Cyber Security
GDPR and Privacy Enhancing Technologies
Shane McEntagart (shmcentagart@deloitte.ie)
9th February 2018
Event briefing and overview
Shane McEntagart
(Deloitte)

GDPR alignment with Cyber Security
Liam O’Connor
(Deloitte)

Mark Oldroyd
(Sailpoint)

David Higgins
(CyberArk)

Clive Finlay
(Symantec)

Panel discussion
Chair: Jacky Fox
(Deloitte – Cyber Security Lead)

Presenters
Nicola Flannery
(Deloitte – Data Privacy)
Cyber Security
GDPR and Privacy Enhancing Technologies
Liam O’Connor (loconnor@Deloitte.ie)
What changes does the GDPR bring?

Facts & figures

4% Potential fines as a percentage of global turnover

7 Core individual rights afforded under the GDPR

72 Hours given to report a data breach

€203m Cost of 4% fine for a typical FTSE 100 company

28,000 Estimated number of new Data Protection Officers required in Europe (IAPP study 2016)

190+ Countries potentially in scope of the regulation

80+ New requirements in the GDPR
What changes does the GDPR bring?
Changes compared to the 1995 Directive (95/46/EC)

- Broader territorial scope
- Enforcement
- Accountability
- Expanded definitions
- Data subjects rights
- Consent
- Data breach notification
- One-stop shop
- International data transfers

**General Data Protection Regulation**

- Applies to players **not established in the EU** but whose activities consist of targeting data subjects in the EU
- Data Protection Authorities will be entitled to impose **fines ranging between 2% to 4% of annual turnover, or 10 – 20 million euros**
- Explicit obligation to the controller as well as the processor to be able to **demonstrate their compliance to the GDPR**
- Personal data now **might include location data, IP addresses, online and technology identifiers**
- **Reinforced rights**: Access, rectification, restriction, **erasure, portability**, objection to processing; no automated processing and profiling
- **Spelled out more clearly** and focus on ability of individuals to distinguish a consent
- Report a personal data breach to the Data Protection Authority within 72 hours
- **Data Protection Authorities (DPA) of main establishment can act as lead DPA**, supervising processing activities throughout the EU
- BCRs as tools for data transfers outside the EU and EEA are now embedded in law
GDPR Transformation Programme

A best practice privacy programme distinguishes six main focus areas. This can help to formulate key objectives:

Layer 1: Strategy
Layer 2: Organisation and accountability
Layer 3: Policy, process & data
Layer 4: Culture, training & awareness
Layer 5: Privacy operations
Layer 6: Processing inventory
The GDPR presents a number of challenges:

Under Article 32 of the GDPR - Security of Processing – “implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate”

1. Consent – ensuring consent is informed, unambiguous and recorded
2. Right to erasure – managing and facilitating data subjects’ right to request the deletion of personal data
3. Records of processing activities – developing and maintaining a register of personal data processing
4. Accountability – keeping records of decisions and positions, and demonstrating compliance
5. Data portability – providing the ability to port personal data from one data controller to another in certain circumstances
GDPR Alignment With Your Cyber Security Strategy

- Data Breaches
- Risk Based Approach
- Security Best Practice
- Identity & Protect Crown Jewels
- Threat Landscape
- Data Protection & Cyber Security Interconnected
- Technology As An Enabler
- GDPR & Cyber Security Alignment
  - Governance
  - Secure
  - Vigilant
  - Resilient
- Maintaining Compliance After May

Organizations need a holistic, business-driven, and threat-based approach to manage cyber risks. While security assets are important, being vigilant and resilient in the face of cyber attacks is imperative.
GDPR – Privacy Enabling Technologies

Complying with the GDPR requires the management of privacy risks. Implementing industry leading tools can assist privacy governance, risk, and compliance management.

Key elements to consider:

- Before adopting and implementing privacy technology, companies should go through prerequisite steps.

1. Establish Governance
2. Define & Implement Controls & Processes
3. Define Requirements For Supporting Technologies
4. Discover Existing Tools That Satisfy Requirements
5. Assess PET Vendors Based On Requirement Gaps

Sample of tool classification types:

- Identity Access Management
- Unstructured Data Management
- Data Loss Prevention
- Governance, Risk & Compliance Management
- DPIA Automation & Management
- Data Breach Management & Reporting
- Reporting & Record Keeping
- Anonymisation & Pseudonymisation
- Vulnerability Management
- eDiscovery
- Monitoring – SIEM / SOC
- Training & Awareness
Business-Focused Identity Governance

The Power of Identity
Do you know WHERE your (Sensitive) data is?

