IBM Security

CISO Alliances

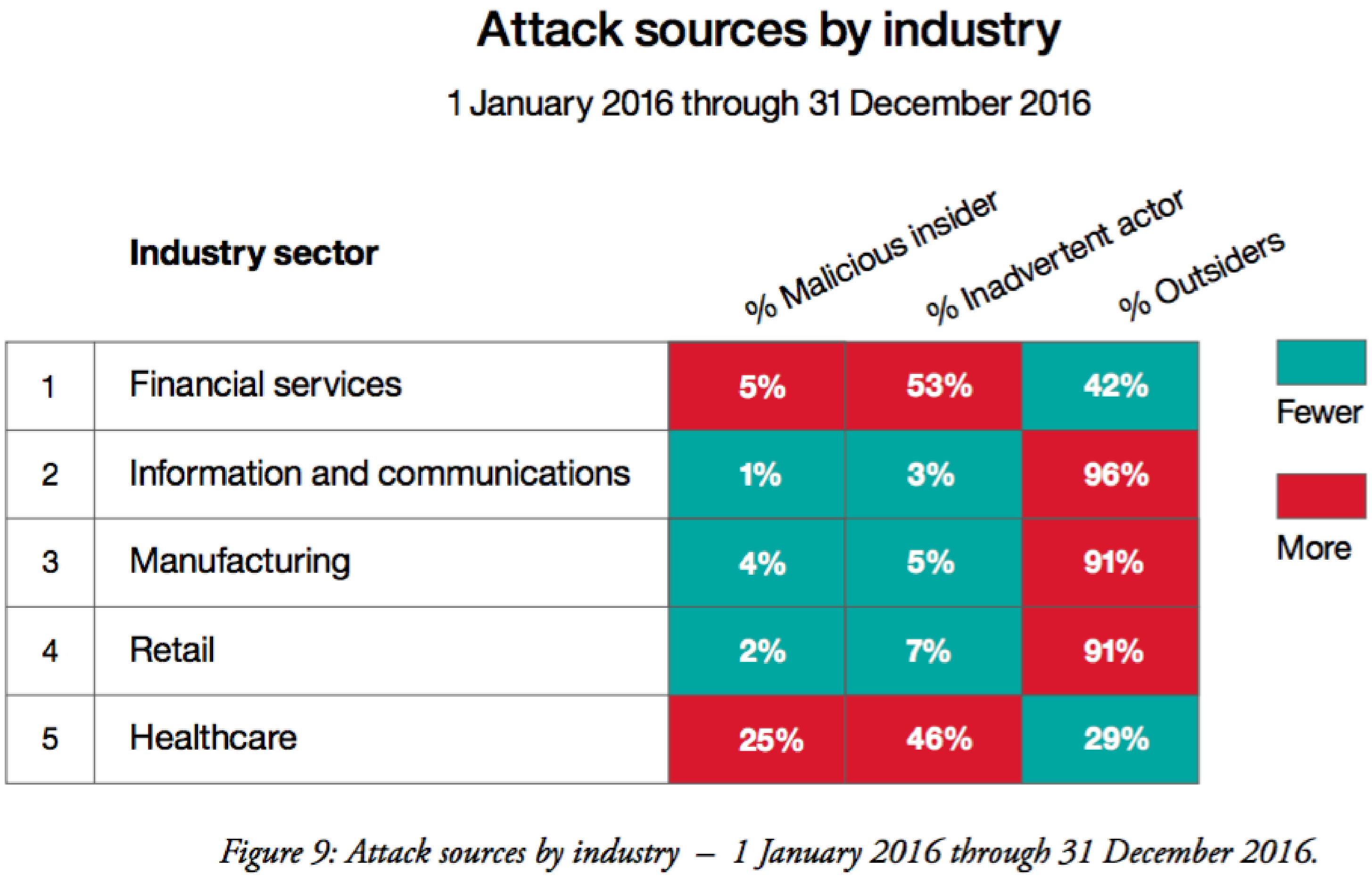
22 SEPTEMBER 2017

Sheldon Hand

IBM Security BU Leader

Cyber Threat Landscape

- IBM X-Force Research – March 2017 (Jan - Nov 2016)
- Year of Mega Breaches - Cost of lost / stolen data record average of $ 158



Attack sources by industry

1 January 2016 through 31 December 2016

	Industry sector	% Malicious insider	% Inadvertent actor	% Outsiders
1	Financial services	5%	53%	42%
2	Information and communications	1%	3%	96%
3	Manufacturing	4%	5%	91%
4	Retail	2%	7%	91%
5	Healthcare	25%	46%	29%

🟩 Fewer

🟥 More

Figure 9: Attack sources by industry – 1 January 2016 through 31 December 2016.

Ponemon INSTITUTE

2017 Cost of Data Breach Study

South Africa

Benchmark research sponsored by IBM Security
Independently conducted by Ponemon Institute LLC
June 2017

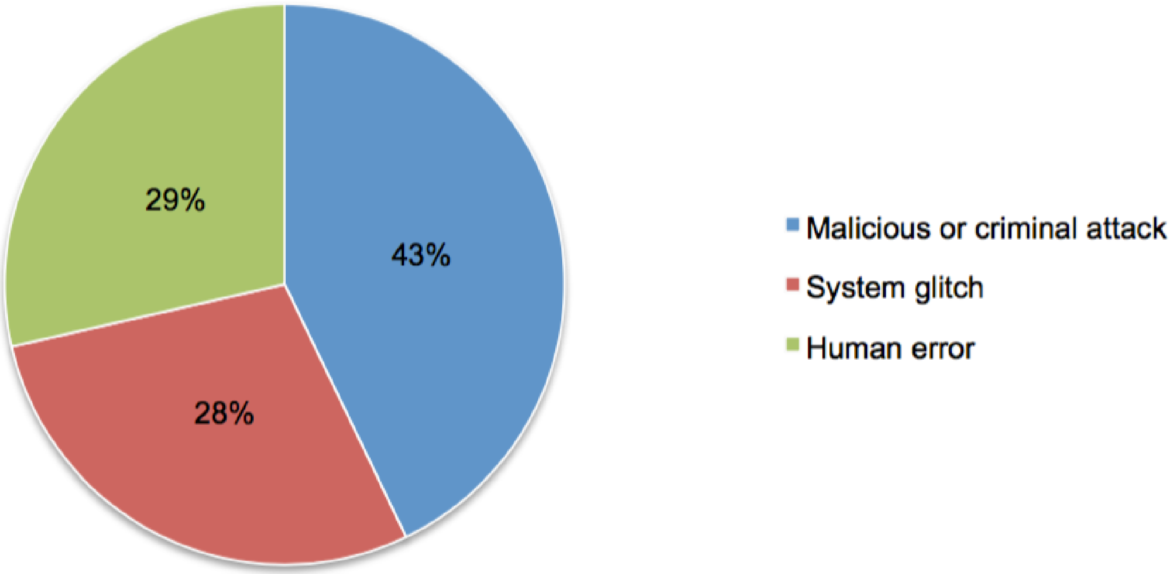
Ponemon Institute©
Research Report

IBM Security

South Africa at a glance

- 21 South African companies participated
- 32.36 million ZAR is the average total cost of data breach
- 12% increase in the total cost of data breach
- 1,632 ZAR is the average cost per lost or stolen record
- 5% increase in the cost per lost or stolen record

