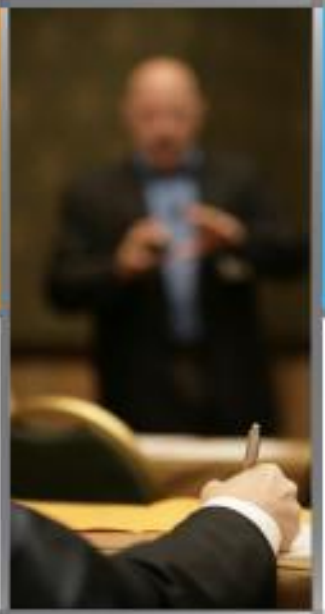
@CSOevents
#CSO50

CSO50 CONFERENCE+AWARDS

Aligning Proactive Security with Modern Threats



May 1-3, 2017

The Scottsdale Resort
Scottsdale, Arizona

PRODUCED BY
CSO
FROM IDG

CSO 50 CONFERENCE +AWARDS

Improving and Automating File Transfer Governance with Business Partners

Jerry Fink

Director, Information Security

Blue Cross and Blue Shield of North Carolina

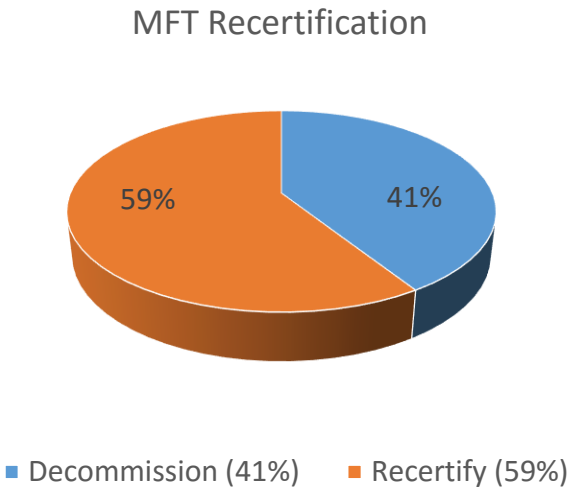
(Un) Managed File Transfer

- Highly regulated industry
- Many business and trading partners with whom we share data
- Good Governance processes on the intake side of new file transfers
- Not as good decommissioning

Audit Findings

- Time to spin up a project
- Recertify all transfers
- Develop a sustainable, automated model for the future

Recertification, The Hard Way



Summary

2272 transfers (59%) recertified

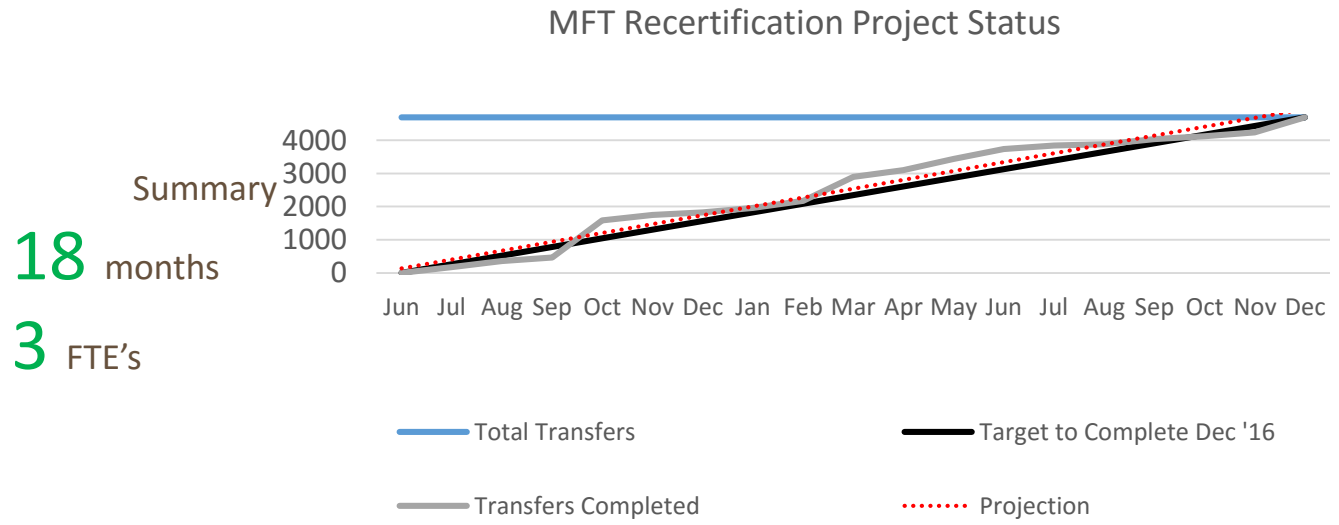
1882 transfers (41%) decommissioned.

as of 12/31/2016.

