Risk Assessment and Decision Support for Security Policies

IEEE Policy 2011 Symposium

Marco Casassa Mont (marco.casassa-mont@hp.com), Richard Brown (richard.brown@hp.com)

Cloud & Security Lab, HP Labs Bristol, UK

 © Copyright 2010 Hewlett-Packard Development Company, L.P.

OUTLINE

- Addressed Problem
- Risk Assessment and Decision Support for Security Policies
- Approach: Security Analytics
- Case Study on Identity and Access Management (IAM)
- Conclusions

© Copyright 2010 Hewlett-Packard Development Company, L.P.

OUTLINE

- Addressed Problem
- Risk Assessment and Decision Support for Security Policies
- Approach: Security Analytics
- Case Study on Identity and Access Management (IAM)
- Conclusions

© Copyright 2010 Hewlett-Packard Development Company, L.P.

KEY PROBLEM

– How to provide Strategic Decision Makers (e.g. CIOs/CISOs) with Risk Assessment and Decision Support Capabilities when dealing with their Strategic Security Policies?

– Key Related Questions:
  – What business and security risks is the organisation exposed to due to the security policies and related operational processes currently in place?
  – How effectively are these policies enforced at the operational level?
  – What is the impact of a change in policy or a change in the threat environment?

© Copyright 2010 Hewlett-Packard Development Company, L.P.

OUTLINE

- Addressed Problem
- Risk Assessment and Decision Support for Security Policies
- Approach: Security Analytics
- Case Study on Identity and Access Management (IAM)
- Conclusions

© Copyright 2010 Hewlett-Packard Development Company, L.P.

STRATEGIC SECURITY POLICIES

- Complex activity
- Different priorities for different stakeholders:
  - CISOs, CIOs, Risk Managers, Compliance Managers, Business Managers …
- Taking into accounts trade-offs between:
  - Security Risks, Productivity, Business Availability, Compliance, Cost …
    - Authentication Policies
    - Access Management Policies
    - Vulnerability and Threat Management Policies
    - Data Protection Policies
    - Web Access Policies
    - Security Monitoring Policies
    - Policies about Access to Physical Sites
    - …

© Copyright 2010 Hewlett-Packard Development Company, L.P.

DECISION MAKING PROCESS IN IT SECURITY

- Increasing demand for a more rigorous, scientific approach to the security decision making process and risk assessment
  - Provide Evidence to justify policy decision and attract investments
  - Provide Insights about impact of policy decisions at the operational level
  - Explore in advance the impact of various options, by means of What-if Analysis
- Current risk assessment approaches, based on ISO 2700x, provide generic guidelines and coarse grained analysis. But they still need to be instantiated within operational environments

© Copyright 2010 Hewlett-Packard Development Company, L.P.

OUTLINE

- Addressed Problem
- Risk Assessment and Decision Support for Security Policies
- Approach: Security Analytics
- Case Study on Identity and Access Management (IAM)
- Conclusions

© Copyright 2010 Hewlett-Packard Development Company, L.P.

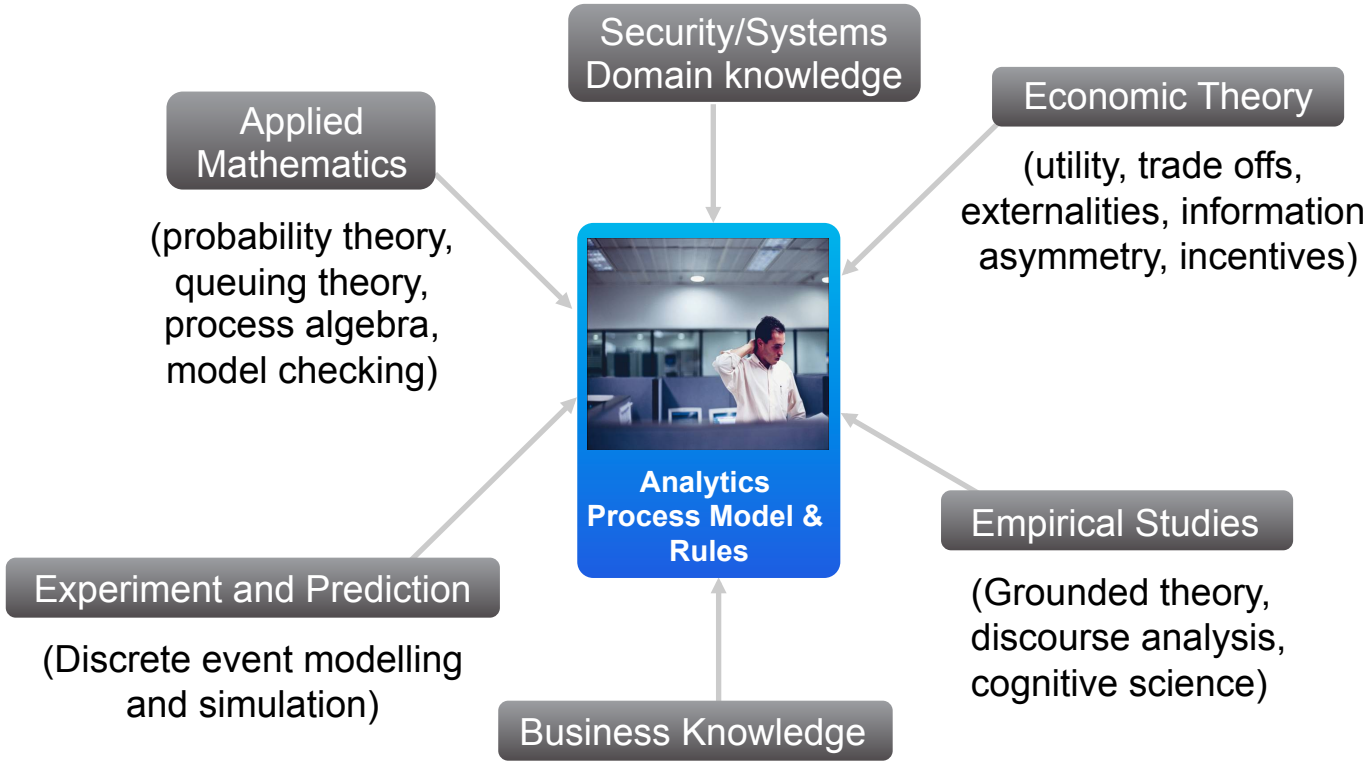
SECURITY ANALYTICS

Putting the Science
into Information Security
Management

© Copyright 2010 Hewlett-Packard Development Company, L.P.

