Mitigating the Insider Threat to the Financial Industry

Chris Hurran

19 November 2014

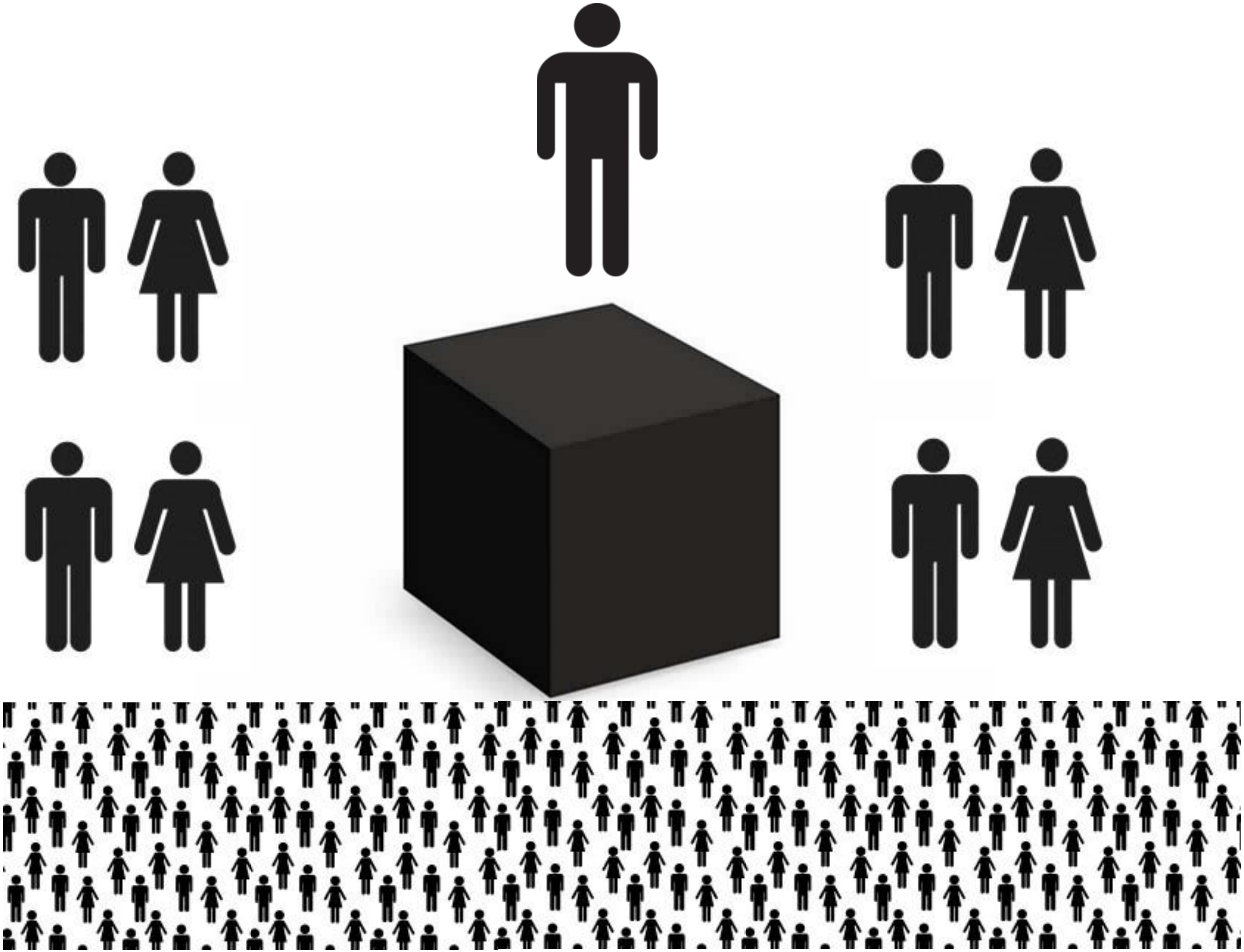
People risk is the risk of damage from the actions of employees or contractors working on your behalf.

Employee risk is defined as counterproductive behaviour, whether inadvertent, negligent or malicious, that can cause harm to an organisation.

An insider is a person who exploits, or has the intention to exploit, their legitimate access to an organisation's assets for unauthorised purposes.

Employee risk is the likelihood of an organization being harmed by a threat or a loss of some kind caused by an employee, and how serious the harm could be.

A *malicious insider threat* to an organization 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.



CPNI
Centre for the Protection
of National Infrastructure

CPNI INSIDER DATA COLLECTION STUDY

REPORT OF MAIN FINDINGS

APRIL 2013

Freedom of Information Act (FOIA)

This information is supplied in confidence and may not be disclosed other than to the agreed readership, without prior reference to CPNI. Within the UK, this material is exempt from disclosure under the relevant Freedom of Information Acts and may be subject to exemption under the Environmental Information Regulations and the Data Protection Act 1998.