Do you know WHO has access?

Is the access APPROPRIATE?

Can you PROVE it?

$158 is the average cost per lost or stolen record.
71% of staff have access to data they should not see

Ponemon Institute Report

80% of company data is held in unstructured content

Forbes Report

1 in 7 employees will sell their credentials for $150

SailPoint Survey

89% believe they are now at risk from insider threat

IT Governance Report
SECURITY PARADIGMS HAVE SHIFTED FROM NETWORK-CENTRIC...
TO USER-CENTRIC
GDPR Highlights

What is it?
- Homogenous Data privacy law
- All organizations processing EU citizen data
- Live date May 2018
- Unstructured data in scope
- 28 PII conventions

Sanctions & litigation risk
- Fines: 4% of annual revenue or €20m
- Breaches notified to regulator within 72 hours
- Citizen compensation lawsuits
- Audit, Clean up, reputation

Data Access Governance
- Privacy Policies
- Data Discovery
- Need to know basis access
- Retention Policies
- Breach detection & Disclosure

Governance & Compliance
- Data Protection Officers
- Data owner accountability
- Least privilege principle
- Breach disclosure
- Fine grained audit trails
SailPoint’s Relevance to GDPR

Technology (15 Articles)

SailPoint Relevant (12 Articles)

Identity Governance for Files (11 Articles)

Identity Governance for Applications (6 Articles)

People (18 Articles)

Process (66 Articles)

80% Coverage
IAM Market Leader

Gartner IGA MQ 2017, Continued Leader
Forrester IMG Wave 2016, Continued Leader
Kuppinger Cole IDaaS Compass 2017, Leader

850+ Customers and Growing

40% International Business

World’s LARGEST Dedicated Identity & Access Management Vendor

95% Customer Satisfaction

Founded in 2005 by IAM veterans

World’s LARGEST Dedicated Identity & Access Management Vendor
Customers by Vertical

Banking/Financial Services
- ABN AMRO
- UBS
- CIT
- Bank of America
- BNP Paribas
- Allianz
- AIG
- Aviva
- Aon
- Swedbank
- Fidelity
- DekaBank
- Student Loans Company
- ING
- Computershare
- RBS
- RBS
- SEB
- JPMorgan Chase
- American Express
- Westpac
- The World Bank
- Nationwide
- On Your Side
- Manulife
- Progressive
- Mayo Clinic

Insurance
- Fireman's Fund Insurance Company
- UNIVE
- New Life
- Allstate
- Nationwide
- Aetna
- Humana
- AstraZeneca
- Bristol-Myers Squibb
- Travelers

Health/Pharma
- Boehringer Ingelheim
- Pfizer
- Sanofi Aventis
- Allina Health
- Regence
- The Container Store
- CenterPoint Energy

Manufacturing
- Intel
- Philips
- Intel
- Freescale
- ConocoPhillips
- Iberdrola
- Ford
- General Motors
- Spirit AeroSystems
- Spirit AeroSystems
- Spirit AeroSystems

Energy/Utilities
- ConocoPhillips
- Iberdrola
- Enbridge
- RWE
- Exxon
- Mobil
- CenterPoint Energy

Other
- Weight Watchers
- Yale University
- Enbridge
-(x)
- Rockwell Automation
- Adobe
- KPMG
- PwC
- Weight Watchers
- Enbridge
-(x)
- Rockwell Automation
- Adobe
- KPMG
- PwC
Guaranteeing the Appropriateness of Access
Get Visibility

Authoritative Sources

Applications And Services

Build Current State

Identity Collection
Correlation
Entitlement Cataloguing
Discovery & Classification
Get Clean

Authorize Sources

Build Current State

Validate Current State

Applications And Services

Identity Collection
Correlation
Entitlement Cataloguing
Discovery & Classification

Analytics
Reporting
Access Certification
Governance Insights

Get Clean

Authoritative Sources

Applications And Services

Identity Collection
Correlation
Entitlement Cataloguing
Discovery & Classification