SECURITY ANALYTICS:

Integrating Scientific Knowledge



© Copyright 2010 Hewlett-Packard Development Company, L.P.

AN EXAMPLE: VULNERABILITY MANAGEMENT

– How do we evaluate the effectiveness of our vulnerability management processes and policies?
  - when we have a combination of protections and processes: patch management, AV, HIPS, emergency escalation, temporary workarounds

– How do we estimate in advance the impact on overall protection of a change in policy or the addition of a new security mechanism?

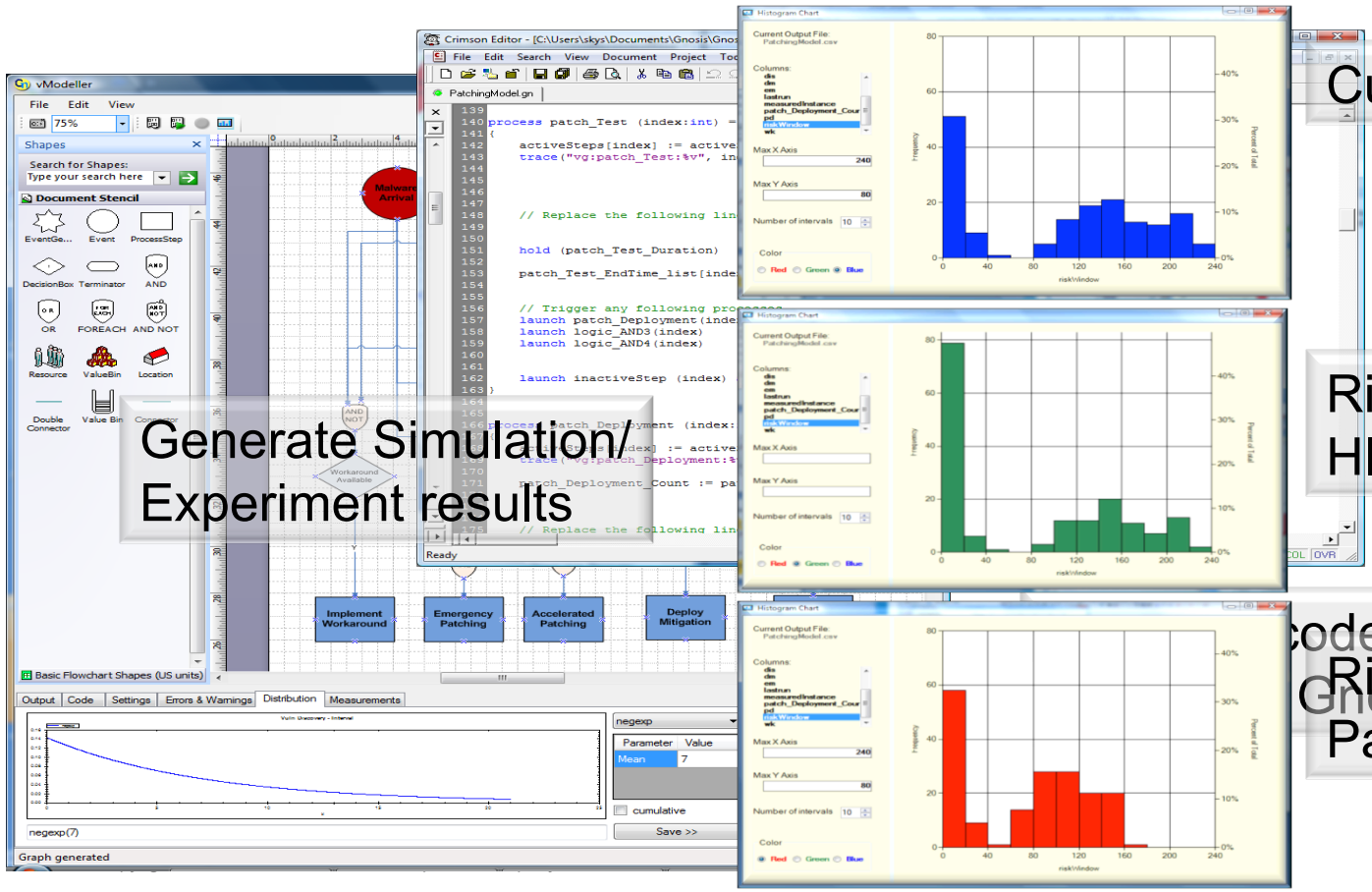
© Copyright 2010 Hewlett-Packard Development Company, L.P.

THE SOLUTION: BUILD A MODEL

- Stochastic model of threat environment
- Process model of organization's protections
- Validate with experts and against known data sources
- Select a metric
  - e.g. Time until "risk mitigated"
- Execute the model as a discrete event simulation
  - ~100K vulnerabilities
  - check for sensitivities in parameters
- Adjust the model to reflect proposed changes in policy and see how well the changes perform

© Copyright 2010 Hewlett-Packard Development Company, L.P.

SECURITY ANALYTICS TOOLS



Current Risk Window

Risk Window with HIPS investment

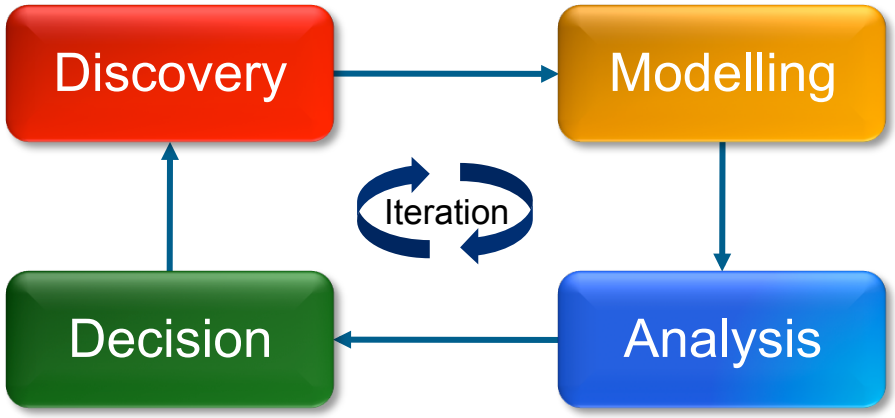
code for the Gnosis Engine

Risk Window with Patch Investment

PACKAGED SECURITY ANALYTICS

Transforming security management to one based on scientific rigour

- Iterative consultancy engagement approach to define the problem and explore possible solutions and their tradeoffs
- Generation of full report including a summary of the analysis performed and recommendations



© Copyright 2010 Hewlett-Packard Development Company, L.P.

