British American Tobacco

Identity & Access Management

John Taylor

Global Head of IT Security & Service Continuity

Presentation Overview

- Overview of BAT
- Context
  - Where Has BAT Security Come From?
  - Strategic Aims
- The IAM Business Problem
- How Did BAT Tackle IAM?
- Key Achievements & Advice.

BRITISH AMERICAN TOBACCO

Who is BAT?

- World's second largest tobacco company.
- Founded over 100 years ago.
- Operates in approximately 186 countries.
  - A number of them being in the more interesting areas of the globe.
- Has 250 brands.
- Approximately 95,000 employees with 45,000 'knowledge workers'.
- Gross turn over £40,700 million per year - £26 billion year raised for governments in taxes.
- Currently undertaking a major re-alignment of business practices from a federated model to a centralised business model.

VICEROY

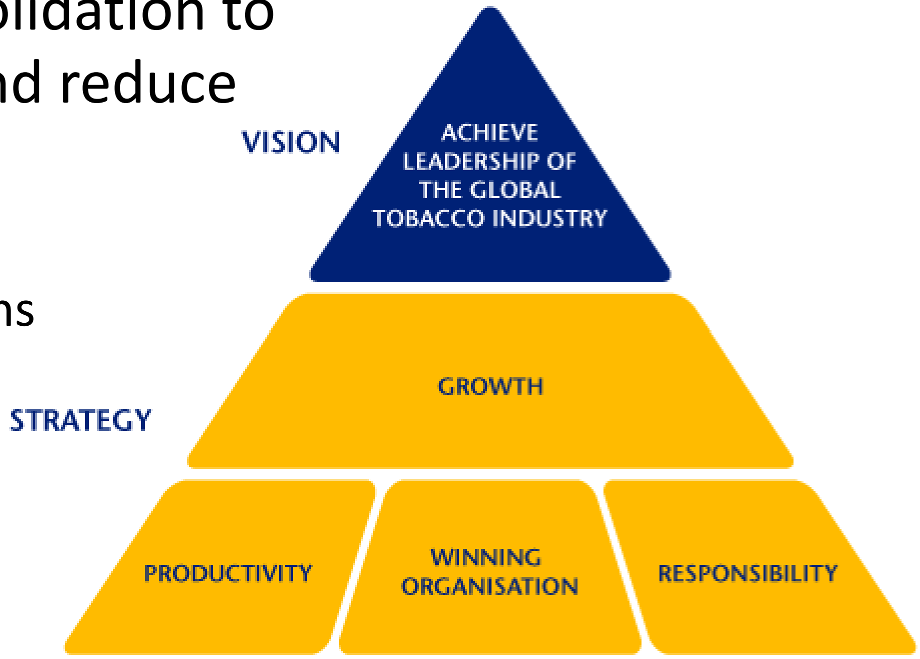
DUNHILL
SINCE 1907

PALL MALL

LUCKY STRIKE

Business & Technology Direction

- Historically had a highly federated business model and now migrating to a centralised operating model
- Looking for consolidation of business practices and supporting IT systems globally.
- Whilst the underlying business is the same, there is a drive for more shared services.
- A heavy focus on consolidation to leverage capabilities and reduce costs through -
  - Standardisation
  - Enterprise class solutions
  - Increased governance



Security needs to be Innovative to address the pressures

BRAND CAMP
by Tom Fishburne
FAILED
FAILED
FAILED
FAILED
FAILED
FAILED
FAILED
FAILED
FAILED
SO, WHAT BREAKTHROUGH IDEA DID YOU WANT TO SHARE WITH ME?
©2010
TOMFISHBURNE.com

How Do You Create Innovation? – IAM Can Enable Security to Support the Business

The Security Challenge When We Started

- Was unable to meet the changing business needs.
- The capability and approach was immature against BAT's peer group.
- The security model was inconsistent across geographies.
- Suffered from limited effectiveness due to a lack of ownership.
- There was an inability to move from the technical to risk based capabilities.
- Was a re-active function with limited pro-active capabilities.
- A number of pieces of infrastructure and practices were near or at end-of life.
- A limited tool-set was in place to provide services.

What Are Our Strategic Aims?

