Mitigating Insider Threats

ChiSen GAY, IBM Tivoli Security Sales Leader, ASEAN
Email : gaycs@sg.ibm.com

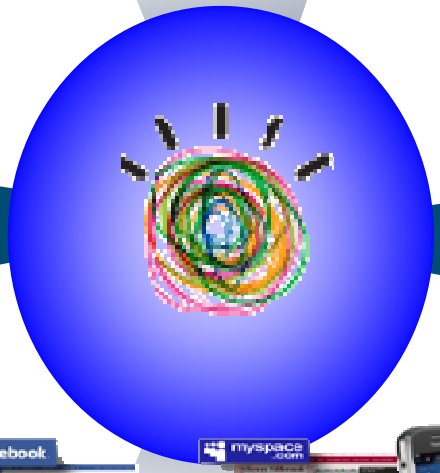
Agenda

- **An overview of Security**
- **Threats and Challenges in managing security**
- **Tivoli Security Focus Areas**
- **Identity & Access Assurance**
- **Customer success**

Welcome to the **smarter planet**

Globalization and Globally Available Resources

Billions of mobile devices accessing the Web



Access to streams of information in the Real Time

New Forms of Collaboration

New possibilities.
New complexities.
New risks.

Security: an overview

Top 5 Security Deficiencies

Improper Change Management

- Lack of formal program change procedure
- Lack of understanding of system configurations
- Oversight of changes and review of change logs

Insufficient Segregation of Duties

- NOT JUST Separation of requestor, approver, implementer --Separation of developers and operators

Excessive Access to Systems / Databases

- Developer / programmer / DBA /Admin access to production environment
- Developer / programmer DBA /Admin access to production data

Lack of Access Controls

- User provisioning and administration
  - Changes in responsibilities
  - Changes in organization
  - Terminations
- No documented access policies and standards

Lack of general monitoring of the security infrastructure

Top 5 material deficiencies derived from last two years Auditors Reports

Security in the Market

Threats and challenges

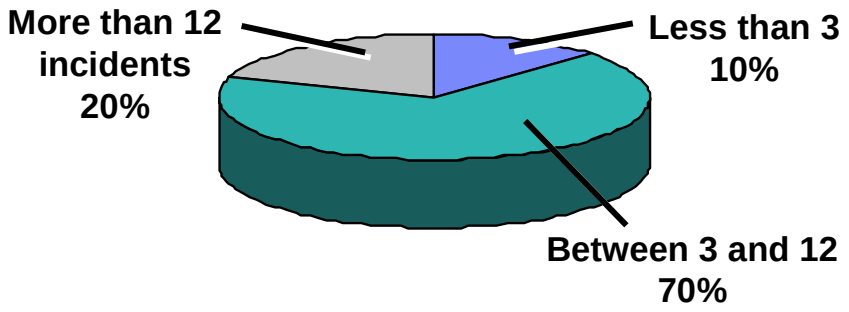
- **Threats continue to rise: mergers, acquisitions, layoffs. 59 percent of workers who left their positions took confidential information with them.**
  - **24% of these former employees responding to the survey said they still had access to their former employer's computer systems after they left,**
  - **50% between one day to a week,**
  - **20% more than a week.** **study by Ponemon Institute**
- **Weak passwords are easily compromised by insiders.**
  - **Internal attacks cost 6% of gross annual revenue -- costing USD 400 billion in the U.S. alone.**
- **30% of all help desk calls are password related.**
  - **Password resets can cost as much as $20-$25 per call.**

Key Business Drivers

Lower IT Costs (While Enabling Innovation)

Source: Customer Interviews

Address Rising Incidents



Source: IBM; IT Policy Compliance Group

Manage Insider Threat

Internal attacks cost 6% of gross annual revenue or $9 per employee per day.

Sources: Forrester research, IdM Trends 2006; USSS/CERT Insider Threat Survey 2005/6; CSI/FBI Survey, 2005; National Fraud Survey; CERT, various documents.

Demonstrate Compliance

Example: Need to Meet the Requirements of the PCI "Digital Dozen"

Security: an overview

Today's Security Challenges

Trusting Identities

Customers or criminals?

Partners or competitors?

