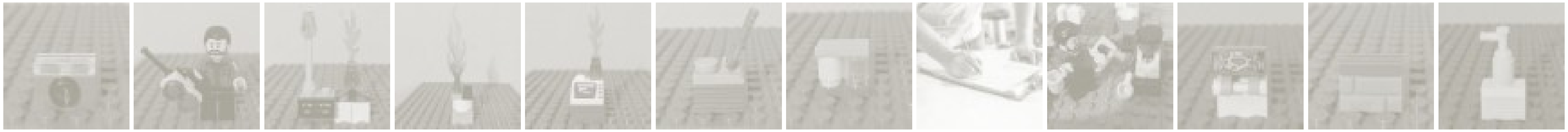
European Union
European Regional
Development Fund

Script Kiddies

- Based on their scans the attackers launch a denial of service ransom attack
- Lose £1000 from your reserves to deal with the loss of work time



Round 3 – Buy and Decide



Round 3a – Social Media Defacement

Script Kiddie

- The attacker has brute forced your passwords on your social media
- Public humiliation. Lose £500 from reserves

Round 3b – Ecommerce Attack

European Union
European Regional Development Fund

Script Kiddie

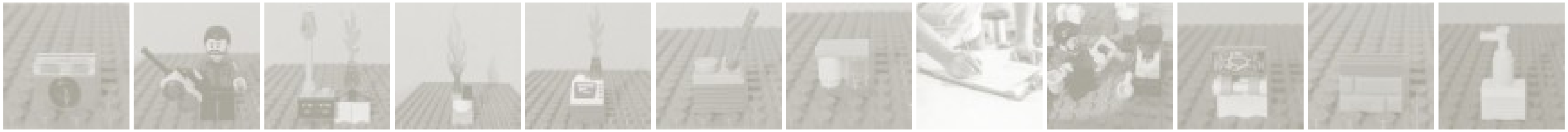
- The attacker has brute forced your passwords on your social media
- Public humiliation. Lose £500 from reserves

Criminal Gang

- A criminal Gang has targeted you brute forcing you passwords on ecommerce
- Lose all but £500 from your reserves

Round 4 – Buy and Decide

European Union
European Regional
Development Fund



Round 4a – Website Defacement

Script Kiddie

- Targets your webservice and brute forces password
- Public embarrassment. Lose £500 from reserves

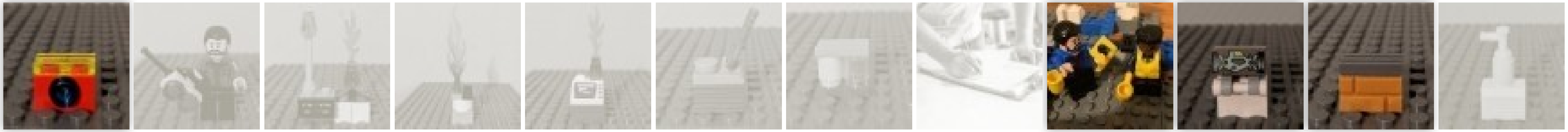
Round 4b – Social Engineering

Script Kiddie

- Targets your webservice and brute forces password
- Public embarrassment. Lose £500 from reserves

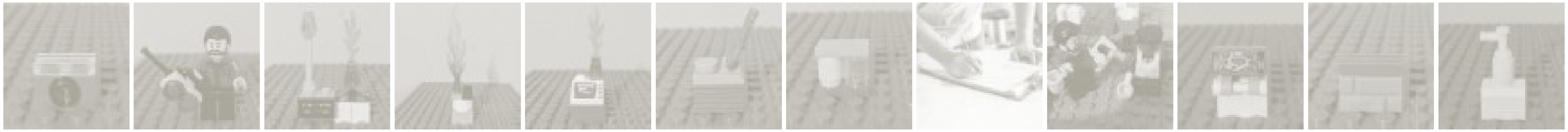
Criminal Gang

- Drop pen drives near your office with ransomware
- Lose £1,000 from your reserves



Round 5 – Buy and Decide

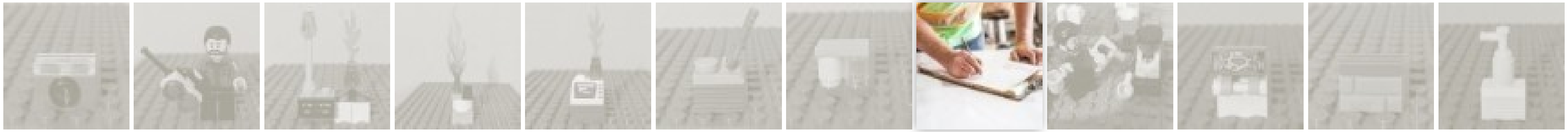
European Union
European Regional
Development Fund



Round 5a – Hidden Wifi Access

Criminal Gang

- They find a hidden Wi-Fi access point on your network. Attack Client database with a 0-day vulnerability
- Steal GDPR-covered data. Lose 50% (rounding up to nearest £500) from reserves



Round 5a – Hidden Wifi Access

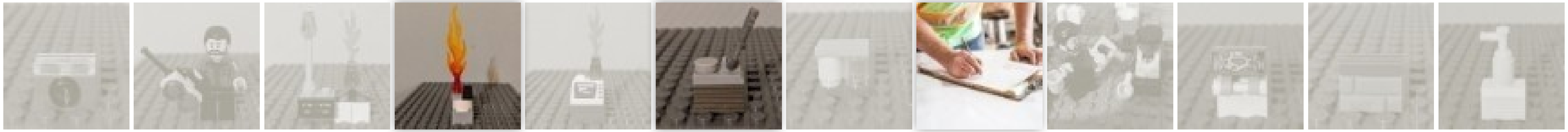
European Union
European Regional Development Fund

Criminal Gang

- They find a hidden wifi access point on your network. Attack Client database with a 0-day vulnerability
- Steal GDPR-covered data. Lose 50% (rounding up to nearest £500) from reserves

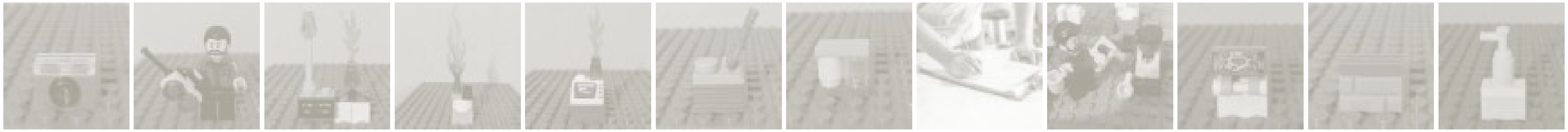
Nation State

- Using the same access point and brute force weak passwords on user machines
- Steal IP data
- Lose £1,500 from reserves



Round 6 – Buy and Decide

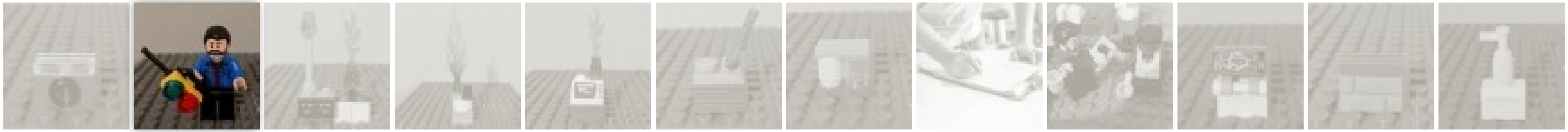
European Union
European Regional
Development Fund



Round 6a – BYOD Attack

Criminal Gang

- Targets personal devices to steal client Data so GDPR breach
- Lose 50% (rounding up to nearest £500) from reserves



Round 6a – BYOD Attack

European Union
European Regional
Development Fund

Criminal Gang

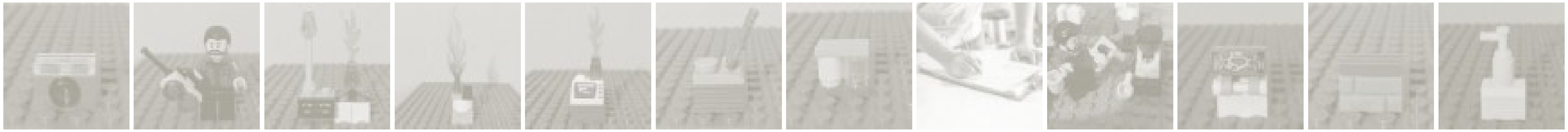
- Targets personal devices to steal client Data so GDPR breach
- Lose 50% (rounding up to nearest £500) from reserves

Script Kiddies

- Targets your Cloud File Store and brute forces a password
- Steal a load of data about the company and publishes it online
- Lose £1,500 from the reserves

Round 7 – Buy and Decide

European Union
European Regional
Development Fund

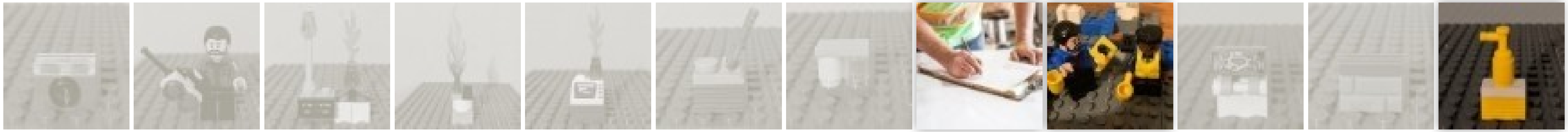


Round 7 – Nation State 0-day

European Union
European Regional Development Fund

Nation State

- A nation state targets you with sophisticated 0-day attacks to get to your one of you new clients
  - The NCSC notifies you have been successfully attacked
- The nation state attempts to breach the client and compromise their systems
- Lose (rounding up):
  - all reserves if no incident response plan
  - 50% of reserves (rounding up) if you have staff training & asset/threat intel
  - 25% of reserves (rounding up) (leaving at least £500) if incident response plan in place



