PUBLIC DELIVERABLE

H2020 Project: Smart Resilience Indicators for Smart Critical Infrastructure

D5.3 - Resilience Joint Evaluation and Test Report (JET report) for the case study "SmartResilience Project: ALPHA: Financial System"

Coordinator: Aleksandar Jovanovic EU-VRi

Project Manager: Bastien Caillard EU-VRi

European Virtual Institute for Integrated Risk Management
Haus der Wirtschaft, Willi-Bleicher-Straße 19, 70174 Stuttgart

Contact: smartResilience-CORE@eu-vri.eu

Resilience Joint Evaluation and Test Report (JET report) for the case study "SmartResilience Project: ALPHA: Financial System"

Author(s):	Mary-Ellen Lang, Kimberley Campbell
Responsible Project Partner:	City of Edinburgh Council
Contributing Project Partners:	City of Edinburgh Council
Deliverable No:	D5.3
Due date:	Oct. 1, 2018
Submission date:	Oct. 1, 2018

Summary / Main facts & findings

Main findings after the exercise:

The City of Edinburgh Council, as UK Project Alpha Case Study leads, developed and facilitated a workshop with representatives from Edinburgh's finance sector, which involved 16 attendees from 9 organisations. The objectives of the workshop were to:

- *provide a project overview and context*
- *consider two scenarios designed to challenge and disrupt critical infrastructure*
- *validate and refine Alpha's draft resilience and functionality indicators*
- *agree further actions to enhance the city of Edinburgh's resilience, including business involvement*
- *following the workshop, to stress-test the agreed indicators*

These objectives were fully met.

The scenarios were examined by a financial industry expert (workshop non-participant) in advance of the workshop to ensure they were fit-for-purpose and suitably challenging and meaningful.

The main threat was a terrorist cyber attack on critical infrastructures of finance and, ICT, with some considerations of transport (smart element), all with cascading effects.

Following the workshop, as agreed with the work package leader, the D5.3 Alpha case study team worked with an identified industry leader within Edinburgh's finance sector to stress test the resilience and functionality indicators which had been validated during the workshop.

The resulting workshop data is included within the case study report as far as commercial sensitivities allow.

The workshop and follow up data collection were carried out by the Resilience Assessment Manager and the Main Analyst.

1. Introduction

Main objectives and challenges of the exercise:

The main challenge was to ensure a suitably developed scenario to meaningfully challenge and validate the draft resilience indicators.

In addition, the financial sector in the UK is highly regulated and, as such, there are metrics and regulations, including on resilience, imposed on financial organisations. These are in addition to those drafted for the purposes of the SmartResilience Project. As a result of close working with one leading participating organization, the City of Edinburgh Council was able to understand these additional metrics and these have been noted in the findings for information.

Description of the conducted exercise:

The purpose of the workshop was for relevant subject area experts from Edinburgh's finance sector to use the Critical Infrastructure Resilience Assessment Method developed by the SmartResilience Project to stress test and validate the draft resilience indicators also developed by the Project. This was carried out under simulated conditions using scenarios based on real life situations.

2. Assessed Critical infrastructure

2.1. General description of the assessed critical infrastructure

This case study was responsible for assessing the financial sector. Other CIs potentially affected as part of the scenarios were the energy supply system and the water supply system.

2.2. Smart critical infrastructure features

Smart critical infrastructure featured as part of the workshop scenario were financial systems, the transportation system and ICT systems.

3. Assessment Setup

3.1. Threat

The Alpha case study threat types were: cascading effect, terrorist attack and cyber attack.

3.2. Scenario

Incident Scenario 1: It is 10.30 a.m. on Monday, 14 January 2019. The UK is returning to normal following a prolonged period of severe winter weather. Information is being received that Edinburgh's power networks are undergoing some form of major disruption and there are reports of various system failures across the City. Transport for Edinburgh is advising that tram and local rail services are currently suspended and bus services are facing severe delays due to congestion caused by multiple traffic light signal failures. Power supplies appear to be operating intermittently in a number of areas. Security alarms are sounding at various buildings. Scottish Power Energy Networks (SPEN) have posted information onto their website stating that they are experiencing problems in some areas and are investigating. National media outlets are reporting that infrastructure across large parts of the country appears to be subject to some form of cyber attack.At 11 a.m. the mains electricity supply across the City fails.