Summary

18 months

3 FTE's

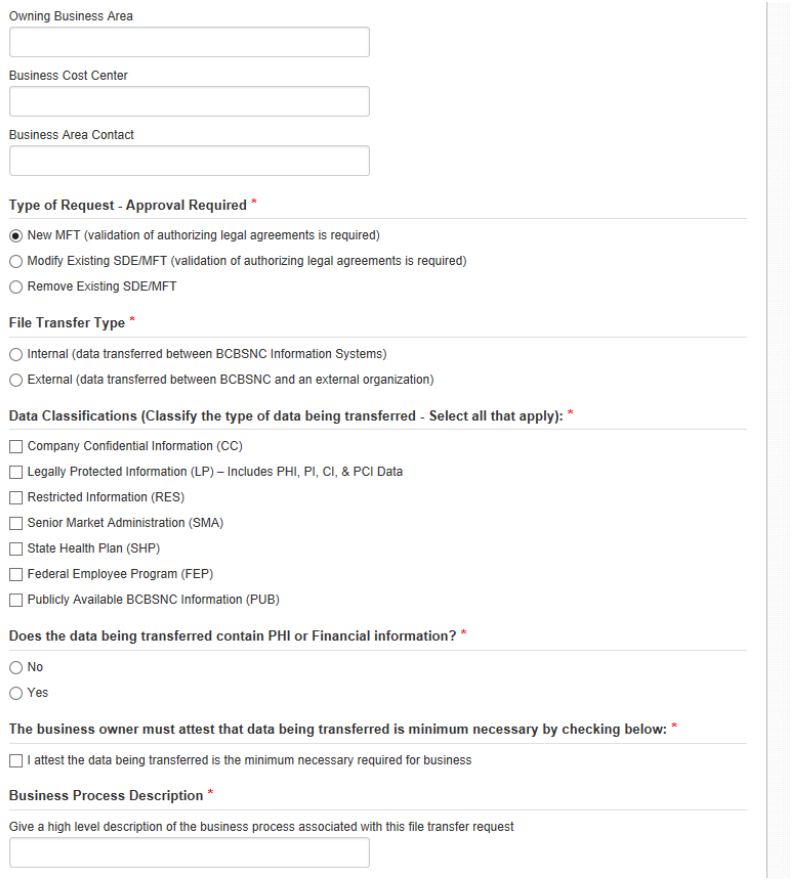


MFT Certification 2.0

- Recertifying MFT, is generically
  - Certifying appropriateness on a regular basis
- Sounds a lot like…
  - Entitlement Reviews
  - Privileged access reviews
- Don’t we have a tool and well defined process for that?

Planning for the Future

- Gather the right data up front
- V1.0, request was technical
  - Encryption, Protocol, Passwords, Technical contact
- V2.0
  - Business owner
  - Type of data
  - Contracts
    - PHI
    - Confidential
    - 3rd Party



Owning Business Area

Business Cost Center

Business Area Contact

Type of Request - Approval Required *

- (•) New MFT (validation of authorizing legal agreements is required)
- ( ) Modify Existing SDE/MFT (validation of authorizing legal agreements is required)
- ( ) Remove Existing SDE/MFT

File Transfer Type *

- ( ) Internal (data transferred between BCBSNC Information Systems)
- ( ) External (data transferred between BCBSNC and an external organization)

Data Classifications (Classify the type of data being transferred - Select all that apply): *

- [ ] Company Confidential Information (CC)
- [ ] Legally Protected Information (LP) – Includes PHI, PI, CI, & PCI Data
- [ ] Restricted Information (RES)
- [ ] Senior Market Administration (SMA)
- [ ] State Health Plan (SHP)
- [ ] Federal Employee Program (FEP)
- [ ] Publicly Available BCBSNC Information (PUB)

Does the data being transferred contain PHI or Financial information? *

- ( ) No
- ( ) Yes

The business owner must attest that data being transferred is minimum necessary by checking below: *

- [ ] I attest the data being transferred is the minimum necessary required for business

Business Process Description *

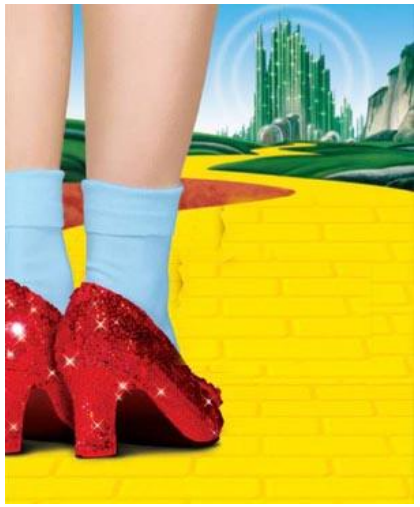
Give a high level description of the business process associated with this file transfer request

Design

- Collect data in Ticketing System
- Add to staging spreadsheet
- Periodic feed into IAM tool
- Run Annual certification campaign
- Celebrate

Summary and Takeaways

- V1.0
  - Highly manual, $1 Million, 18 Months
  - Wrong data collected upfront cause downstream issues
- V2.0
  - Fits into existing processes
    - Twice annual entitlement certification
    - Entitlement Certification for employee transfers
  - Effective Audit trail for “need”
  - Recertification is a “click of a button”
  - Already had the tools and techniques
  - Highly automated, Low $, 2 weeks



Contact info

- Jerry.Fink@BCBSNC.COM