OUTLINE

- Addressed Problem
- Risk Assessment and Decision Support for Security Policies
- Approach: Security Analytics
- Case Study on Identity and Access Management (IAM)
- Conclusions

© Copyright 2010 Hewlett-Packard Development Company, L.P.

IAM CASE STUDY

– Applying Security Analytics for risk assessment and decision support

– Focus on access management processes and related policies

– Jointly carried out with a major HP customer in the UK Government

 © Copyright 2010 Hewlett-Packard Development Company, L.P.

IAM CASE STUDY: PROBLEM SETTING

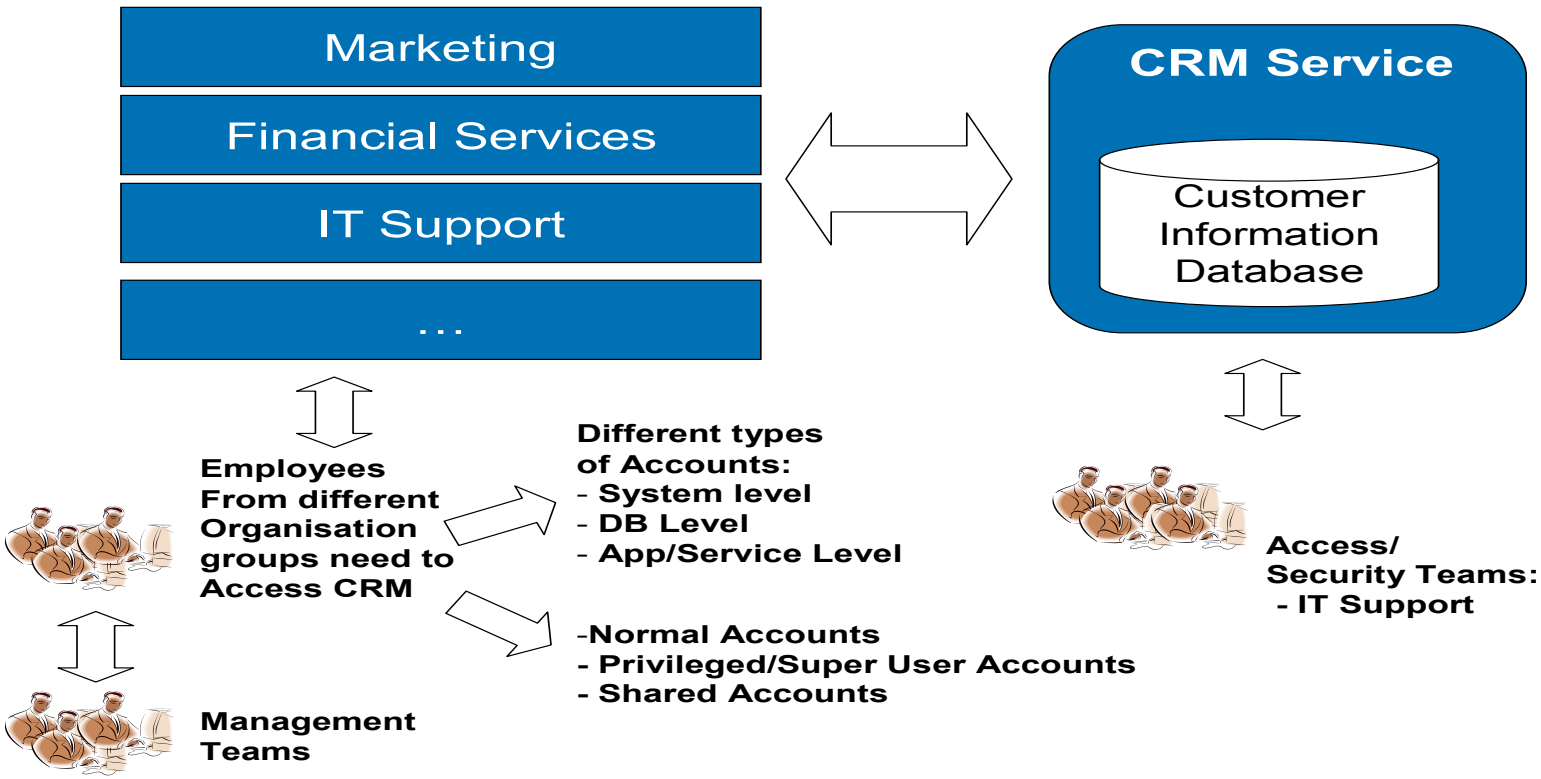
– What is the Risk Exposure for the organisation due to their current access management policies and their implementation at the operational Level?

– What would be the consequences of changing these policies?

– Specifically, what is the impact of investing in IAM Automation?

 © Copyright 2010 Hewlett-Packard Development Company, L.P.

COMPANY (IT) ORGANISATION



 © Copyright 2010 Hewlett-Packard Development Company, L.P.

AGREED APPROACH

- Focus on:
  - Specific Critical Application:
  - CRM Service and Customer Information Database
  - Provisioning and Deprovisioning Processes

© Copyright 2010 Hewlett-Packard Development Company, L.P.