Disclaimer

To the fullest extent permitted by law, CPNI accepts no liability for any loss or damage (whether direct, indirect or consequential and including, but not limited to, loss of profits or anticipated profits, loss of data, business or goodwill) incurred by any person and howsoever caused arising from or connected with any error or omission in this document or from any person acting, omitting to act or refraining from acting upon, or otherwise using, the information contained in this document or its references. You should make your own judgement as regards use of this document and seek independent professional advice on your particular circumstances.

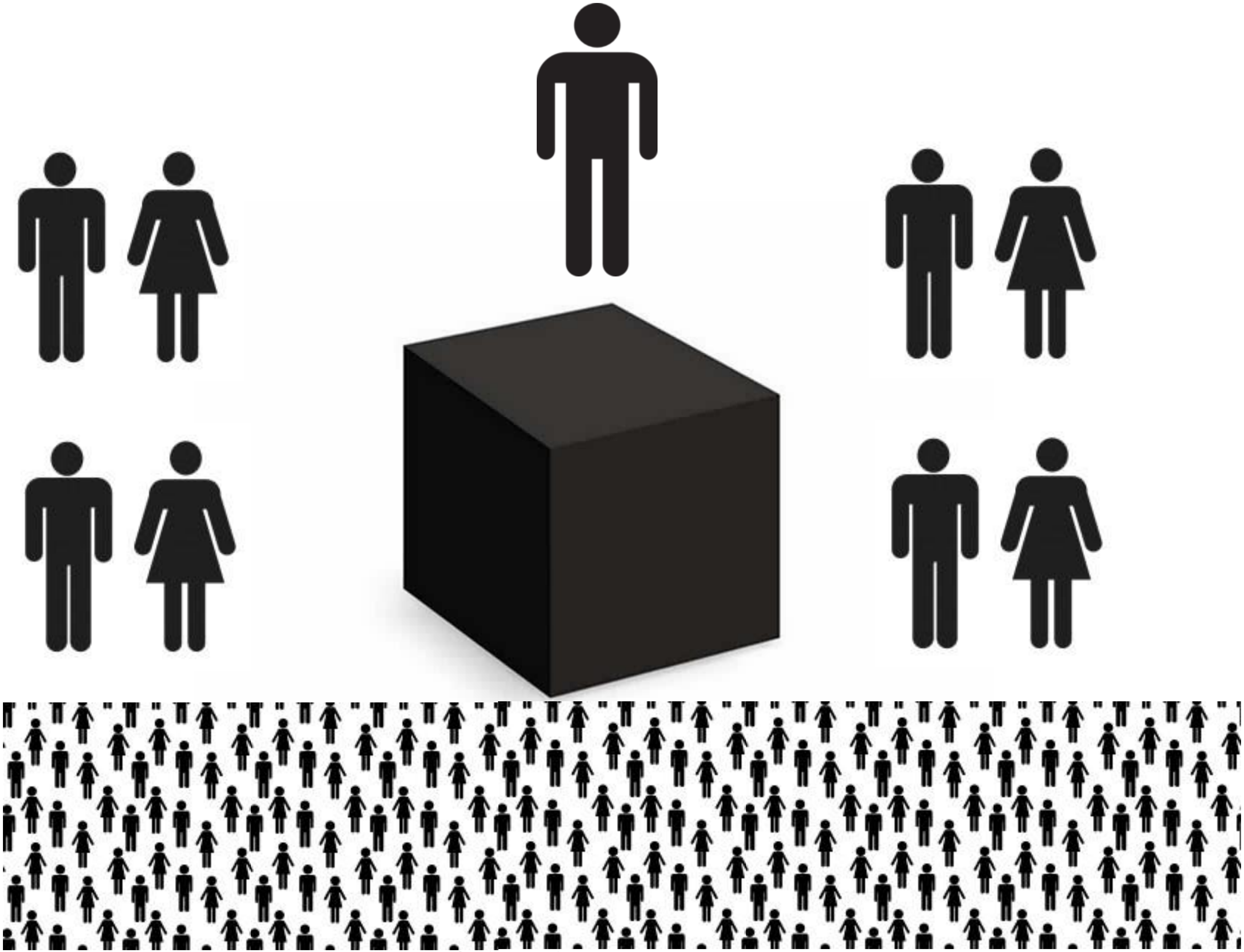
PWC Global State of Information Security Survey 2015

- “Employees are the most-cited culprits of incidents.”

- “The percentage of respondents who point the finger at current employees jumped by 10% over 2013.”