Greater Manchester | Greater Security | Greater Business

Cyber Foundry

The Online Game

European Union
European Regional
Development Fund

Lancaster University

MANCHESTER 1824
The University of Manchester

Manchester Metropolitan University

University of Salford MANCHESTER

The Online Game

European Union
European Regional Development Fund

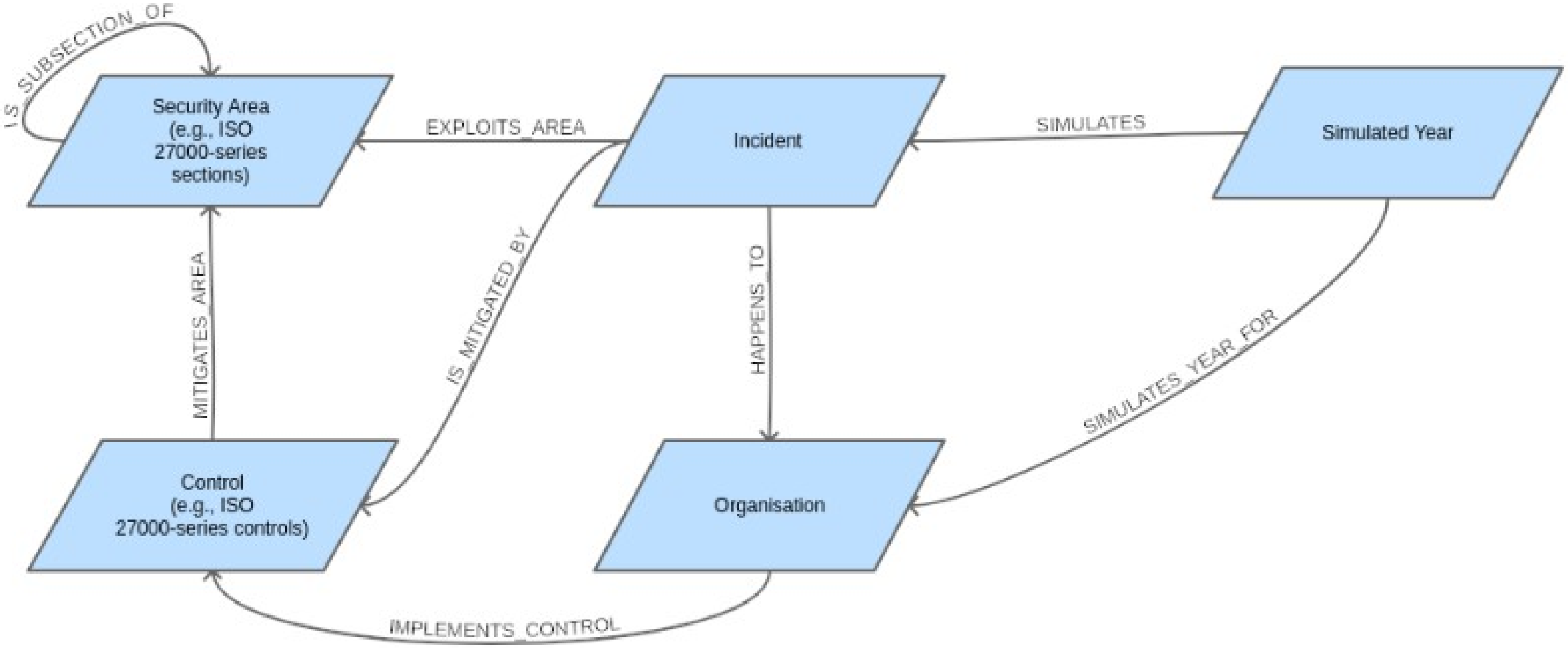
Everyone’s stuck at home, and we can’t run in-person workshops any more

How can we extend the idea?

1. Online play
2. Non-deterministic (i.e., make it replayable)
3. Multiplayer (both competitive and co-operative)

Data Architecture

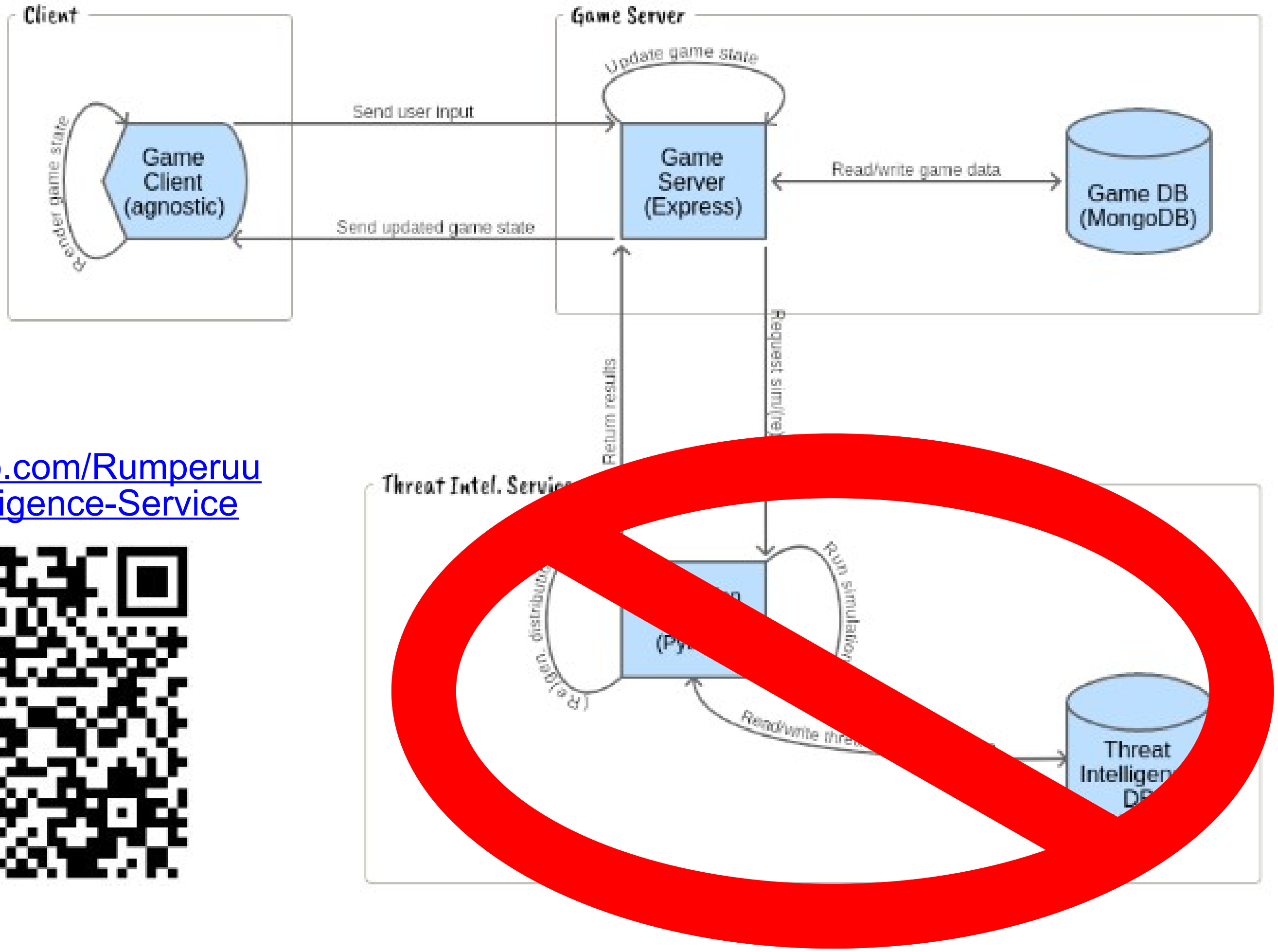
European Union
European Regional Development Fund



