European Crime Prevention Award (ECPA)

Annex I – new version 2014

Please complete the template in English in compliance with the ECPA criteria contained in the RoP (Par.2 §3).

General information

1. Please specify your country.

The Netherlands.

2. Is this your country's ECPA entry or an additional project?

ECPA entry.

3. What is the title of the project?

SME Cybersecure, Cybersecurity Business edition.

4. Who is responsible for the project? Contact details.

Ellen Jacobs *Project manager MKB-Nederland* Email: jacobs@mkb-amsterdam.nl Telephone: 0031 6 1135 1730

5. Start date of the project (dd/mm/yyyy)? Is the project still running (Yes/No)? If not, please provide the end date of the project.

The start date of the project is 18 August 2015. The project is still running, until 9 December 2015.

6. Where can we find more information about the project? Please provide links to the project's website or online reports or publications (preferably in English).

Campaign: www.veiligzakelijkinternetten.nl Online Report Amsterdam - http://magazine.veiligzakelijkinternetten.nl/aa

7. Please give a **one page** description of the project (**Max. 600 words)**

Cybercrime is – as in many other states - a major problem in the Netherlands. However, the main thought in The Netherlands is that cybercrime does not exist on a large scale in our small country. Contrariwise, with our big mainport Schiphol and our big harbour Rotterdam, the presence of a lot of headquarter offices and the huge penetration of internet uses makes The Netherlands number 3 on the list of being popular for DDoS-attacks, behind China and the USA.

In addition, the impact of cybercrime on businesses is enormous. Cyber attacks, online fraud and digital theft accounts for 8,8 billion euros of economic loss in the Netherlands. This is about 1.5% of the Gross National Product, which ranks the Netherlands second in the European Union.

Subsidised by the Dutch ministry of Security and Justice, MKB-Nederland together with parties as the Dutch Network Group, the Electronic Commercial Platform, KPN (Dutch Telecom and IT service provider), het Verbond van Verzekeraars (The Dutch Association of Insurers), ThreadStone and the Regional Networks for Safe Entrepreneurship (RPC's), developed a project to make entrepreneurs more aware of the impact of cybercrime on their businesses. Fact is that the impact of cybercrime is growing and a lot of Small Medium Sized companies (SME's) do not realise that also their websites and databases can be potential targets for cyber criminals.

In accordance with the wish to make the SME's more aware of their own cybersecurity, this project organises an awareness campaign. The awareness campaign is based on a roadshow through the country, focussed on 5 regions. In partnership with the regional networks for safe entrepreneurship (RPC's) an interesting programme has been developed for SME's with information about cybercrime.

In this regional campaign the "MKB Buzz", a big orange old-fashioned city bus, rides through the different regions of the country. When arriving on location, the bus enters an area of shops (shopping mall) or a business area to start the campaign. A promotion team goes along the entrepreneurs to invite them inside the bus. Insides the bus, advisors of both KPN and the Dutch Association of Insurers are seated to provide entrepreneurs with information about cybercrime and how to prevent it affecting your business.

In addition to the information that is provided about cybercrime, entrepreneurs are offered a free 'social' hack, which gives them a clear insight into their vulnerabilities and the measurements they can take to improve their cybersecurity. In all, a maximum of 300 social hacks are provided by this project.

The partnership with KPN (Telco) offers SME's a professional service, with a discount. This means the SME's can immediately take action to improve their cybersecurity. Moreover, the partnership with the Dutch Association of Insurers offer SME's a clear insight into possible insurances for cybercrime.

I. The project shall focus on prevention and/or reduction of everyday crime and fear of crime within the theme.

8. How does the project contribute to crime prevention and/or to the reduction of crime or the fear of crime? (**Max. 150 words**)

The project focusses on making SME's aware of the danger of cybercrime and encourages them to take immediate action and improve their cyber security when it is necessary. Therefor, this project contributes to both the prevention of cybercrime and the reduction of cybercrimes committed against SME's. When aware of their vulnerabilities, SME's will take the necessary precautions to protect themselves against cybercrime.

The project can also contribute to a reduction of the fear of cybercrime. When SME's know where they are vulnerable and have been told how to take measures to prevent them being affected by cybercrime, entrepreneurs will feel safer conducting their business online.

9. How is the project contributing to raising citizens' awareness of crime prevention? (**Max. 150 words**)

A sizeable proportion of the Dutch population works for SME's and most of them are not aware of the risks of cybercrime and how it can affect them. This project contributes to raising citizens' awareness of cybercrime and how it can affect their businesses by sharing information and actually showing them (via the social hacks) how vulnerable they are. By doing this, the project makes them realise that cybercrime can have a big impact and that they can be a victim of it as entrepreneur, but also as a person.

The good thing is that cybercrime is a fascinating subject in general. It is an interesting theme to get the attention of entrepreneurs. The challenge is to convince them of their own vulnerability regarding their business for cybercrime attacks. The social hacks are a good approach in convincing both entrepreneurs and citizens' that it is important to protect themselves online.