STANDARDS
UX
WOW
FUN
SEAMLESS
EFFICIENT
SATISFYING
EARNABLE
EFUL
BASIC
Excellent
Very go
Good
.com
!
#
@
?
&
$
www
%

Improve End-User Experience

Standardisation of Process & Technology

Enable Integrated Enterprise Services

Strong & Effective Governance

Improve Over-Arching Maturity

Establish Agile Services

End-to-End Visibility of the Environment

Effective User Awareness

British American Tobacco

What Have Been the Main Areas of Focus?

"Open Internet"
Access to the Internet is managed via a cloud solution with the right protection for BAT

Management of Internet risks

"Secure End-Points"
All devices are protected & consumer devices are able to securely access the BAT network

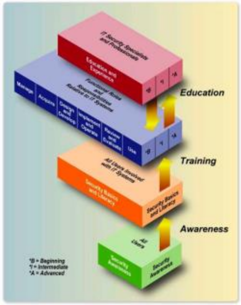
Access is secure and easy

"Securing the Core"
BAT's Core Applications are Secured within the BAT Data Centres

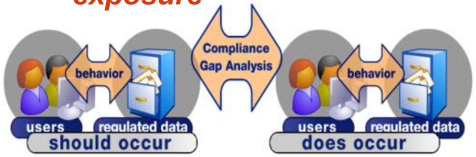
"Externalised Applications"
Applications are compliant with IT Security Standards and are able to be accessed securely from any location

Implement long-term cultural change

"IT Security Training & Awareness"
Global, standard approach to awareness targeted at long term organisational cultural change



Reporting on current application risk exposure

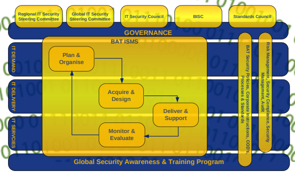


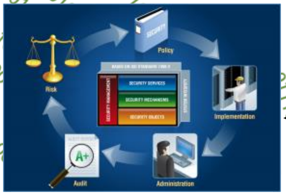
"Penetration Testing & Managed Security Provider"
Visibility of the BAT environment & on-going compliance checking against BAT policies.

Reporting on current application risk exposure

Effective response to Business Incidents

Know who has access to what information

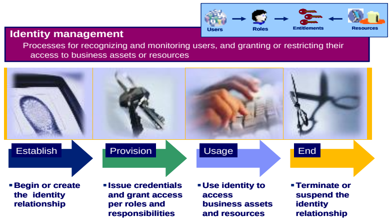

Regional IT Security Steering Committee
Global IT Security Steering Committee
IT Security Council
BISC
Standards Council
GOVERNANCE
BAT ISMS
IT DEMAND
IT DELIVERY
IT SERVCIES
Plan & Organise
Acquire & Design
Deliver & Support
Monitor & Evaluate
BAT Security Policies, Corporate Instructions, COD's, Processes & Standards
Risk Management, Security Compliance, Security Management, Audit
Global Security Awareness & Training Program



"Compliance Management – ISO & CoBIT"
IT Security Governance in place via an established Information Security Management System. Risk is identified and managed in accordance with residual risk targets. BAT partnered with a Security Provider.

"IT Service Continuity"
Global approach to system availability linked to BCM and incident management

Identity and Access Management
Enable more secure, identity-based access to applications on-premises and in the cloud from virtually any location or device
Help PROTECT everywhere ACCESS anywhere
INTEGRATE and EXTEND security
SIMPLIFY security, MANAGE compliance


Users
Roles
Entitlements
Resources
Identity management
Processes for recognizing and monitoring users, and granting or restricting their access to business assets or resources
Establish
Provision
Usage
End
Begin or create the identity relationship
Issue credentials and grant access per roles and responsibilities
Use identity to access business assets and resources
Terminate or suspend the identity relationship

"Identity & Access Management"
Effective and consistent Joiner, Mover & Leaver Process.
Controlling Access risks to applications within the Core.
Ability to control BAT employee & third party access.

What Were the IAM Business Problems?