Data Source: Cyber Security Breaches Survey 2020

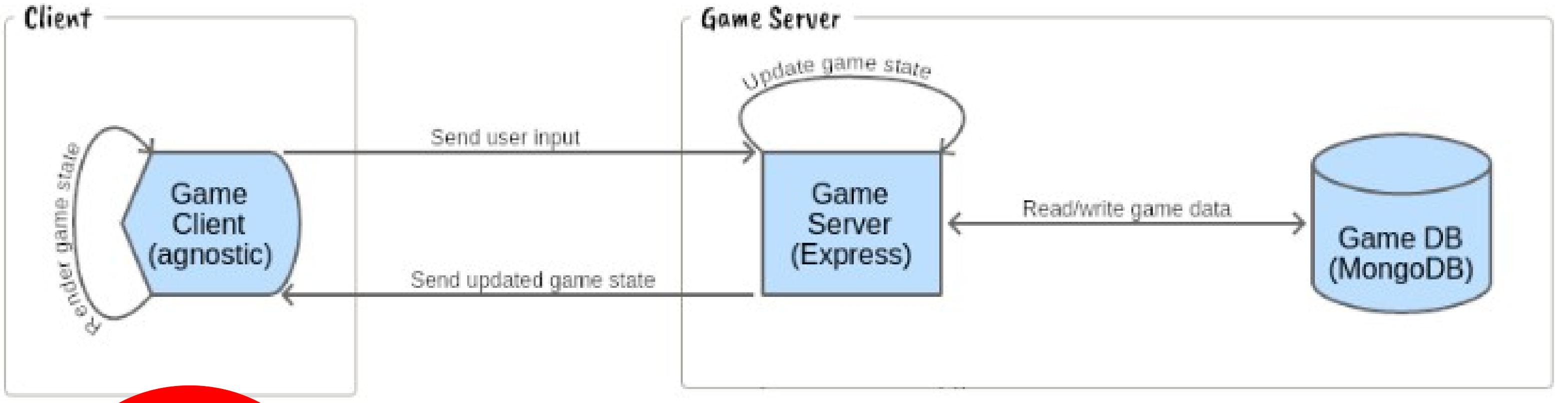
System Architecture

European Union
European Regional
Development Fund



https://github.com/Rumperuu/Threat-Intelligence-Service

System Architecture



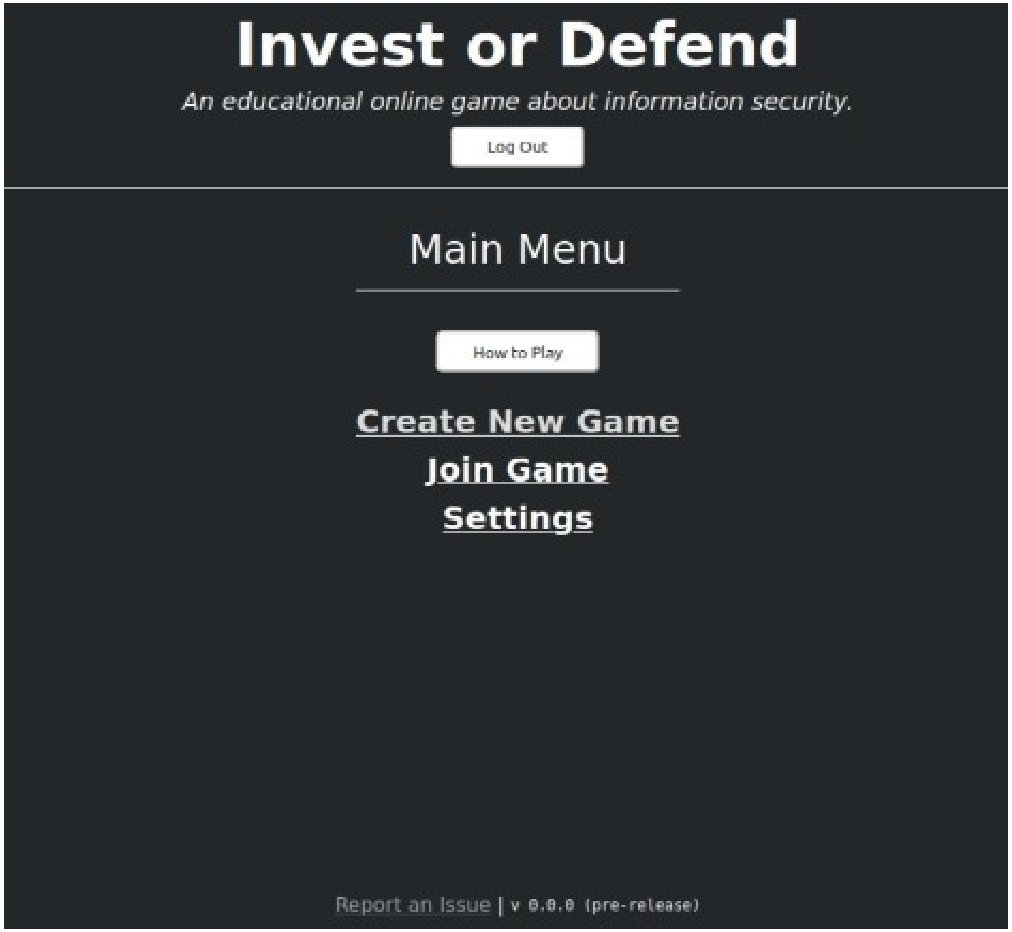
Express

mongoDB®

TS TypeScript

System Architecture

European Union
European Regional
Development Fund



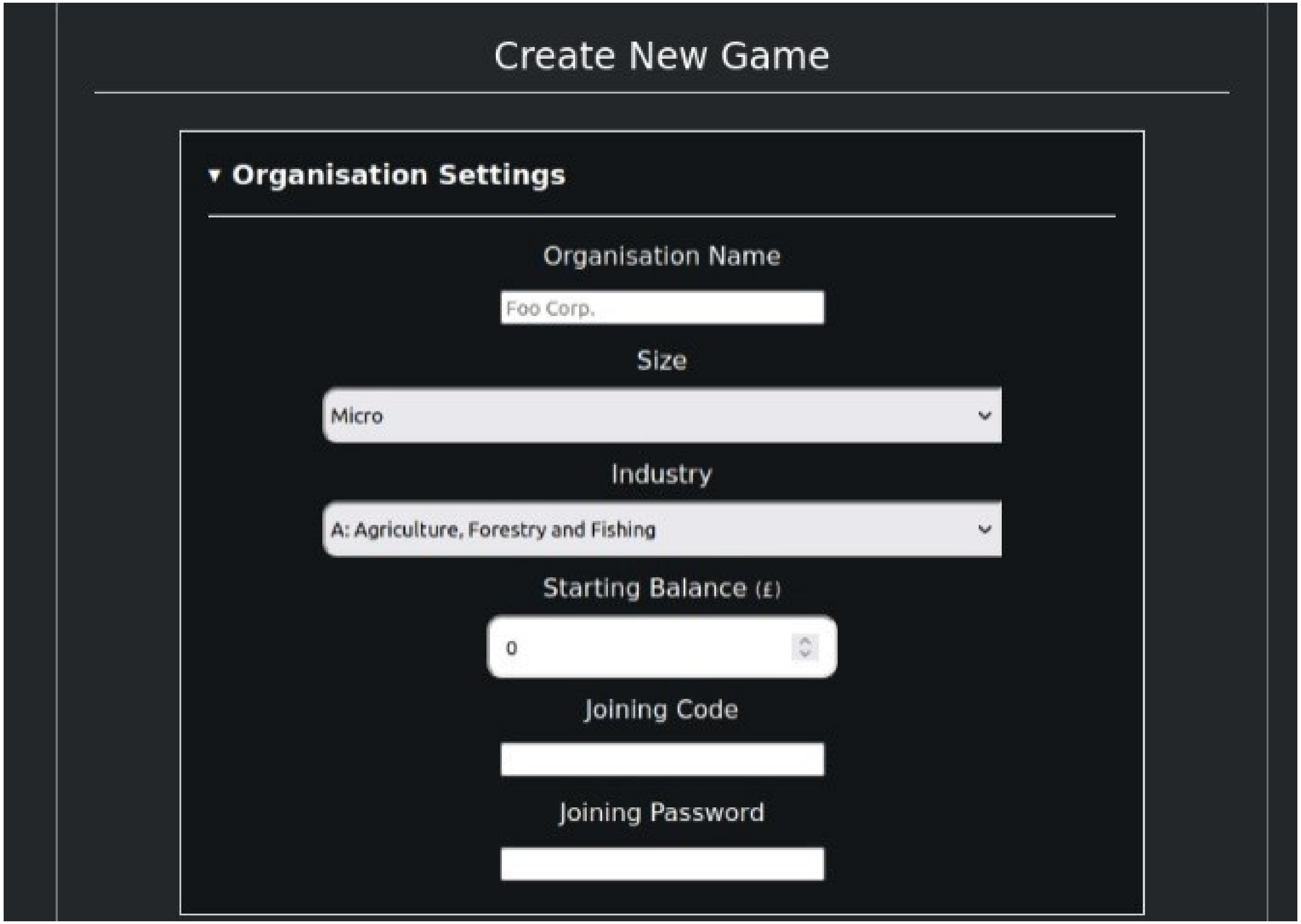
Invest or Defend

An educational online game about information security.

Main Menu

System Architecture

European Union
European Regional
Development Fund



Create New Game

▾ Organisation Settings

Organisation Name

Foo Corp.

Size

Micro

Industry

A: Agriculture, Forestry and Fishing

Starting Balance (£)

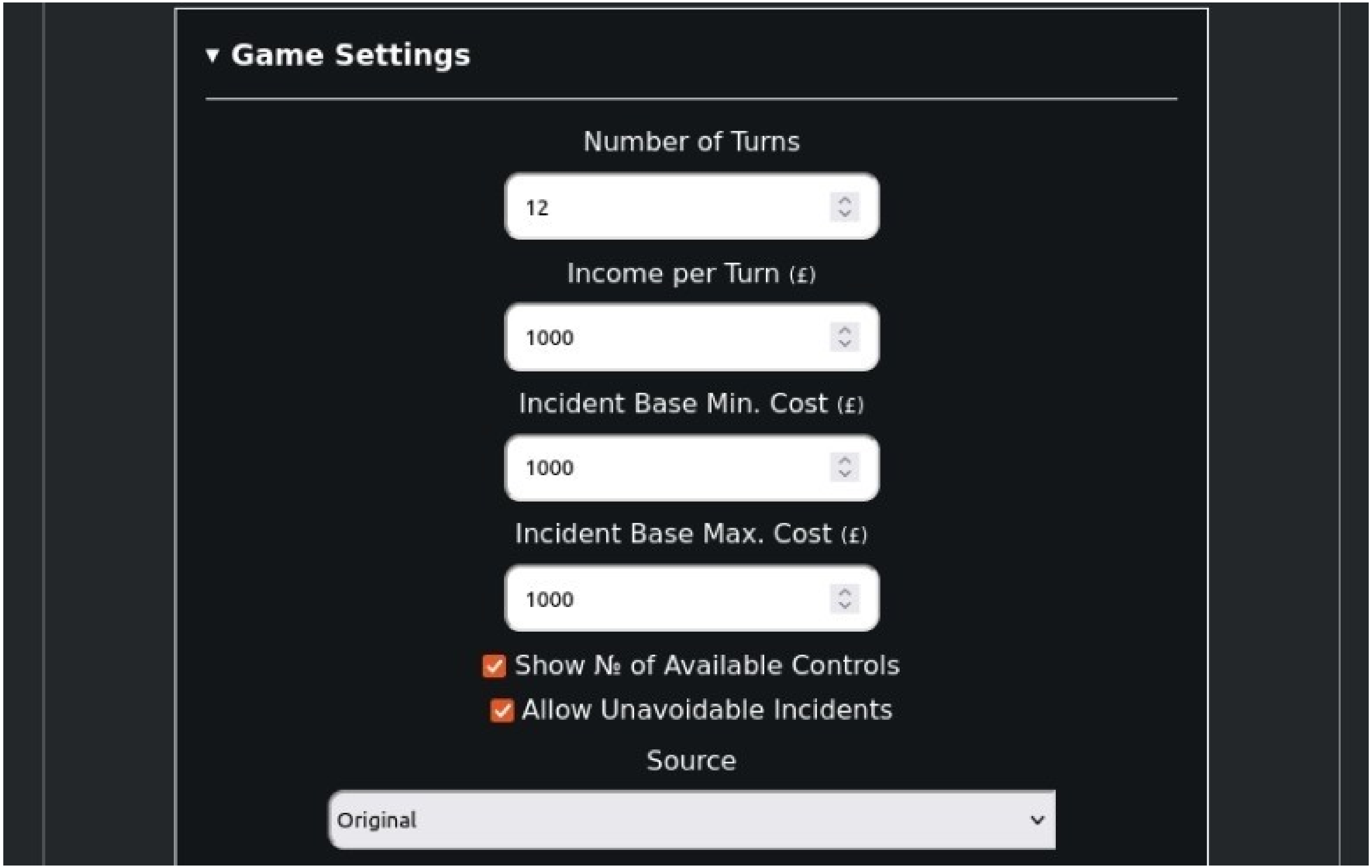
0

Joining Code

Joining Password

System Architecture

European Union
European Regional
Development Fund



▾ Game Settings

Number of Turns

12

Income per Turn (£)

1000

Incident Base Min. Cost (£)

1000

Incident Base Max. Cost (£)