Analytics
Reporting
Access Certification
Governance Insights

Validate Current State

Build Current State
Stay Clean

Define Desired State
- Policy Enforcement
- Business Role Modelling
- Risk Analysis
- Owner Identification

Validate Current State
- Analytics
- Reporting
- Access Certification
- Governance Insights

Build Current State
- Identity Collection
- Correlation
- Entitlement Cataloguing
- Discovery & Classification

Authoritative Sources

Applications And Services

Copyright © SailPoint Technologies, Inc. 2016. All rights reserved.
Manage & Secure

Build Current State

Validate Current State

Define Desired State

Manage & Secure

Lifecycle Processes
Self-Service
Identity Context Distribution

Policy Enforcement
Business Role Modelling
Risk Analysis
Owner Identification

Analytics
Reporting
Access Certification
Governance Insights

Identity Collection
Correlation
Entitlement Cataloguing
Discovery & Classification

Applications And Services

Authoritative Sources

Applications And Services

Authoritative Sources

Applications And Services

Authoritative Sources

Applications And Services

Authoritative Sources

Applications And Services

Authoritative Sources

Applications And Services

Authoritative Sources

Applications And Services

Authoritative Sources

Applications And Services

Authoritative Sources

Applications And Services
SailPoint Vision: Comprehensive Governance

Applications & infrastructure
- Mainframes
- Databases
- CRM/HR/Financial
- Applications

Access

Identity Governance

File storage systems
- File servers
- Cloud storage
- NAS
- Collaboration systems
SailPoint Vision: Comprehensive Governance

Access

Applications & infrastructure
- Mainframes
- Databases
- CRM/HR/Financial
- Applications

File storage systems
- File servers
- Cloud storage
- NAS
- Collaboration systems

Identity Governance
SailPoint Platform: The “Business” of Identity

**Business Functionality**
- Certification & Remediation
- Policy Enforcement
- Self-Service
- Automated Lifecycle Events
- Identity Analytics
- Data Classification

**Analytics & Reporting**
- Role & Risk Modeling
- Business Process Management
- Change Automation
- Password Management
- Activity Monitoring

**Aggregation & Provisioning Broker**
- Provisioning Connectors
- Manual Work Items
- Service Desk Integration
- Provisioning Integration
- PUM Integration
- Mobile Integration
- Security/GRC Integration
- Specialist Integration
- Unstructured Data Management

**Flexible Change Fulfillment and Data Collection**
- Business Functionality
- Analytics & Reporting
- Aggregation & Provisioning Broker

SailPoint Identity+ Alliance Partnership

SailPoint Open Identity Platform
Ground to Cloud Deployment Options

- On Premise
- Public Cloud
- Managed Service
- SaaS
Azure AD Access Management + SailPoint

- Single Sign-On
- Conditional Access and Multi-factor Authentication
- Risk-based Identity Protection
- B2B Collaboration
- Self-Service Password Reset

- User and Group Management and Provisioning

- Password Reset Extension
- Fine-grained & Life Cycle Provisioning
- Access Request
- Access Certification
- Compliance & Audit Reporting
- Policy-based Workflow & Approvals
Azure Solution Architecture

HR Application (Authoritative Source)

Workflow

Governance

Change Notification

Modeling

Provisioning

Directory
- Group m, Entitlement x
- Group n, Entitlement y
- ...

Cloud and On-Premises Applications

Provisioning

Access

End User

Authentication

Copyright © SailPoint Technologies, Inc. 2016. All rights reserved.
“By 2021, organizations with complementary/integrated IGA and DAG capabilities will suffer 60% fewer data breaches.”