Incident Scenario Two: It is 9 a.m. on Tuesday, 15 January 2019. Power, water and communications across Edinburgh are in the process of being restored. The media are reporting widely that a cyber-attack is currently taking place affecting a range of computer data centres and a large number of individual personal computers across the UK. Banks, financial service and technology companies appear to be the main targets of the attack but industry, health and government services are also being affected. The attack is being spread on systems with inadequate security by various methods including phishing emails. The form of attack is described as being similar to previous ransomware "WannaCry" incidents but more technically sophisticated. To date no demand for any payment has been made and the purpose behind the attack is not clear. A group calling itself "GhostWatch" is claiming to be responsible for the incident but this information has not been verified. There is no known record of this organization. Experts from the UK National Cyber Security Centre have warned the outbreak could continue to infect more systems. Specialist investigators, including the UK National Crime Agency (NCA), are working with international counterparts to identify those responsible for the incident.

3.3. Issues/elements/indicators refinement

3.3.1. Selection of issues/elements/indicators

ID	*Element / Indicator*	*Name of Element / Indicator formulated as a Question or as number, percentage, fraction, etc.*	*Description*
2830	*Element*	*Lack of appropriate board level technical expertise; ID-2830*	*Board members require to have appropriate technical expertise to fully understand the risks and make informed decisions about whether they should be tolerated, transferred, terminated or treated and how this response is best undertaken.*
2831	*Indicator*	*Is this system evidenced?; ID-2831*	*Evidence could include a Competencies Framework, a Training Needs Analysis document and Training Records*
2832	*Indicator*	*Are learning points identified?; ID-2832*	*Identifying and learning from incidents, training and exercising to ensure that the training being delivered and the board members' technical expertise remains up-to-date and relevant.*
2833	*Indicator*	*Are corrective measures taken and monitored regularly?; ID-2833*	*Undertake corrective actions identified following a non-conformity/incident or a risk/threat has changed to ensure systems remain effective and suitable. Monitor corrective actions through to resolution/completion*
2834	*Element*	*Vulnerability expertise needs analysis conducted?; ID-2834*	*A procedure involving a number of processes including: development and maintenance of a Competencies Framework to identify the competencies required; maintenance of a Training Needs Analysis (based on the Competencies Framework) to determine current competency levels; and training records*
2830	*Indicator*	*Does a process exist for establishing minimum technical expertise of the individual board members?; ID-2830*	

			A procedure involving a number of processes including: development and maintenance of a Competencies Framework to identify the competencies required; maintenance of a Training Needs Analysis (based on the Competencies Framework) to determine current competency levels; and training records
2835	Indicator	Percentage of specialist positions filled with specialists?; ID-2835	Holders of specialist roles have the relevant specialist knowledge and expertise to fully understand and communicate risks
2836	Indicator	Number of trained specialist graduating from Universities?; ID-2836	To identify whether a local, accessible source of qualified specialists is available to fill the specialist roles.
2837	Element	Expertise needs analysis conducted for system / architecture / Cyber Defence?; ID-2837	A procedure involving a number of processes including: development and maintenance of a Competencies Framework to identify the competencies required; maintenance of a Training Needs Analysis (based on the Competencies Framework) to determine current competency levels; and training records
2838	Indicator	Percentage of specialist positions filled with specialists?; ID-2838	Holders of specialist roles relating to system / architecture have the relevant specialist knowledge and expertise to anticipate and prepare for cyber threats
2850	Element	Response / recovery capability; ID-2850	Appropriate levels of capability are required to respond to, and recover from, incidents effectively
2851	Indicator	Does a process exist for establishing minimum technical expertise of the response/BCM teams?; ID-2851	A procedure involving a number of processes including: development and maintenance of a Competencies Framework to identify the competencies required; maintenance of a Training Needs Analysis (based on the Competencies Framework) to determine current competency levels; and training records
2852	Indicator	Is relevant training needs part of the annual training need analysis?; ID-2852	The Training Needs Analysis needs to include competencies relevant to responding to, and recovering from, an incident
2853	Indicator	Is training for the response and recovery conducted?; ID-2853	Delivery of training products which raise awareness and knowledge of participants for all key issues and procedures relating to incident response and recovery
2854	Indicator	Percentage of training conducted against requirements?; ID-2854	Proportion of company staff who are trained to respond and recover from incidents as detailed in the Training Needs Analysis
2855	Indicator	Percentage of staff training against planned?; ID-2855	Proportion ofcompany staff who are trained to respond and recover from incidents as detailed in the company's Training Programme
2856	Element	Lack of adequate change management?; ID-2856	The management of changes and developments within an company or an IT system which could impact the company's resilience
2857	Indicator	Robust Change Management process in place; ID-2857	Identifying the scale of vulnerability facing a company as a result of changes to the company itself or to its IT systems