Distribution of the benchmark sample by root cause of the data breach

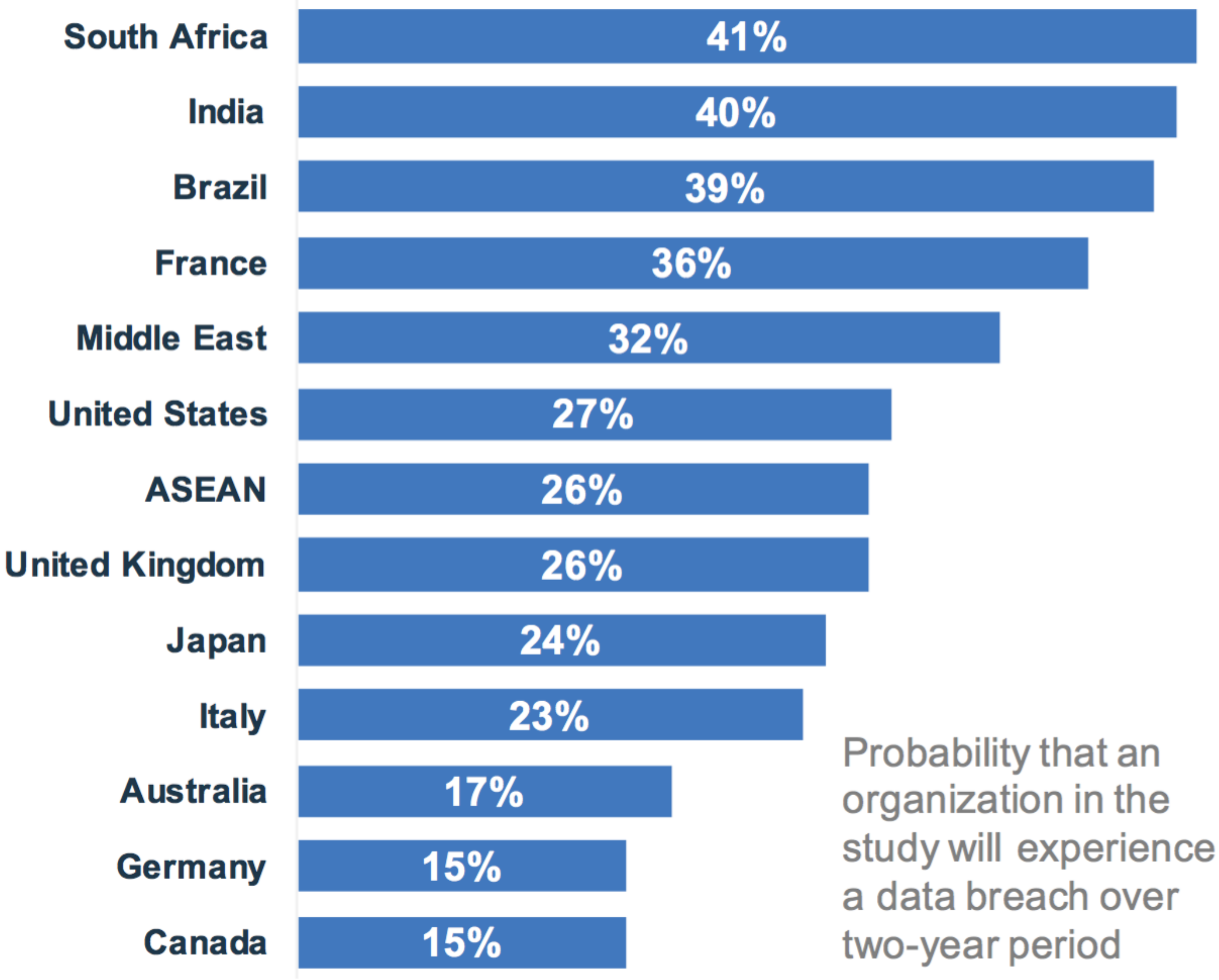


The odds are much greater that you will experience a data breach

Experiencing a data breach?

1 in 4

(Global average 28%)



Probability that an organization in the study will experience a data breach over two-year period

IBM Security

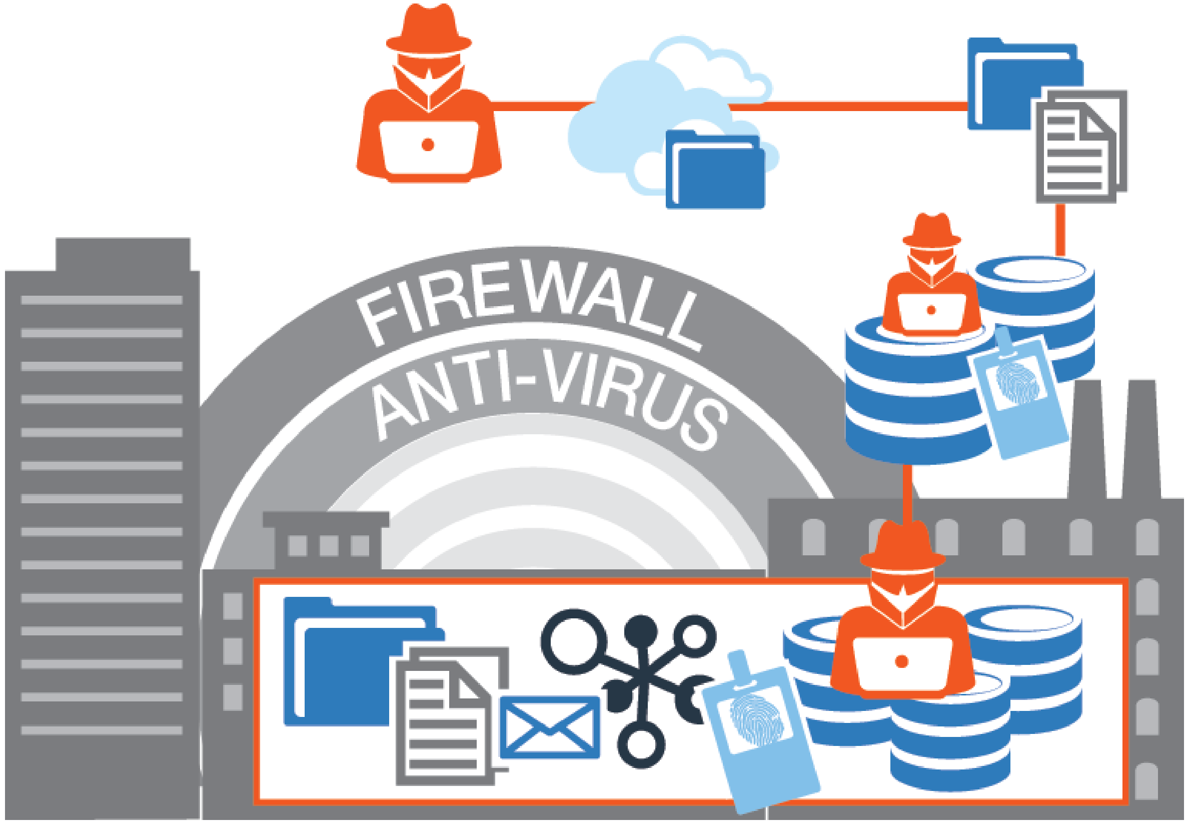
Tackle Insider Threats before They Tackle You!

CLEMENT MONAKHISI
SENIOR MANAGING CONSULTANT, IDENTITY AND ACCESS MANAGEMENT; DATA AND APPLICATION SECURITY, IBM SECURITY SERVICES

1. IBM’s Service Approach to Insider Threat Protection

2. myeyedr. Insider Threat Protection Case Study

What’s on the inside counts



60% of all attacks are caused by insider threats**

Damaging security incidents involve loss or illicit modification or destruction of sensitive data

Many security programs only focus on what’s happening beyond the perimeter

**Source: 2016 X-Force Report

Not all insider threats are created equal

Who represents an insider threat?

- An inadvertent actor
- A malicious employee
- A 3rd party/partner with access to sensitive data
  (And falls into one of the categories above)

Employees with privileged access to sensitive data carry the greatest risks!

60% of all attacks were carried out by insiders

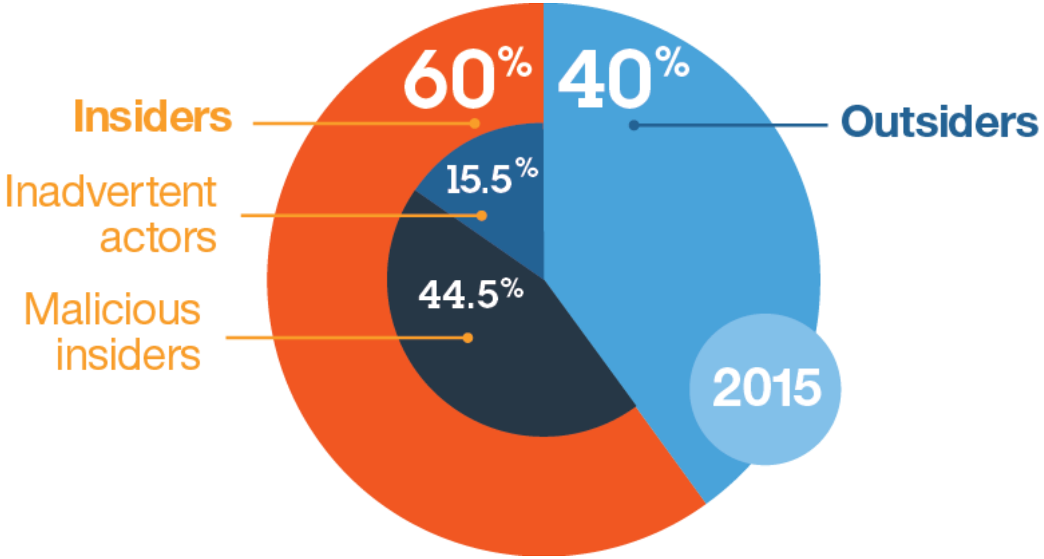
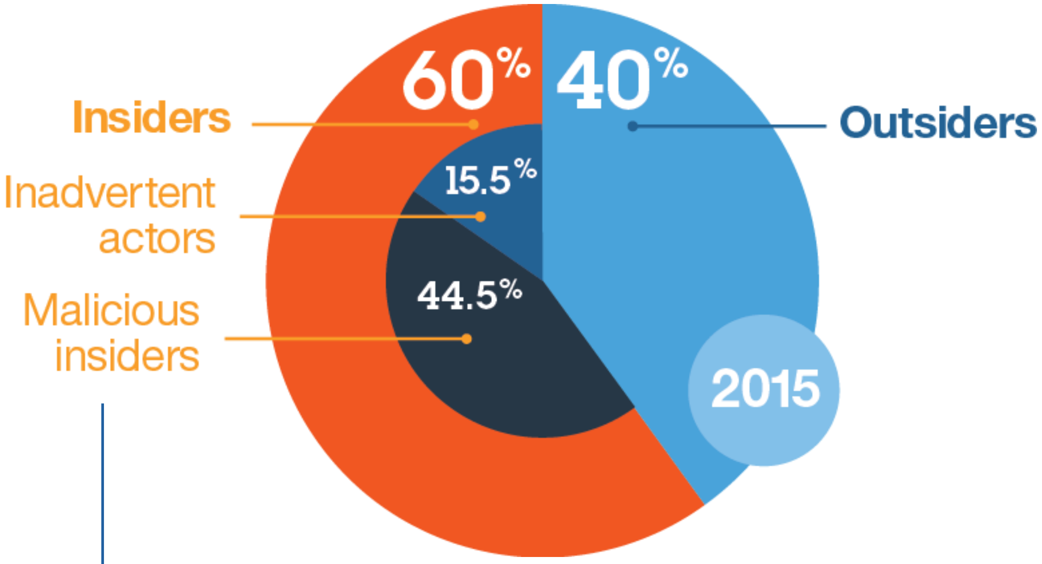


