

Memex

The answer to your search

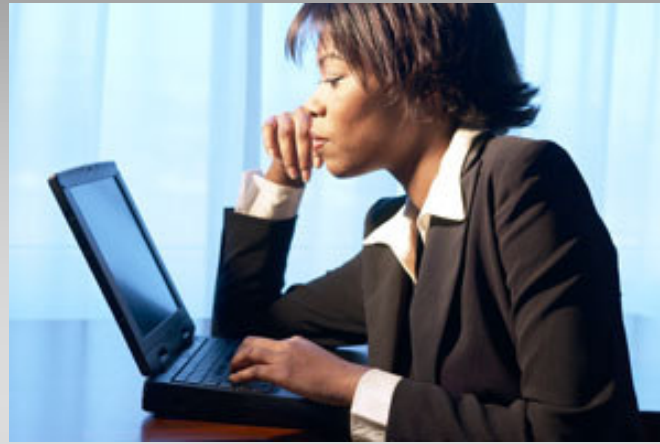
www.memex.co.uk

“Trust In Software”

Jim McCumesty, Head of Software Development, Memex.

ADS Programme / ScotlandIS / CybersecurityKTN seminar
Edinburgh - 26 February 2007

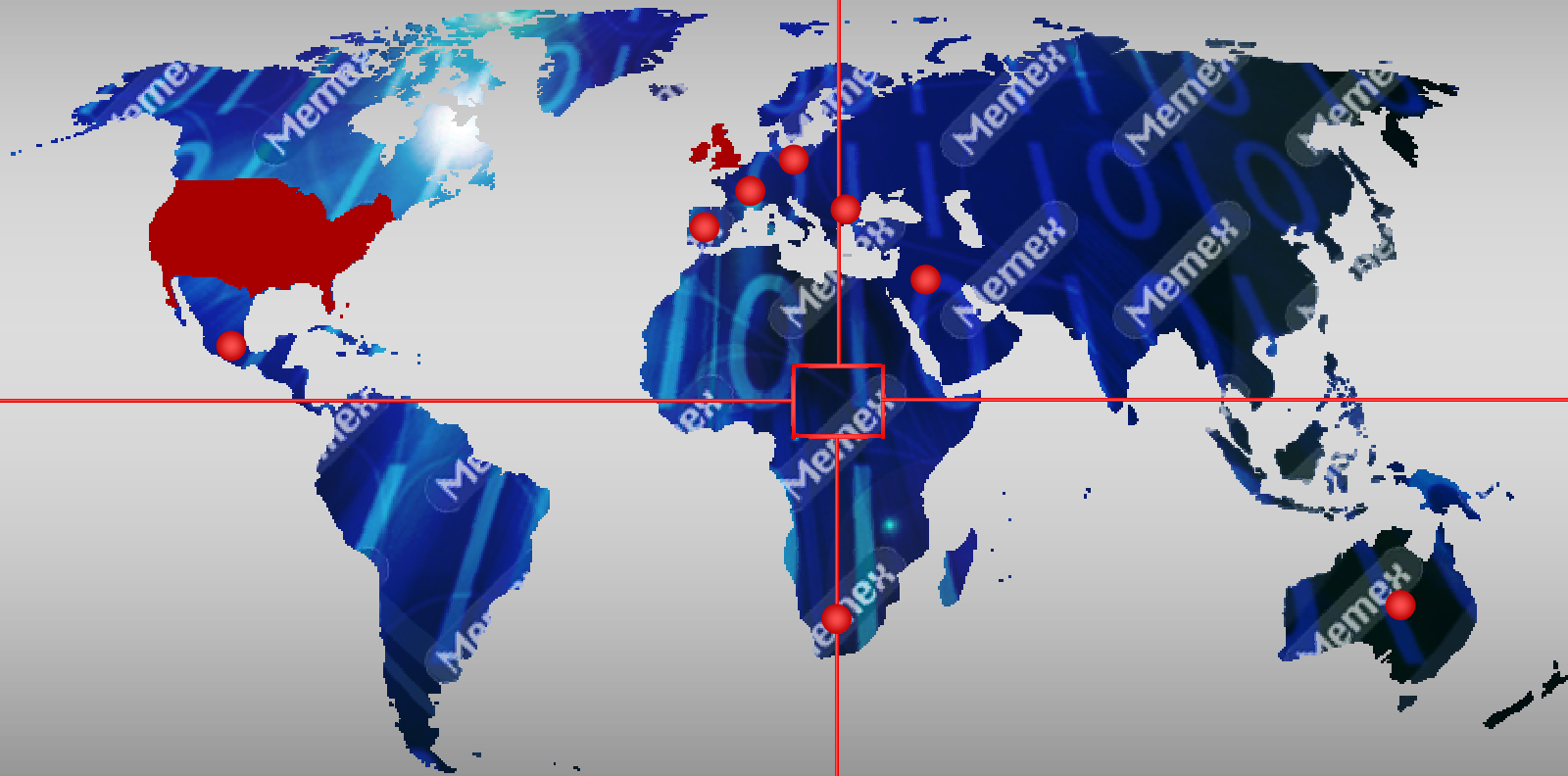
Our Customers



The Problems We Solve



Markets and Partners



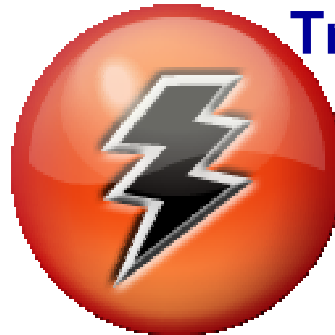
Challenges for Intelligence-Lead Organisations

Memex
The answer to your search

www.memex.co.uk



**Allocation of
scarce
resources**



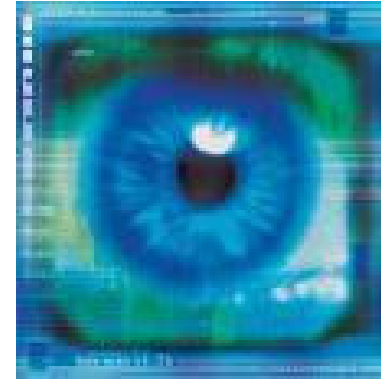