RELEVANT SECURITY POLICIES

– ***P1:*** *All users' accounts and access rights must be approved both by managers and security teams;*

– ***P2:*** *User accounts should be configured according to best security practices;*

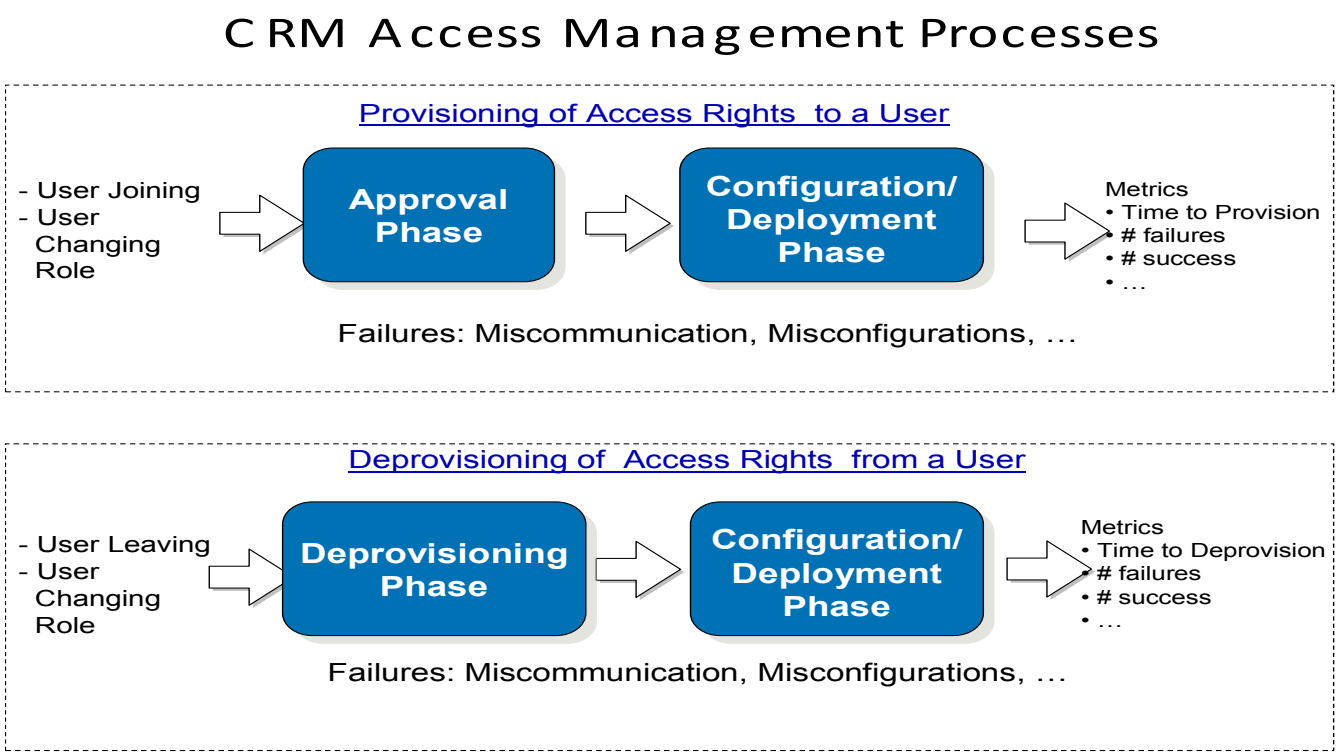
– ***P3:*** *Managers should immediately notify the security team when their employees leave or change their role;*

– ***P4:*** *Unnecessary user accounts and access rights should be removed as soon as possible.*

 © Copyright 2010 Hewlett-Packard Development Company, L.P.

ACCESS MANAGEMENT PROCESSES

- Users can Join & Leave the Organisation; Change their Roles
- Different types of Accounts: Normal Users, Super Users, Shared Accounts



© Copyright 2010 Hewlett-Packard Development Company, L.P.

IAM CASE STUDY

Model and Analysis of CRM Provisioning Process

© Copyright 2010 Hewlett-Packard Development Company, L.P.

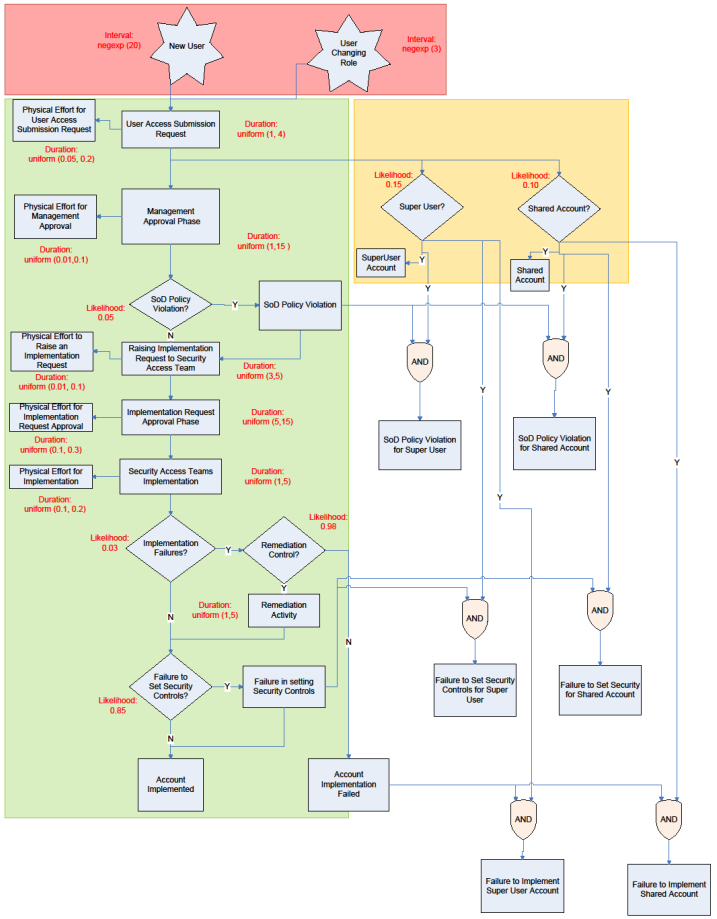
SECURITY ANALYTICS MODELS

- Analysis and Modelling of Current CRM Provisioning Process
- Analysis and Modelling of CRM Provisioning Process with IAM Automation