Image Source: IBM X-Force Research 2016 Cyber Security Intelligence Index

Past the stats - threats at MyEyeDr.

60% of end users tested fell prey to phishing:
80% of those who clicked the link revealed their credentials



Email Fraud:
Requests from the CEO

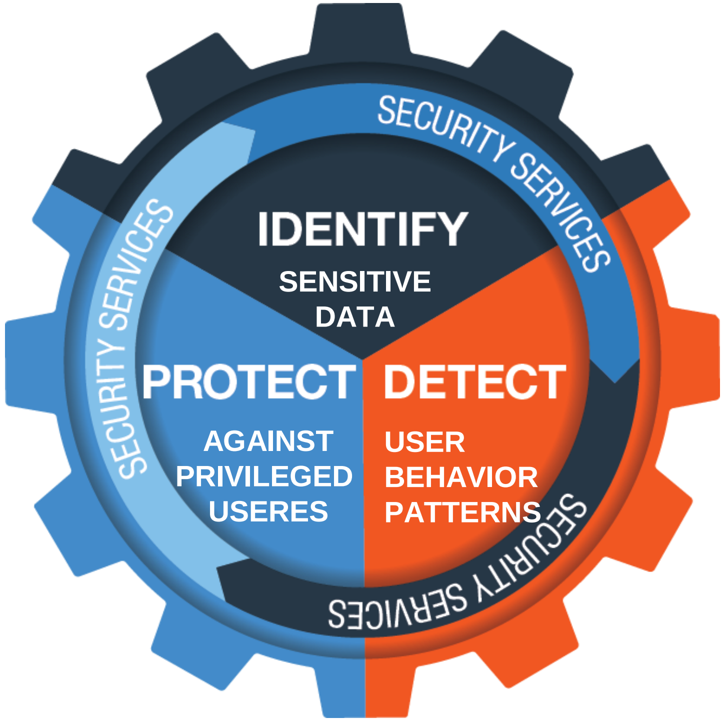
Terminated employee
Circumstances leading to disgruntled employee raise concerns over his access

Image Source: IBM X-Force Research 2016 Cyber Security Intelligence Index

Insider threat is a pressing problem for companies around the world, but the solution is not straightforward

- **Privacy concerns** around monitoring user activities
- Limited understanding about what actually constitutes “**crown jewels access**”
- **Inability to minimize or remove access** from privileged users
- No visibility or foresight into **user behavior changes** against the company
- Lack of an **integrated security approach**

In order to address these challenges, companies must integrate and optimize previously siloed security capabilities in three key areas

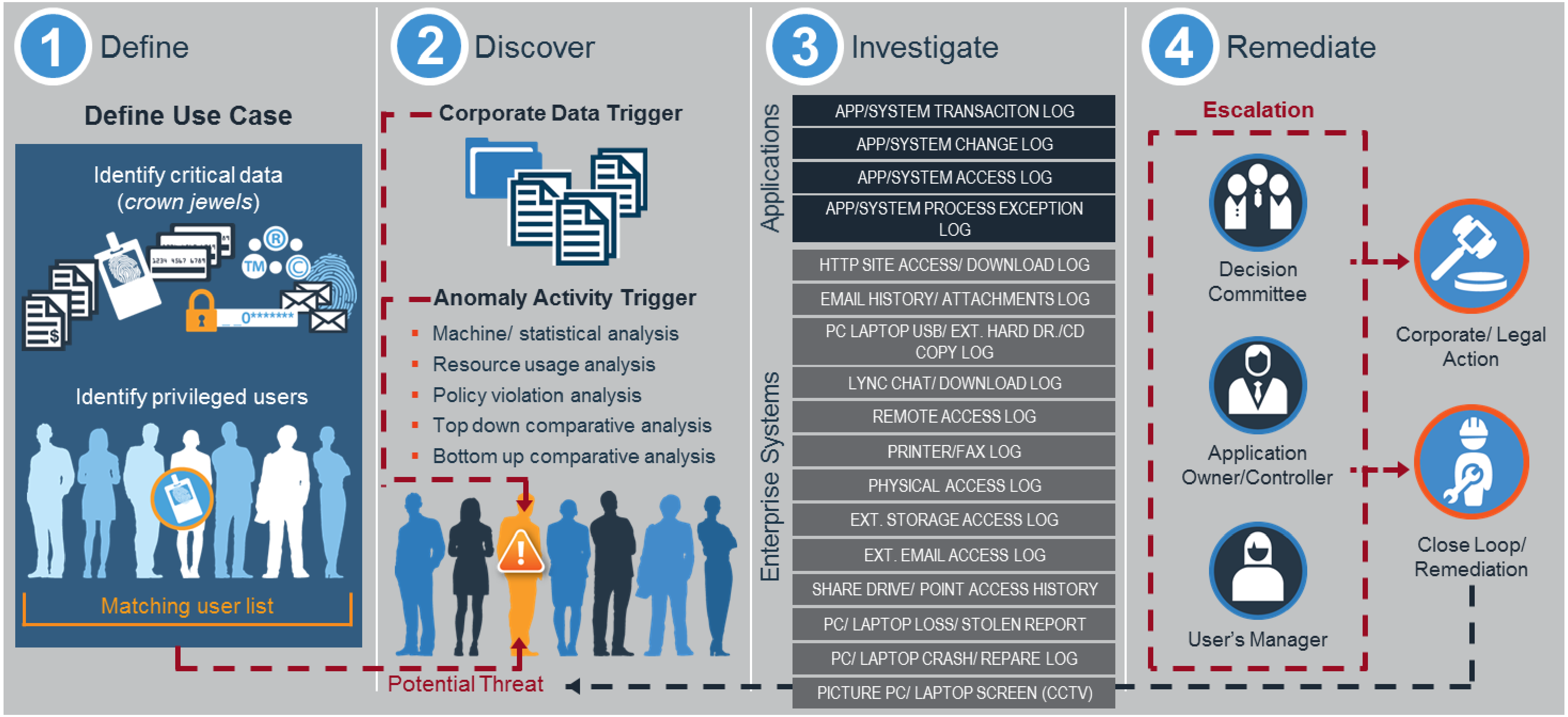


1. **Identify Sensitive Data** across the environment, and determine the privileged users who have access to the sensitive data

2. **Protect against the Privileged Users** - ensure least privilege / appropriate access is applied to the privileged users who has and uses the “keys to the kingdom”

3. **Detect user behavior changes and pattern** using analytics

Putting an insider threat solution into practice with a consistent and repeatable four step operational model with emphasis on high risk assets



1 Define

Define Use Case

Identify critical data (*crown jewels*)

Identify privileged users

Matching user list

2 Discover

Corporate Data Trigger

Anomaly Activity Trigger

- Machine/ statistical analysis
- Resource usage analysis
- Policy violation analysis
- Top down comparative analysis
- Bottom up comparative analysis