1000

☑ Show № of Available Controls

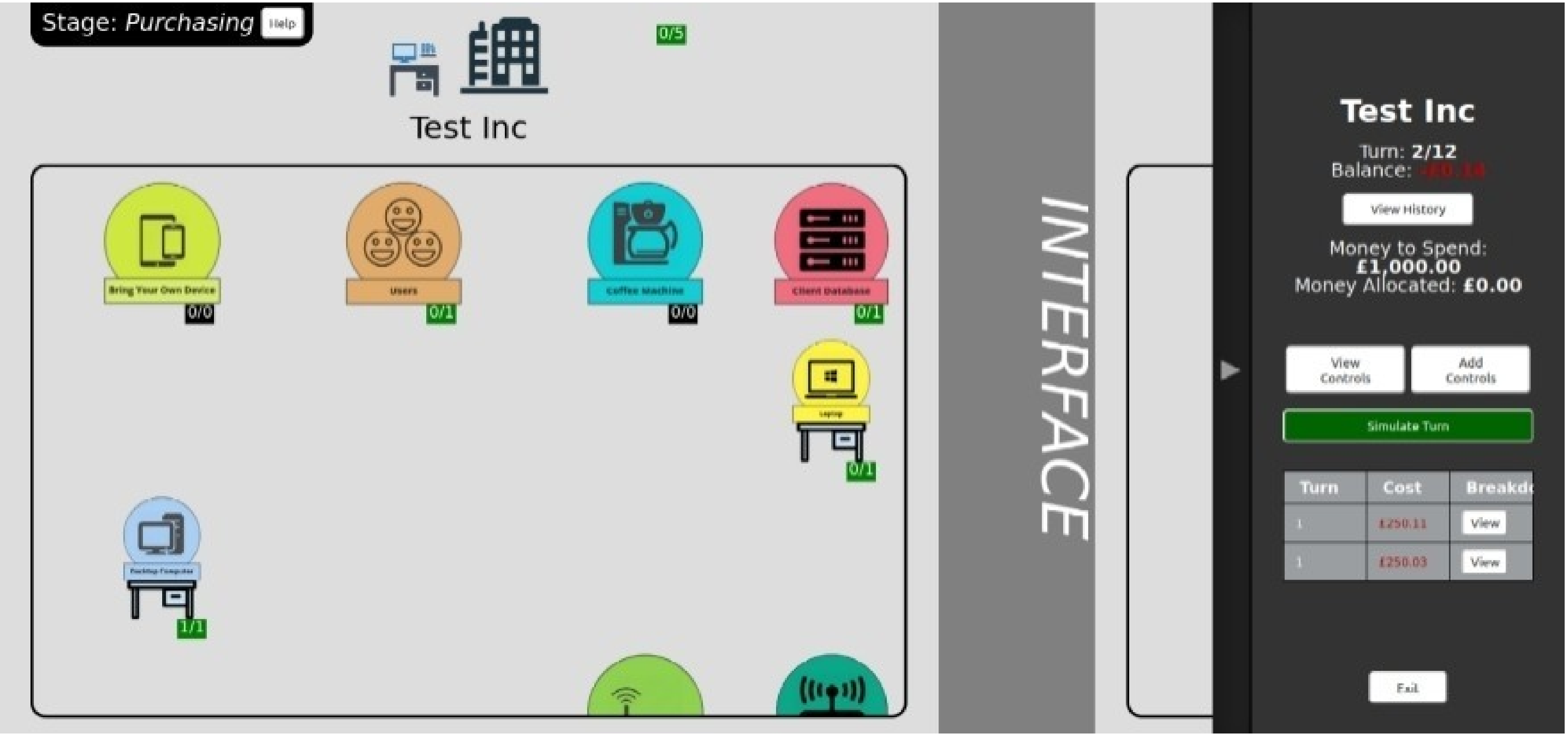
☑ Allow Unavoidable Incidents

Source

Original

System Architecture

European Union
European Regional
Development Fund



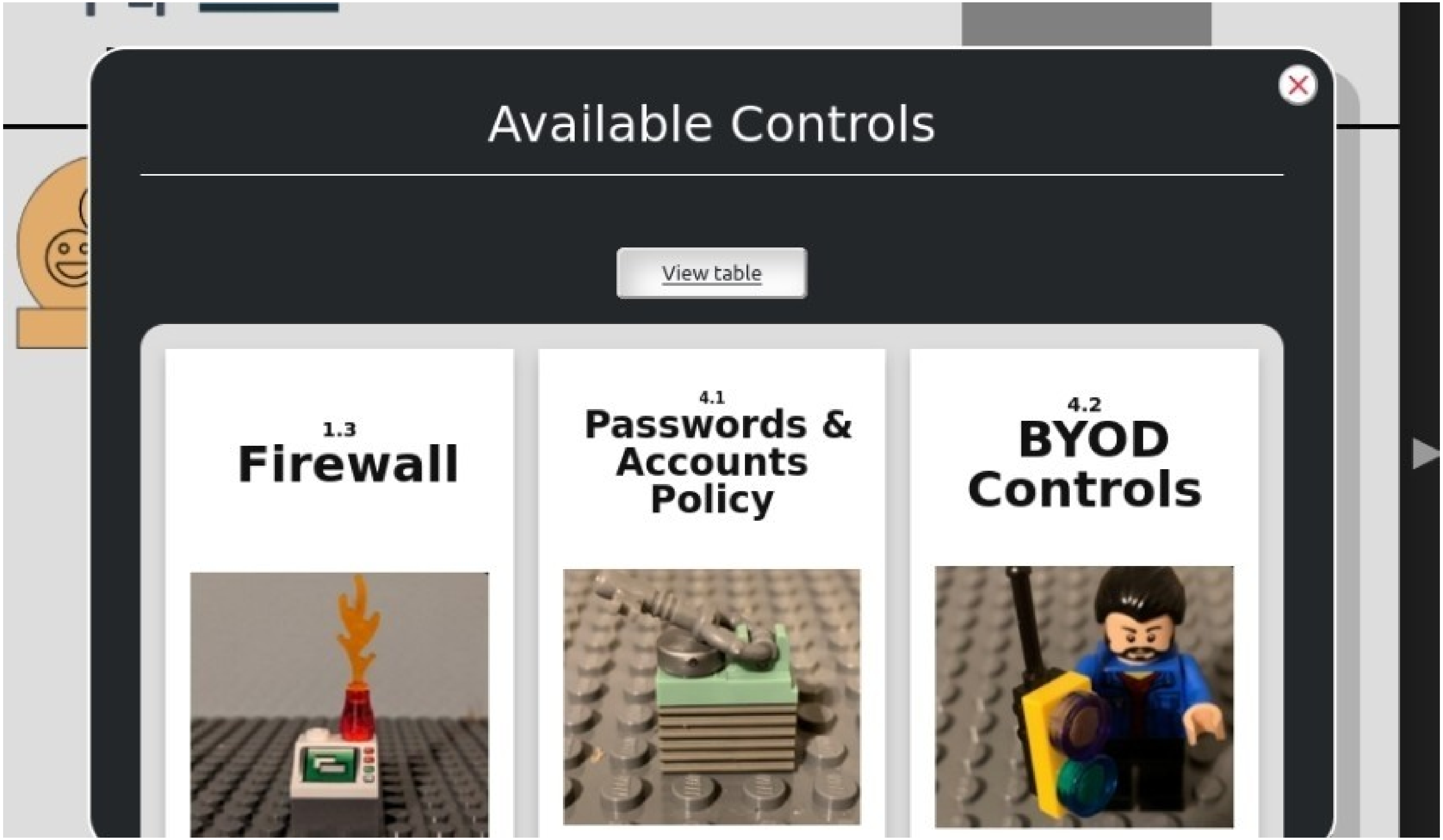
Test Inc

Turn: **2/12**
Balance: [illegible]

Money to Spend:
£1,000.00
Money Allocated: **£0.00**

Turn	Cost	Breakdo
1	£250.11	View
1	£250.03	View

System Architecture



Available Controls

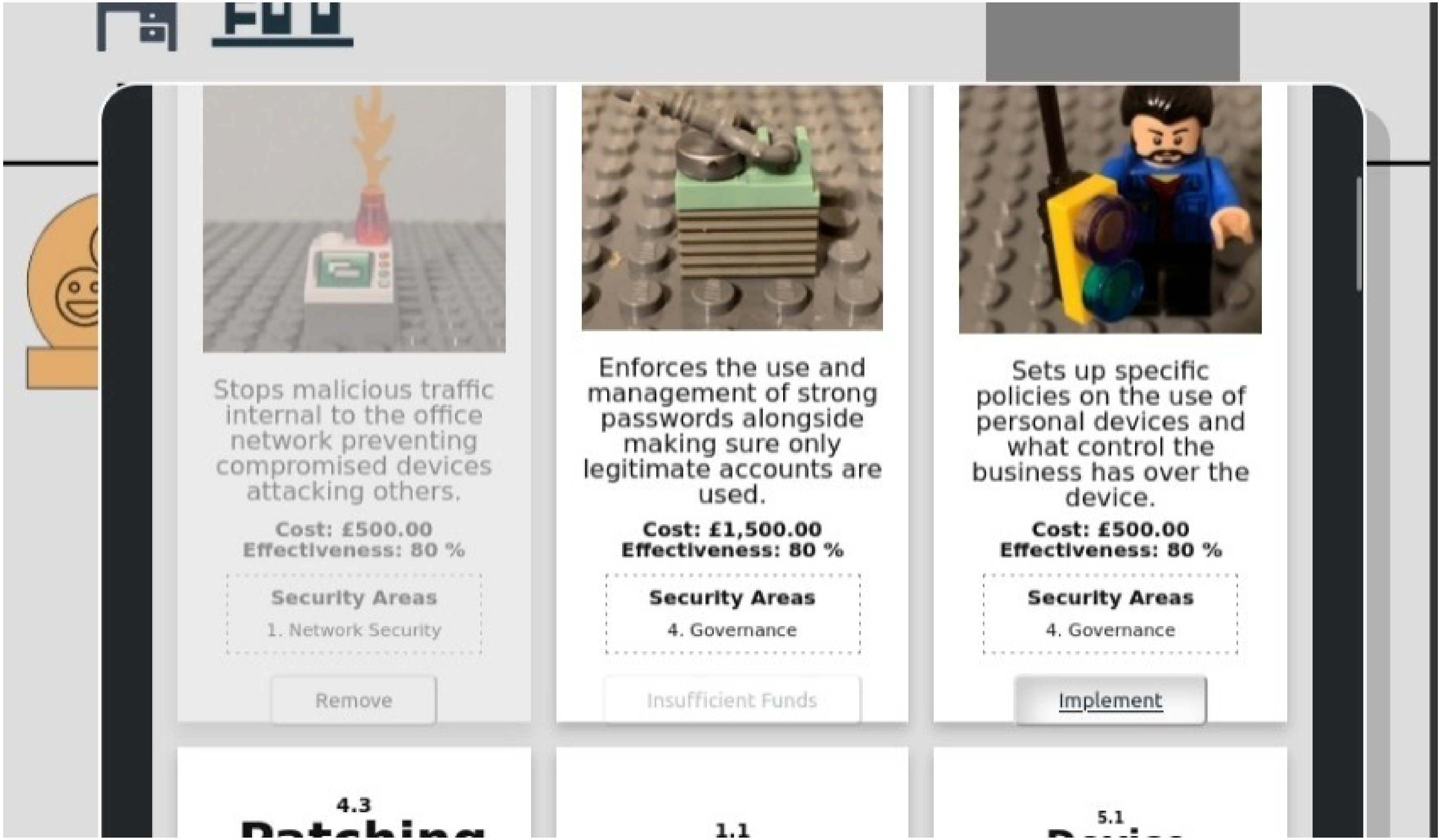
View table

1.3
Firewall

4.1
Passwords & Accounts Policy

4.2
BYOD Controls

System Architecture



Stops malicious traffic internal to the office network preventing compromised devices attacking others.

Cost: £500.00
Effectiveness: 80 %

Security Areas
1. Network Security

Enforces the use and management of strong passwords alongside making sure only legitimate accounts are used.

Cost: £1,500.00
Effectiveness: 80 %

Security Areas
4. Governance

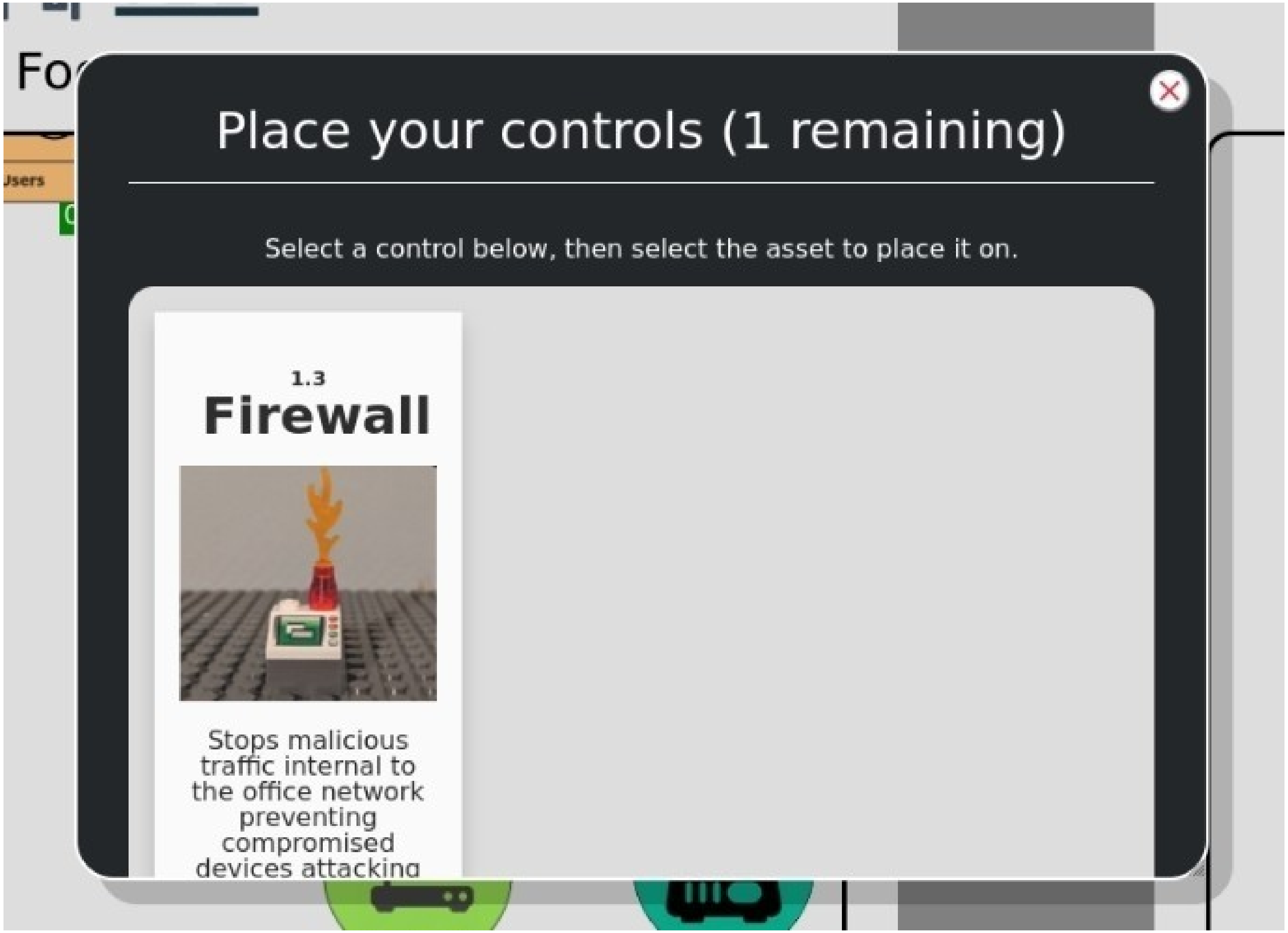
Sets up specific policies on the use of personal devices and what control the business has over the device.