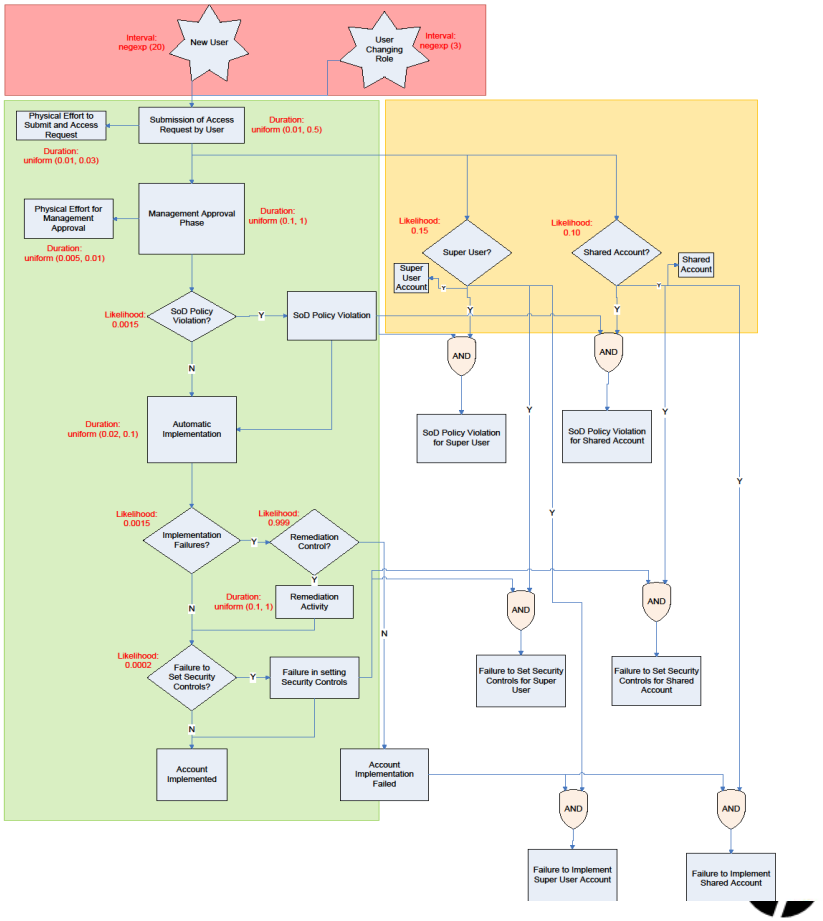
- → Comparing and Contrasting Results Obtained from Simulations

© Copyright 2010 Hewlett-Packard Development Company, L.P.

Model of Current CRM Provisioning Process

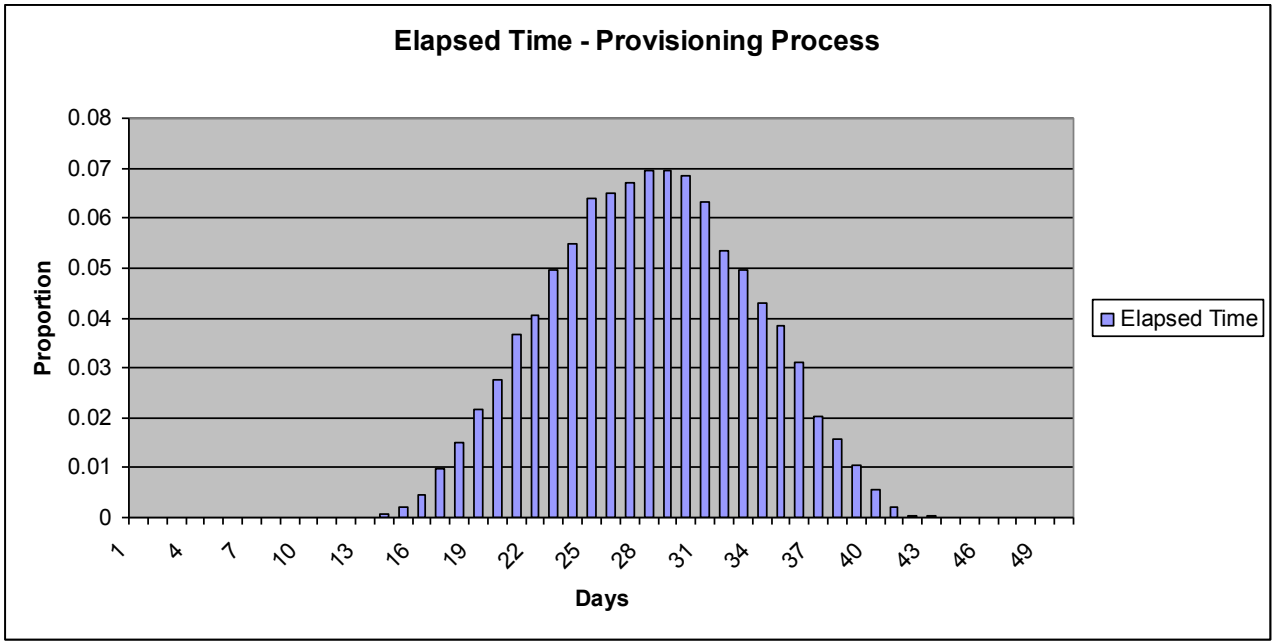


Model of CRM Provisioning Process with IAM Automation



 © Copyright 2016 Hewlett-Packard Development Company, L.P.

