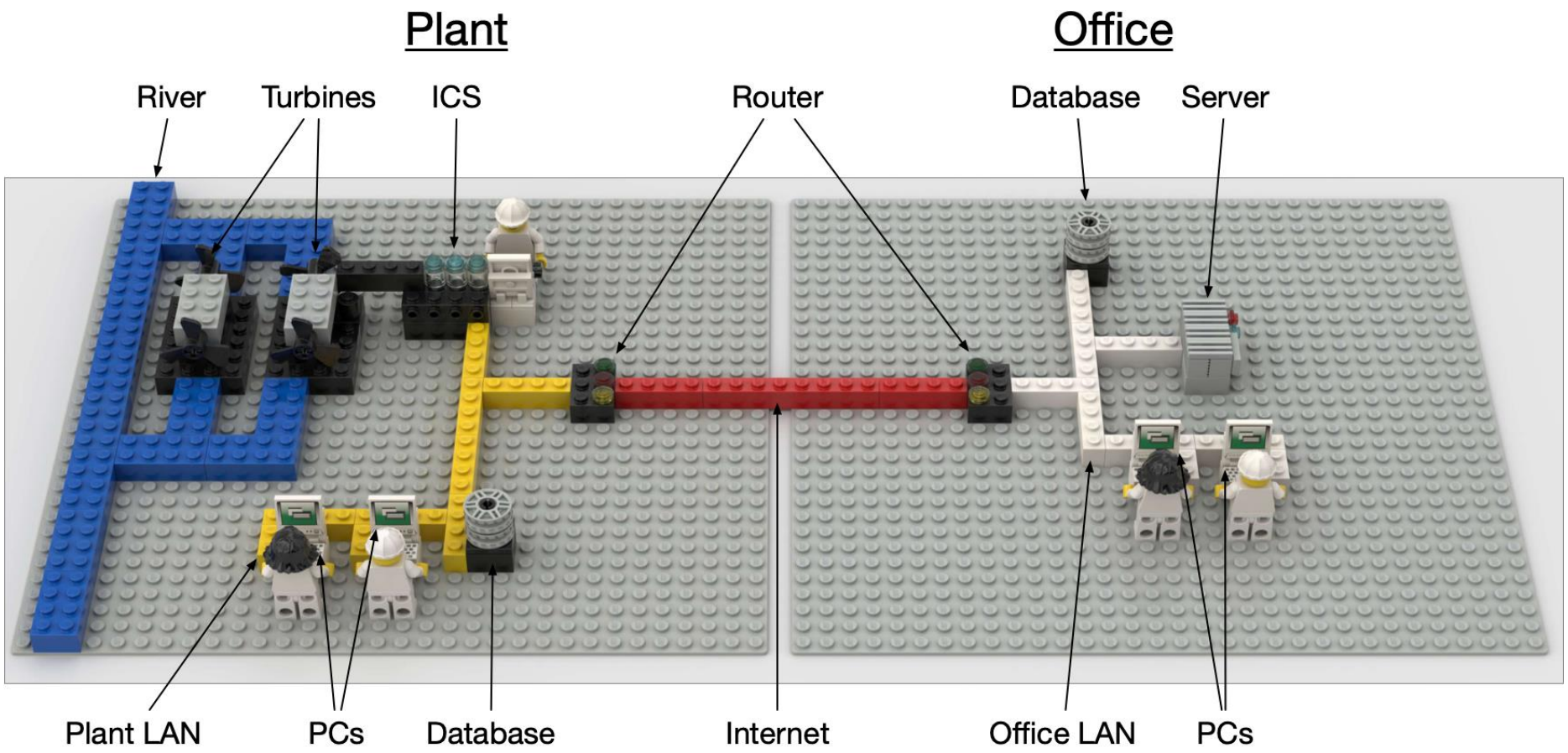
Decisions & Disruptions

Dr Benjamin Shreeve

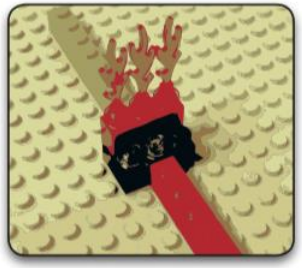
ben.shreeve@bristol.ac.uk

University of BRISTOL

Bristol Cyber Security Group


Plant
Office
River
Turbines
ICS
Router
Database
Server
Plant LAN
PCs
Database
Internet
Office LAN
PCs