–Gartner (2017)
Identity at the Center of Security

- Security Incident & Event Management
- IT Service Management
- Mobile Device Management
- Governance, Risk, & Compliance
- Applications & Infrastructure
- Data Governance
- Privileged User Management
- Data Loss Prevention
Beyond GDPR: Enterprise Identity Governance

Protect access to all applications and data – on-premises and in the cloud

- Access Request
- Access Certification
- Provisioning Workflow
- Access Policies
- User Risk-based Modeling
- Password Management
- Data Classification
- Activity Monitoring
- Permission Analysis

Benefits
- Greater visibility into access risks
- Centralize all access to applications and data
- Reduced complexity by providing a consistent set of controls
Thank You
The Privileged Pathway...
...to Critical Data

David Higgins,
Director of Customer Development, EMEA
Agenda

• The Human Element

External:

• The Privileged Pathway
• Isolating the Attack

Internal:

• The forgotten Data Access Vector
Key GDPR Requirements and Privileged Security

**Article 25**
Data protection by design and by default
- **PROTECT ACCESS** to sensitive personal data

**Article 32 (2)**
Security of processing
- Detect and **RESPOND RAPIDLY** to breaches early in the attack lifecycle

**Article 33**
Notification of a personal data breach
- **ASSESS RISK** and test the effectiveness of data protection processes

**Article 35**
Data protection impact assessment

**Article 82**
Protection from non-compliance
- **DEMONSTRATE COMPLIANCE** and prove you have the necessary security controls in place

**Key GDPR Requirements and Privileged Security**

- Article 25: Data protection by design and by default
- Article 32 (2): Security of processing
- Article 33: Notification of a personal data breach
- Article 35: Data protection impact assessment
- Article 82: Protection from non-compliance
<table>
<thead>
<tr>
<th>PROTECT ACCESS</th>
<th>RESPOND RAPIDLY</th>
<th>ASSESS RISK</th>
<th>DEMONSTRATE COMPLIANCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure the privileged pathway and privileged access to systems containing personal data</td>
<td>Monitor, detect, alert, and respond to high-risk activity and enable security teams to stop attackers before they can access personal data</td>
<td>Improve your security posture by identifying all privileged user and application accounts and conduct penetration testing to ensure the right security controls are in place</td>
<td>Have the operational controls to prove compliance and protect yourself from litigation</td>
</tr>
</tbody>
</table>
Data Breach – Attackers: The Privileged Pathway
The Starting Position

Because many existing implementations of Active Directory Domain Services have been operating for years at risk of credential theft, organisations should assume breach and consider the very real possibility that they may have an undetected compromise of domain or enterprise administrator credentials

—MICROSOFT,
“MITIGATING PASS-THE-HASH AND OTHER CREDENTIAL THEFT, VERSION 2,” 2014

...doesn’t matter how much you train and educate your users...
The Privileged Pathway to
THE DOMAIN CONTROLLER

Initial intrusion, often phishing

WORKSTATION
Steal admin password
WORKSTATION
Steal admin password used for a server

SERVER
Use password. Find nothing. Move on.

SERVER
Steal hash for an admin password with broad access

DOMAIN CONTROLLER
Generate tickets for all assets in domain

CRITICAL WORKSTATIONS

CRITICAL SERVERS

SECURITY SYSTEMS
Gain access to ALL critical assets
<table>
<thead>
<tr>
<th>Step 1</th>
<th>Focus first on eliminating irreversible network takeover attacks (e.g., Kerberos Golden Ticket).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Control &amp; secure infrastructure backdoor accounts.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Limit lateral movement.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Protect 3rd party privileged accounts.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Manage SSH keys on critical Unix servers.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Defend cloud &amp; DevOps backdoors.</td>
</tr>
<tr>
<td>Step 7</td>
<td>Secure shared IDs for business users (integrate and accelerate adoption of MFA).</td>
</tr>
</tbody>
</table>
Step 1: Irreversible Network Takeover Attacks

- Manage Domain Admin and Enterprise Admin Credentials
- Kerberos Attack Detection
- Enforce Tiered Account Model
- Enforce Application Control on Domain Controllers

ENDPOINT ➔ INFRASTRUCTURE ➔ DOMAIN CONTROLLERS

Session Isolation
Step Two: Control & Secure Infrastructure and End Point
Well-known Infrastructure Accounts

- Manage Local Administrator Accounts
- Manage Local Administrator Accounts on Windows
- Manage Root Accounts on UNIX/Linux
- Manage Domain Admin and Enterprise Admin Credentials
- Kerberos Attack Detection
- Enforce Tiered Account Model
- Enforce Application Control on Domain Controllers
Step Three: Limit Lateral Movement

- Manage Local Administrator Accounts
- Application Control
- Least Privilege
- Block Credential Theft

