Corporate Insider Threats – Perceptions on Scale and Risk, and Research Into New Detection Solutions

ICT Forum 2013 Conference, Professor Sadie Creese, July 11th 2013

Michael Goldsmith (Oxford), Monica Whitty, (Leicester), Min Chen (Oxford), David Upton (Oxford), Michael Levi (Cardiff), Phil Legg (Oxford), Eamon Mcquire (Oxford), Jason Nurse (Oxford), Jassim Happa (Oxford), Nick Moffat (Oxford), Ioannis Agrafiotis (Oxford), Gordon Wright (Leiceser)
But first......
Cyber Security Across University

Research
- information theory
- cryptography
- CS theory
- systems
- usability
- human factors
- privacy
- law, regulation
- process and risk management
- economics
- corporate governance
- international policy
- intelligence
- national security

Education
- MSc in Software and Systems Security
- CS Security Modules
- executive education
- doctoral programmes
- elements in Masters programmes in OII, Blavatnik, ...

University itself
- Good practice
- awareness and general education
- experimental test community
- information security Policy
Academic Centres of Excellence in Cyber Security Research

GCHQ-EPSRC sponsored programme; modelled on a large, established scheme in the USA.

Review process: assessment based on research portfolio, doctoral programme, staff profile, vision and plans

Eight centres recognised in 2012; three more in 2013
Oxford, Bristol, Royal Holloway, Imperial, UCL, Southampton, QUB, Lancaster, Cambridge, Birmingham, Newcastle
Our aim is to understand **how to deliver effective cyber security** both within the UK and internationally. We will make this knowledge available to governments, communities and organisations to **underpin the increase of their capacity** in ways appropriate to ensuring a cyber space which can continue to grow and innovate in support of well-being, human rights and prosperity for all.
Global Centre for Cyber Security Capacity-Building

Sadie Creese
Dept. of Computer Science

Ian Brown
Oxford Internet Institute

Angela Sasse
UCL

Marco Gercke
Cybercrime Research Inst.

Paul Cornish
Exeter University

Bill Dutton
Oxford Internet Institute

Ivan Toft
Blavatnik School of Govt.

Andrew Martin
Dept. of Computer Science

Michael Goldsmith
Dept. of Computer Science

Fred Piper
Royal Holloway U. London
Data Collection & Synthesis

Reflection & Hypothesizing

Testing & Validation

Knowledge Transfer

Assists

Best Practice

Case Studies

Expert Community

Capacity Maturity Metrics and Model

Gap Analysis and Policy Options

International Community

Industry

National

Civil Society

Cyber Security Science and Humanities Knowledge

Capacity Building Expertise

Cyber Security Science and Humanities Knowledge
new model of PhD/DPhil

- promoted and funded by research councils
- £3.6m grant; 12 funded places per year; 3 annual intakes

year one:

- intensive education in cyber security
- two mini-projects (internships encouraged)
- seminars, industry ‘deep dives’, field trips

years two–four:

- research in an Oxford academic department
- skills training throughout
- retain contacts with internship companies

security of big data

cyber-physical security

effective verification and assurance

real-time security
And back......
Part 1 – Overview of Technical Approach
What is Insider Threat?

An employee, affiliate or entity (person or not) of an enterprise with legitimate credentials who deliberately or unknowingly poses a risk to the enterprise it is tied to wholly or partially.

An insider threat is [posed by] an individual with privileges who misuses them or whose access results in misuse [Hunker 2011].

A malicious insider is a current or former employee, contractor, or other business partner who has or had authorized access to an organization’s network, system, or data and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization’s information or information systems [Cappelli 2009].

The insider threat refers to harmful acts that trusted individuals might carry out; for example, something that causes harm to the organization, or an unauthorized act that benefits the individual [Greitzer 2012].
Aims and Objectives

• **Aim:** To deliver a significantly enhanced capability for insider threat detection.

• **Objective:** To provide an all-encompassing approach on both the detection system required, and the contributing factors that impact on insider threat detection from related disciplines.
• Conceptual model -> computational model for insider threat and detection
• Psychological indicators
• Pattern extraction, correlation and mining algorithms
• Enterprise culture and common practices, operational issues
• Visual analytics interface to support human understanding
• Education and awareness tools
Lead Investigators

- Professor Sadie Creese
  - Cybersecurity, University of Oxford
- Professor Michael Goldsmith
  - Cybersecurity, University of Oxford
- Professor David Upton
  - Operations Management, University of Oxford
- Professor Min Chen
  - Visual Analytics, University of Oxford
- Professor Monica Whitty
  - Contemporary Media and Cyber- Psychology, University of Leicester
- Professor Michael Levi
  - Criminology, Cardiff University
Project Outputs

- **Survey** that captures the *current perception and practice* for insider threat detection within organisations.

- **Prototype detection system** that can alert of malicious employee activity and misuse in near real-time based on both observable patterns and cyber-psychological behaviours.

- **Visual analytics interface** for analyst exploration of organisation and employee alerts and activities.

- Education and raising awareness of insider threat through white paper publications and *teaching materials*.

- Contribution to recognised standards for future IDS systems.
Modeling Approach

• Conceptual
  – What is the scope of information that could possibly be collected?