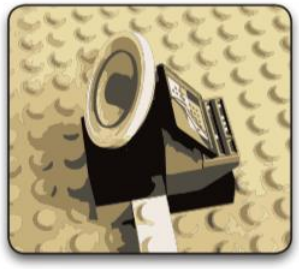
FIREWALL
(plant)



Firewall (plant) : 30k

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

NETWORK MONITORING



Network Monitoring (plant) : 50k

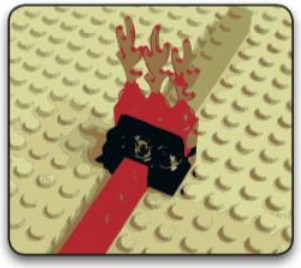
This big, shiny piece of bleeding-edge technology is quite expensive but also very effective

CCTV
(plant)

CCTV Surveillance : 50k

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

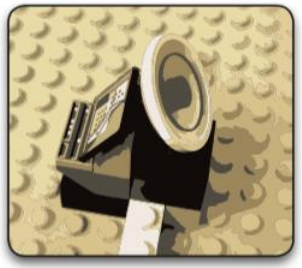
FIREWALL
(office)



Firewall (office) : 30k

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

NETWORK MONITORING



Network Monitoring (office) : 50k

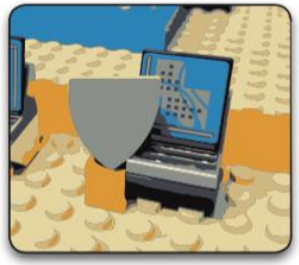
This big, shiny piece of bleeding-edge technology is quite expensive but also very effective

CCTV
(office)

CCTV Surveillance : 50k

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

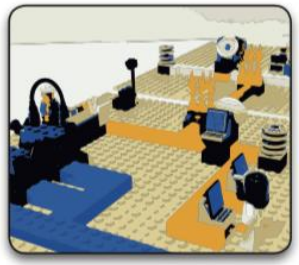
ANTIVIRUS
(plant & office)



Antivirus : 30k

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

ASSET AUDIT



Asset Audit : 30k

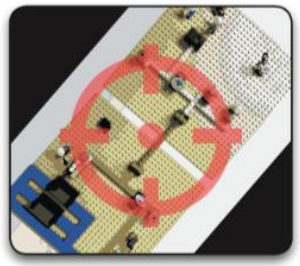
The entire infrastructure is thoroughly assessed for vulnerabilities

SECURITY TRAINING

Security Training : 30k

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

THREAT ASSESSMENT



Threat Assessment : 20k

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

CONTROLLER UPGRADE

Controller Upgrade : 30k

Software patches and an update to the firmware of the SCADA controller

PC UPGRADE

PC Upgrade : 30k

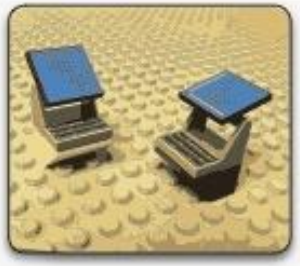
A brand new, up-to-date OS and software suite for all Personal Computers