Potential Threat

3 Investigate

Applications

- APP/SYSTEM TRANSACITON LOG
- APP/SYSTEM CHANGE LOG
- APP/SYSTEM ACCESS LOG
- APP/SYSTEM PROCESS EXCEPTION LOG

Enterprise Systems

- HTTP SITE ACCESS/ DOWNLOAD LOG
- EMAIL HISTORY/ ATTACHMENTS LOG
- PC LAPTOP USB/ EXT. HARD DR./CD COPY LOG
- LYNC CHAT/ DOWNLOAD LOG
- REMOTE ACCESS LOG
- PRINTER/FAX LOG
- PHYSICAL ACCESS LOG
- EXT. STORAGE ACCESS LOG
- EXT. EMAIL ACCESS LOG
- SHARE DRIVE/ POINT ACCESS HISTORY
- PC/ LAPTOP LOSS/ STOLEN REPORT
- PC/ LAPTOP CRASH/ REPARE LOG
- PICTURE PC/ LAPTOP SCREEN (CCTV)

4 Remediate

Escalation

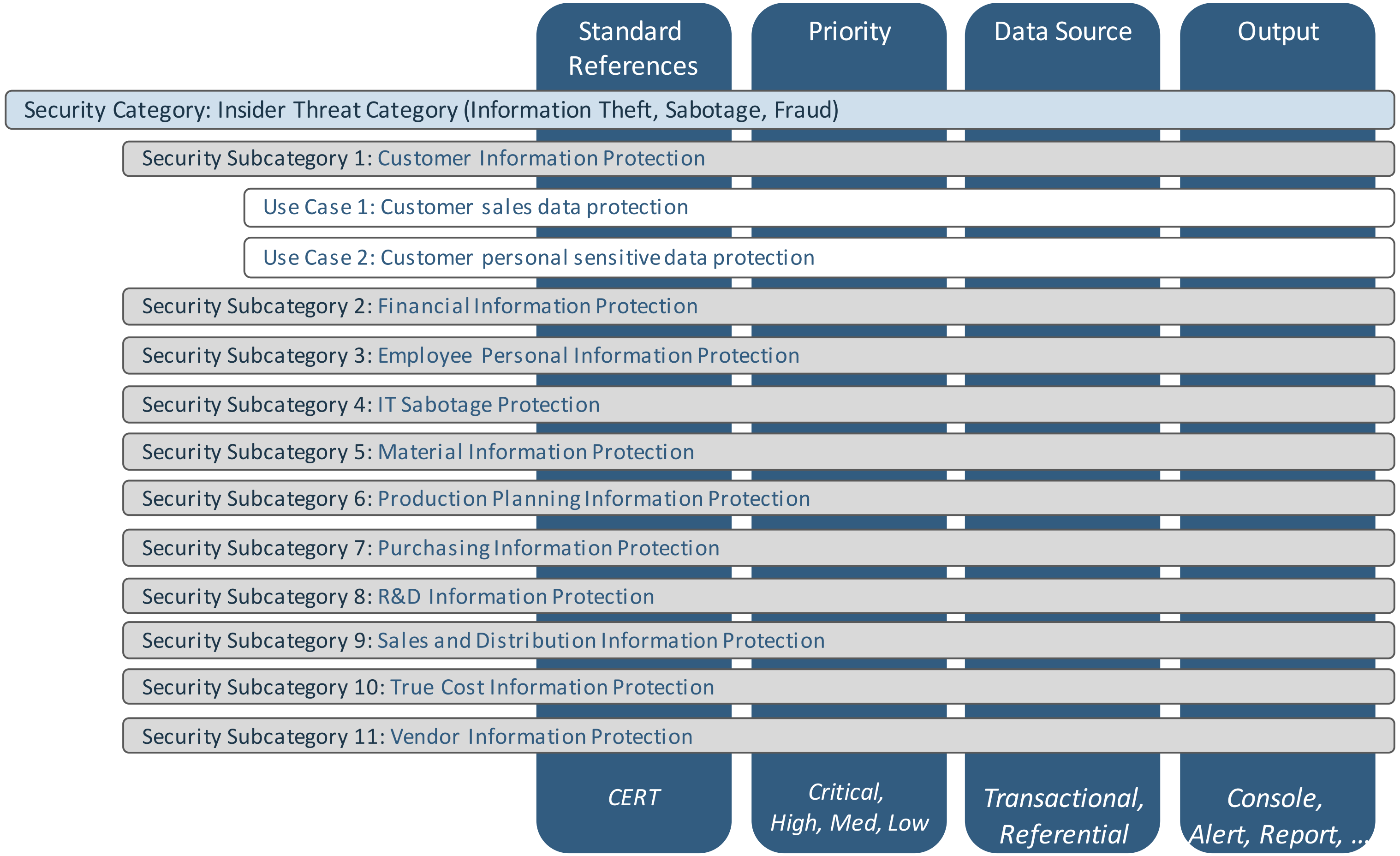
- Decision Committee
- Application Owner/Controller
- User's Manager

Corporate/ Legal Action

Close Loop/ Remediation

Sample Insider Threat Use Cases

Over 50 predefined business focused use cases to select from…

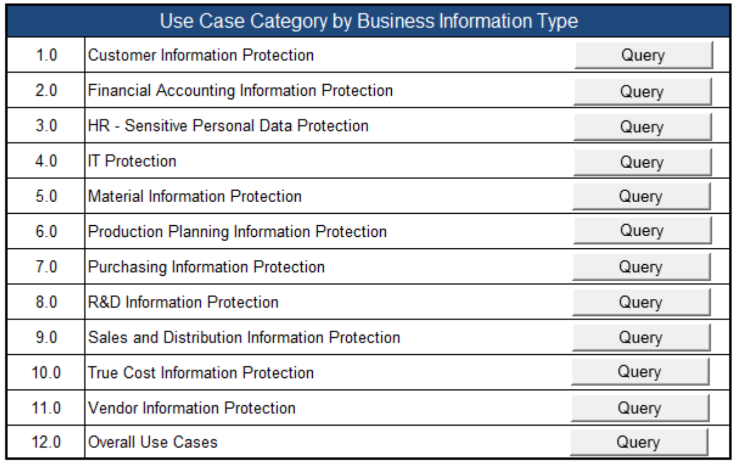


Standard References | Priority | Data Source | Output

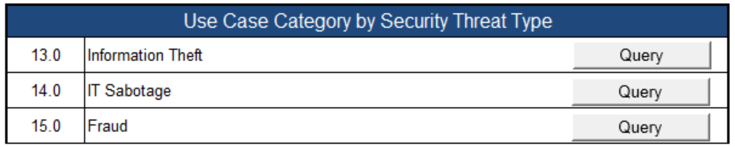
Security Category: Insider Threat Category (Information Theft, Sabotage, Fraud)

- Security Subcategory 1: Customer Information Protection
  - Use Case 1: Customer sales data protection
  - Use Case 2: Customer personal sensitive data protection
- Security Subcategory 2: Financial Information Protection
- Security Subcategory 3: Employee Personal Information Protection
- Security Subcategory 4: IT Sabotage Protection
- Security Subcategory 5: Material Information Protection
- Security Subcategory 6: Production Planning Information Protection
- Security Subcategory 7: Purchasing Information Protection
- Security Subcategory 8: R&D Information Protection
- Security Subcategory 9: Sales and Distribution Information Protection
- Security Subcategory 10: True Cost Information Protection
- Security Subcategory 11: Vendor Information Protection

CERT | *Critical, High, Med, Low* | *Transactional, Referential* | *Console, Alert, Report, …*