ENDPOINT

SESSION ISOLATION

INFRASTRUCTURE

SESSION ISOLATION

DOMAIN CONTROLLERS

- Manage Local Administrator Accounts on Windows
- Manage Root Accounts on UNIX/Linux
- Manage 3rd Party Application Accounts
- Manage Domain Admin and Enterprise Admin Credentials
- Kerberos Attack Detection
- Enforce Tiered Account Model
- Enforce Application Control on Domain Controllers
- Least Privilege
- Block Credential Theft

3rd Party Application Accounts

Domain Admin and Enterprise Admin Credentials

Kerberos Attack Detection

Enforce Tiered Account Model

Enforce Application Control on Domain Controllers
Secure the Eco-System
C³ Alliance
Data Access – Infra Admins: The Forgotten Vector

APPLICATION

DATABASE

OPERATING SYSTEM

Application Environment

FILE SHARES

Business User

Application User

DBA Access

3RD PARTY

IT Admins

Infrastructure Admin Access

STORAGE
Session Management for Critical Assets / Accounts

Native Support for RDP and SSH Based Clients
Identifying Key Risks – Lateral Movement

Pass-the-Hash: Organizational Vulnerability Map

- Machine 1
- IT file server 2
- Backup server 2
- Database server 2
- Exchange server
- IP phone server

See a map of all vulnerable machines and vulnerabilities found in your organization.

OPEN PTH MAP
Identifying Key Risks – Domain Compromise

Pass-the-Hash: Organizational Vulnerability Map

- Domain Controller(s)
  - WIN2008R2
  - WIN2008R2-2
  - WIN2008R2-3
  - WIN2008IIS
  - WIN200864B
  - WINVISTA32B
  - DNA-Win81-32b

- Machines expose network to Golden Ticket attacks
  - 21
  - 13

Causing vulnerability:
- Vulnerable
- Causing vulnerability and vulnerable
Get Your Head in the Cloud
A Practical Model for Enterprise Cloud Security
Technology Considerations for the GDPR

- Know your Personal data
- Process Data Lawfully
- Embed privacy
- Protect Personal Data

PROTECT PERSONAL INFORMATION THROUGH ITS LIFECYCLE
What is the one word you need to be wary of when talking about the cloud
CONTROL
All the benefits you receive from moving to the cloud: agility, elasticity, and low cost are received by giving up...
CONTROL
All the challenges you face in the cloud: security, compliance, data residency, data privacy and management are rooted in your lack of...
CONTROL
The only reason you have not moved your critical workloads to the cloud is because you cannot afford to give up...
CONTROL
CONTROL

How do you give it away and keep it at the same time?
This is your enterprise – your realm of complete CONTROL
Before the cloud, you held your infrastructure and applications safe within its walls
Then the cloud happened...
...your infrastructure started moving over and you lost some CONTROL
...your applications started moving over too
and you lost more CONTROL
Additionally... cloud endpoint, mobile, BYOD, have all spiraled...
out of your CONTROL
CONTROL

How do we regain it?
WE NEED A NEW CONTROL POINT
Protecting Infrastructure
Does it really matter, isn’t Amazon (or Microsoft) providing all the security I need?

Let’s have a quick look under the covers
AWS “Shared Security Model”

Where?

- Workloads
  - Compute
  - Storage
  - Database
  - Networking

- AWS Global Infrastructure
  - Regions
  - Availability/Zones
  - Edge Locations

What needs to be Protected?

- Customer Data
- Platform, Applications, Identity & Access Management
- Operating System, Network & Firewall Configuration
- Client Side Data Encryption & Data Integrity Authentication
- Server Side Encryption (File system and/or Data)
- Network Traffic Protection (Encryption, Integrity, Identity)

Who is Responsible?

Customer

Security Services include IAM, MFA, CloudWatch, VPC CloudTrails, AWS Config, Inspector, Other...
Key Customer Challenges for Security in Public IaaS Cloud

1. **Shared Responsibility Model For Security in Public Cloud**
   - **Apps**
   - **Data**
   - **OS**
     - Customer responsible for Security
   - **Physical Infrastructure**
     - AWS/Azure responsible for Security

2. **Speed and Agility in Public Cloud**
   - **Private Cloud**
     - 1-2 server releases per year
     - 100 servers per admin
     - Bolted-on
   - **Public Cloud**
     - 6 server releases per minute
     - 500 servers per admin
     - Built into the process
     - **15,000% increase**
     - **5X increase**

**Loss of Visibility:** Infrastructure deployment leaves a blind spot in security
- What instances are running? What is deployed on them?
- What Regions, VPC, Subnets are they part of?
- What if there is a known vulnerability? Should they be In Scope for compliance?