Employees or hackers?

Managing Access

Securing Services

Payroll

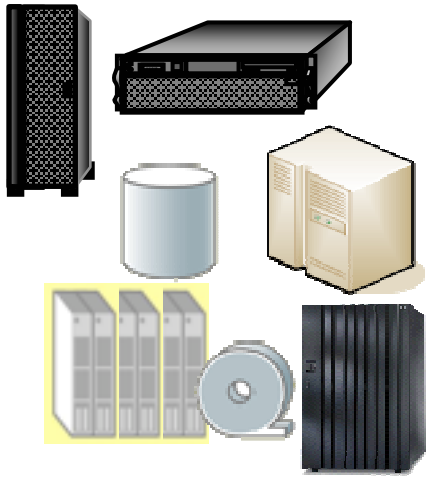
Online banking

Loan applications

Retail sales

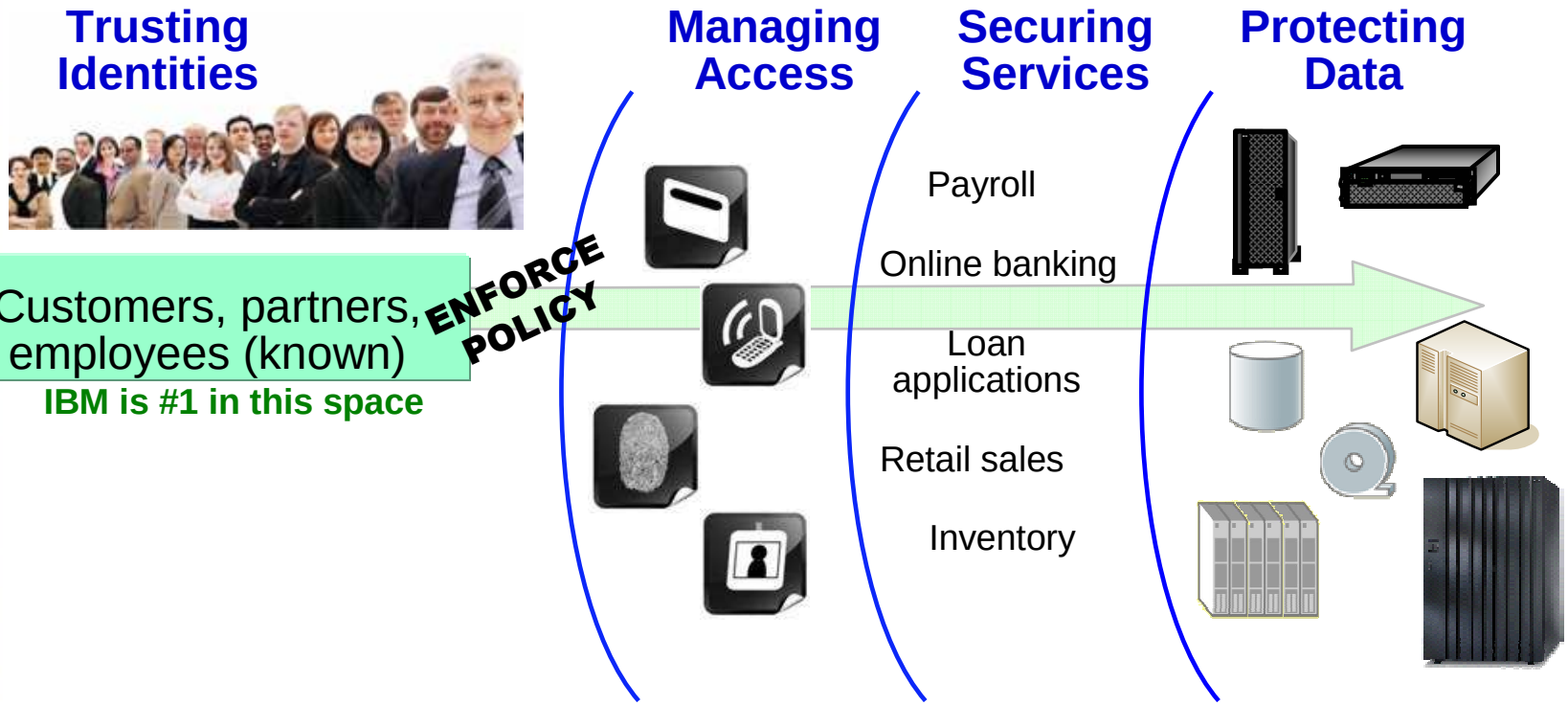
Inventory

Protecting Data



Security has to be applied within a Business context fused into the fabric of business and not as a bespoke solution to the next security threat