SERVER UPGRADE

Server Upgrade : 30k

A brand new, up-to-date OS, web server and database management system

PC ENCRYPTION



PC Encryption : 20k

Military grade, proven encryption mechanism for the hard drives of all PCs

DATABASE ENCRYPTION

Database Encryption : 20k

Military-grade, proven encryption mechanism for all databases

Findings

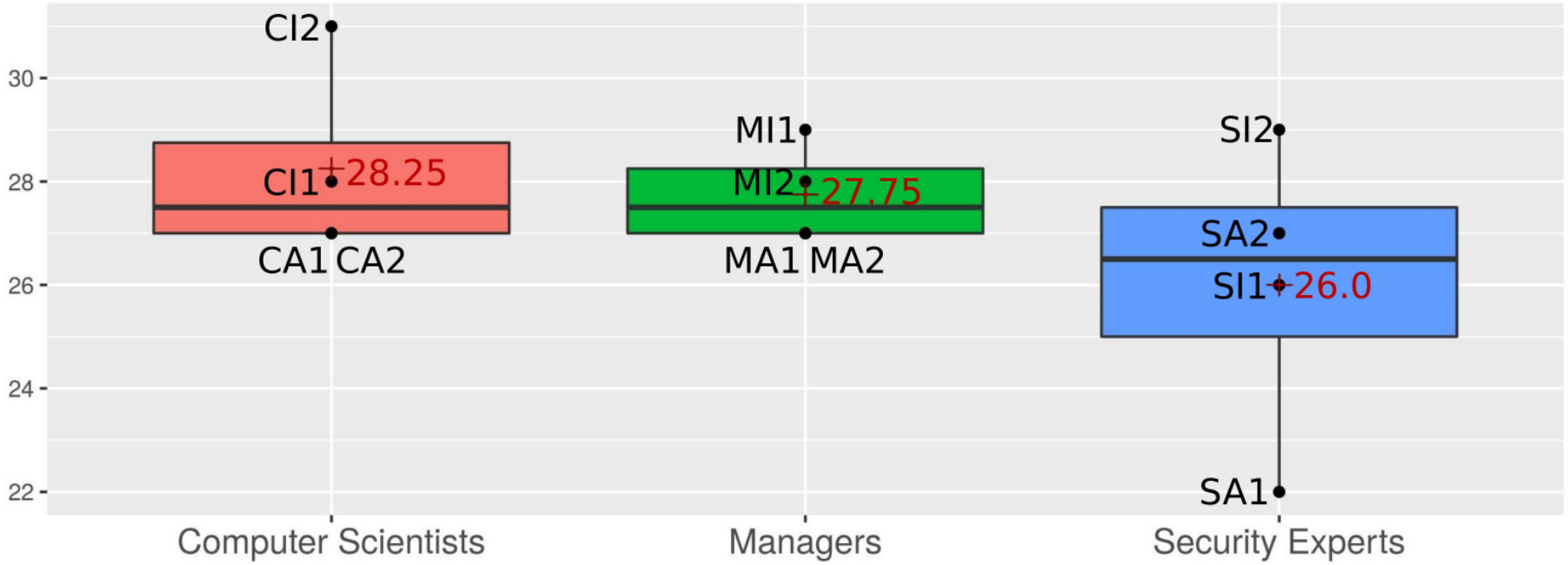
A Study of Security Decisions in a Cyber-Physical Systems Game

University of BRISTOL

43 Players, divided into 12 homogeneous groups

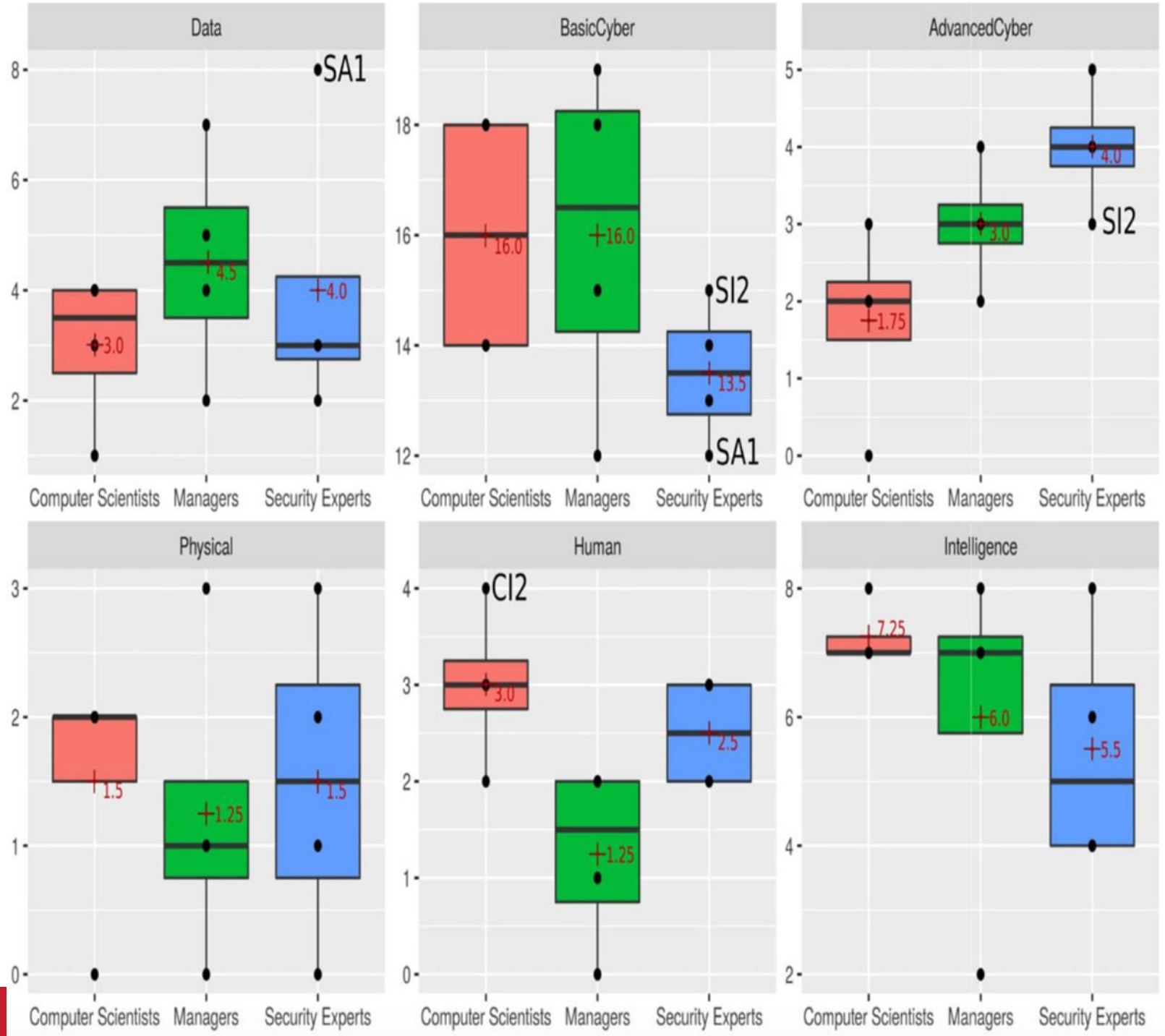
	Academia	Industry
Security experts	SA1 (4 PhD students) SA2 (3 undergr. stud.)	SI1 (4 consultants) SI2 (5 consultants)
Computer scientists	CA1 (2 academics) CA2 (4 postgrad. stud.)	CI1 (6 IT engineers) CI2 (4 IT engineers)
Managers	MA1 (3 postgrad. stud.) MA2 (4 undergr. stud.)	MI1 (2 managers) MI2 (2 managers)

