

How to Handle Insider Threats

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.



AWARDS
2006
WINNER



AWARDS
2007
FINALIST



AWARDS
2007
FINALIST

How do insider threats fit in?

Risk Areas	Description	Specific Risks
EXTERNAL THREATS	<ul style="list-style-type: none"> Threats originating outside the bank Motivated by illegal financial gain or 'personal challenge/fun' 	<ul style="list-style-type: none"> Organised crime Journalists Malicious Code Hackers Social Engineering
INSIDER THREATS	<ul style="list-style-type: none"> Threats originating from employees and contractors Motivated by revenge and greed (MICE) 	<ul style="list-style-type: none"> Leavers Logical Access Data Theft
MATERIAL ERRORS	<ul style="list-style-type: none"> Unintended mistakes that are large enough to matter Usually caused by manual error 	<ul style="list-style-type: none"> Data Quality Spreadsheet errors
REGULATORY AND LEGAL BREACHES AND FAILURES	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> Privacy/Data Protection Records Management

MI CE

- [M]oney
- [I]deology
- [C]ompromise
- [E]go

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%).

The Basics

What are you doing about

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

- How do you reduce the risk of hiring problems?
- - Security screening of individuals employed in a security environment.

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

Outsiders

What is the core goal of outsider attackers?

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

Case studies

Roger Duronio



Case studies

Ian Parr



Case studies

Single Issue Groups

Case studies



Case studies



Case studies



Case studies



Case studies



WE WILL BE BACK

Case studies



Case studies

Northern Bank



Questions?

<Witty image to do with insiders>

Question

OH, HI; I'M HERE
FROM THE INTERNET.

\ WHAT ARE YOU DOING!?

GLUING CAPTIONS
TO YOUR CATS.



<http://xkcd.com>

Questions?

Stephen Bonner

Stephen.Bonner@barclays.com