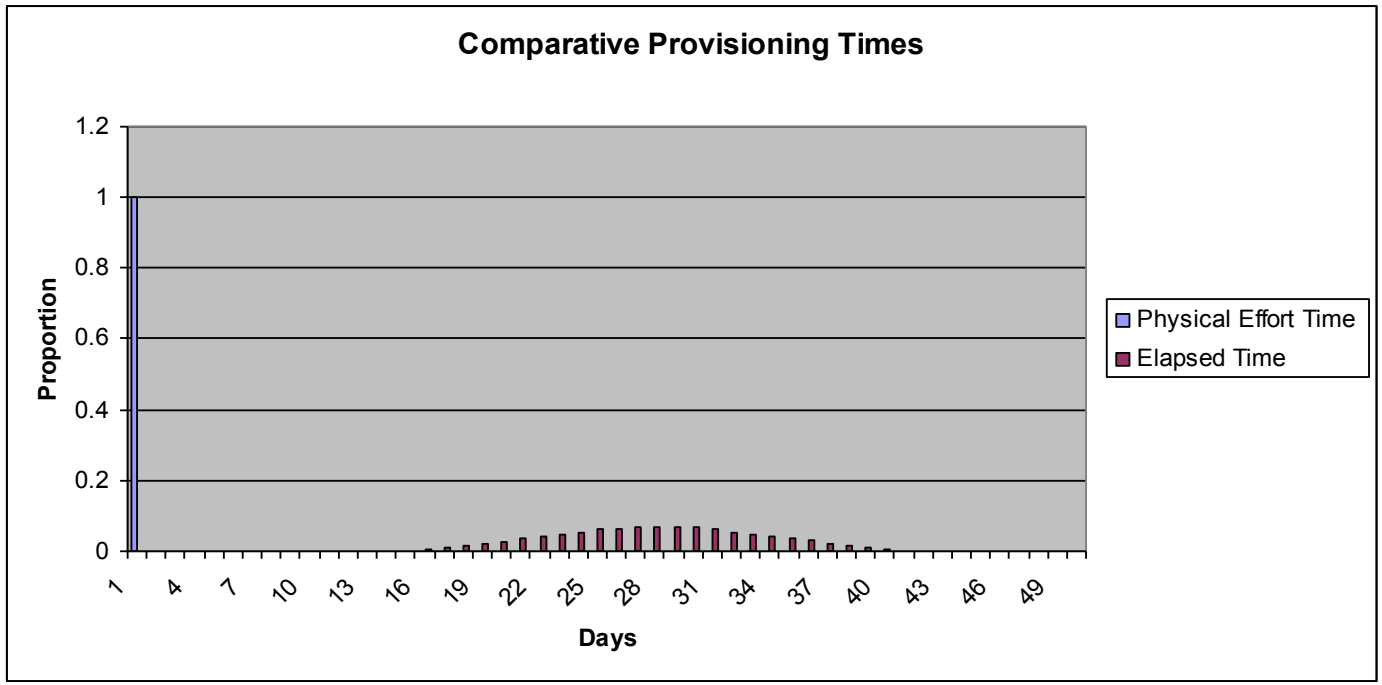
RESULTS FOR CURRENT CRM PROVISIONING



Average Number of Provisioning Requests (per Year): ***133*** *of which* ***19*** *Super User Accounts and* ***14*** *Shared Accounts*
NOTE: Only 15% lock-out controls are set

© Copyright 2010 Hewlett-Packard Development Company, L.P.

RESULTS FOR CURRENT CRM PROVISIONING



 © Copyright 2010 Hewlett-Packard Development Company, L.P.

ANALYSIS OF RESULTS

– The results gave an indication of the potential risk exposure of the organization and policy failures.

– Long provisioning times can induce people in misbehaving, such as bypassing the process or inducing managers to hold into credentials, as previously explained.

– Failures in implementing security controls (i.e. lock-out control) are in violation of Policy ***P2*** (User accounts should be configured according to best security practices).

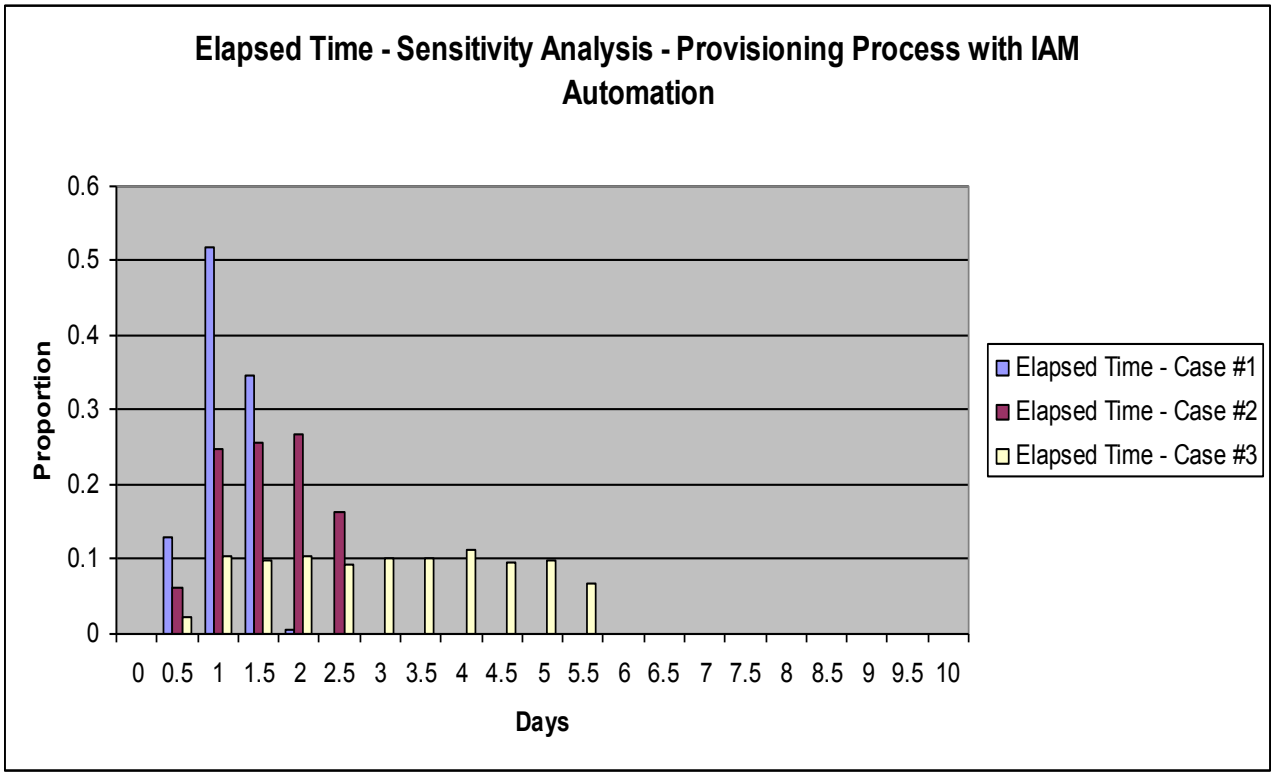
 © Copyright 2010 Hewlett-Packard Development Company, L.P.

RESULTS FOR CRM PROVISIONING WITH IAM AUTOMATION

Assumptions
- Usage of Role-based Access Control
- Preapproved Roles
- Passive Approval for normal situations (majority of cases …)
- Automated Config.