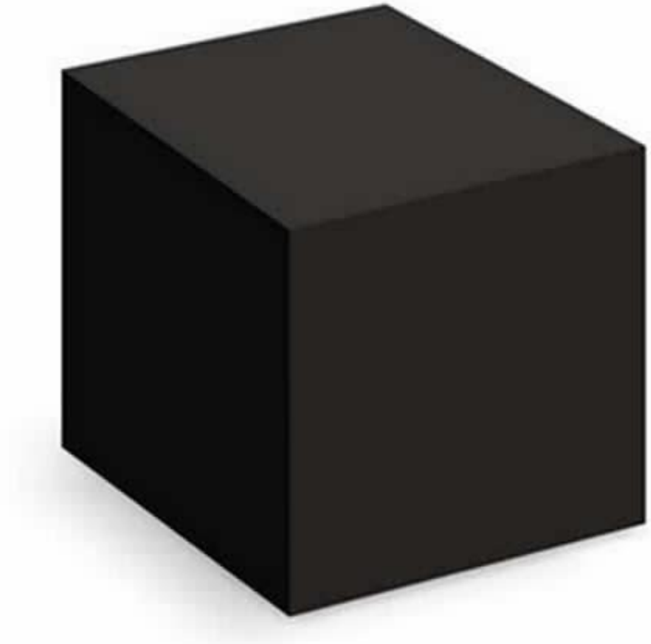
- “insiders, current and former employees in particular, have become the most cited culprits of cybercrime.”

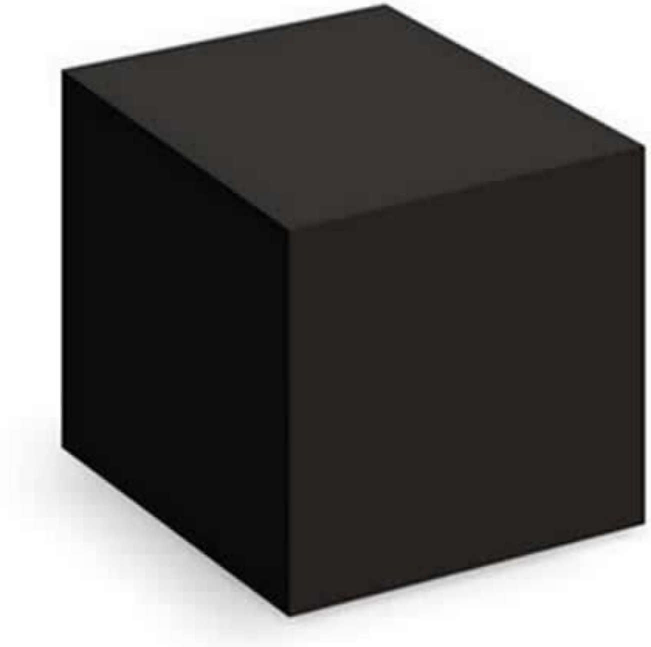
- “Yet many companies do not have an insider threat program in place, and are therefore not prepared to prevent, detect, and respond to internal threats.”