**Treat causes
not
symptoms**

**Intelligence
only useful
If shared**



Security - Authentication

- Passwords, PINs (**knows**)
- Tokens, Cards (**has**)
- Biometrics (**is**)
- Voice, Signature (**does**)



Doesn't matter how good

- Some known failings, but generally very good
- Can become expensive
- Diminishing £ returns (is 99.9% good enough?)



Misuse - reasons / incentives ?:

- Criminal (intelligence is valuable)
- Unethical
- Procedural

Preventative measures - human side

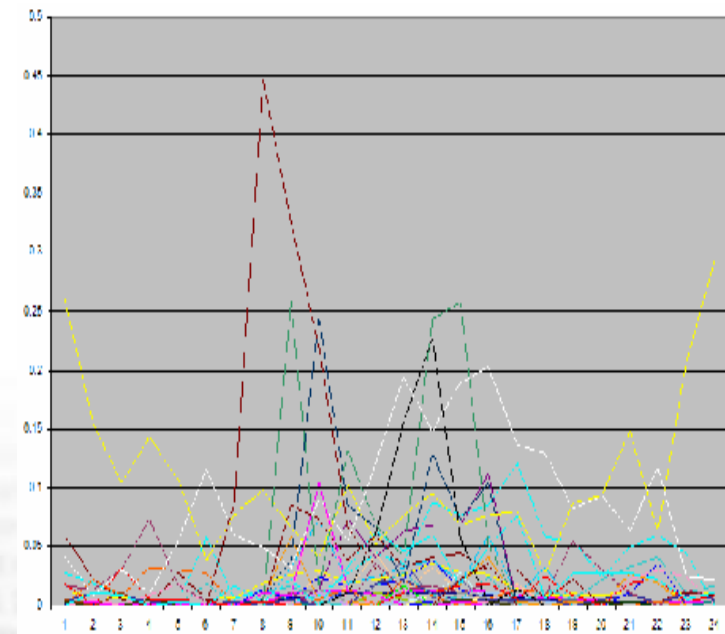
- Vetting
- Background Checks
- Security Clearance
- Disclosures