Tivoli Security Focus Areas



1 *Manage those you know.*

Tivoli Security Focus Areas

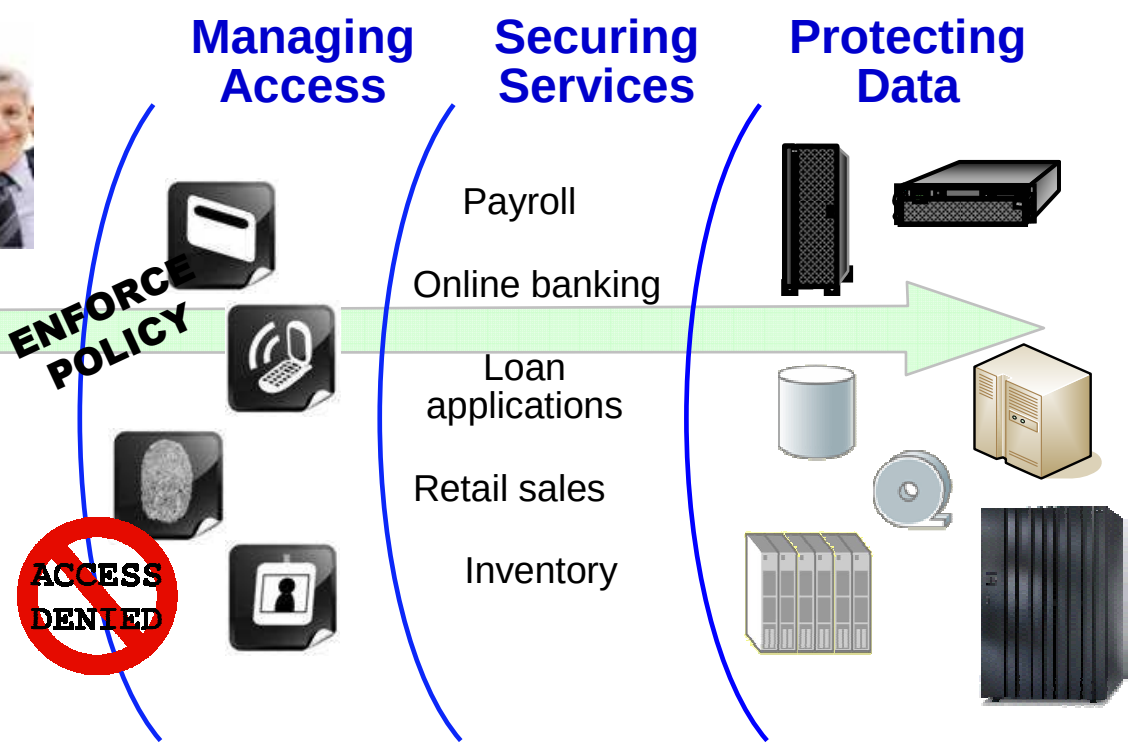
Trusting Identities

1 Customers, partners, employees (known)

IBM is #1 in this space

2 Criminals, competitors, hackers (unknown)

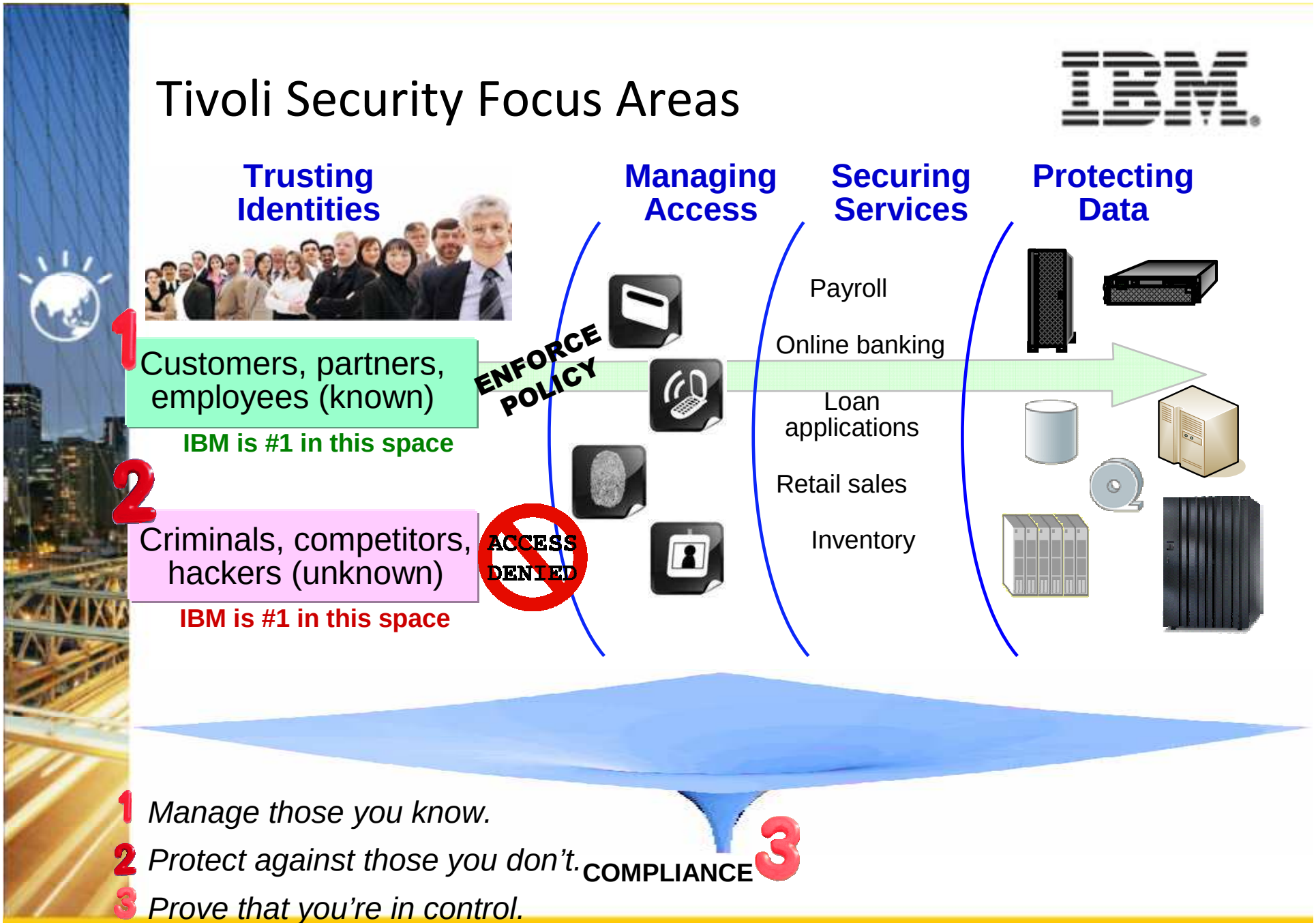
IBM is #1 in this space



1 *Manage those you know.*

2 *Protect against those you don't.*

Tivoli Security Focus Areas



1 *Manage those you know.*

2 *Protect against those you don't.*

3 *Prove that you're in control.*

Tivoli Security Focus Areas

1

2

3

Identity and Access Management Assurance

Improve Service

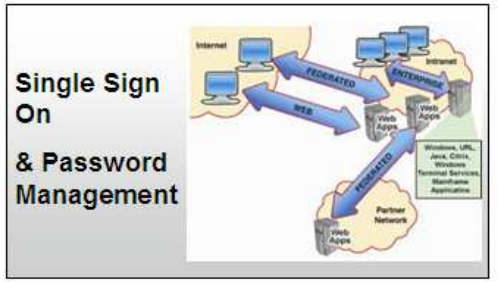
- Enable collaboration via role based portals with access to enterprise services and applications
- Increase market reach with federated business models leveraging trusted identity information