**Loss of Control:** New network paradigm still requires security with new tools
- How can I detect and eliminate rogue instances in Security Implementations?
- My old tools do not work as there are no SPAN/TAP ports for Network
- How do I ensure AV is deployed and applications are segmented to be compliant?

**Risk & Compliance:** Need Security monitoring to meet compliance
- Gain insight into the potential known and unknown vulnerability exploits on the software deployed in you AWS/Azure accounts
- Prioritize & Remediare with ample network and asset context

**Cloud Native Delivery:** Need efficient deployment
- How can I deploy security technology at cloud speed?
- How can I detect my infrastructure scale out and ensure that security is in lock step?

Pain Points articulated in customer validation
Cloud Workload Protection – The IaaS Control Point

- Instances in auto-scaling group with policies applied
- Complete instance mapping with real-time protection status
- Automatic policy recommendations

Continuous Visibility Across Cloud Workloads
Cloud Workload Protection – The IaaS Control Point

Application Isolation & OS Hardening
User & Process Behavioral Analysis
Discover and view security postures of workloads wherever they are

Shut down rogue instances to reduce attack surfaced

Global Security Dashboard With Drill-Down Capability
Protecting Information
Extending cyber controls and processes to the cloud

- Cloud Data Protection & Shadow IT Discovery
- Enforcing Cloud Policy & Remediation
- Cloud IAM & User Analytics
- Cloud Incident Response & Investigation
- Cloud Compliance

Cloud API

Outside Perimeter

CASB Gateway

Proxy

Events

Enterprise Perimeter
Extending cyber controls and processes to the cloud

Cloud Data Protection & Shadow IT Discovery
Enforcing Cloud Policy & Remediation
Cloud IAM & User Analytics
Cloud Incident Response & Investigation
Cloud Compliance

Cloud API

Casb Gateway

CloudSOC

Outside Perimeter
Proxy
Events

Enterprise Perimeter
Data Protection Sources

- Web Gateway
- Endpoint
- DLP Enforce
- Threat Intelligence
New Challenges

- Proliferation of Cloud Apps
- Shadow Data Problem
- Compromised Accounts

26% of Cloud Docs are Broadly Shared

DLP Detection
DLP Enforce
Management Server

Cloud Data Protection & Shadow IT Discovery
Enforcing Cloud Policy & Remediation
Cloud IAM & User Analytics
Cloud Incident Response & Investigation
Cloud Compliance

Policy Workflow
On-premises DLP Detection
Extending DLP into cloud applications

- Extend DLP to Cloud Apps
- Apply Existing DLP Policies
- Leverage existing DLP Workflow

Gain Full CASB Functionality
- Inline Blocking and Offline Remediation
- Shadow IT Analysis
- User Behavior Analytics
Cloud Data Protection & Shadow IT Discovery

Enforcing Cloud Policy & Remediation

Cloud IAM & User Analytics

Cloud Incident Response & Investigation

Cloud Compliance
Cloud Data Protection & Shadow IT Discovery

Enforcing Cloud Policy & Remediation

Cloud IAM & User Analytics

Cloud Incident Response & Investigation

Cloud Compliance
External and public content exposures, including compliance risks

- 2,037 files stored in the cloud per user (average)
- 185 files per user are externally shared (average)

13% Public
19% External
68% All Company

20% of these files contain compliance-reared data (average)

56% SSN
29% PHI
15% PCI

Inbound risky content shared with employees (e.g., malware, IP)

Risky users and user activities

Marketing
Business
Health
Finance
Legal

Malware
Copyrighted Material
Passwords
Prohibited Material
Design Docs

5% of the users are responsible for
85% of the total risk exposures

Where to start? Understand what’s important to your business and where it is.
Complete a Shadow Data Risk Assessment.
There is only one word you need to know when talking about the cloud
CONTROL
Bring all that control together
... to give comprehensive information security with
GDPR – Privacy Enhancing Technologies

Panel Discussion – Q&A

30 minutes