



PCI DSS

The Human Factor Risks

Presented by Stephen Brown, CEO



Contents

1. Background to SRM
2. Background to Human Factor
3. The Threat
4. The Risks
5. Mitigation
6. Audit



1. Background to SRM

- Established in 2002
- Information Security, Compliance and Audit
- Specialists in PCI DSS, ISO27001 and BS7858
- ISO9001, ISO 27001, PCI QSA and PA QSA accredited
- Computer Forensic & Incident Response/Investigation
- UKAS Accredited Security Vetting



2. Background to Human Factor

Human Factor Definition “Is a physical property or behaviour of an individual which is specific to humans and influences functioning of technology’



2. Background to Human Factor

Equipment Design: changes the nature of the physical equipment with which humans work.

Task Design: focuses more on changing what operators do than on changing the devices they use.

Environmental Design: implements changes, such as improved lighting, temperature control and reduced noise in the physical environment where the task is carried out.



2. Background to Human Factor

Training the individuals: better preparing the worker for the conditions that he or she will encounter in the job environment by teaching and practicing the necessary physical or mental skills.

Selection of individuals: is a technique that recognizes the individual differences across humans in every physical and mental dimension that is relevant for good system performance. Such a performance can be optimized by selecting operators who possess the best profile of characteristics for the job.



3. The Threat

- Insider Crime –
 - Employees
 - Contractors/Visitors
 - Collusion between Employees/Outsiders



3. The Threat

- Fraud
- Theft
- Misuse
- Over 65% of Security Incidents are internal
- 46% of UK Large Companies have experienced an incident of internal staff losing or leaking confidential data

Statistics : PWC ISBS 2010

SRM



4. The Risks and Costs

- Fines
- Poor Public Relations
- Reputation Damage
- Loss of Operation
- Loss of Sales



4. The Risks and Costs continued

- Cost of investigation
- Recovery costs to resume BAU
- Further fraud
- Customer confidence falling
- Shareholder price threatened



5. PCI DSS Mitigation

- **Train your staff on security matters**
- **Screen/Net your staff**



5. PCI DSS Mitigation

- **12. Maintain an Information Security Policy**
- **12.1 Establish, publish, maintain, and disseminate a security policy**



5. PCI DSS Mitigation

12.7 Screen potential personnel prior to hire to minimize the risk of attacks from internal sources. (Examples of background checks include previous employment history, criminal record, credit history, and reference checks.)

Note: For those potential personnel to be hired for certain positions such as store cashiers who only have access to one card number at a time when facilitating a transaction, this requirement is a recommendation only.



5. PCI DSS Mitigation – How To?

- **Identity Verification (incl. in UK Right to Work).**
- **Credit History**
- **Criminal Record Check**
- **Previous Employment History**



6. Audit Essentials – What to do!

- Show me the evidence!
- Create Standard Operating Procedures and Policies
- Complete report for each relevant individual
- Set time limits for completion
- Starters and Leavers Process and Policy

Do it properly and be seen to be doing it properly.



Q & A.

Disclaimer: Security Risk Management Limited has made every attempt to ensure the accuracy and reliability of the information contained in its publications, however, it is unable to provide any warranty, either express or implied, concerning the accuracy or completeness of any such information. This publication may contain technical or other inaccuracies or typographical errors. From time to time Security Risk Management may make changes to the information contained in its publications; these changes will be incorporated in new editions of the publication without notice. Security Risk Management Limited, its employees and agents will not be responsible for any loss or damage incurred as a result of any use of or reliance upon the information and material contained in its publications.

Company registration: 3950239. Head Office: Fabriam Centre, Cobalt Business Exchange, Cobalt Parkway, Newcastle upon Tyne. NE28 9NZ. Telephone: 08450 212 151. Fax: 08452 808 182

© 2010 Security Risk Management Ltd.

SRM

Consultancy. Outsourcing. Technology.