ID	Element / Indicator	Name of Element / Indicator formulated as a Question or as number, percentage, fraction, etc.	Description
3491	Element	Key banking engines performance (eg core banking)	Production output is one of the key functions of any infrastructure.
3492	Indicator	Number of new Financial products sold	Number of products sold
n/a	Indicator	% of existing critical products being serviced / maintained	% of critical products
3493	Indicator	Value of core banking transactions – deposits	Financial transactions successfully completed
3494	Indicator	Value of core banking transactions – payments	Financial transactions successfully completed
3495	Element	Economic performance	The economic dimension of resilience of the CI concerns the economic status of the organisation. It helps in understanding not just the current state but also the impact of a disruption on the performance of the CI in short and long-term.

3496	Indicator	Rate of Investment (ROI)	Expected ROI
3497	Indicator	Sales - number of products sold	Number of products sold
3498	Indicator	Share Price (£)	Predicted shareprice
3500	Indicator	Income (£)	Total income from all activities
1271	Element	Global / international interconnectedness	Global interconnectedness of the critical infrastructures imply the interdependencies between Cis in different countries
3501	Indicator	Global economic indicators - Exchange Rates	Projected market movement of global economic indicators (%)
3502	Element	Critical societal life preserving interdependencies	Health and social care services, e.g primary and secondary care, dependent on production and delivery of goods and services
3503	Indicator	Critical supply chain is assured. Supply chain maintained to contractual levels	Supply chain failure of critical products and services
3504	Element	Treasury function	Planning and Operations. Cash and Liquidity Management. Funding and Capital Markets
3505	Indicator	Liability / asset levels	Ability to meet liabilities to pre-defined levels
3506	Element	Failure of systems supporting Straight Through Processing (STP)	Accelerated automated processing
3493	Indicator	Number of core banking transactions – deposits	Financial transactions successfully completed
3494	Indicator	Number of core banking transactions – payments	Financial transactions successfully completed

3.3.2. Quality assurance

The Alpha case study workshop involved a range of stakeholders from the financial sector. Following the event there were further discussions to stress test the above items validated during the workshop. Feedback was welcomed at all stages.

4. Description of the exercise method (type of event) and other practical details

4.1. Exercise method

The exercise method was a workshop, including relevant subject area experts from Edinburgh's finance sector. These experts used the Critical Infrastructure Resilience Assessment Method developed by the SmartResilience Project to stress test and validate the draft resilience indicators, also developed by the Project.

This was carried out under simulated conditions using scenarios based on real life situations.

4.2. Stakeholders involved in the exercise

A range of stakeholders representing Edinburgh's financial sector, attended the workshop. Represented organisations were from Edinburgh's finance sector, including banking, investment, and fintech.

4.3. Planning of the exercise

The event was planned and organized to encourage as much participation as possible; delegates were sent detailed information on the aims, objectives and format in advance, as well as:

- *a project overview*
- *draft resilience indicators for advance consideration*

These instructions were provided as joining instructions, a copy of which is available on request.