Sensitivity Analysis for Passive Approval (Duration of this Step)

- Case #1: 1 day
- Case #2: 2 days
- Case #3: 5 days



© Copyright 2010 Hewlett-Packard Development Company, L.P.

IAM CASE STUDY

Model and Analysis of CRM Deprovisioning Process

© Copyright 2010 Hewlett-Packard Development Company, L.P.

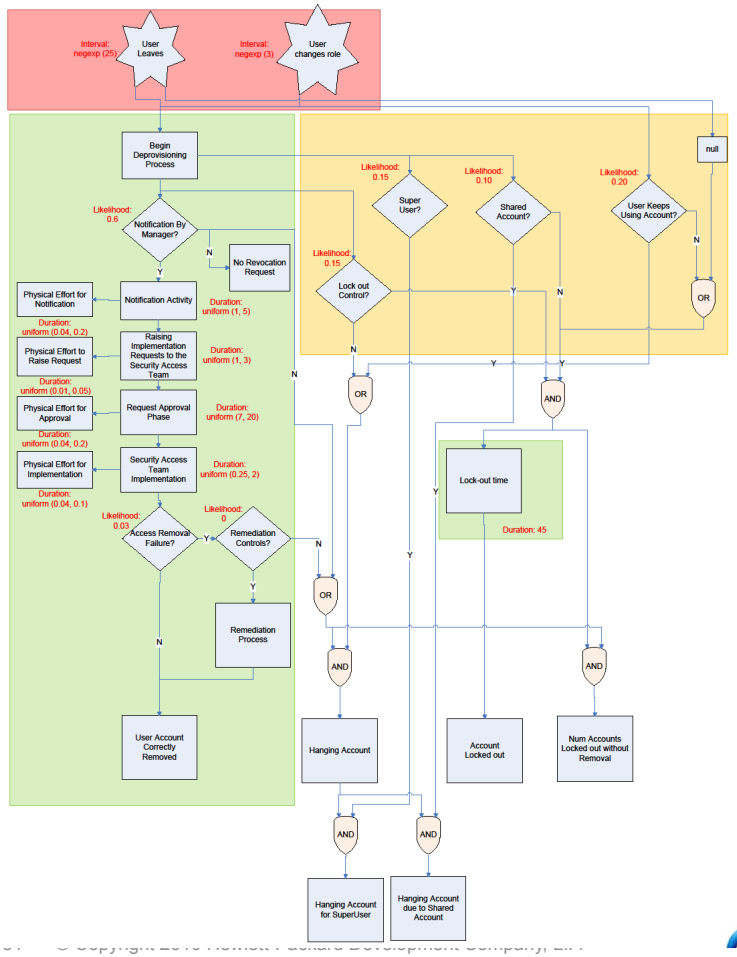
SECURITY ANALYTICS MODELS

- Analysis and Modelling of current CRM Deprovisioning Process
- Analysis and Modelling of CRM Deprovisioning Process with IAM Automation

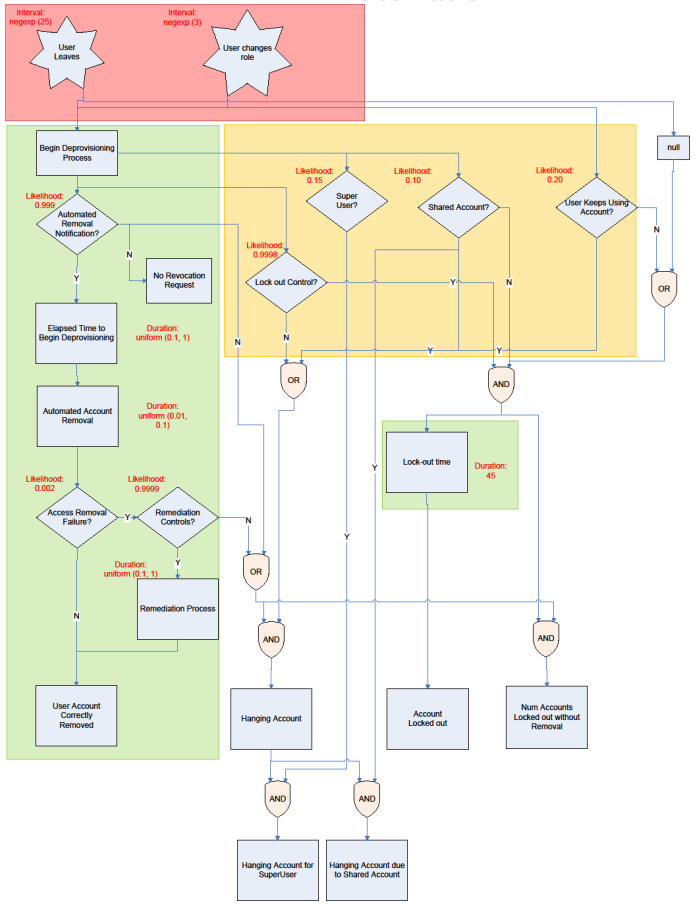
- → Comparing and contrasting results obtained from simulations

© Copyright 2010 Hewlett-Packard Development Company, L.P.