Cost: £500.00
Effectiveness: 80 %

Security Areas
4. Governance

System Architecture

European Union
European Regional
Development Fund



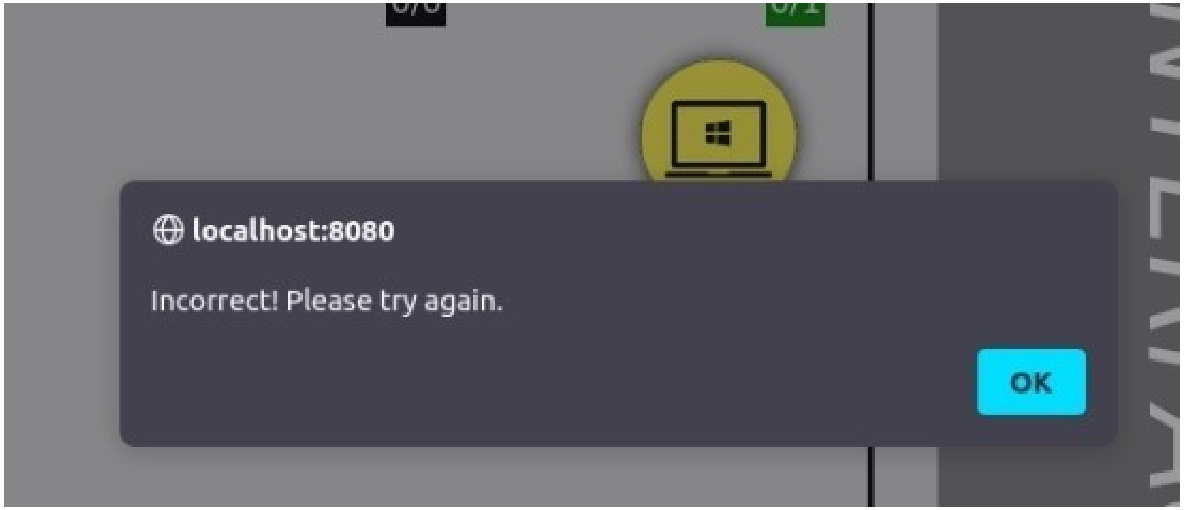
Place your controls (1 remaining)

Select a control below, then select the asset to place it on.

1.3
Firewall

Stops malicious traffic internal to the office network preventing compromised devices attacking

System Architecture

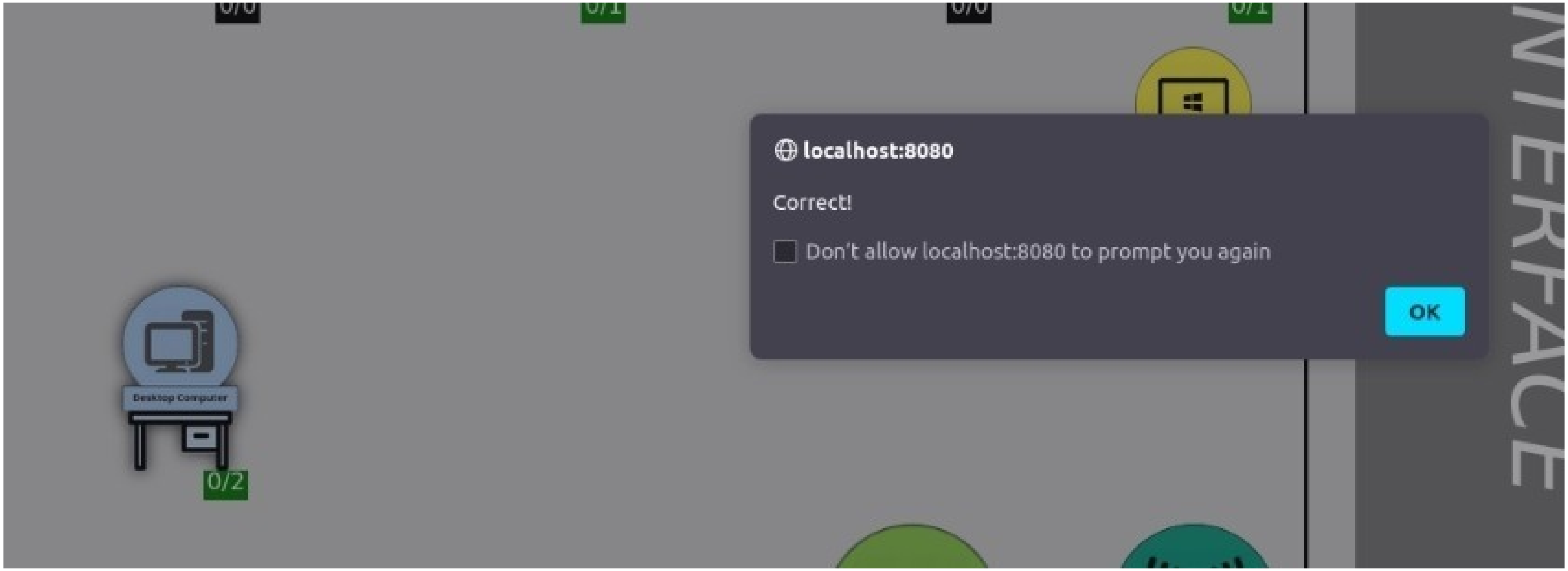


localhost:8080

Incorrect! Please try again.

System Architecture

European Union
European Regional Development Fund

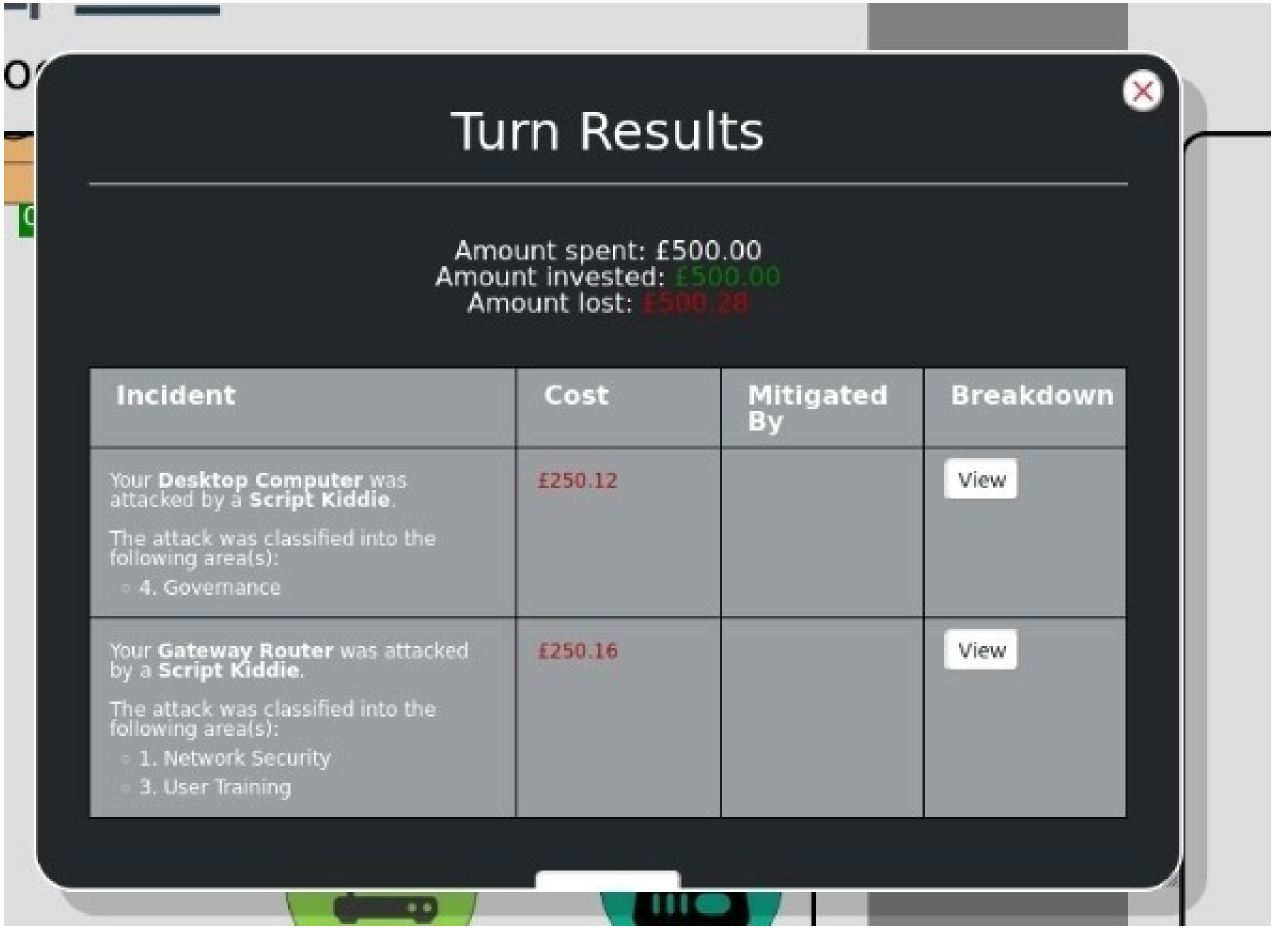


localhost:8080

Correct!

