

INFORMATION SECURITY DECISIONS

How to Handle Insider Threats



INFORMATION SECURITY DECISIONS

Who am I?

Maths degree, Academic IT, UKERNA (JANET and UK Naming Committee), Virgin Net, Investment Bank Information Risk Contracts (ING, Barcap), LIFFE, Barcap, Barclays.







How do insider threats fit in?

Risk Areas	Description	Specific Risks
EXTERNAL THREATS	 Threats originating outside the bank Motivated by illegal financial gain or 'personal challenge/fun' 	 Organised crime Journalists Malicious Code Hackers Social Engineering
I NSI DER THREATS	 Threats originating from employees and contractors Motivated by revenge and greed (MICE) 	LeaversLogical AccessData Theft
MATERIAL ERRORS	 Unintended mistakes that are large enough to matter Usually caused by manual error 	Data QualitySpreadsheet errors
REGULATORY AND LEGAL BREACHES AND FAILURES	 Failure to meet new and evolving regulatory and legal demands Often caused by combinations of lack of awareness, process and reliance on legacy technologies that don't meet newer demands 	 Privacy/Data Protection Records Management

[C]ompromise [E]go

• [M]oney

• [I]deology

MICE





INFORMATION SECURITY DECISIONS

The Pareto principle – and insulting those you work with.



http://www.cert.org/insider_threat/insidercross.html

- A negative work-related event triggered most of the insiders' actions.
- Sixty-two percent of incidents were planned in advance.
- Eighty percent of the insiders exhibited unusual behavior in the workplace prior to carrying out their activities.
- Fifty-seven percent of insiders exploited systemic vulnerabilities in applications, processes and/or procedures.
- Thirty-nine percent used relatively sophisticated attack tools.
- Sixty percent of insiders compromised computer accounts, created unauthorized backdoor accounts or used shared accounts in their attacks.
- Most incidents were carried out via remote access.
- Less than half of the insiders (43%) had authorized access at the time of the incident.
- Insider activities caused financial losses (81%), negative impacts to business operations
- (75%) and damage to the organizations' reputations (28%).

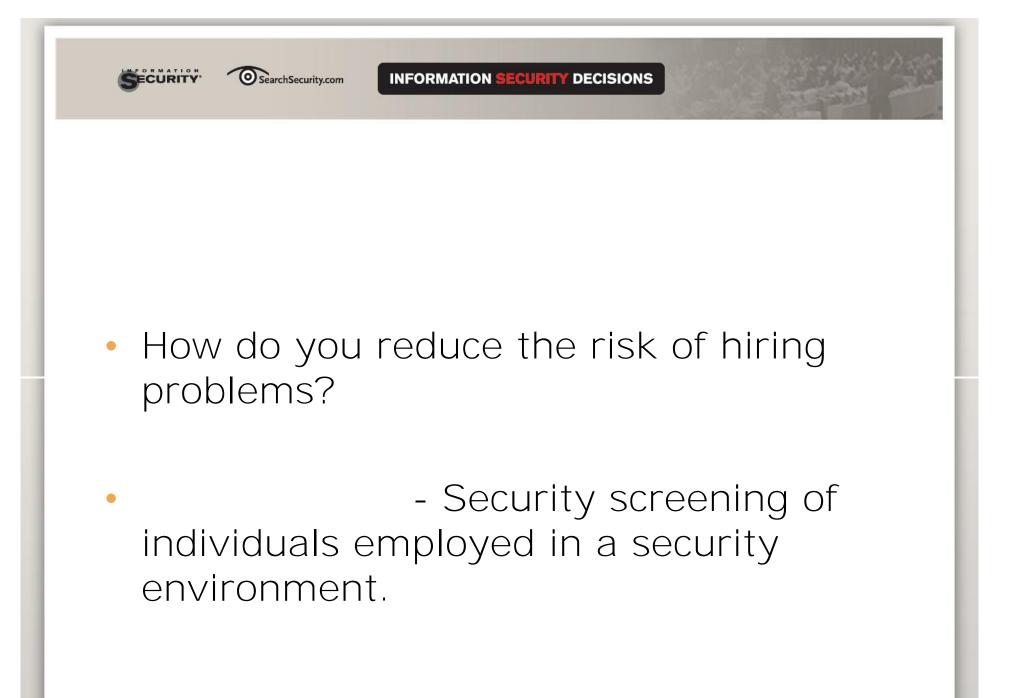


INFORMATION SECURITY DECISIONS

The Basics

What are you doing about

- Highly privileged access?
- Remote access?
- Logical access?
- Least privilege?
- Leavers?