As part of the planning, the workshop scenarios were examined by a financial industry expert (workshop non-participant) in advance of the workshop to ensure they were fit-for-purpose and suitably challenging and meaningful. The main threat was a terrorist cyber attack on critical infrastructures of finance and, ICT, with some considerations of transport (smart element), all with cascading effects.

The purpose of the workshop was for relevant subject area experts to use the Critical Infrastructure Resilience Assessment Method developed by the SmartResilience Project to stress test and validate the draft resilience indicators also developed by the Project.

This was carried out under simulated conditions using scenarios based on real life situations.

The workshop programme was as follows:

09:00 – 09:30 Delegate Registration

09:30 – 09:40 Welcome and Introductions

09:40 – 10:30 Scenario 1 – Issue and Syndicate Discussion

10:30 – 11:00 Syndicate Feedback

11:00 – 11:15 Break

11:15 – 12:10 Scenario 2 – Issue and Syndicate Discussion

12:10 – 12:45 Syndicate Feedback

12:45 – 13:00 Plenary

13:00 Lunch

The workshop included a range of subject matter experts in finance, resilience and ICT.

Attendees considered an escalating scenario, which had two main parts.

The first part of the scenario was a disruption to utilities (water, then electricity) in the city that is at a point in the workshop, identified as a deliberate attack.

The second part of the workshop was a realisation that the incidents are coordinated attacks on Edinburgh's critical infrastructure with the finance sector also being targeted.

This resulted in a range of additional disruptions to the city, in sectors and organisations dependant on the compromised critical infrastructure; these included traffic lights outage, security systems outage, mobile network outage, broadband outage, transport disruption and schools closures. Other cascading effects were discussed as part of the workshop and included ATM outage, bank branch closures and contactless payments outage.

During the sessions, participants discussed and fed back on a series of questions designed to assess and validate the draft resilience indicators.

The scenarios included SmartCity elements for Edinburgh's transport network, including transport (traffic lights and bus tracking) and cascading effects.

4.4. Informed consent

All external workshop attendees signed a consent form.

5. Results

5.1. Main results

The City of Edinburgh Council, as UK Project Alpha Case Study lead, developed and facilitated a workshop with representatives from Edinburgh's finance sector, which involved 16attendees from 9 organisations. The objectives of the workshop were to:

- *provide a project overview and context*
- *consider two scenarios designed to challenge and disrupt critical infrastructure*
- *validate and refine Alpha's draft resilience and functionality indicators*
- *agree further actions to enhance the city of Edinburgh's resilience, including business involvement*
- *following the workshop, to stress-test the agreed indicators*

These objectives were fully met.

5.2. Other information

Additional information was also gathered from the identified industry leader, including:

- *The UK finance regulator expects appropriate monitoring/metrics/governance/processes/incident management to be in place to respond and recover extremely quickly to a business incident.*
- *Finance organisations in the UK monitor metrics regularly in order to detect problems in advance with business processes and issues; these also provide an indicator of general resilience.*
- *In terms of incident timings (i.e. T0-T5) the key times known would be end and recover (to business as usual level, as well as recovery to pre-defined levels).*
- *Each finance organisation is specific about recovery to pre-defined levels. For banking within 24 hours it is critical, as failure to do so brings risks of, for example, civil unrest, a bank losing its license, a bank losing its liquidity and / or negative impact on the global economy.*
- *The emphasis on the UK finance industry is on operational resilience and adaptiveness rather than quantifying retrospective failure; understanding one's organisation through monitoring is more important. This is a recent change from the Bank of England. The paper detailing these changes by the three UK Financial Service Regulators includes a model it is expected firms will move / adhere to. More information is available from the Bank of England's website.*

6. Recommendations

The workshop included the following recommendations to enhance Edinburgh's resilience:

- *private sector involved with risk assessing and mitigating key city resilience risks*
- *share information, alerts and have an agreed planning framework and cascade of information in the case of a serious emergency or major incident (private sector and citizens)*
- *interaction across the finance and other sectors to share of good practice and alignment of plans*
- *collaborative supply chain assurance would assist in strengthening resilience*

ANNEXES

No records to display.