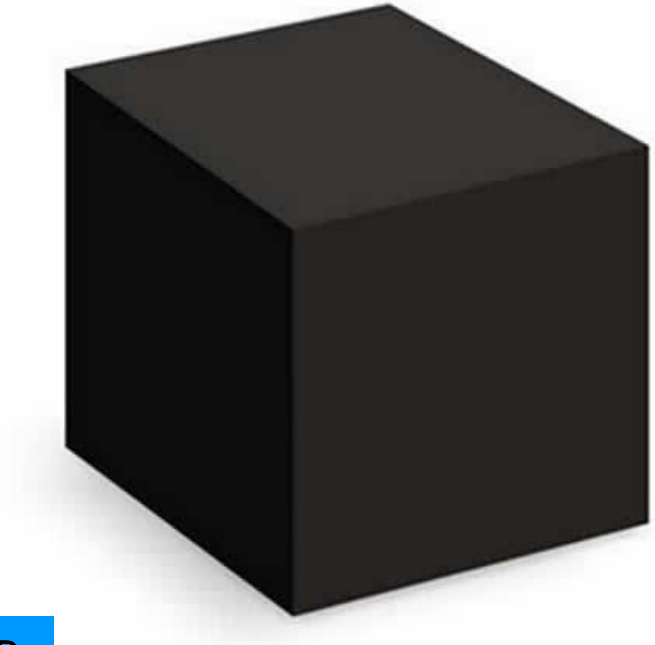
REUTERS

SMBC SUMITOMO MITSUI
BANKING CORPORAT

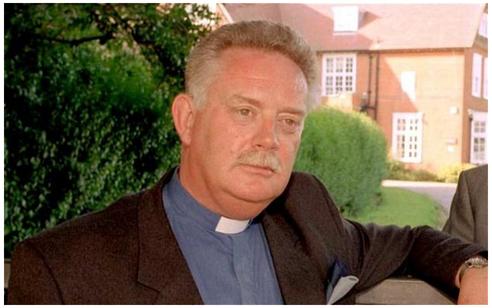


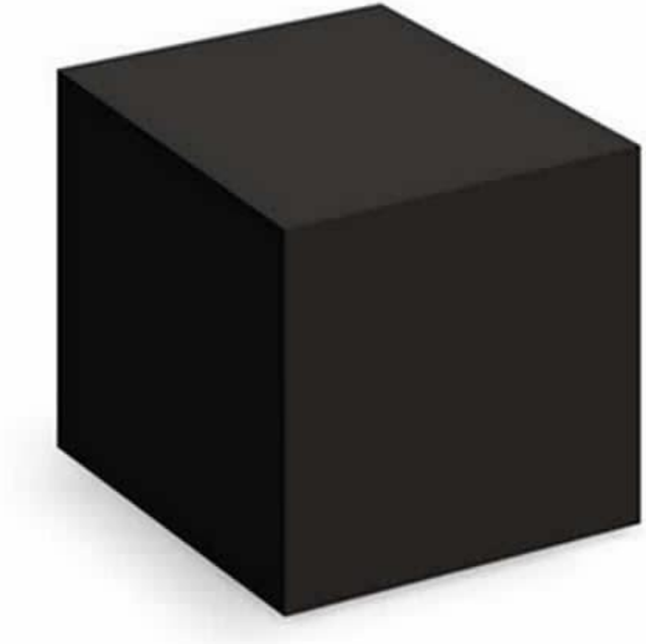


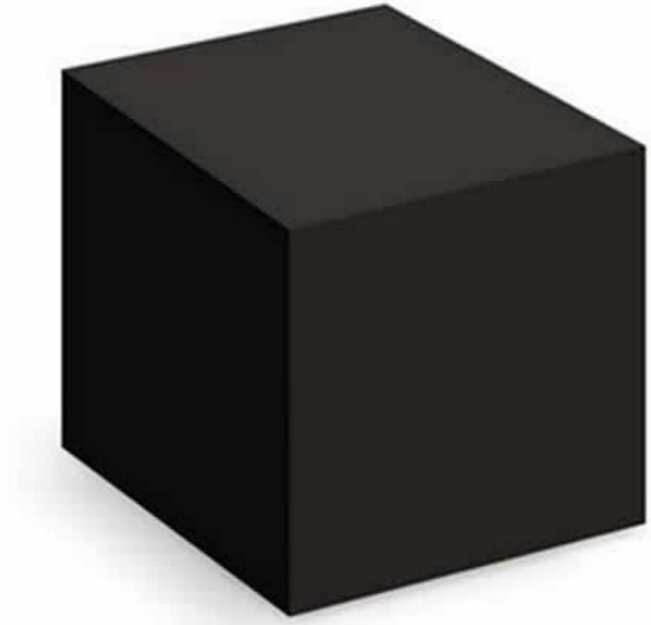
ROGER DURONIO

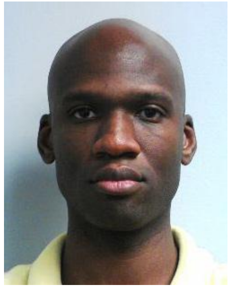


BARCLAYS LIBOR

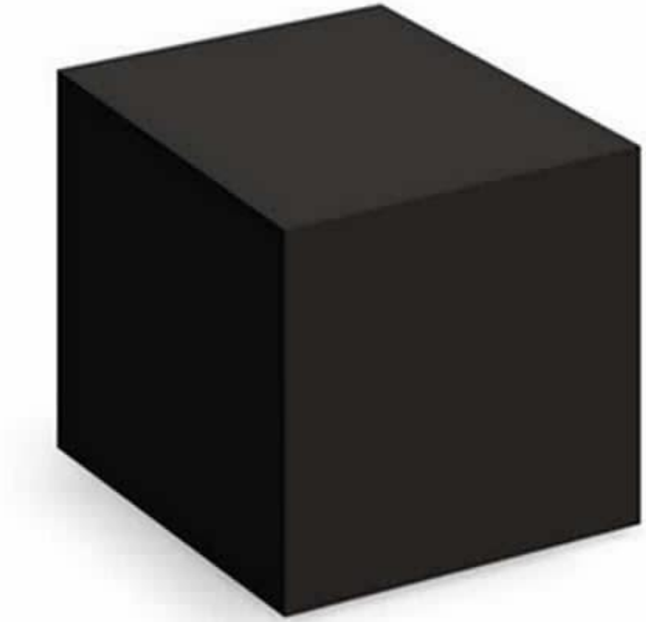


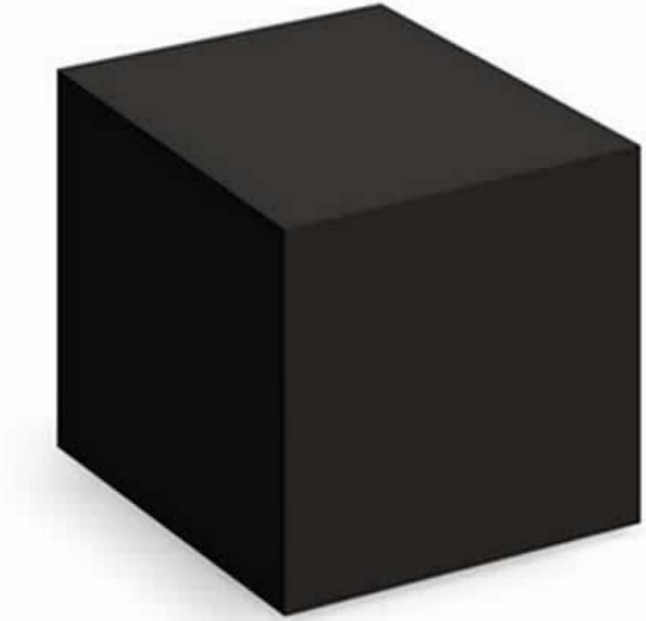


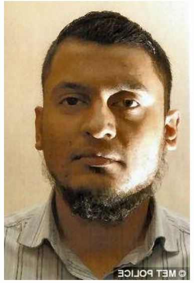


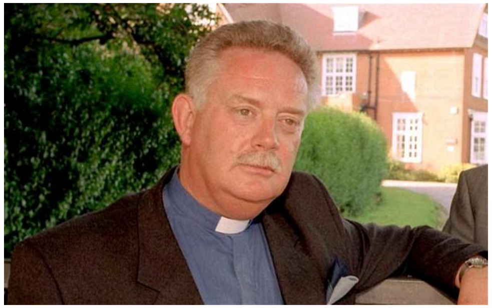


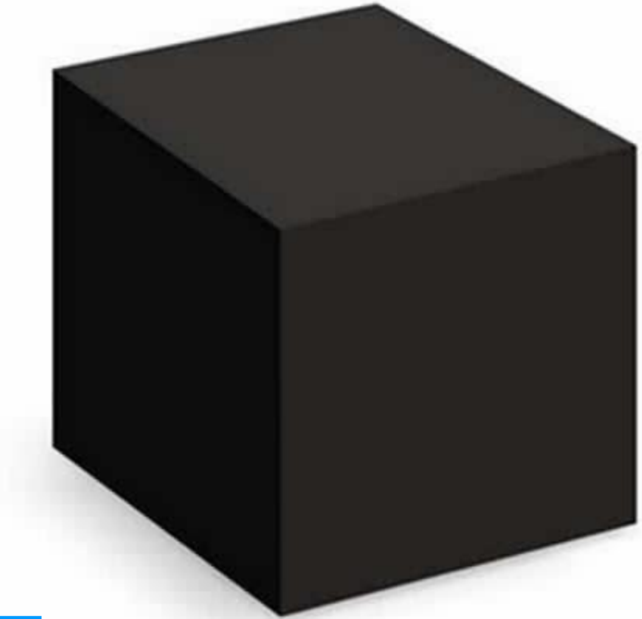
R. DONOVAN






© MET POLICE

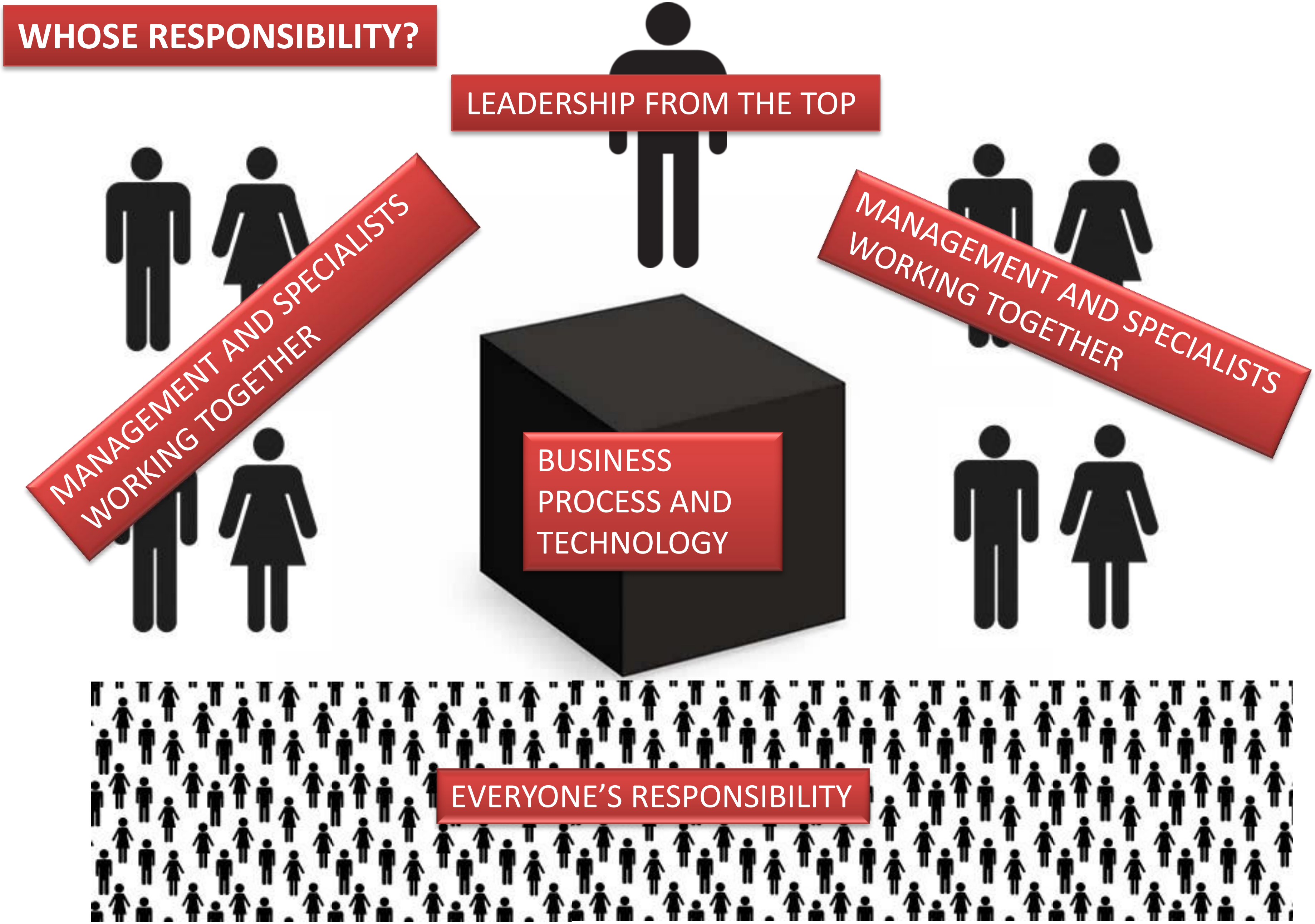




BARCLAYS LIBOR

ROGER DURONIO

WHOSE RESPONSIBILITY?



LEADERSHIP FROM THE TOP

MANAGEMENT AND SPECIALISTS WORKING TOGETHER

BUSINESS PROCESS AND TECHNOLOGY

MANAGEMENT AND SPECIALISTS WORKING TOGETHER