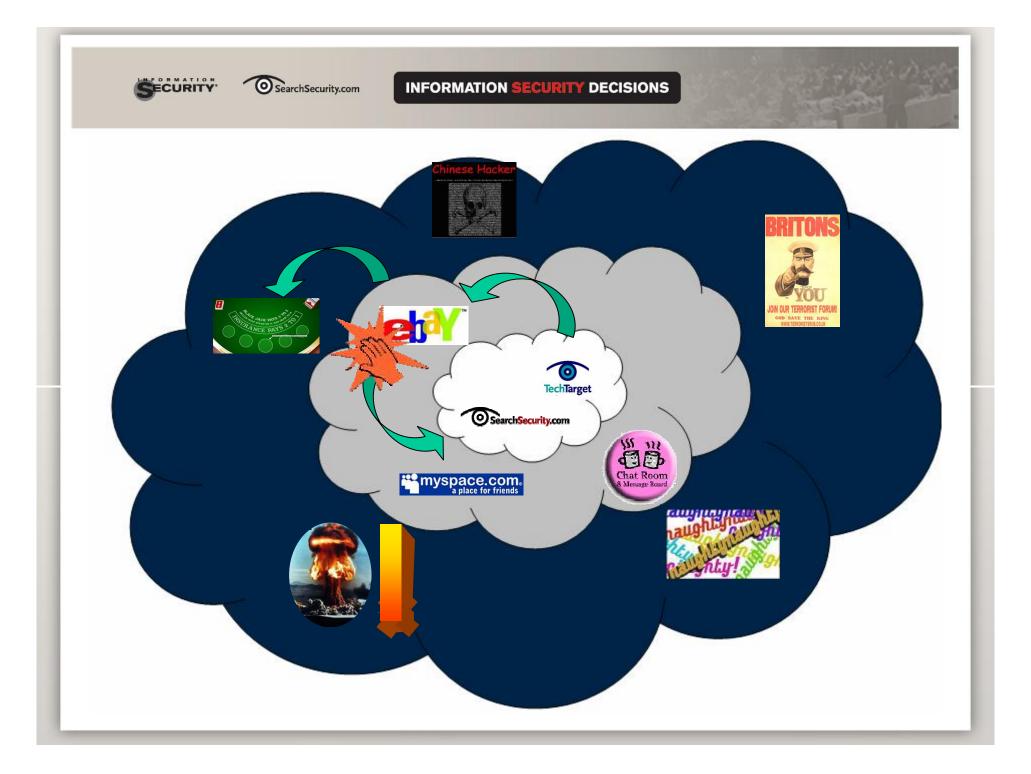
INFORMATION SECURITY DECISIONS

Deterrent

Can you provide a system of evidence to staff that convinces them they will be caught?

Without:

- alienating staff?
- throttling business?





Abuse of:

- Authorized access by authorized staff
- Unauthorized access by unauthorized staff



INFORMATION SECURITY DECISIONS

Outsiders

What is the core goal of outsider attackers?



INFORMATION SECURITY DECISIONS

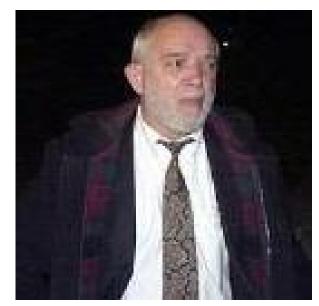
What is the difference between a disgruntled employee and an insider threat?



INFORMATION SECURITY DECISIONS

Case studies

Roger Duronio

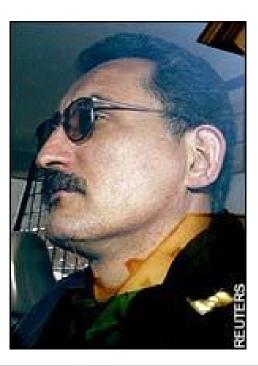




INFORMATION SECURITY DECISIONS

Case studies

Ian Parr





INFORMATION SECURITY DECISIONS

Case studies

Single Issue Groups



INFORMATION SECURITY DECISIONS





INFORMATION SECURITY DECISIONS





INFORMATION SECURITY DECISIONS





INFORMATION SECURITY DECISIONS





INFORMATION SECURITY DECISIONS





INFORMATION SECURITY DECISIONS





INFORMATION SECURITY DECISIONS

Case studies

Northern Bank



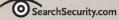


INFORMATION SECURITY DECISIONS

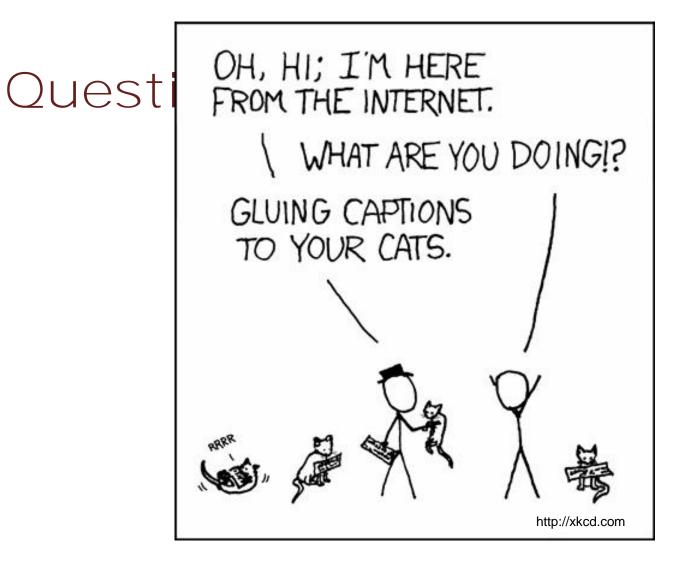
Questions?

<Witty image to do with insiders>





INFORMATION SECURITY DECISIONS





INFORMATION SECURITY DECISIONS

Questions?

Stephen Bonner

<u>Stephen.Bonner@barclays.com</u>