□ Don't allow localhost:8080 to prompt you again

System Architecture

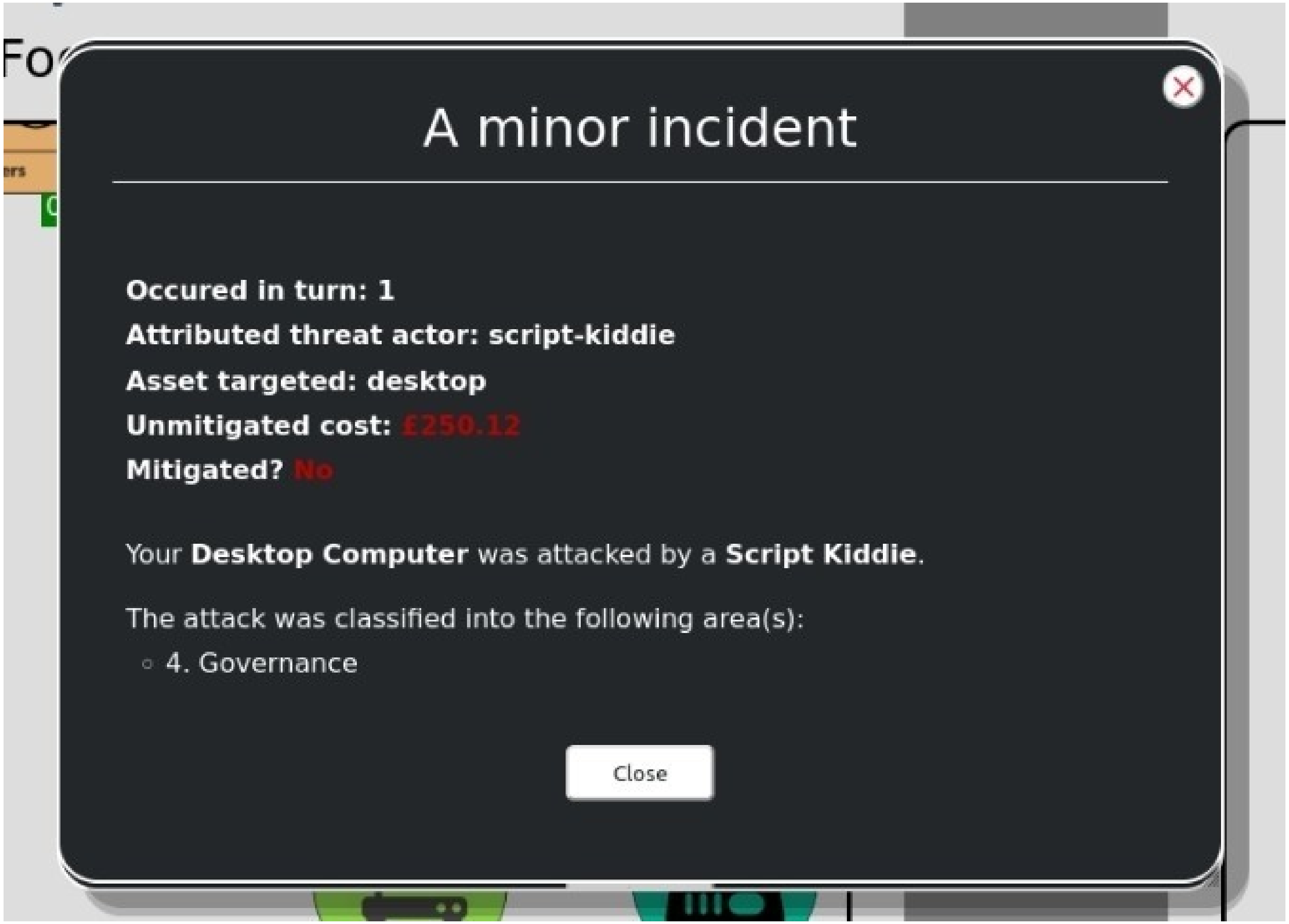


Turn Results

Amount spent: £500.00
Amount invested: £500.00
Amount lost: £500.28

Incident	Cost	Mitigated By	Breakdown
Your **Desktop Computer** was attacked by a **Script Kiddie**. The attack was classified into the following area(s): ○ 4. Governance	£250.12		View
Your **Gateway Router** was attacked by a **Script Kiddie**. The attack was classified into the following area(s): ○ 1. Network Security ○ 3. User Training	£250.16		View

System Architecture



A minor incident

Occured in turn: 1

Attributed threat actor: script-kiddie

Asset targeted: desktop

Unmitigated cost: £250.12

Mitigated? No

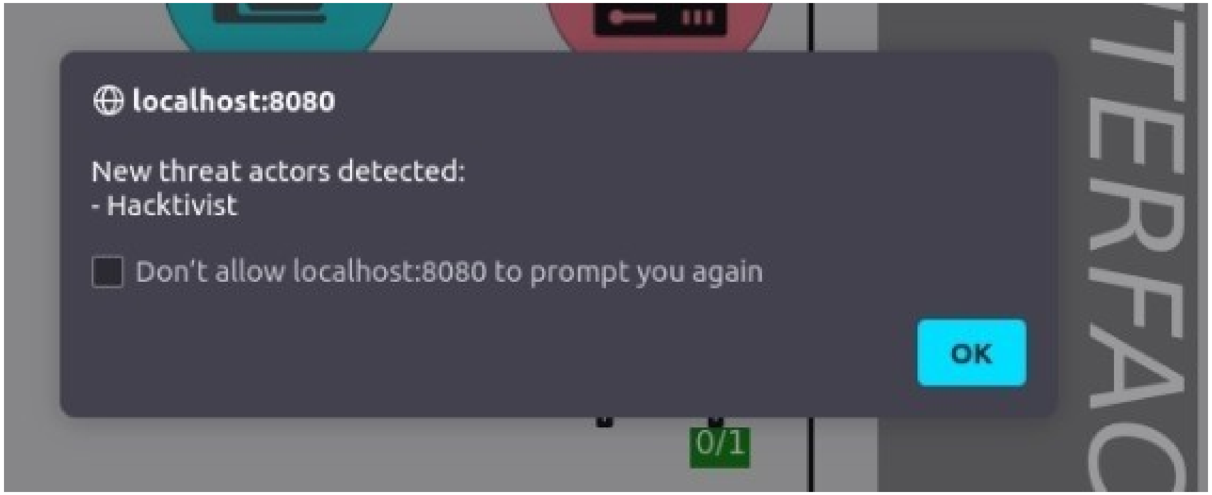
Your **Desktop Computer** was attacked by a **Script Kiddie**.

The attack was classified into the following area(s):

- 4. Governance

System Architecture

European Union
European Regional
Development Fund



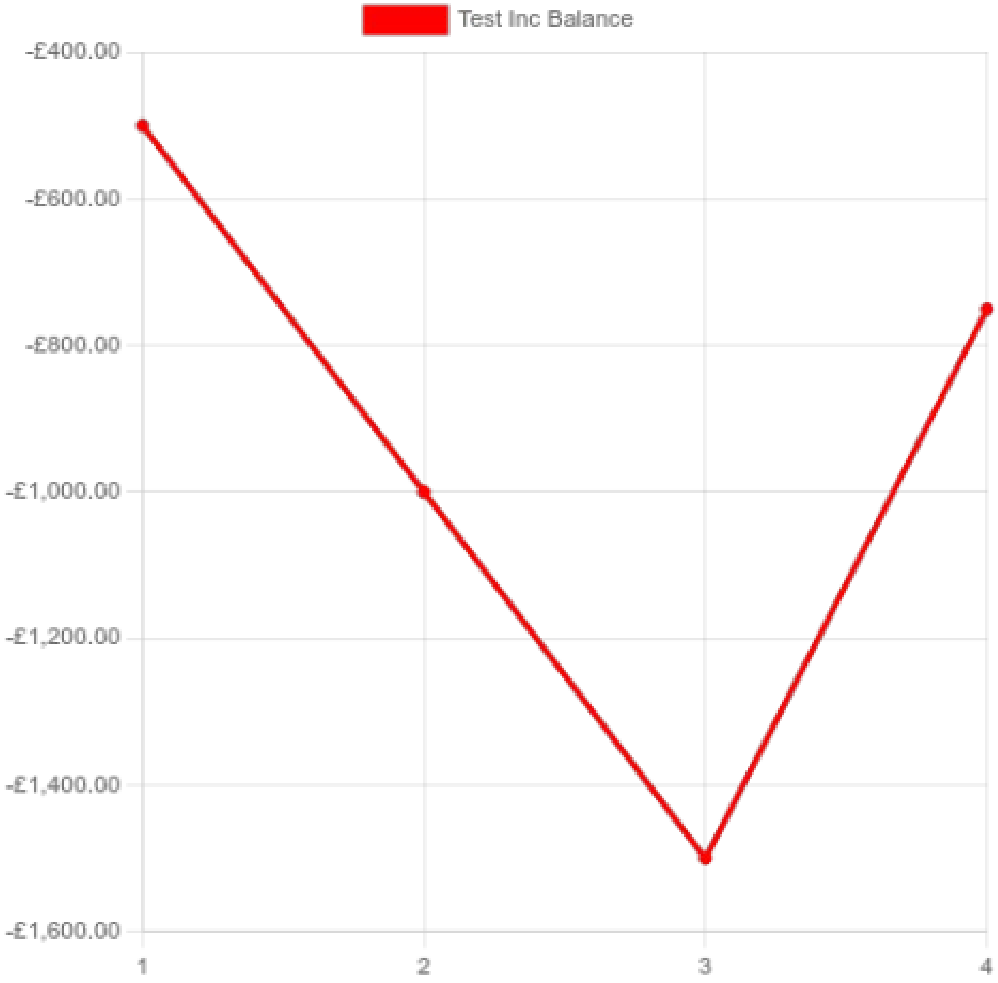
localhost:8080

New threat actors detected:
- Hacktivist

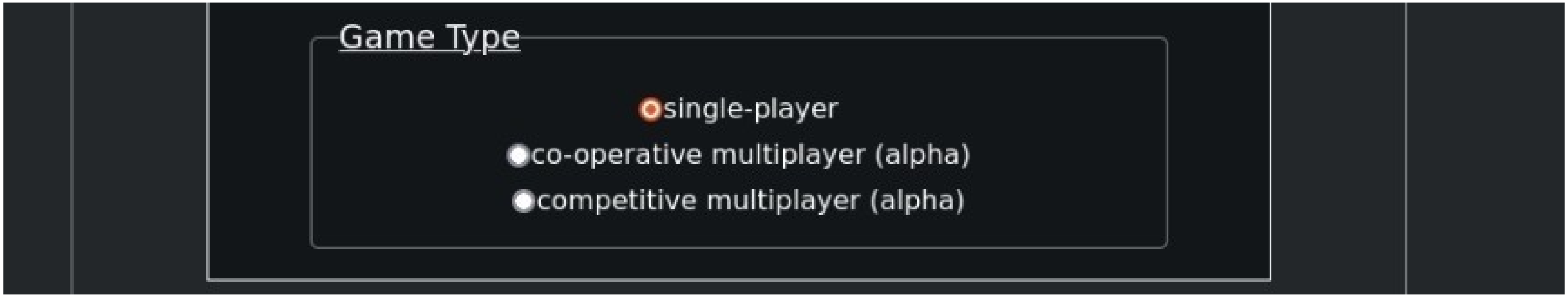
□ Don't allow localhost:8080 to prompt you again