EVERYONE’S RESPONSIBILITY

Insider Risk Mitigation:
Ten Steps for All Organisations

- Governance
- Roles, responsibilities and resources
- Assets
- Risk
- Culture
- Impact
- Response
- Transparency and awareness
- Supply chain
- Audit

Insider Risk Mitigation:
Ten Steps for All Organisations

- **Governance**
- Roles, responsibilities and resources
- Assets
- Risk
- Culture
- Impact
- Response
- Transparency and awareness
- Supply chain
- Audit

Insider Risk Mitigation:
Ten Steps for All Organisations

- Governance
- **Roles, responsibilities and resources**
- Assets
- Risk
- Culture
- Impact
- Response
- Transparency and awareness
- Supply chain
- Audit

Insider Risk Mitigation:
Ten Steps for All Organisations

- Governance
- Roles, responsibilities and resources
- **Assets**
- Risk
- Culture
- Impact
- Response
- Transparency and awareness
- Supply chain
- Audit

Insider Risk Mitigation: Ten Steps for All Organisations

- Governance
- Roles, responsibilities and resources
- Assets
- **Risk**
- Culture
- Impact
- Response
- Transparency and awareness
- Supply chain
- Audit

Insider Risk Mitigation:
Ten Steps for All Organisations

- Governance
- Roles, responsibilities and resources
- Assets
- Risk
- **Culture**
- Impact
- Response
- Transparency and awareness
- Supply chain
- Audit

Insider Risk Mitigation:
Ten Steps for All Organisations

- Governance
- Roles, responsibilities and resources
- Assets
- Risk
- Culture
- **Impact**
- **Response**
- Transparency and awareness
- Supply chain
- Audit