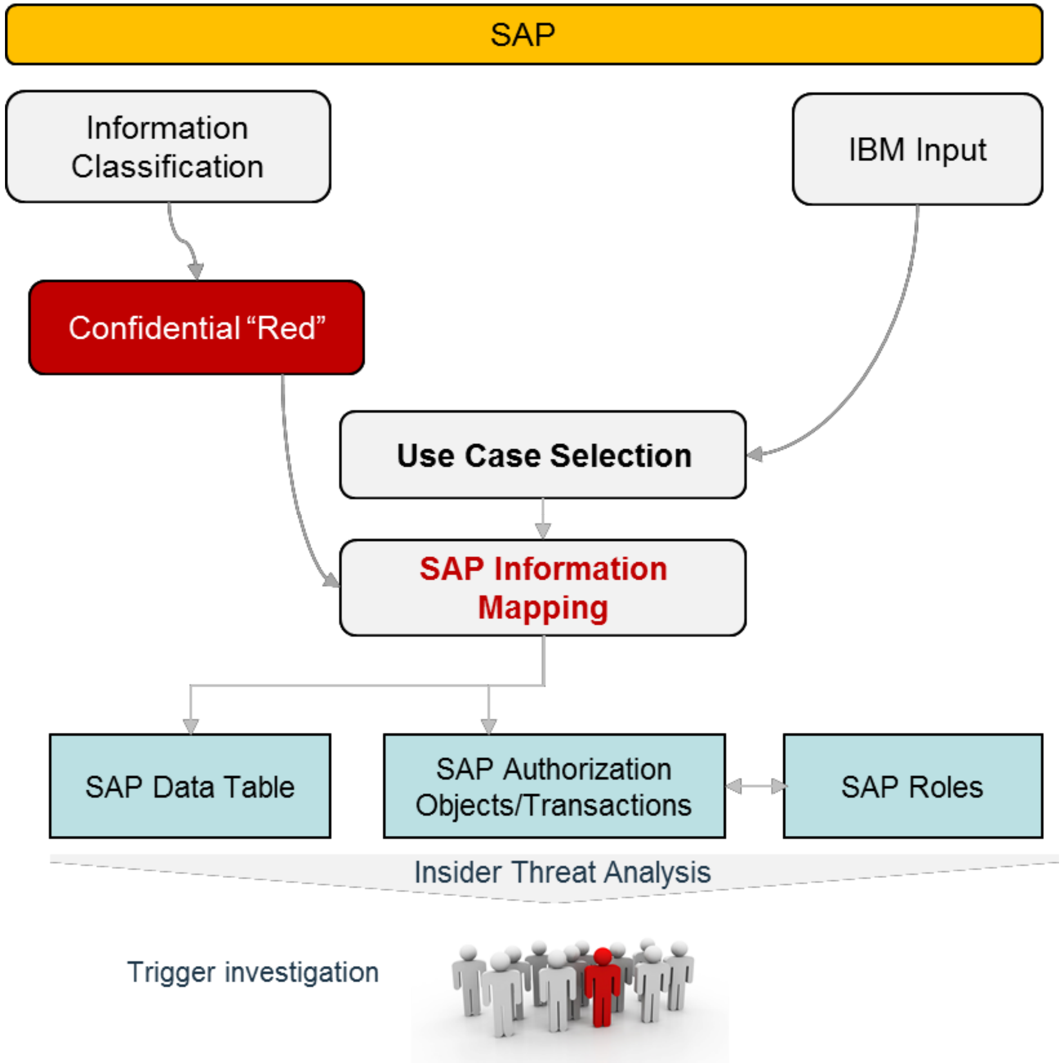


Use Case Category by Business Information Type		
1.0	Customer Information Protection	Query
2.0	Financial Accounting Information Protection	Query
3.0	HR - Sensitive Personal Data Protection	Query
4.0	IT Protection	Query
5.0	Material Information Protection	Query
6.0	Production Planning Information Protection	Query
7.0	Purchasing Information Protection	Query
8.0	R&D Information Protection	Query
9.0	Sales and Distribution Information Protection	Query
10.0	True Cost Information Protection	Query
11.0	Vendor Information Protection	Query
12.0	Overall Use Cases	Query



Use Case Category by Security Threat Type		
13.0	Information Theft	Query
14.0	IT Sabotage	Query
15.0	Fraud	Query

We implemented this solution for one of our global pharma clients to help address concerns about the impact of major re-org on employee morale



SAP

Information Classification

IBM Input

Confidential "Red"

Use Case Selection

SAP Information Mapping

SAP Data Table

SAP Authorization Objects/Transactions

SAP Roles

Insider Threat Analysis

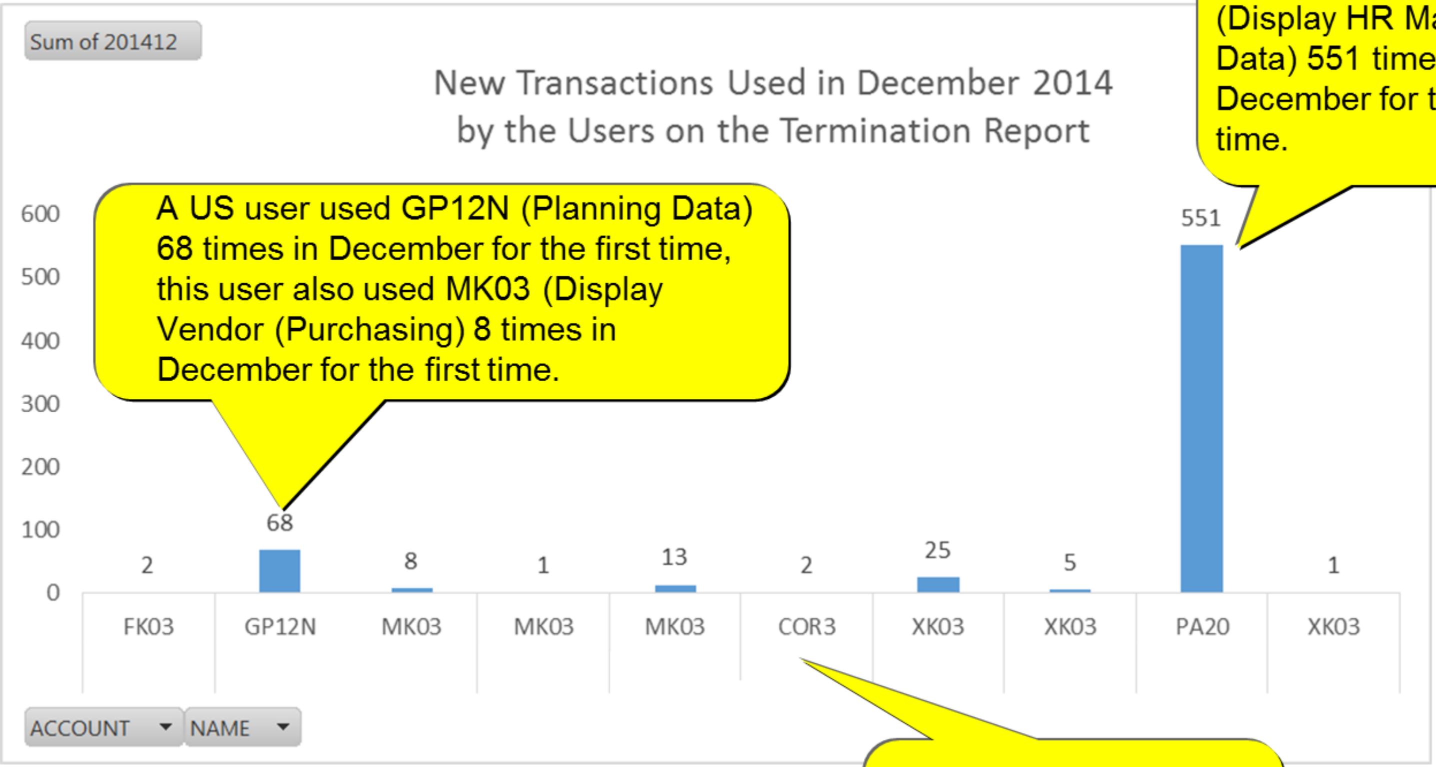
Trigger investigation

Project Overview:

1. Identified 7 areas of Information Classification in scope for the project.
   - Finance Management, Financial Transactions, Procurement-Sourcing, HR, Tax, Planning, and Risk Management
2. Out of the 7 areas of Information Classification, identified 11 Confidential "Red" information for use cases.
   - True Cost Data, Process Order, Serialization, Employee SPI, Investigation and Disciplinary, Purchasing and Contractual, Vendor SPI, Customer SPI, Undisclosed Financial Data, Project System
3. Mapped "Red" data to specific SAP tables, transactions, and roles which expose the information.
4. Collected 7 months of SAP transaction logs to analyze user activities across the sensitive transactions identified.
5. Identified anomaly activities for further investigation.

Outcome: Insider Threat Analysis #1: Sensitive transactions used for the first time on the month leaving the company

1st Analysis Findings



A US user used GP12N (Planning Data) 68 times in December for the first time, this user also used MK03 (Display Vendor (Purchasing) 8 times in December for the first time.

A MX user used PA20 (Display HR Master Data) 551 times in December for the first time.

A MX user used COR3 (Process Order Display) 2 times in December for the first time.