Cost Related

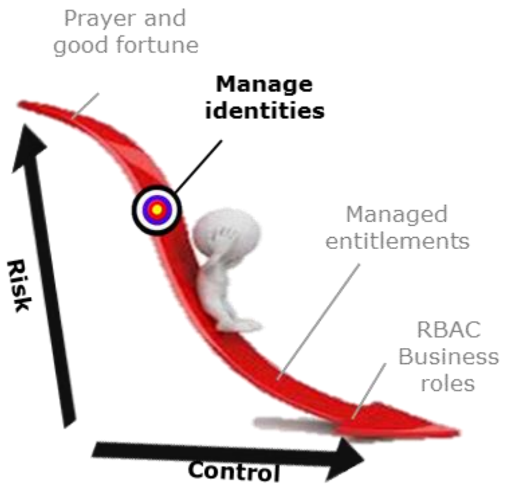
- Multiple solutions.
  - Burning platforms in some geographies
  - No platforms in others…
- High integration costs and lengthy time to market for protected applications.
- Poor and disjointed processes – often manual.
- Ineffective user access and password management practices.
- Duplication of effort and expense in the day-to-day management of users.

User Experience & Governance Related

- Excessive privileges granted to Administrative Users.
- No clear visibility of identities and user access to BAT resources.
- Inherently difficult and costly to provide user & account access data for audit-requests.
- Extremely frustrating end-user experience.
- At least 30% of accounts identified as inactive or dormant accounts.

The BAT Challenge

- There are three approaches that organisations can take to managing identities
  - ✓ Policy and capability (difficult)
  - x No policy or capability (brave and rare!)
  - x Policy but with no effective capability (expect audit points and incidents)



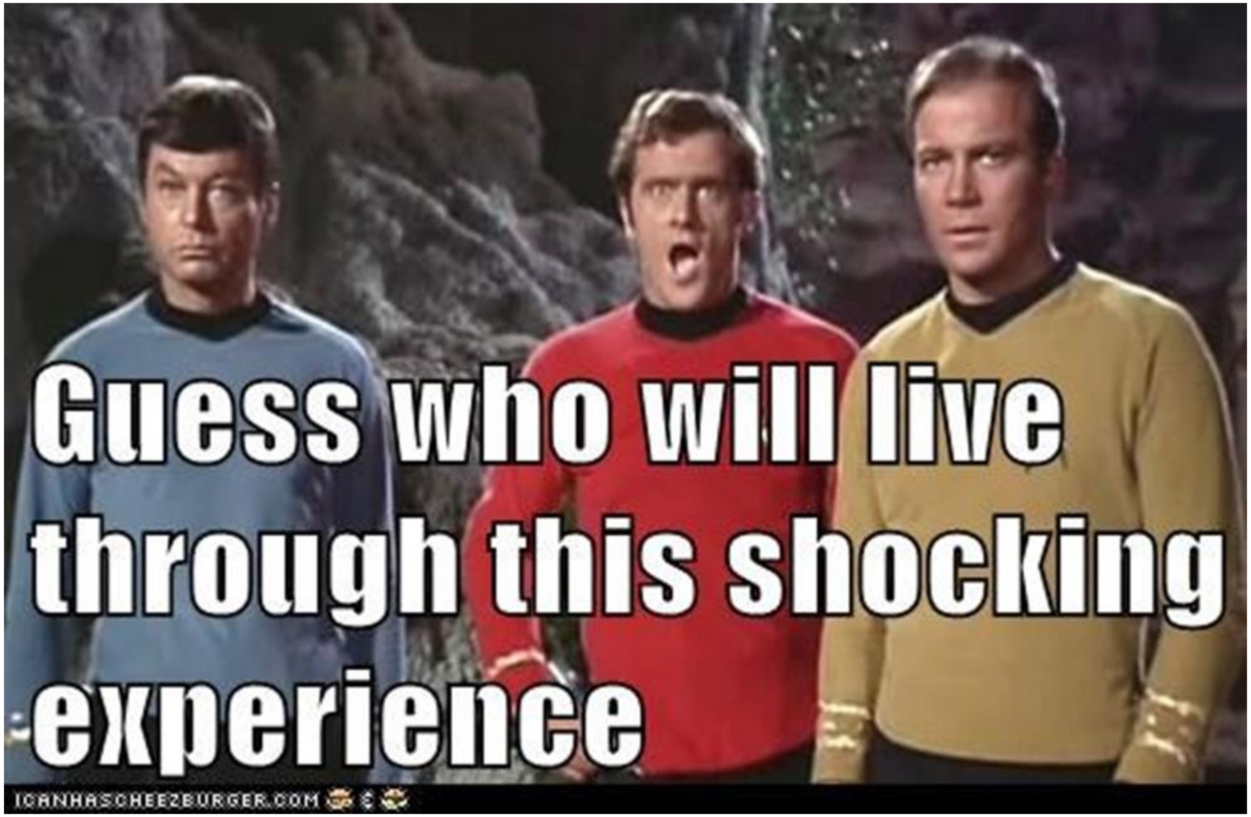
- Low IT security starting point
- Major change in ALL areas of organisation and IT
- Sand is always shifting
- Transformation velocity is hard to maintain
- Security strategy must be enduring, not a flash in the pan.