Investigation of Bad behaviour in IT systems

- Those that Watch the Watchers
- Retrospective, too late (Audit Data Analysis).
- Forensics = time-consuming

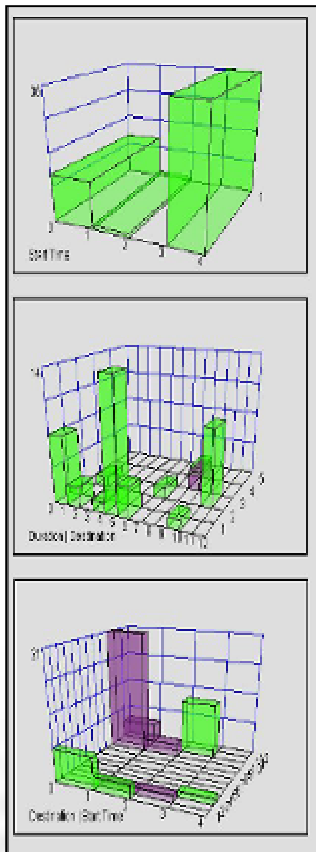
Our Approach

- Anomalous Behaviour Detection
- Detect behaviour as it happens
- Analyse all audits together
- Quickly spot “out-of-profile” activity
- However, can be ‘taboo’ subject.



“Out of Profile” Detection

- Following on from **DTI**-funded research project partnered with **Glasgow University** / large Telecomms Company
- Detection by Statistical Mathematical Models
 - Analysis of disparate sources of audit data
 - User activity profiles
 - Temporal profiles
 - Job function / group / other profiles
- Apply many degrees of sensitivity
 - Has found positive behaviour as well as negative behaviour



$$\begin{aligned}
 P(\mathbf{a}_m | \alpha_m^s) &= \int_{\theta_m^s} P(\mathbf{a}_m | \theta_m^s) P(\theta_m^s | \alpha_m^s) d\theta_m^s \\
 &= \frac{a_{m,s}! \Gamma(\alpha_m^s)}{\prod_{i=1}^{|\mathcal{S}|} a_{m,s=i}! \Gamma(\alpha_{m,i}^s)} \int \prod_{i=1}^{|\mathcal{S}|} (\theta_{m,i}^s)^{(a_{m,s=i} + \alpha_{m,i}^s - 1)} d\theta_m^s \\
 &= \frac{a_{m,s}! \Gamma(\alpha_m^s)}{\prod_{i=1}^{|\mathcal{S}|} a_{m,s=i}! \Gamma(\alpha_{m,i}^s)} \frac{\prod_{i=1}^{|\mathcal{S}|} \Gamma(a_{m,s=i} + \alpha_{m,i}^s)}{\Gamma(a_{m,s} + \alpha_m^s)}
 \end{aligned}$$

To sum up...

Memex
The answer to your search

www.memex.co.uk

➡ **Funds** currently going into **authentication & trust**. Only *part* of the problem.

➡ We could improve **vetting**, but:

➡ Last part of puzzle is to ensure that **Trusted people continue to be Trusted**

ADS Programme / ScotlandIS / CybersecurityKTN seminar
Edinburgh - 26 February 2007

Thanks

Memex

The answer to your search

info@memex.com

ADS Programme / ScotlandIS / CybersecurityKTN seminar
Edinburgh - 26 February 2007