Insider Risk Mitigation: Ten Steps for All Organisations

- Governance
- Roles, responsibilities and resources
- Assets
- Risk
- Culture
- Impact
- Response
- **Transparency and awareness**
- Supply chain
- Audit

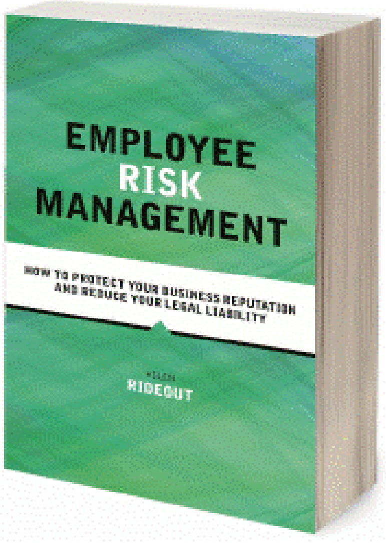
Insider Risk Mitigation: Ten Steps for All Organisations

- Governance
- Roles, responsibilities and resources
- Assets
- Risk
- Culture
- Impact
- Response
- Transparency and awareness
- **Supply chain**
- **Audit**

Insider Risk Mitigation:
Ten Steps for All Organisations

- **Governance**
- **Roles, responsibilities and resources**
- **Assets**
- **Risk**
- **Culture**
- **Impact**
- **Response**
- **Transparency and awareness**
- **Supply chain**
- **Audit**

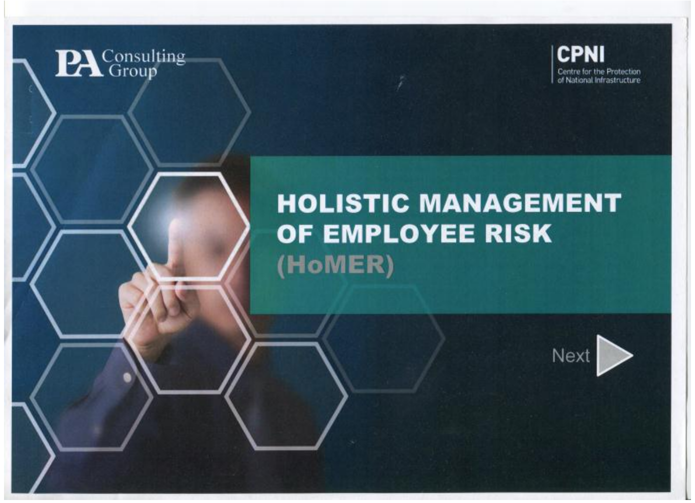
Further Reading



EMPLOYEE RISK MANAGEMENT

HOW TO PROTECT YOUR BUSINESS REPUTATION AND REDUCE YOUR LEGAL LIABILITY

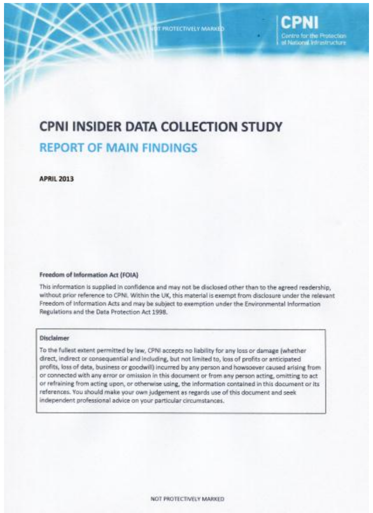
HELEN RIDEOUT



PA Consulting Group

CPNI
Centre for the Protection of National Infrastructure

HOLISTIC MANAGEMENT OF EMPLOYEE RISK (HoMER)



NOT PROTECTIVELY MARKED

CPNI
Centre for the Protection of National Infrastructure

CPNI INSIDER DATA COLLECTION STUDY

REPORT OF MAIN FINDINGS

APRIL 2013

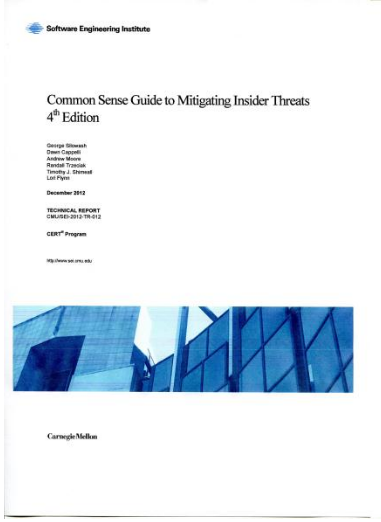
Freedom of Information Act (FOIA)

This information is supplied in confidence and may not be disclosed other than to the agreed readership, without prior reference to CPNI. Within the UK, this material is exempt from disclosure under the relevant Freedom of Information Acts and may be subject to exemption under the Environmental Information Regulations and the Data Protection Act 1998.