Data Summary:

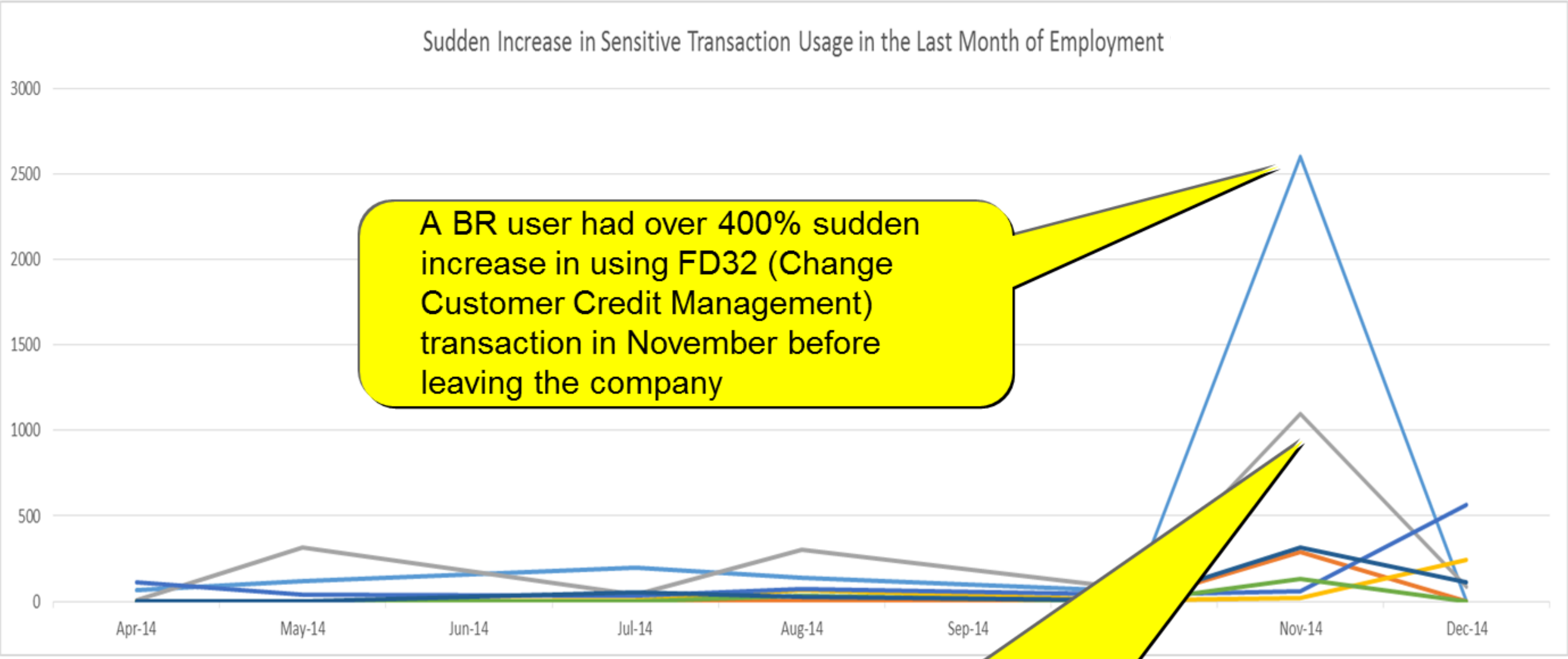
- 7 months of SAP transaction logs obtained
- Termination report obtained 1,984 users
  - Over 1M lines of transaction log entries captured
  - Of 1M entries, 56k sensitive transactions used
  - Of 56k transactions, 885 sensitive transactions were used by users on the terminated report

Outcome:

- 1st Analysis Finding: 8 users used 10 sensitive transactions for the first time in month the users were leaving company

Outcome: Insider Threat Analysis #2: Sudden (significant) increases in using sensitive transaction on the month leaving the company

2nd Analysis Findings



A BR user had over 400% sudden increase in using FD32 (Change Customer Credit Management) transaction in November before leaving the company

RU user had over 150% sudden increase in using ZPU109 (Easy Cost Planning FI) transaction in December before leaving the company

Data Summary:

- 7 months of SAP transaction logs obtained
- Termination report obtained 1,984 users
  - Over 1M lines of transaction log entries captured
  - Of 1M entries, 56k sensitive transactions used
  - Of 56k transactions, 885 sensitive transactions were used by users on the terminated report

Outcome:

- 2nd Analysis Finding: 7 users show sudden increase in sensitive transaction usage right before the termination

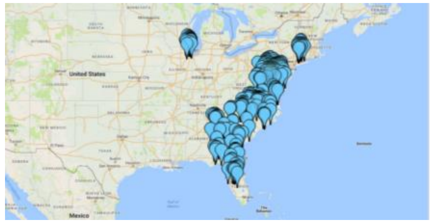
1. IBM’s Service Approach to Insider Threat Protection

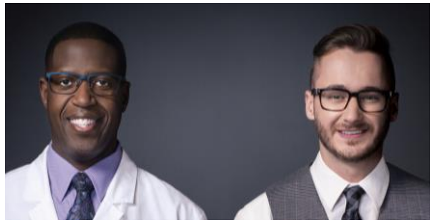
2. myeyedr. Insider Threat Protection Case Study

Who is MyEyeDr - exceptional full-service vision care, a wide selection of prescription eyeglasses and sunglasses, and standard and specialty contact lenses.

Market leader, founded in 2001

325 locations in 11 states and DC

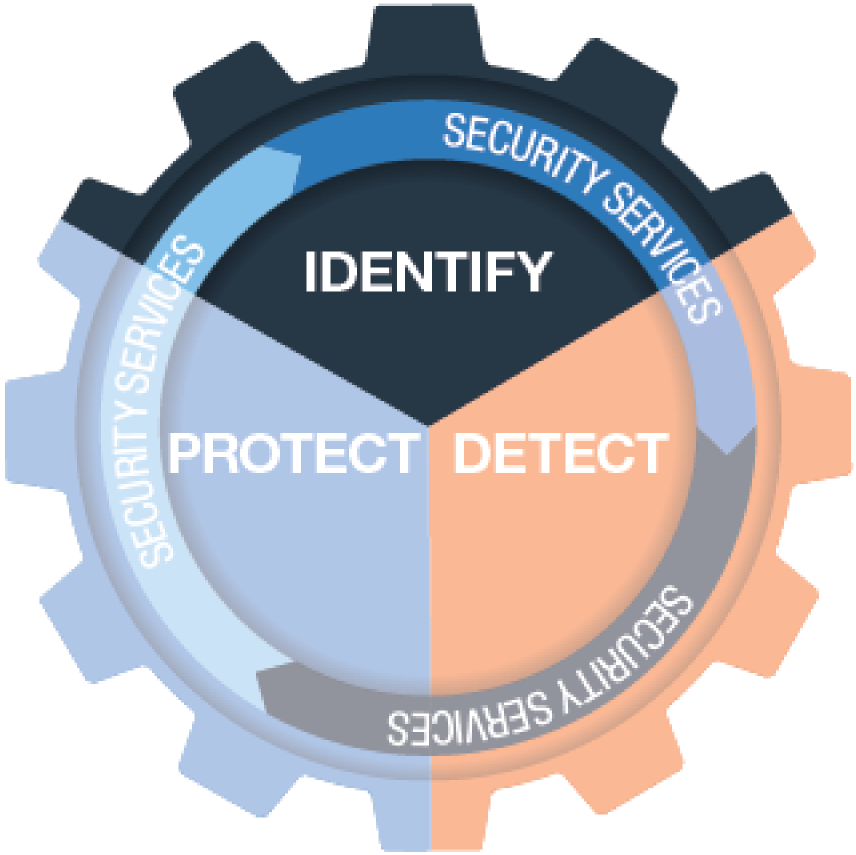




Nearly 3,000 employees

Serving approximately 3 million active patients

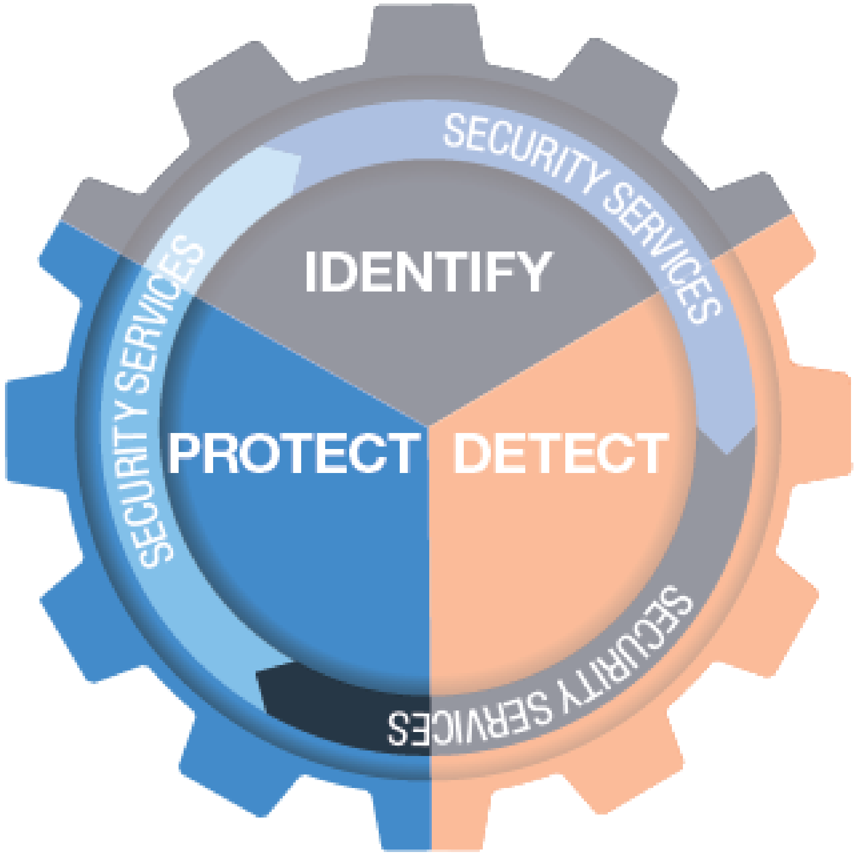
Identify – What data is sensitive?