The best players are …?



“We are security experts, we don’t need a threat assessment.” *Team SA1*

“You told us what we already knew.”
Team SI1



University of BRISTOL

Bristol Cyber Security Group

Security Experts

+ + Advanced cyber protection
− − Basic cyber protection
− − Intelligence gathering

Computer Scientists

+ + Intelligence gathering
+ + Human factors
− − Advanced cyber protection
− − Data protection

Managers

+ + Basic cyber protection
+ + Advanced cyber protection
+ + Data protection
− − Human factors

Procedure-driven

“We should start with an asset audit, then we can know what we are protecting and invest accordingly.”

Experience-driven

“I have never seen an IT infrastructure without a firewall.”, “Remember the news last week? They got owned by a phishing email, we should care about it.”

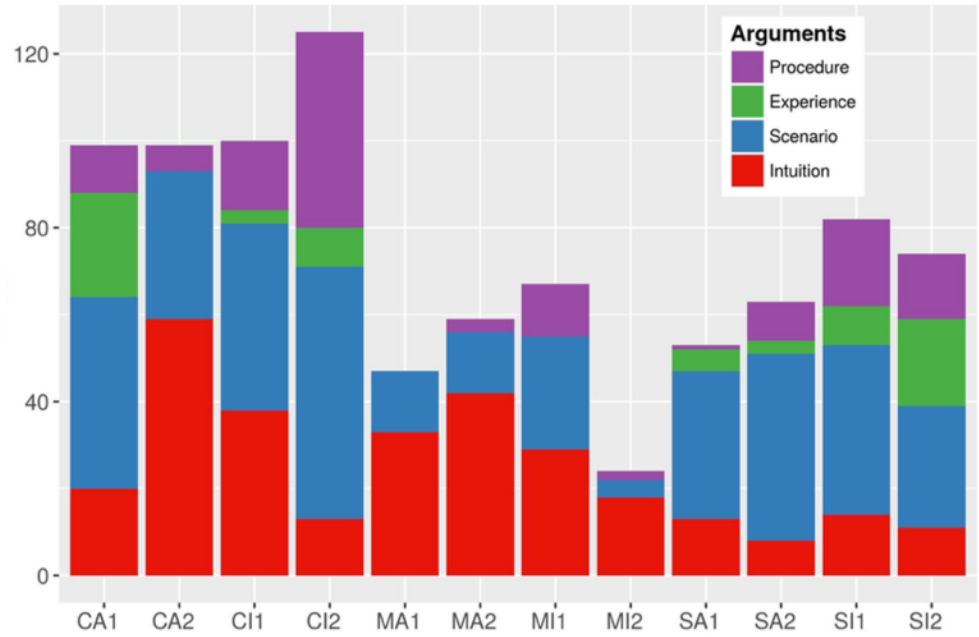
Scenario-driven

“What if someone got access to our database? We need to encrypt it.”