System Architecture

European Union
European Regional
Development Fund



System Architecture

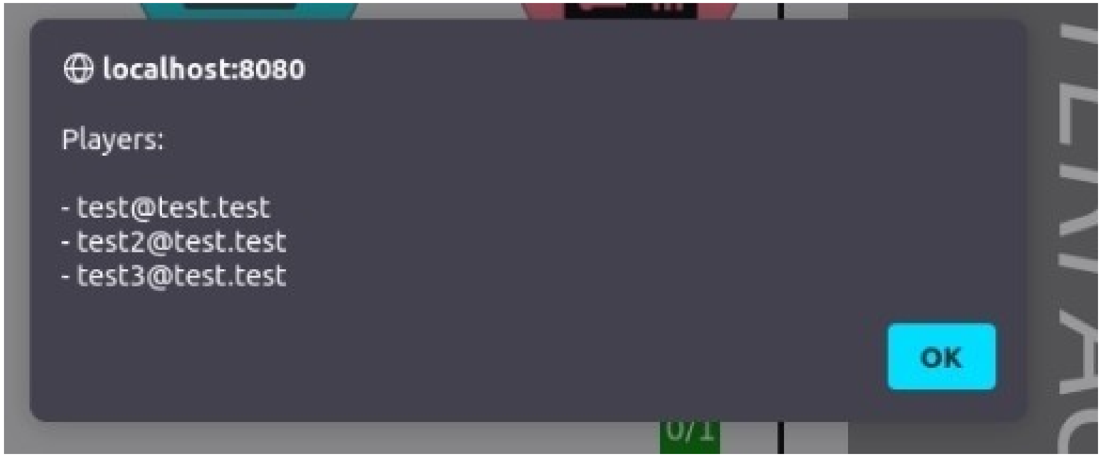


Game Type

● single-player
○ co-operative multiplayer (alpha)
○ competitive multiplayer (alpha)

System Architecture

European Union
European Regional
Development Fund



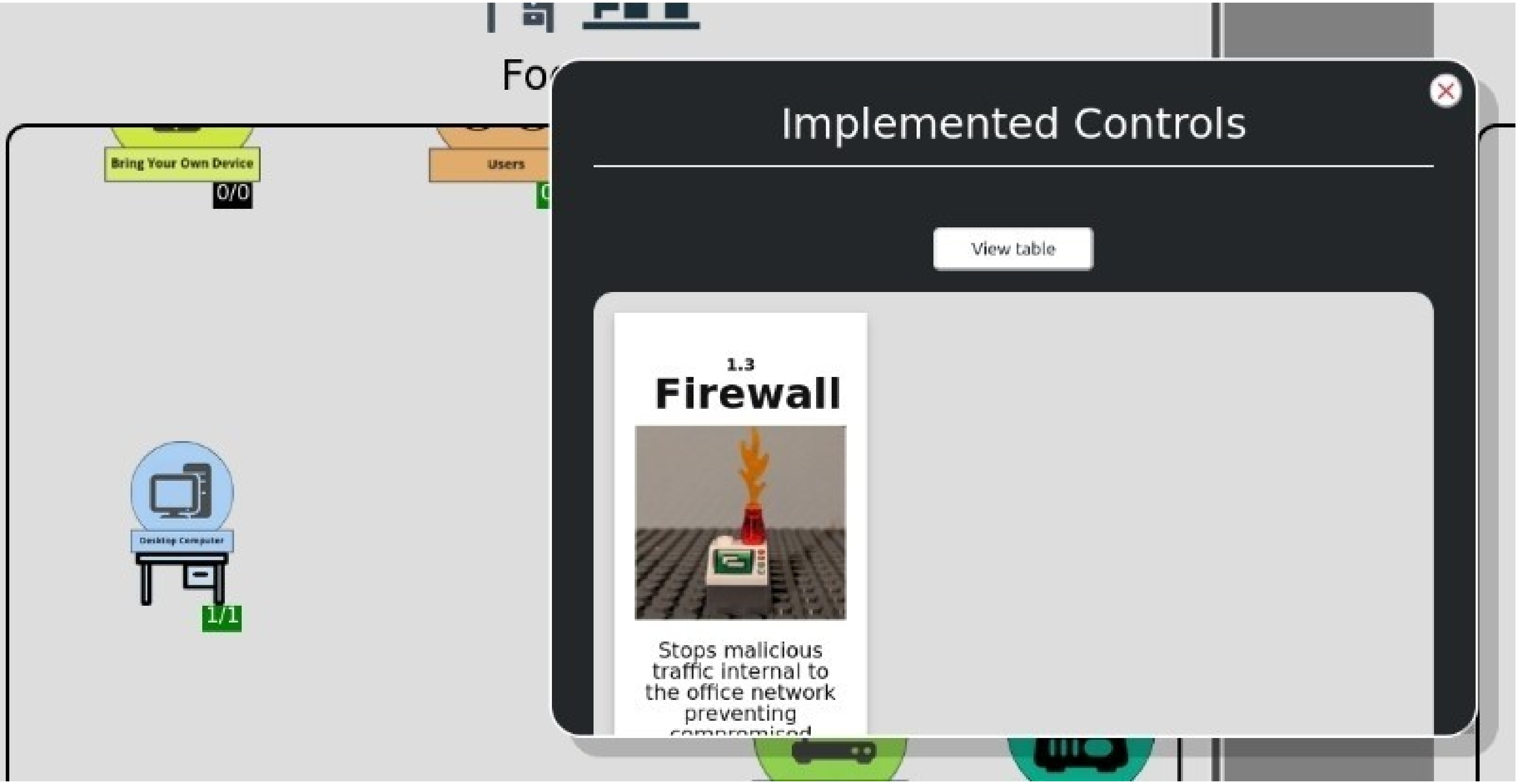
localhost:8080

Players:

- test@test.test
- test2@test.test
- test3@test.test

System Architecture

European Union
European Regional
Development Fund

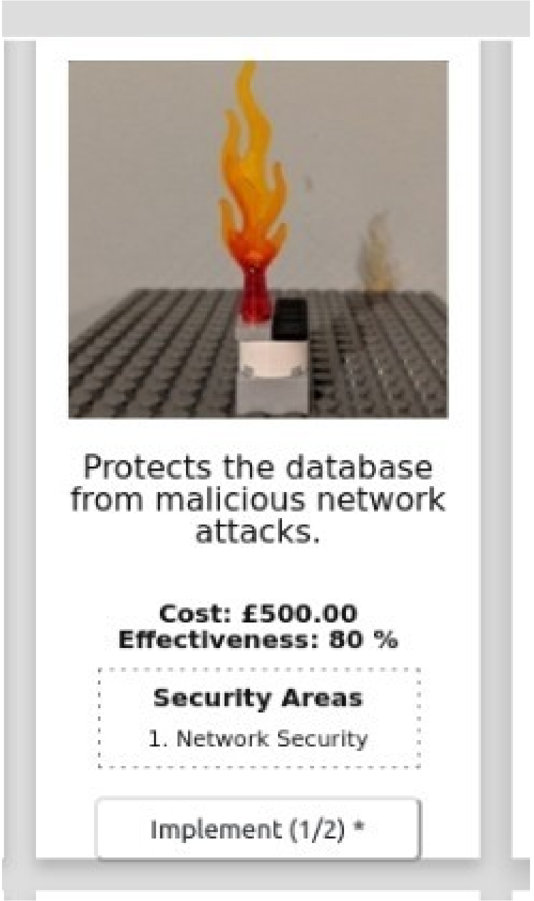


Implemented Controls

1.3
Firewall

Stops malicious traffic internal to the office network preventing compromised

System Architecture



Protects the database from malicious network attacks.

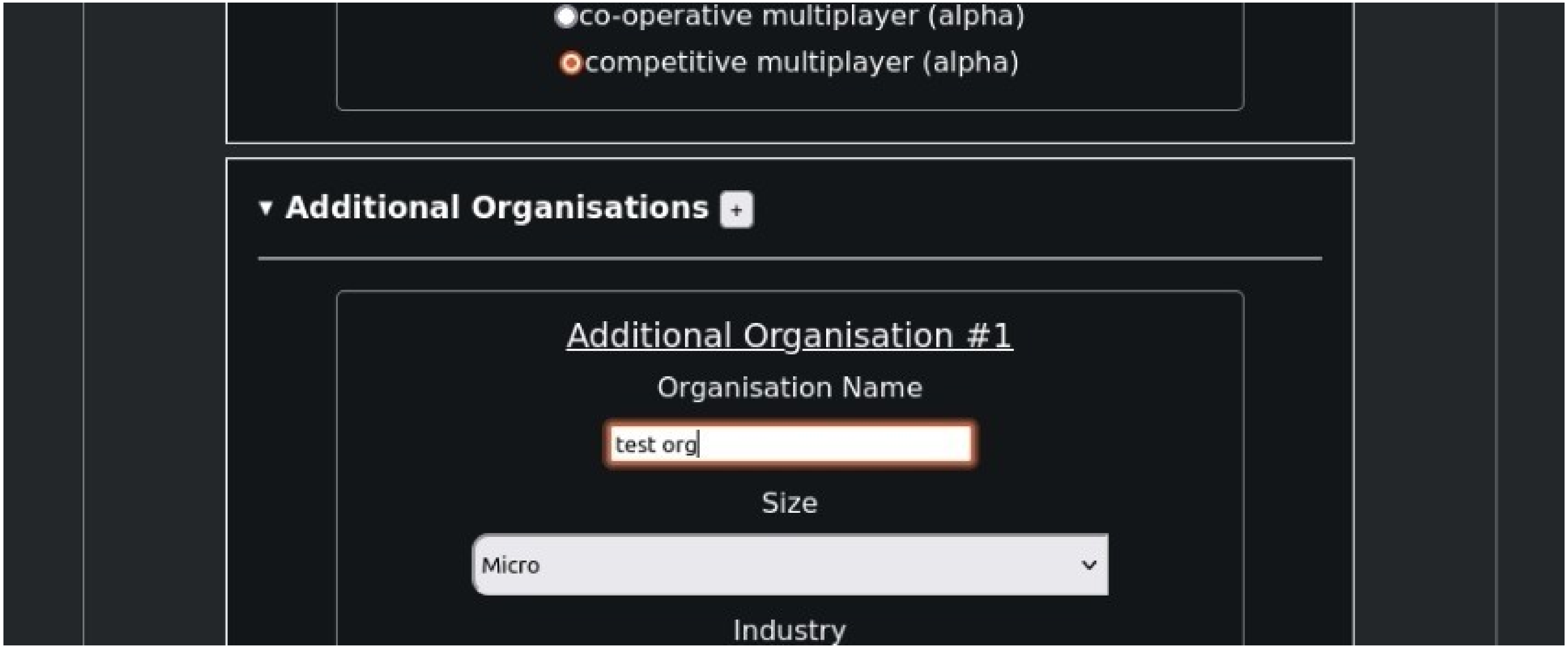
Cost: £500.00
Effectiveness: 80 %

Security Areas

1. Network Security

System Architecture

European Union
European Regional Development Fund



○ co-operative multiplayer (alpha)

● competitive multiplayer (alpha)