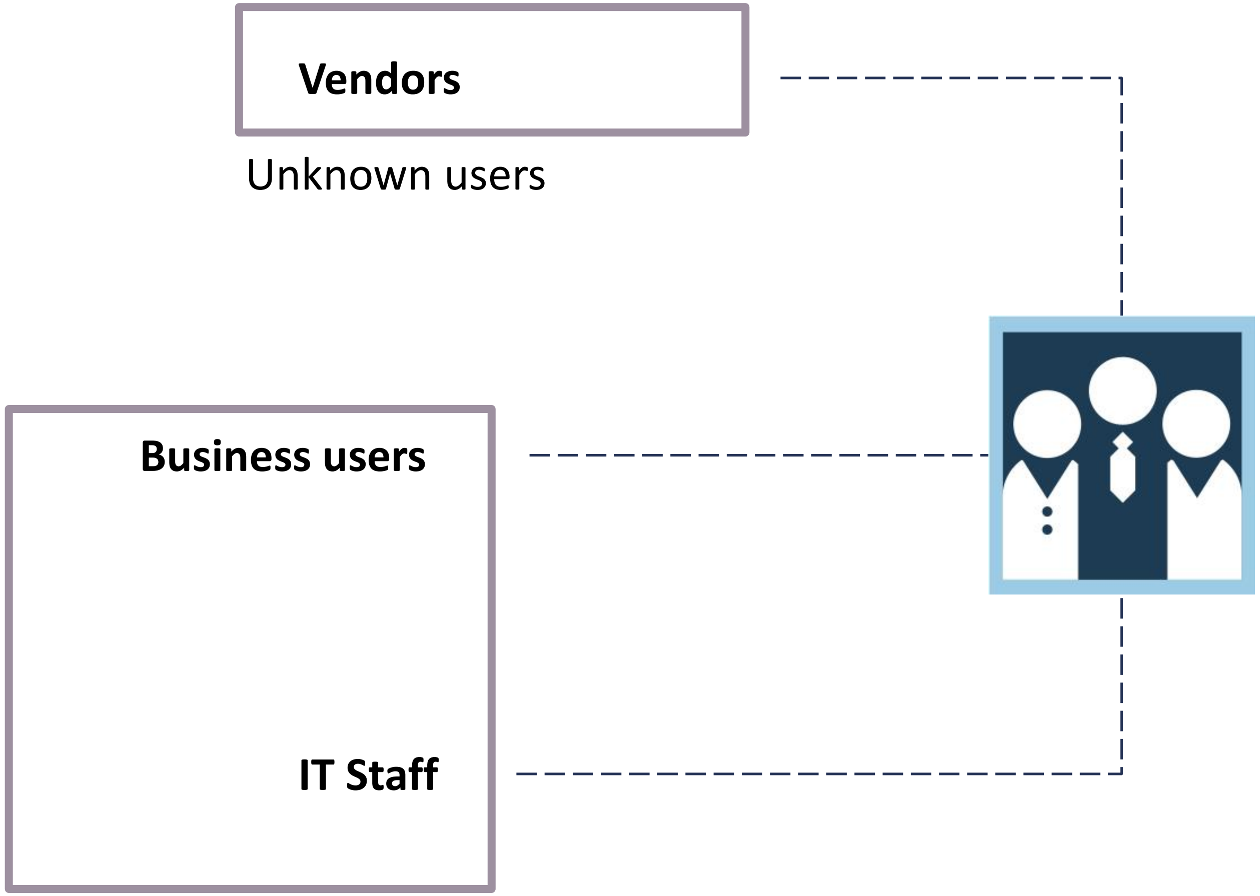


Patient Database

- Nearly 7 million patient records
- Single database
- Must be PCI and HIPAA compliant

Protect – Who is accessing your data?

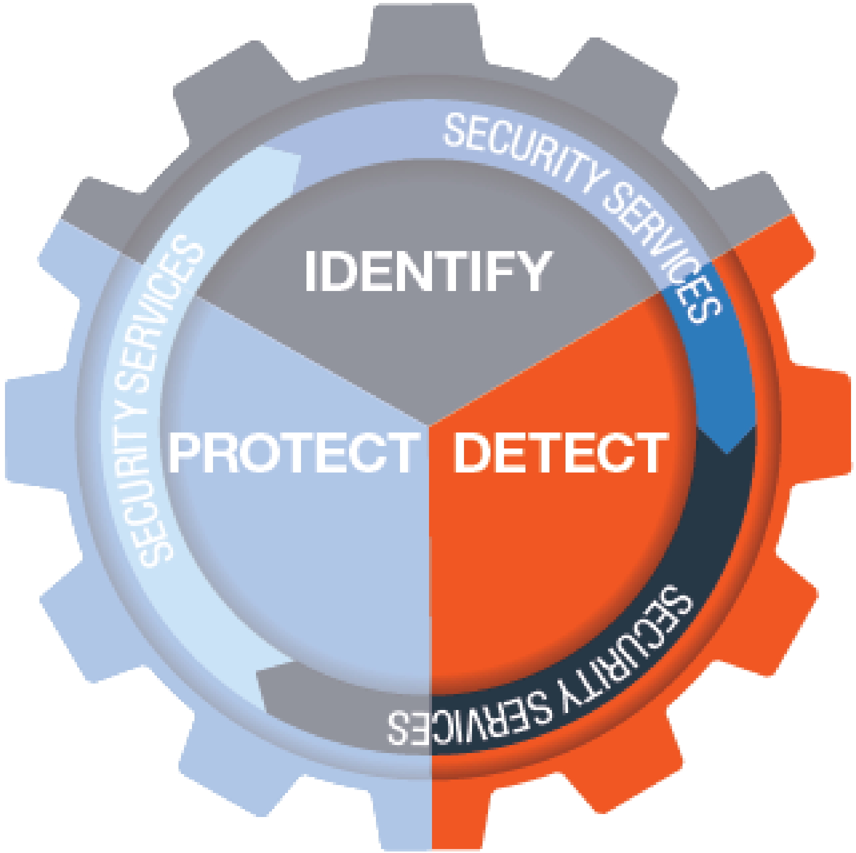




Unknown users

High turnover rates
Personally accountable

Detect – what are users doing with the data?