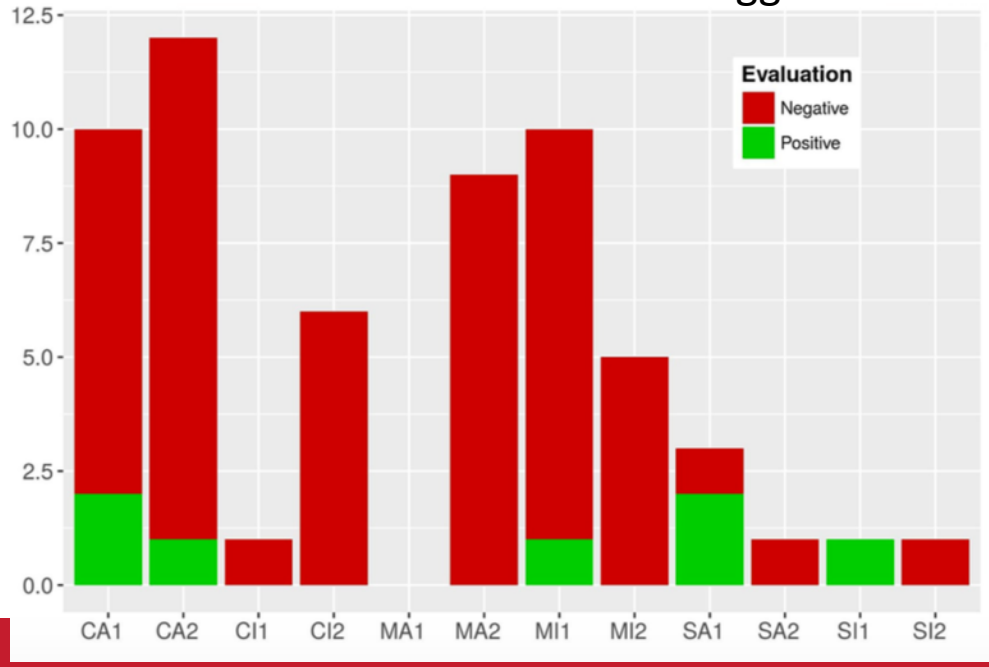
Intuition-driven

“I like the antivirus.”