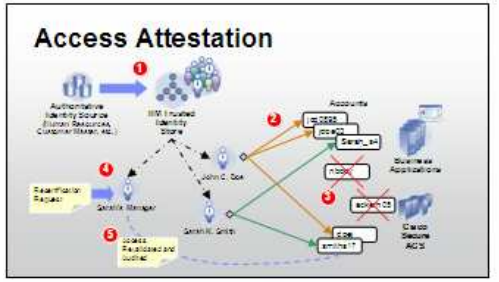
Reduce Cost

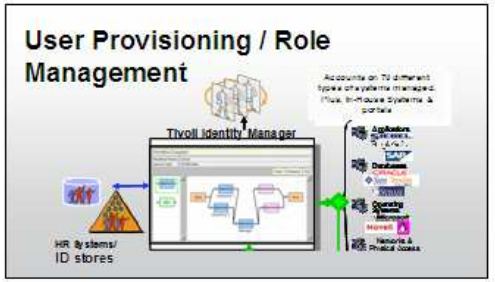
- Reduce help desk costs, password reset requests
- More efficiently manage restructuring
- ERP deployments / upgrades

Manage Risk

- Privileged users
- Failed audits,
- Insider breach
- Recertification, entitlements management
- National ID / Trusted ID – provisioning of strong / trusted credentials.
- Unauthorized IT change detection







Data and Application Security

Data Disclosure and Privacy Compliance

•Comply with data disclosure and privacy regulations including PCI DSS, GLBA worldwide data privacy laws

•Reduce the cost of compliance

Application Security and Agility

•Secure 3rd party collaboration and outsourcing

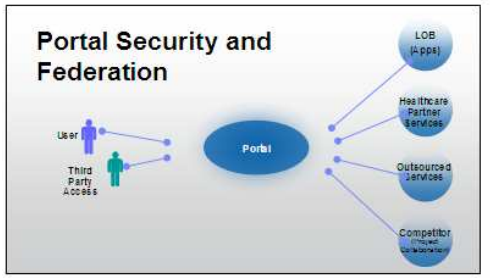
•Simplify management and quickly implement policy changes to protect data in critical applications

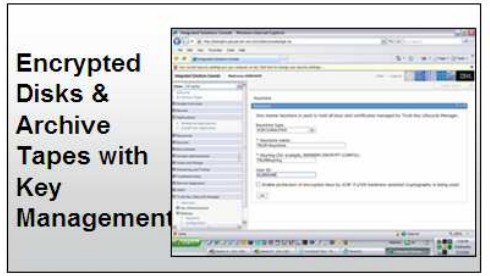
Manage business risk by protecting business information / IP

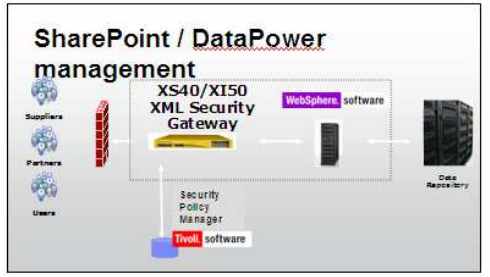
•Protect access to data in use within applications and data at rest including confidential employee, customer and financial data, and IP

Secure Storage

•Protect data at rest, on disk and tape







IBM is helping our clients advance their objectives through Security

- Objectives
  - Compliance with SOX, PCI, GLBA mandates
  - Management of insider threats and reduction of risk from privileged insiders
  - Monitoring of external threats to *generate reports/data on where to invest on perimeter defense and to feed incident management process where service availability may be affected*
  - *Automation and operational efficiency to reduce costs in audit and compliance reporting, identity and user entitlement administration, and application security*
- Challenges
  - World wide workforce and dealerships subject to complex regulatory requirements
  - Controlling access to sensitive information
  - Greater visibility into who has actually accessed sensitive information
  - Reduce administrative cost
  - Identify and protect against threats
- IBM Solution
  - Tivoli Identity Manager and Access Manager for managing users and their rights
  - Tivoli Access Manager manages Harley-Davidson Dealer Portal authorizations
  - Tivoli Security Information and Event Management for monitoring and reporting on user activity

Thank You