▾ Additional Organisations +

Additional Organisation #1

Organisation Name

test org

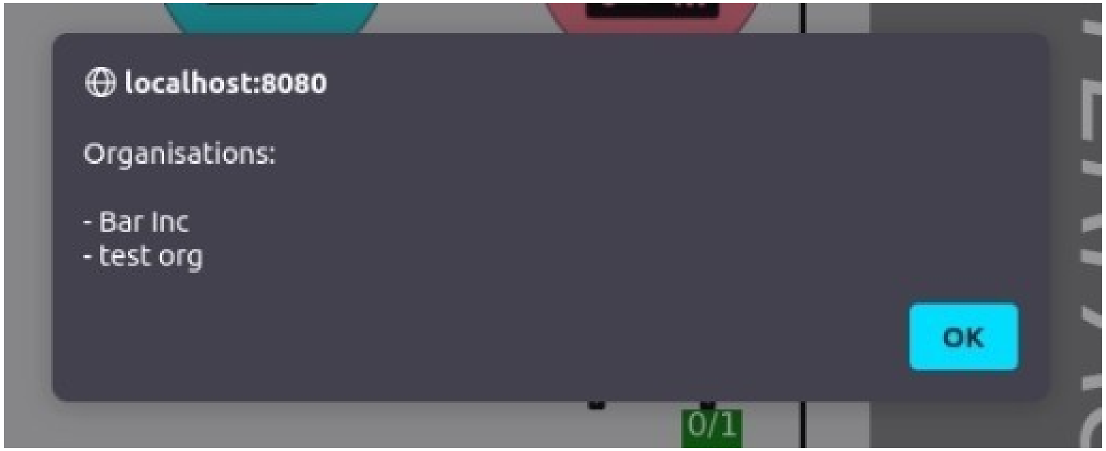
Size

Micro

Industry

System Architecture

European Union
European Regional
Development Fund

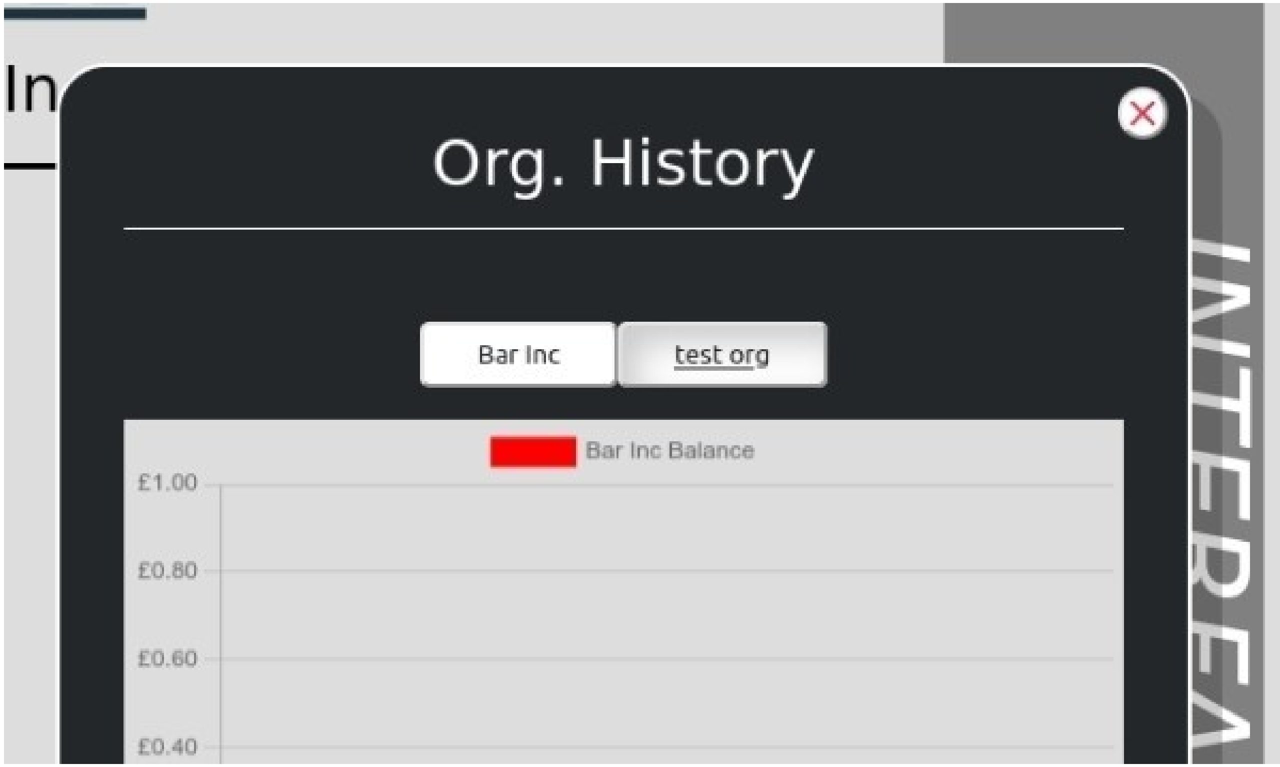


localhost:8080

Organisations:

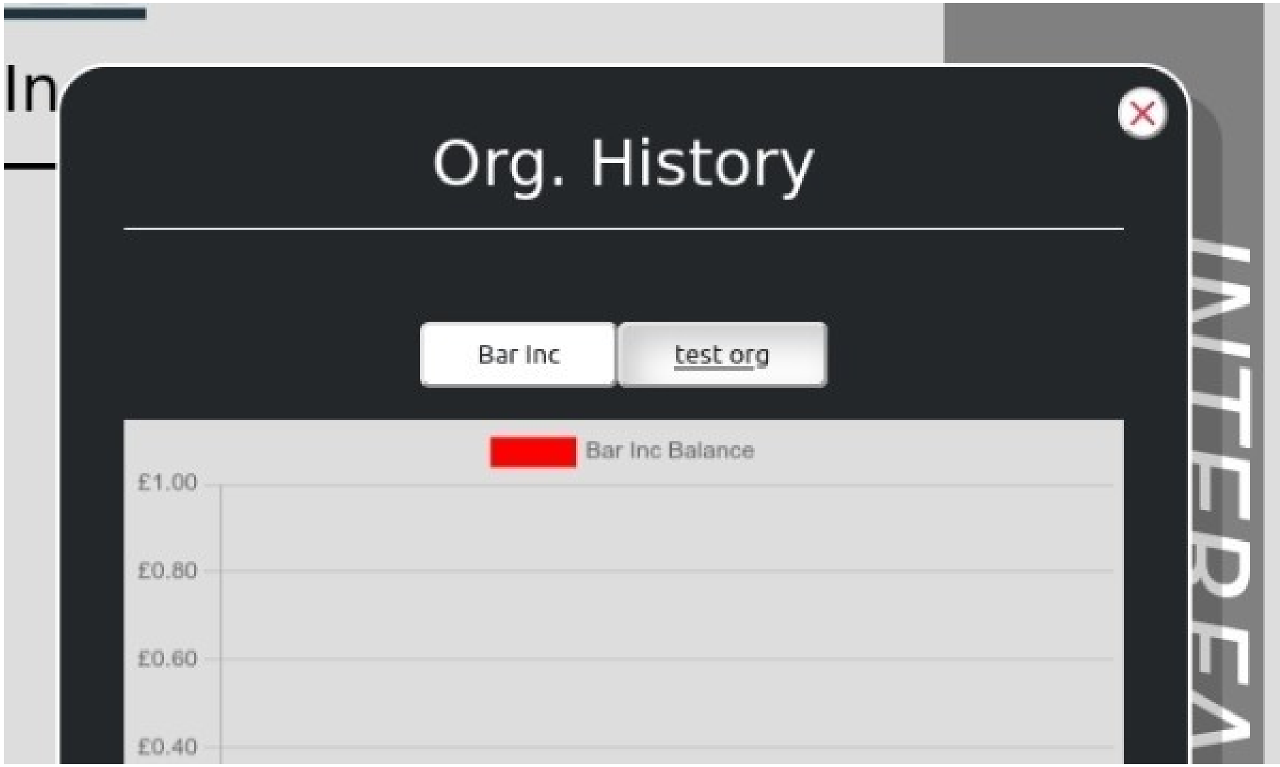
- Bar Inc
- test org

System Architecture



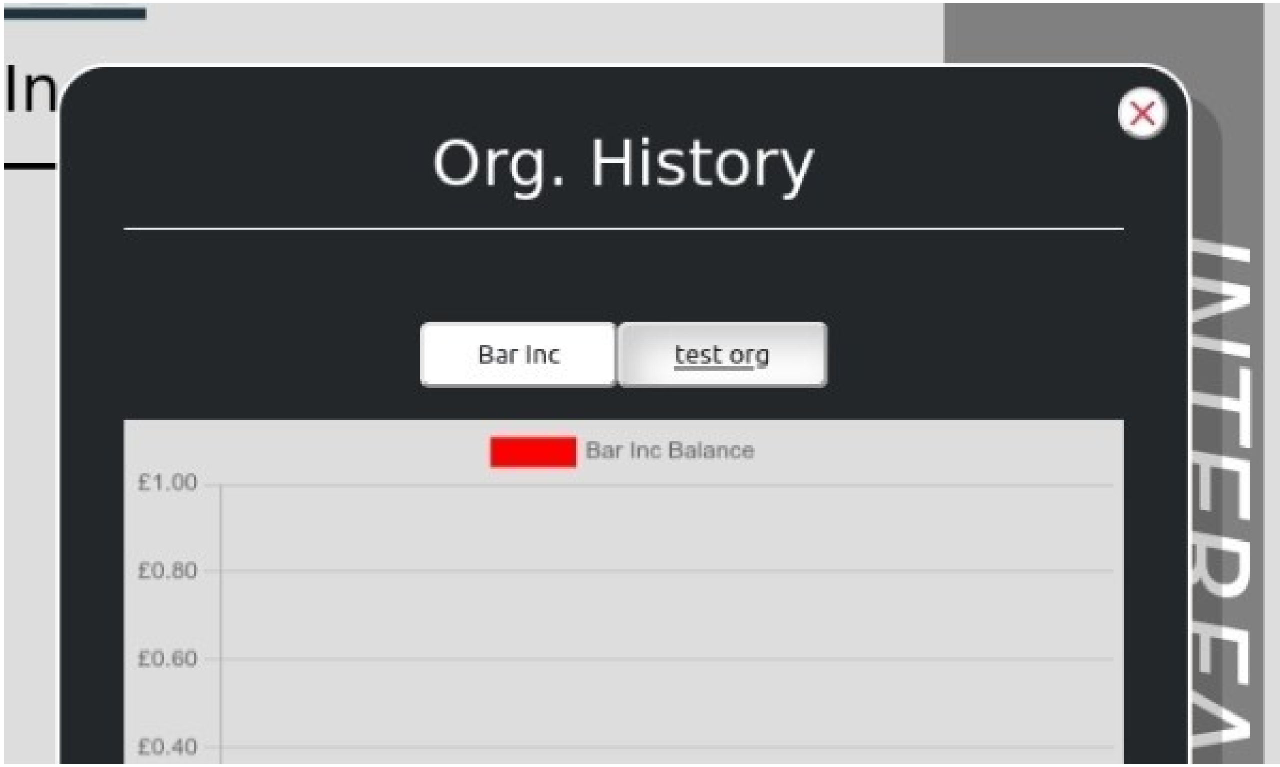
System Architecture

European Union
European Regional
Development Fund



System Architecture

European Union
European Regional
Development Fund



Greater Manchester | Greater Security | Greater Business

Cyber Foundry

Questions?

European Union
European Regional
Development Fund

Lancaster University

MANCHESTER
1824
The University of Manchester

Manchester
Metropolitan
University

University of
Salford
MANCHESTER