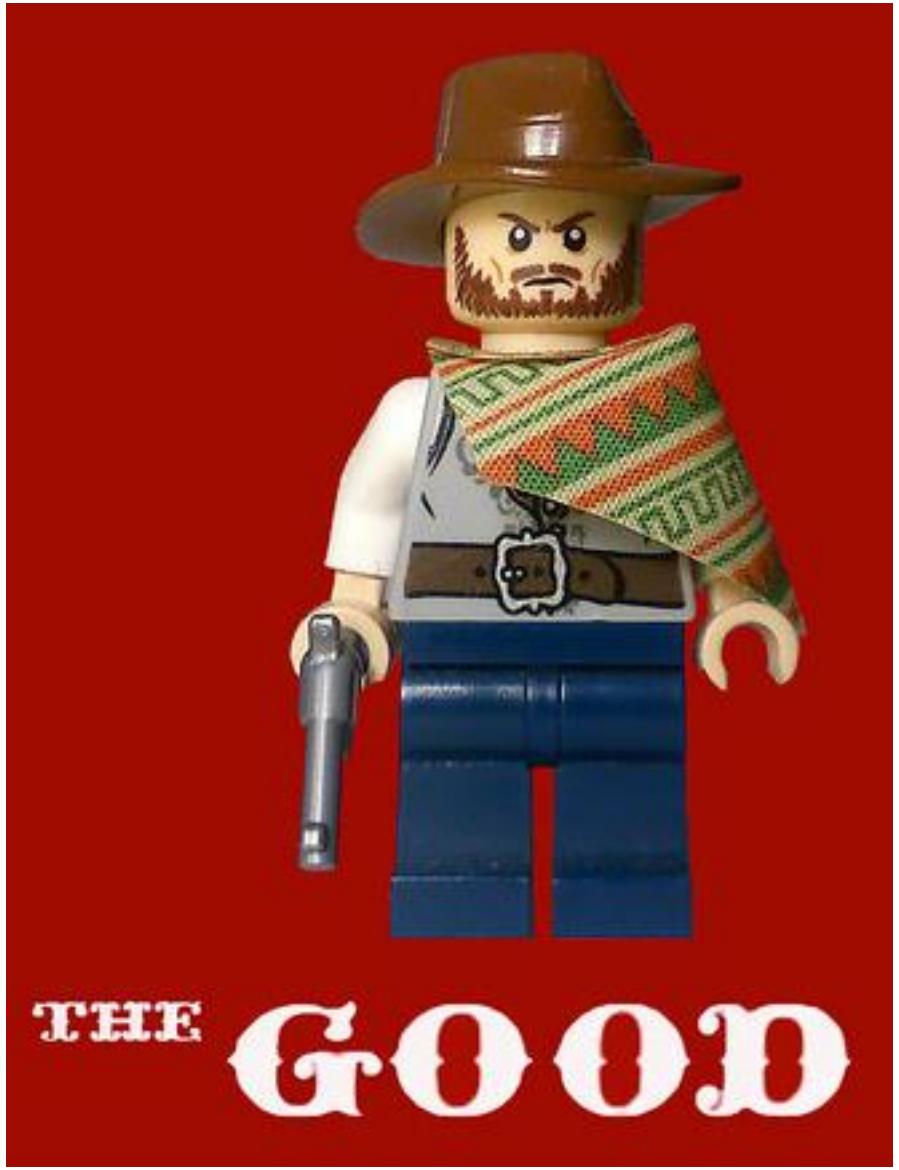
Analysis of arguments used



Measure of self-confidence in suggestions



Characteristic game play styles



Balance is key

The Beginner's Syndrome

A little knowledge is a dangerous thing

Beware of the champion!

For better or worse

The “tunnel vision” syndrome

“This company’s data has little value: you could publish it all.”

“I don’t feel the encryption is any priority even though there has been a data breach.”

Next stages

- Incident response within the finance sector

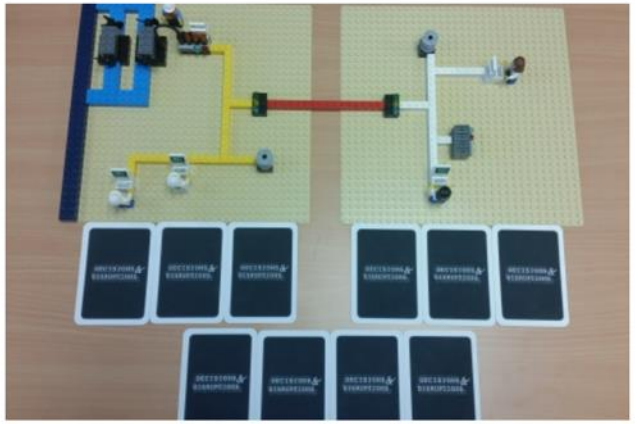
www.decisions-disruptions.org

University of BRISTOL

New exercise unveiled to help businesses in the fight against cyber attacks

Press release issued: 8 March 2018

The Metropolitan Police Service (MPS) has unveiled an innovative new exercise that teaches business leaders how to protect their companies from cyber attacks. The resource, entitled 'Decisions and Disruptions', funded by the Engineering and Physical Sciences Research Council (EPSRC), was first developed by a group of academics, currently based at the University of Bristol, in partnership with the National Cyber Security Centre.



Officers in the Met's Fraud and Linked Crime Online (Falcon) unit have adapted it to be included in their regular cyber awareness presentations given to businesses and organisations.

Share this article

Full paper

Sylvain Frey, Awais Rashid, Pauline Anthonysamy, Maria Pinto-Albuquerque, and Syed Asad Naqvi

The Good, the Bad and the Ugly: A Study of Security Decisions in a Cyber-Physical Systems Game.

IEEE Transactions on Software Engineering (Pre-print is online)

EPSRC Grant: EP/M002780/1

ben.shreeve@bristol.ac.uk

decisions-disruptions.org