Key Scope Questions…

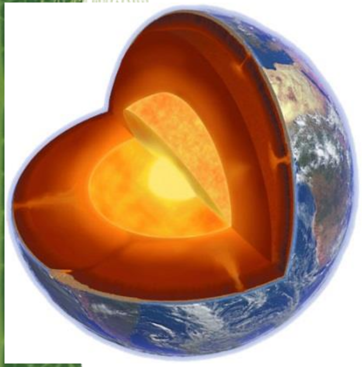
- **Scope** – All systems? All users? Does anyone have a list?
- **Accountability** – Whose problem is it? Do they know? Do they have the levers to address it?
- **Authoritative HR processes –** SAP HR (s), Excel etc? Is there any full view of employees, temps, contractors etc?
- **Process** – Is there one, is it defined, is it followed, is it global.
- **Landscape** – What technologies are in use? How many instances? How configured?
- **Data** – Does it exist? How many parts? How clean is it? Mapped? Global identities?
- **Access Roles** – Defined? In use? Applied to function?
- **Organisation** – Parties defined? Authorisers known? Authorisers know what they're approving?

IAM Needs Persistence & Support In Delivery

- Implementations are not easy.
- Require engaged senior stakeholder support.
- …a willingness to stay focused and calm.



How Did BAT Tackle IAM?



Secure the core

- Automate what we can today
- Wrap IAM around the core repositories and platforms within BAT today
- Provide Digital Identity Management despite the limitations in process

***Build IAM as an enduring service*:**

- With BAU integration factory
- With transformation built in to support contracts
- Leaving the incubator of the project.
- IAM is a journey not a sprint

Bring the blame to the problem!

- If we know who has access to our IT systems, and all their linked accounts
- The question becomes “Do these people still work for BAT!”
- This can only be addressed outside of IT
- IAM can help but not in isolation.

And deliver Access Management “treats”

- The visible side of IAM.
- Benefits visible to users after initial hurdle

Key Achievements

- BAT now have a global IT Joiner/Mover/Leaver process for the first time
  - HR processes have not caught up.
- End markets report faster joiner process to provision core accounts
  - Further automation required to enhance accuracy, and further reduce time
- Security offering for Cloud and BYOD Applications to ensure some form of control.
  - Single sign-on capabilities lacking.
- Automated movers between countries has landed and is improving accuracy.
  - Not enough focus on data clean up and business analysis.
- Externalisation of internal applications
  - Limited to Web based app's only.
- Improved process capability for core managed systems.
  - Still a number resisting integration outside Active Directory and SAP.

In summary

- **Process**
  - IAM provides the cornerstone of BAT’s security transformation.
  - IAM cannot be solved in isolation from the business.
  - IAM must facilitate the Jointer/Mover/Leaver process and accountabilities.
  - *Engage a Business Analyst or two or three up front.*

- **Toolset**
  - IAM must land successfully as a credible, robust platform.
  - IAM must be able to integrate with everything we can throw at it – key for BYOD & Cloud.
  - IAM must be able to provide a unified access management layer.
  - *Treat as a data project – do not think ‘it’s only usernames and passwords’.*

- **BAT Service**
  - IAM must be an enduring platform with innovation built into the service and product.
  - With BAU integration factories.
  - And sold internally as a service line with defined costs.
  - *Treat as a critical component of ‘middleware’. System down time will have flow-on effects.*

British American Tobacco

IT

BRITISH AMERICAN TOBACCO