Disclaimer

To the fullest extent permitted by law, CPNI accepts no liability for any loss or damage (whether direct, indirect or consequential and including, but not limited to, loss of profits or anticipated profits, loss of data, business or goodwill) incurred by any person and howsoever caused arising from or connected with any error or omission in this document or from any person acting, omitting to act or refraining from acting upon, or otherwise using, the information contained in this document or its references. You should make your own judgement as regards use of this document and seek independent professional advice on your particular circumstances.

NOT PROTECTIVELY MARKED



Software Engineering Institute

Common Sense Guide to Mitigating Insider Threats
4th Edition

George Silowash
Dawn Cappelli
Andrew Moore
Randall Trzeciak
Timothy J. Shimeall
Lori Flynn

December 2012

TECHNICAL REPORT
CMU/SEI-2012-TR-012

CERT® Program

http://www.sei.cmu.edu

CarnegieMellon

INSIDER RISK

CYBER INSIDERS: A BOARD ISSUE

Cyber security is an issue on the agenda for most boards. The insider threat generally receives less attention. As a result, the human factors aspects of cyber security can become the weak link in organisations' cyber defences, leaving the organisations vulnerable and their boards open to criticism and reputational damage. This article explores the subject of cyber insiders and the key measures all boards should take to ensure that their organisation is appropriately protected against this threat.

By Chris Hurran, OBE, Senior Associate Fellow of the Institute for Security and Resilience Studies at University College London.

Institute for Security & Resilience Studies

INTRODUCTION

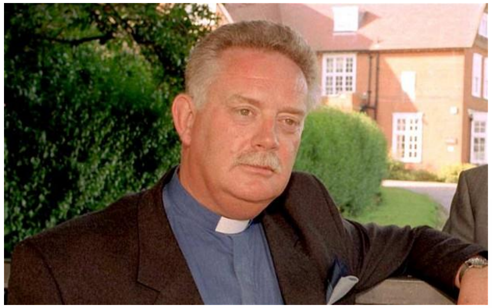
Boards are increasingly concerned about the threat to their business from cyber-attack. Businesses invest significantly in technical measures to protect their assets and they employ highly qualified and highly paid technical experts to deliver this protection. Alternatively, they may attempt to outsource the whole problem by paying others to provide the protection on their behalf. Of course, technology and high priced help have an important role to play in cyber security, but all this investment can be undermined all too easily from another source – **the organisation's own employees**. There is limited definitive data on the scale of this issue, but the PwC 2013 Information Security Breaches Survey' indicates that 36 per cent of the worst security breaches in the year were caused by inadvertent human error (and a further 10% by deliberate misuse of systems by staff), and 57% of small businesses suffered staff-related security breaches in the last year. So this is a non-trivial problem and boards ignore it at their peril.

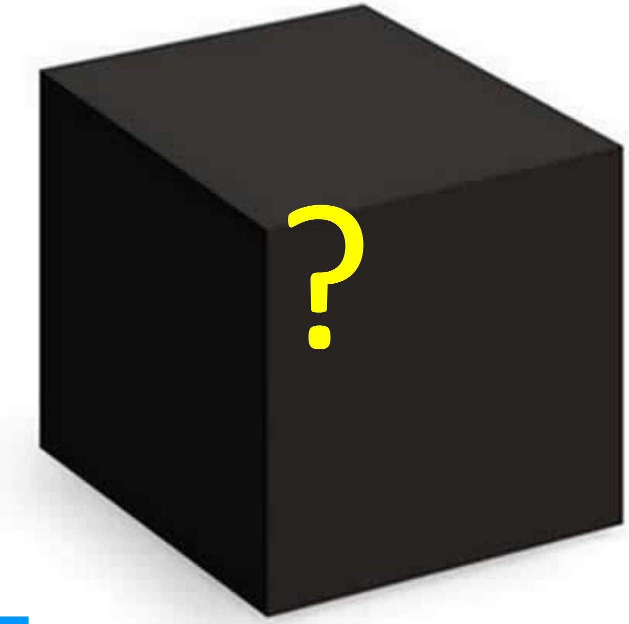
THE EMPLOYEE AS A CYBER INSIDER

Who are these troublesome employees? Cyber insiders can come from any part of the business (including the board itself!) and manifest themselves in three types:

Non-malicious and unintentional: These employees do not mean to do anything wrong. The fact that they cause harm is the organisation's fault. Either unsuitable people were recruited; or they were not trained properly; or the security culture is defective; or the organisation

cybersecurity-review.com 1





BARCLAYS LIBOR

ROGER DURONIO

christopher.hurran@gmail.com