



University of
Leicester



Briefing Notes - Longitudinal Survey of Employees

Corporate Insider Threat Detection: Cyber Security Inside and Out

Project Overview:

Under the current UK Cyber Security Strategy, the Centre for the Protection of National Infrastructure (www.cpni.gov.uk) commissioned a multi-disciplinary team comprising the Universities of Oxford, Leicester and Cardiff to examine insider threat to businesses in the UK. The objectives of this joint venture being to develop a conceptual model of insider threat and a prototype monitoring solution, designed to detect cyber-insider threat before that threat is realised.

The project team is unique in drawing together expertise in the fields of cyber security, visual analytics, psychology, criminology and business management. This multi-disciplinary team is tasked with extending our understanding of insider threat, developing a practical and effective detection tool, and raising awareness and preparedness throughout UK businesses.

More detail on the project, the project team, and the Principle Investigator, Sadie Creese, Professor of CyberSecurity at the Department of Computer Science, University of Oxford, can be found here: <http://www.cs.ox.ac.uk/projects/CITD/>

The current study:

Previous phases of this research programme have allowed us to highlight a number of possible indicators which may permit the identification of insider threat risks. Currently we do not have a sufficiently good understanding of the 'normal' psychological and behavioural characteristics of staff in workplaces across the UK. We need to understand more about the baseline levels and variability of these psychological and behavioural indicators to allow us to accurately detect anomalies.

We ask for your assistance in recruiting volunteers for this study. We would like to discuss the opportunity to distribute an online survey to staff within your organisation.

This research study aims to widely survey staff across industries in UK business, in differing job functions and throughout the business hierarchy. The survey comprises 4 sets of online questionnaires, delivered via a secure online survey tool, and is run by psychologists at the University of Leicester, led by Professor Monica Whitty. Each of the 4 phases of the survey takes around 25 minutes to complete and are scheduled at broadly-spaced intervals over the coming year. The study has been approved by the University of Leicester Research Ethics Committee and has been determined not to pose risk of harm or distress to participants. All data collected are confidential and individuals or organisations participating in the study will never be identified.

On-going research activity:

Organisations participating in this study will be preferentially invited to participate in future activity. In early April 2014 the CPNI will host an invitation-only event under the working title of **"Insider Threat Detection: Integrating Theory and Practice"** which will bring together academics and practitioners in the field to share results and stimulate discussion on the topic of insider threat as it relates specifically to UK businesses. Further research initiatives propose to investigate attitudes towards insider Threats and approaches to insider threat detection in UK businesses, surveying business leaders and specialists in UK organisations. Our research team is also developing real-life, current case studies of insider threat and designing a series of educational courses to be delivered over the coming year, aimed at sharing experiences of insider threat and encouraging best practice within the UK business environment. We believe participation in the current study as well as in the future activity outlined above will be of benefit to organisations and UK business alike.

If you would like to discuss your organisation's involvement in the current study and register interest for future activity, please contact the Research Associate at the University of Leicester, Gordon Wright at grw9@le.ac.uk

Please contact the Research Associate at the University of Leicester, Gordon Wright, with any queries or for more information grw9@le.ac.uk

On behalf of Professor Monica Whitty (Principal Investigator, University of Leicester)



Longitudinal Survey of Employees – FAQs

Corporate Insider Threat Detection: Cyber Security Inside and Out

<http://www.cs.ox.ac.uk/projects/CITD/>

FAQs

What exactly is required from our organisation?

- We ask that you circulate the URL for the secure online study widely to your staff. Your staff may choose to participate entirely voluntarily. We guide participants through an informed consent procedure, carefully presenting their rights to privacy and to withdraw at any time if they wish. Once a participant clicks on the link, we ask for their email address and remind them about the later stages of the study directly. Nothing else is required from the organisation. We will share the published results with all individual participants and participant organisations once they are available, circa January 2015.

How much time does it take?

- Each of the 4 survey parts will take around 25-30 minutes to complete and can be done on any internet-connected device at the participant's convenience. The 4 survey parts are delivered between now and August 2014.

Who do you want to take the survey?

- We would like respondents from as many parts of your business as possible, and at as many levels of the business as possible. The data are better if we can get a representative sample of your entire organisation.

What's in it for the participants?

- Participants will be given feedback on their personality after the first part of the study. We have found that participants enjoy this insight. The later 3 stages of the survey include entries into a free prize draw for high-value cash prizes of £500, £1,000 and £2,000 respectively.

What's in it for us as an organisation?

- For reasons of data protection and confidentiality we have chosen to NOT share any data collected with participant organisations. We shall not report the names of organisations that have taken part in this research study.
- This research programme is on-going and organisations participating in this study will be preferentially invited to participate in future activity. In March 2014 the CPNI will host a 2-day event under the working title of "**Insider Threat Detection: Integrating Theory and Practice**" which will bring together academics and practitioners in the field of Security and Cyber Security to share results and stimulate discussion on the topic as it relates to UK security and preparedness. Further research initiatives propose to investigate attitudes and approaches to insider threat detection enacted by businesses, surveying business leaders in UK organisations. Our research team is also developing real-life, current case studies of insider threat and designing a series of educational courses to be delivered over the coming year, aimed at encouraging best practice within UK business. We believe participation in the current study and future projects outlined above will be of benefit to organisations and UK business alike.

Can we obtain access to the data collected in this survey?

- As specified above, we shall not be sharing the data generated in this study with participant organisations. We shall be undertaking a series of events including workshops and education events to share our findings to date and to encourage best practice in insider threat detection in the UK. Data from the current study will greatly inform our findings.

What questions are you going to ask?

- We are interested in 'normal' baseline behaviour. We do not suggest at any time that participants pose a threat to the organisation. The survey comprises a series of standard psychological tests of personality and questions about participants' psychological state, use of IT infrastructure and feelings about workplace behaviour. **NONE OF THE QUESTIONS WE ASK ARE DESIGNED TO ELICIT COMPANY SENSITIVE OR CONFIDENTIAL INFORMATION.** If a participant is concerned about any part of the process, we invite them to cease the survey and ask for their data to be withdrawn immediately.