

# Information Security in Social Care Provision

Martyn Croft, CIO

The Salvation Army UK Territory



# About The Salvation Army

- A Christian Church and a Charity, operating in 120 countries
- One of the ***largest providers of social services***, with a range of programmes in the community
- Over 7,000 staff in the UK including officers and lay staff
- The IT team provide support and advice for 4,500 users
- Covering desktop & business applications, and ***including information security***



# One of the largest providers of social services...

- About 8,000 clients per year
- Northern & Central England account for 50% of demand
- Of those presenting, about 90% are single male homeless
- Typical length of stay is 2 months
- 80% have moved on within 6 months
- 50% of departures are planned

# Including Information Security...

- 67% of organisations do nothing to prevent confidential data leaving on USB sticks, etc.
- 78% of companies that had computers stolen did not encrypt hard discs
- Only 49% of companies utilise software that detects, reacts to, and records security policy violations

# Typical Information Security Risks



# Who's data is it anyway?

- Sending attachments through e-mail
- Sharing secrets via instant messaging
- Circumventing USB device controls
- Reliance on Trusted Partners
- Employing Encryption
- Social Networking and Social Engineering



# De-perimeterisation

- When data leaves the organisation there may be little control over it
- Establishing ownership of devices and data becomes important
- Personal working practices can introduce risk



# Encryption, Encryption, Encryption

- Whole disk encryption of laptops
- Mandatory encryption of removable storage devices
- Encrypted email gateways
- Protective marking
- User accounts & key management
- Enterprise or point solutions?

Do Government-funded  
charities have to meet  
Government security  
requirements?

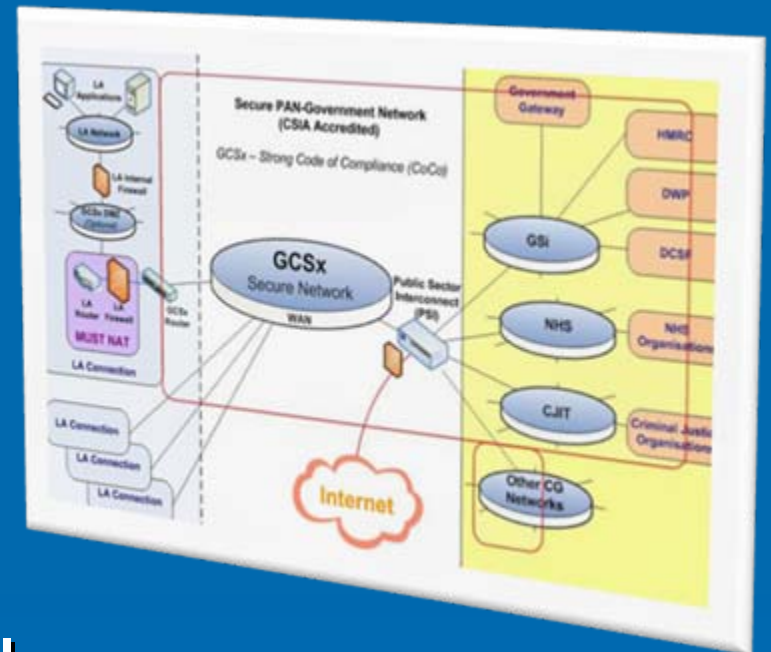


# Cost to Contract


- *“...a reminder that the Department requires all prime contractors and their sub contractors and partners to operate appropriate, secure systems and processes for handling and storing customer information, in line with DWP standards and the Data Protection Act.”*
- *“...I am writing to notify you formally, that the use of unencrypted USB sticks as a means of transfer of customer information must cease with immediate effect. This applies to all Prime Contractors and their Sub-Contractors in line with your contractual Terms & Conditions ”*
- *“...must be sent via encrypted email in all cases, either by Government Connect or using PGP Encryption software - you should also ensure any transfer .... which contains personal information is also encrypted. Under no circumstances should you deviate from this process, for example, do not post the .... to us - **failure to comply will result in a breach of the Data Protection Act.**”*

# Conversing with Government

- Encrypted zip files
- PGP Encrypted email
- Government Connect
- Are there alternatives?  
e.g. Secure Web portal,  
SSL-VPN, Secure Email
- Should GSx extend to the  
Third Sector in addition to the  
Public Sector?



# Third Sector challenges

- Should we be taking Information Security guidance from our Government funders?
  - Could we apply (like Government departments) to the Cabinet Office for a special Ministerial dispensation?
  - Is our client data to be regarded as Government property?
- 

# Charitable Values

*“We are independent, we're not the Government, you can talk to us in confidence.”*

Can we demonstrate that we're a safe pair of hands to contract with, and divulge personal data to, despite being outside of government information security regulation?

# Information Security in Social Care Provision

Martyn Croft, ©2010



# Copyright and Credits

- These materials, together with any training or discussion accompanying the materials provided by the author ("Training"), are intended only to facilitate discussion about issues and do not constitute the provision of advice. Seek professional advice as appropriate. Martyn Croft's services as a practising Information Security professional can be obtained from The Salvation Army UK Territory. This presentation is copyright © Martyn Croft. All rights reserved. Martyn Croft asserts all moral rights pursuant to the Copyright Designs and Patents Act. Persons who participated directly in Training and who have lawfully received a copy of these materials ("participant") may redistribute this presentation to additional persons ("recipients") solely in accordance with the following conditions: (i) the presentation is redistributed in its entirety without alteration, (ii) all text logos names contact details and other content must remain unaltered un-obscured and easily seen by recipients, (iii) no charge is made for such redistribution, (iv) there is no attempt to create an impression or otherwise allow an impression to arise that the presentation is the product of any person other than the author, and (v) each recipient must be a member of the same firm or government agency where the participant was engaged in work, or a student in the same school at which the participant was engaged in study, at the time the participant participated in the Training.
- The Salvation Army name and any related marks are the property of The Salvation Army. Other marks remain the property of their respective proprietors. No rights claimed with respect to government publications including legislation.
- All material copyright Martyn Croft © 2010 and The Salvation Army UK Territory with the Republic of Ireland, except for content under copyright used with permission, or under public license.