II. The project shall have been evaluated and have achieved most or all of its objectives.[1]

10. What was the reason for setting up the project? What problem(s) did it aim to tackle?

This project aims to make SME's more aware of their vulnerability for cybercrime and provide them with the possibility to come into action, to protect their business against cybercrime.

The problem that it aims to tackle is that many SME's are not fully aware of the dangers of cybercrime and how it can affect their businesses. In addition, a second problem is that many SME's do not have the capacity to take effective measure against cybercrime.

[1] For more information on evaluation, see Guidelines on the evaluation of crime prevention initiatives (EUCPN Toolbox No.3): http://www.eucpn.org/library/results.asp?category=32&pubdate

11. Was the context analysed **before** the project was initiated? How, and by whom? Which data were used? (**Max. 150 words**)

Cyber attacks, online fraud and digital theft accounts for 8,8 billion euros of economic loss in the Netherlands (Source: report 'Net Losses: Estimating the Global Cost of Cybercrime - Economic impact of cybercrime II', Center for Strategic and International Studies / McAfee, June 2014). Approximately 75% of this comes at the expense of entrepreneurs.

SME's are companies with up to 250 employees. 99% of all companies in the Netherlands belong to this group. Together they represent 58% of the gross revenue in the Netherland and offer employment to 60% of all employees (Source: 'MKB in beeld', 13 March 2015 by the Dutch Network Group). The vast majority of SME's have up to 10 employees, which means they lack the capacity to form a strategy and take effective measures against cybercrime. This is why the National Network for Safe Entrepreneurship has identified 'cyber' as one of its main themes.

12. What were the objective(s) of the project? Please, if applicable, distinguish between main and secondary objectives. (**Max. 150 words**)

The main objectives are to make SME's more aware of the impact of cybercrime on their business and to make them act accordingly to enhance the cybersecurity of their companies.

The sub objective is to get 300 entrepreneurs into action to protect their business against cybercrime, based on the information of the free social hack and the advice how to cope with it.

13. Did you build in internal goals to measure the performance of the project? If so, please describe at what stage of the project and how you measured whether the project was moving in the planned direction. (**Max. 150 words**)

The following internal goals are measured continuously throughout the project:

- The PR of the project in national and local media;
- The amount of applications for social hacks;
- The amount of visitors of the roadshows;
- The amount of hits on the digital magazines;
- The results of the 'social' hacks (the vulnerabilities that have been exposed).

14. Has there been a process evaluation? Who conducted the evaluation (internally or externally?) and what where the main results? (**max. 300 words) -** *for more information on process evaluation, see EUCPN Toolbox No.3, p.9-10 & part 2 - section 2A*

The project is still running. The roadshow started on Friday 2 October 2015. The project continuously monitors the amount of applications for the hacks, visitors of the roadshows, media attention and digital hits.

The roadshows will end on the 9 December 2016. In this week results will be completed and being shown to the press. Evaluation will take place between MKB-Nederland and the ministry of Security and Justice in December 2016.

15. Has there been an outcome or impact evaluation? Who conducted the evaluation (internally or externally?), which data and evaluation method where used and what were the main results? (**Max. 300 words**) - *for more information on outcome or impact evaluation, see EUCPN Toolbox No.3, p.7-9 & part 2 - section 2A*

The project is still running. Therefore, the results of the project that are shown below, are the results up to 15 October 2016.

Online results:

- Amount of applications for the 'social hack' – 235 entrepreneurs have subscribed for the social hack;
- Number of social hacks that have been carried out – 149 social hacks;
- Number of cities where the social hacks haven been carried out – 105 cities in The Netherlands;
- Number of unique online visitors of the website – more than 10.000 unique visitors.

Offline results:

- Roadshows that have taken place - 4 out of 7 Roadshows have taken place;
- Regions that have been visited by the campaign team: 3 out of 5 regions in The Netherlands;
- Entrepreneurs that have been reached by promotion team – 750 entrepreneurs.

III. The project shall, as far as possible, be innovative, involving new methods or new approaches.

16. How is the project innovative in its methods and/or approaches? (**Max. 150 words**)

The project is innovative because of the offer of free social hacks, a complete report of the results of the hack which immediately offer ways for the entrepreneur to improve the security of his or her company. It is, therefore, an addition to the 'old' forms of awareness campaigns which merely focus on the

general dangers of cyber security, without making the individual dangers really visible for the entrepreneur or giving them the possibility to get an insight into their vulnerabilities and measurements they can take. This project may also be used in other contexts by offering entrepreneurs an easy tool to test their security and to be advised about a constructive follow up, possible with a discounted (IT-service) offer.