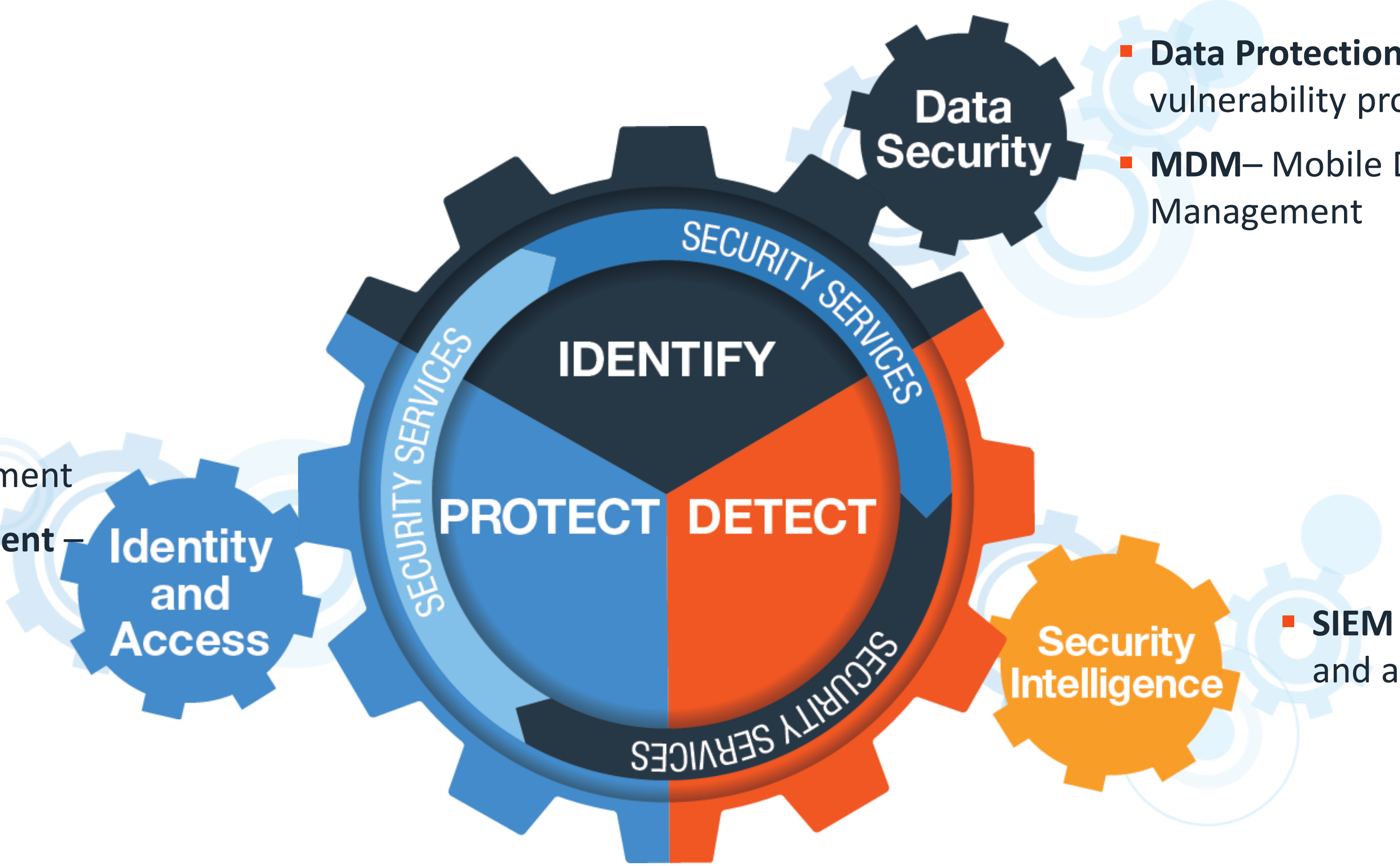


Flagged activities

- Data copying
- Allowed vs. not allowed patient records of each party
- Email of confidential patient information
- Access on mobile devices
- Access of patient data outside the office

Integrated Insider Threat Program at MyEyeDr.

- **Privileged Access Management** – Password Management
- **Identity Management** – Credential Synchronization

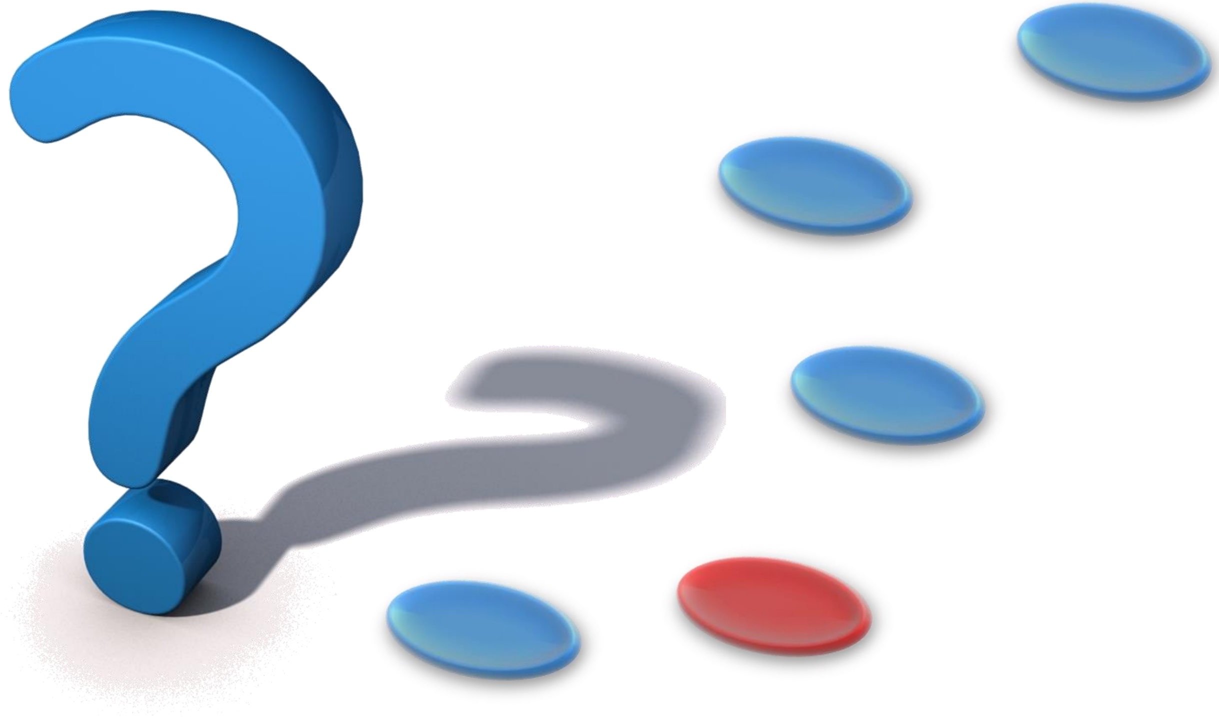


- **Data Protection**– Data and vulnerability protection
- **MDM**– Mobile Device Management

- **SIEM –** security intelligence and analytics

Advice to others – how do you get started?

- Break into smaller projects
- Tackle the most important task first
- Remember the end user
- Find the right partner



Notices and disclaimers

U.S. Government Users Restricted Rights — use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM.

Information in these presentations (including information relating to products that have not yet been announced by IBM) has been reviewed for accuracy as of the date of initial publication and could include unintentional technical or typographical errors. IBM shall have no responsibility to update this information. **This document is distributed "as is" without any warranty, either express or implied. In no event shall IBM be liable for any damage arising from the use of this information, including but not limited to, loss of data, business interruption, loss of profit or loss of opportunity.** IBM products and services are warranted according to the terms and conditions of the agreements under which they are provided.

IBM products are manufactured from new parts or new and used parts. In some cases, a product may not be new and may have been previously installed. Regardless, our warranty terms apply."

Any statements regarding IBM's future direction, intent or product plans are subject to change or withdrawal without notice.

Performance data contained herein was generally obtained in a controlled, isolated environments. Customer examples are presented as illustrations of how those customers have used IBM products and the results they may have achieved. Actual performance, cost, savings or other results in other operating environments may vary.

References in this document to IBM products, programs, or services does not imply that IBM intends to make such products, programs or services available in all countries in which IBM operates or does business.

Workshops, sessions and associated materials may have been prepared by independent session speakers, and do not necessarily reflect the views of IBM. All materials and discussions are provided for informational purposes only, and are neither intended to, nor shall constitute legal or other guidance or advice to any individual participant or their specific situation.

It is the customer's responsibility to insure its own compliance with legal requirements and to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the customer may need to take to comply with such laws. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the customer is in compliance with any law.

Notices and disclaimers continued

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products in connection with this publication and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products. IBM does not warrant the quality of any third-party products, or the ability of any such third-party products to interoperate with IBM's products. **IBM expressly disclaims all warranties, expressed or implied, including but not limited to, the implied warranties of merchantability and fitness for a particular**, **purpose.**

The provision of the information contained herein is not intended to, and does not, grant any right or license under any IBM patents, copyrights, trademarks or other intellectual property right.

IBM, the IBM logo, ibm.com, Aspera®, Bluemix, Blueworks Live, CICS, Clearcase, Cognos®, DOORS®, Emptoris®, Enterprise Document Management System™, FASP®, FileNet®, Global Business Services®, Global Technology Services®, IBM ExperienceOne™, IBM SmartCloud®, IBM Social Business®, Information on Demand, ILOG, Maximo®, MQIntegrator®, MQSeries®, Netcool®, OMEGAMON, OpenPower, PureAnalytics™, PureApplication®, pureCluster™, PureCoverage®, PureData®, PureExperience®, PureFlex®, pureQuery®, pureScale®, PureSystems®, QRadar®, Rational®, Rhapsody®, Smarter Commerce®, SoDA, SPSS, Sterling Commerce®, StoredIQ, Tealeaf®, Tivoli® Trusteer®, Unica®, urban{code}®, Watson, WebSphere®, Worklight®, X-Force® and System z® Z/OS, are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at: www.ibm.com/legal/copytrade.shtml.