• Feasible
  – What is actually feasible to collect?
  – E.g., How would one quantify employee mentality or disgruntlement?

• Ethical / Legal
  – What is ethically feasible to collect?
  – E.g., Social media monitoring may be a breach of privacy.
System vulnerabilities, attack patterns and targets, threat classes / capability, specific events of interest

System components, assets, processes, physical characteristics

Model v1

Available data sets and contexts

Work-flow and role based opportunities for detection

Validate against initial survey, input first psychological indicators

Validate against practice analysis, focus groups, wider community consultation, including executive education and MBA.

Validate against test results and further input from other work packages
**Tiered Approach**

- **Bottom-up approach**
  - The system detects anomaly and alerts to the user.
  - Deviations from normal behaviour may indicate suspicious activity.
  - Need to manage false positives/false negatives rates generated by system.
  - Machine learning / data mining techniques.

- **Top-down approach**
  - Suspicions may arise from observed behaviour.
  - The analyst can investigate recent activity to identify anomalous behaviour.
  - Visual Analytics interface facilitates human understanding of large data.
Part 2 – Early Findings
Survey of Protective Monitoring Practices

Purpose:
Preliminary analysis of common protective monitoring and detection practices in corporate environments, to then feed into wider research tasks.

Literature:
Review of openly published reports from a range of sources revealed three key areas: Level and Nature of Insider Attack, Views on Risk, Detection Practice.

Study:
Conducted a pilot study with 48 participants to discover initial impressions of insider threats in organisations.

Future:
Full scale survey (>1000 participants) to be conclude early 2014.
Insider attacks are a significant proportion of the attacks faced by companies.

Well-defined and prevalent types of attacks.

Nature and potential for insider attacks expanded due to new technologies.

Corporations still lack appropriate measures for the new risks.

Companies continue to underestimate insider threats.

Lack of formal reviews, spending on security, and awareness of the issues.

Cost of trade secret thefts exceeds $250 million per year, predicted to double over the next decade.

Ford Motor Company had an employee steal trade secrets valued at in excess of $50 million.

A variety of approaches proposed, e.g. monitoring suspicious behaviour, establishing a baseline of normal.

Currently many insider incidents are detected by non-technical means.

Growing popularity in the use of automated tools to help manage insider risk, e.g., Enterprise Fraud Management (EFM) solutions.
Highlights from Web-based Survey

Do you think that the threat from insiders is growing or diminishing?

Almost half of the respondents felt that the threat from insiders was growing.

Please describe the extent to which you can predict insider threats before they conduct attacks.

This is an important question that validates the aim of the overall project. 76% of managers said that they were only able to predict an insider attack with difficulty or not at all.

Is insider-threat detection an important part of your organisation’s culture?

A strong majority say that insider threat detection was not part of the culture. This suggests that there may be cultural challenges in changing both attitudes and behaviour on the topic.
Insider attacks are rising, consequences are potentially more significant, under-reported.

View of the community: some best practice in place but more can certainly be done to improve detection.

Poor education on the topic. Highlights the importance of awareness and education needs.
Focus groups & Case Studies

- Considering how the acts took place
- Type of person/personality
- Social/psychological background
- Motivation of staff
- How they were caught out
- What could have been done better in hindsight
Example 1

- Male security
- Stealing data using KVM
- At work or left overnight
  - **Psychological background**: extremely nervous behaviour
  - **Motivation**: money
Example 2

• Male, long term employed (20 years)
• Psychological background: long-term aggressive behavior
• Organisational background: passed from manager to manager; prior to fraud given a written warning for fraud with respect to claims for times/expenses
• After the fraud: discovered long telephone calls to sex lines; breached security
• Attack: fraud: large sums of money, faked hospital letter
• Motivation: disgruntled employee; weak social identity with organisation;
• Detected: fellow workers reported odd behaviour
Example 3

- Male, security; access to most of building
- **Psychological background:** Asperger’s
- Breached security online by creating a replica of the building within second life – which caused problems with security of the building.
- Logged on at work at odd hours.
Immediate Future Cases

• Professional Sporting Organisation – IP theft and receipt
• Global Telecoms Infrastructure – IP theft
• Global Logistics – systems corruption / theft of physical assets
• Cloud Disaster Recovery – systems corruption / Denial of Service
• Financial Sector – more than just fraud
Potential new Cyber-indicators

• Stress
• Change in mood
• Personality (e.g., dark triad)
• Impulsivity
• Change in online behaviours
• Social network information (e.g., bragging; excessive money spent on holidays).
Underpinning the Education

• Investigating Cyber Risk communication within MBA environment
• Strong interest in ‘sexy’ attack / threat material
• Less interest in defence considerations
• => need to adapt message and materials accordingly
• Next steps: bespoke insider sessions and teaching case studies
Statistical Profiling

- Observed data to be incorporated into network through statistical profiling.
  - Time-based, frequency-based, and pattern-based profiles of employees.

Example Video for Time-based profiling

Top: Current observed activity.
Middle: Cumulative observed profile.
Bottom: Normal profile.

Left-to-right: Login, Logout, Duration, Removable Device, Email, Web.

User does not normally use a removable device. However, observed profile shows early morning activity of login, removable device usage, and web activity.
Visual Analytics Interface
Thank you for listening.

Questions?