IV. The project shall be based on cooperation between partners, where possible.

18. Which partners or stakeholders were involved in the project and what was their involvement? (**Max. 200 words**)

- **Ministry of Security and Justice**: subsidised the project;
- **MKB-Nederland**: MKB-Nederland is the largest entrepreneurs' organisation in the Netherlands, promoting the interests of some 150.000 entrepreneurs. MKB-Nederland is responsible for the project management of the project;
- **Dutch Network Group (DNG)**: DNG is a full-service business platform and is responsible for project management of the project and data collection;
- **Electronic Commerce Platform (ECP)**: ECP is a platform for the information society and is providing the base website for the campaign and the application process for the hacks;
- **ThreadStone**: a cybersecurity company, processing the 300 social attacks and providing SME's and their IT staff (internal of external) with a clear report about the cybercrime-weaknesses in their IT environment;
- **Verbond van Verzekeraars**: the Dutch Association of Insurers, providing content regarding the possibilities of insurances against cybercrime damages;
- **KPN**: a Dutch telecom and IT service provider, providing a concrete offer for SME to protect their company against cybercrime: "MKB Veilig";
- **Regional networks for safe entrepreneurship (RPC's):** the RPC's assist in developing an attractive regional programme for entrepreneurs to make them more aware about cybercrime.

V. The project shall be capable of replication in other Member States.

19. How and by whom is the project funded? (**Max. 150 words**)

The project is funded via a grant provided by the Dutch Ministry of Security and Justice with the amount of € 476.900. The Verbond of Verzekeraars (the Dutch Association of Insurers) financed the project with € 15.000.

20. What were the costs of the project in terms of finances, material and human resources? (**Max. 150 words**)

The costs of the project in term of finances, material and human resources are the following:

- € 491.900,00 (including project management, communications, roadshows and free hacks);
  - €72.400 project preparation – Infrastructure, Communication, Service & Support;
  - € 83.900,00 by region (5x): Roadshow, Recruitment, Organisation, Hack (€14.000), Support, Data collection, IT.

21. Has a cost-benefit analysis been carried out? If so, describe the analysis, including how and by whom it was carried out and list the main findings of the analysis. (**Max. 150 words**)

As mentioned earlier in the answer on question 11, cyber attacks, online fraud and digital theft accounts for 8,8 billion euros of economic loss in the Netherlands (Source: report 'Net Losses: Estimating the Global Cost of Cybercrime - Economic impact of cybercrime II', Center for Strategic and International Studies / McAfee, June 2014). This is about 1.5% of the Gross National Product.

SME's represent 58% of the gross revenue in the Netherland and offer employment to 60% of all employees (Source: 'MKB in beeld', 13 March 2015 by the Dutch Network Group). Based on the above mentioned numbers cybercrime against SME's accounts for just over 5 billion euros of economic loss in the Netherlands.

There is no doubt that the relatively small investment this project is, to make SME's more aware of cybercrime and encourage them to take action, can have great benefits in terms of economic loss.

22. Are there adjustments to be made to the project to ensure a successful replication in another Member State?

Adjustments are not needed, but for the project to be replicable in other member states, the following criteria should be kept in mind:

- Developing a constructive partnership between government, entrepreneur organisation, IT provider, Insurance sector organisation and a regional entrepreneur-network;

- Creating a budget for an amount of free social hacks;
- Organisation of a roadshow through different regions of the country to make entrepreneurs more aware.

23. How is the project relevant for other Member States? Please explain the European dimension of your project.

Cybercrime is growing. Faster than a lot of people and companies realise. In that perspective, awareness projects such as **Veilig Zakelijk Internetten**, are very important because they inform people and small medium sized companies that not only large organisations and businesses may become victims of cybercrime, but also small entrepreneurs are at risk of becoming a victim when they do not take enough measures to protect themselves.

Cybercrime against businesses is a worldwide phenomenon and is by its nature not bound by borders. In their (earlier mentioned in the answer on question 11) report from June 2014 the CSIS estimated that cybercrime affects 150.000 jobs in the EU and causes an average of 0,41% economic loss of the Gross National Products in the EU.

Please provide a short general description of the project (abstract for inclusion in the conference booklet – **max. 150 words**).

Subsidised by the Dutch Ministry of Security and Justice, MKB-Nederland (together with other partners) developed a project to make entrepreneurs more aware of the impact of cybercrime on their businesses. A lot of Small Medium Sized companies (SME's) do not realise that their websites and databases are potential targets. To make SME's more aware of their own cybersecurity, the project organises an awareness campaign based on a roadshow through the country. During this roadshow SME's are given the possibility to improve their cybersecurity by offering 300 free 'social' hacks, giving them a clear insight into their vulnerabilities and measurements they can take to improve their cybersecurity. The partnership with KPN (Telco) offers SME's a professional service with a discount, which means SME's can immediately take action to improve their cybersecurity. Moreover, the partnership with the Association of Insurers offers SME's a clear insight into insurances for cybercrime.