Model of Current CRM Deprovisioning Process

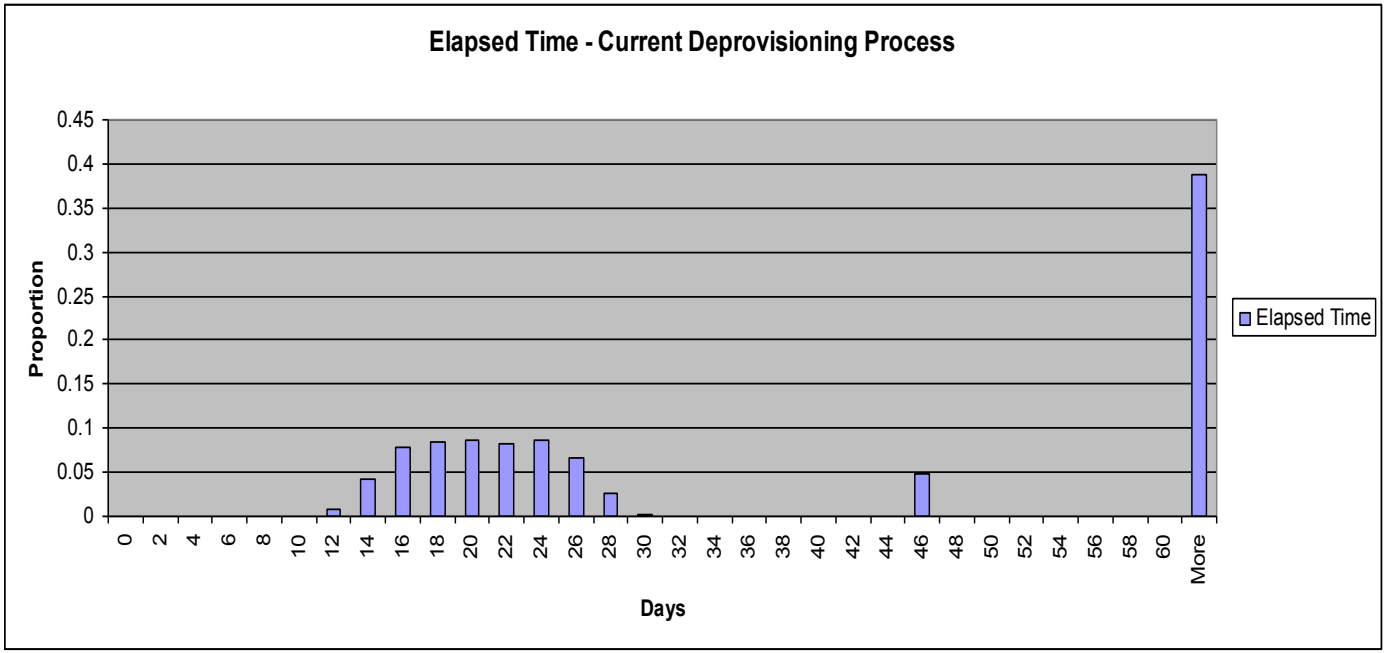


Model of CRM Deprovisioning Process with IAM Automation



© Copyright 2015 Hewlett-Packard Development Company, L.P.

RESULTS FOR CURRENT CRM DEPROVISIONING



Average Number of Deprovisioning Requests (per Year): ***129****.*
Number of Failures (Hanging Accounts): ***49*** *of which* ***7*** *involving Super Users and* ***5*** *involving Shared Accounts.*
Number of Locked-out Accounts (after 45 days) without Removal: 6
NOTE: 15% lock-out controls are set

© Copyright 2010 Hewlett-Packard Development Company, L.P.

ANALYSIS OF RESULTS

- These results highlight the current failure in implementing policies ***P3*** and ***P4*** and the consequent high level of risk exposure for the organization. It is important to notice that failures in correctly implementing policy ***P2***, at the provisioning level, has also a negative impact at the deprovisioning level.
- A major issue is that these policies are too abstract: they do not set precise goals and constraints. This is reflected in the relaxed implementation of the various processes.
- **ACTION:** What-if Analysis about:
  - Improving Implementation of Policy ***P2***
  - Introducing IAM Automation

© Copyright 2010 Hewlett-Packard Development Company, L.P.

RESULTS FOR CURRENT CRM DEPROVISIONING

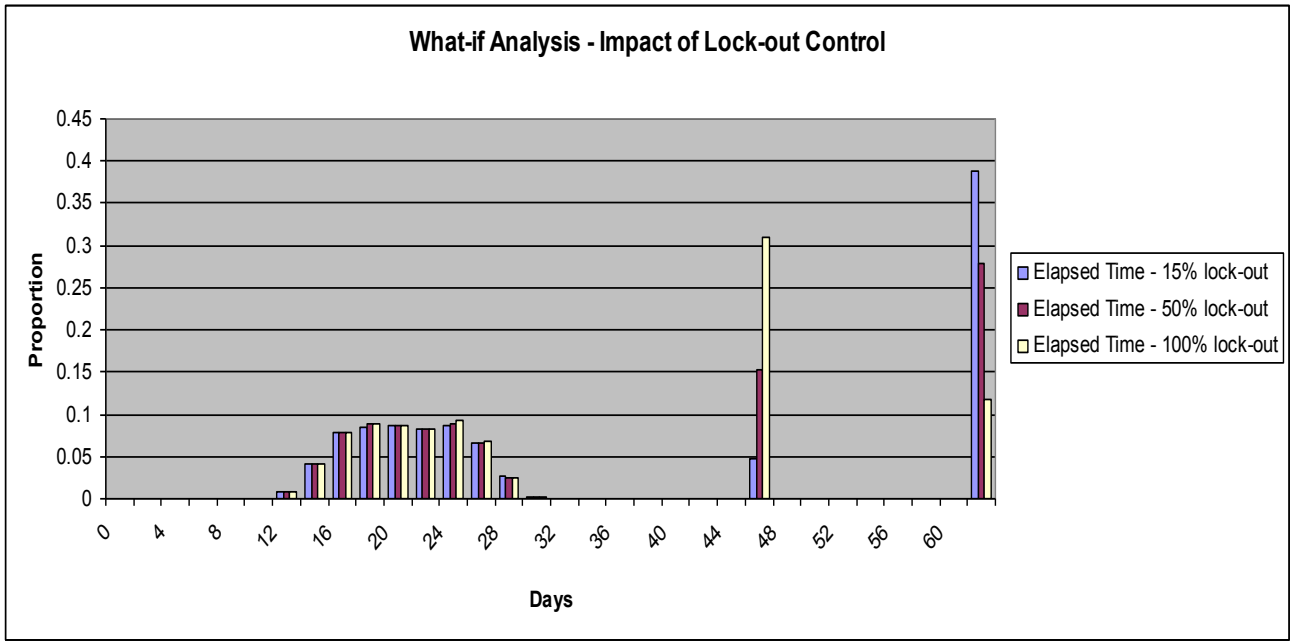
What-if Analysis

Exploring impact of different settings for lock-out controls (set on 30 days):

- 0% Lock-out set (current state)

- 50% Lock-out set

- 100% Lock-out set



*In case of **100% lock-out**, failures can still happen as cannot be handled by the lock-out control (e.g. case of shared accounts or user keeping accessing their accounts)*
*On average (per year), there are **14** hanging accounts, of which **2** Super Users and **5** shared account*

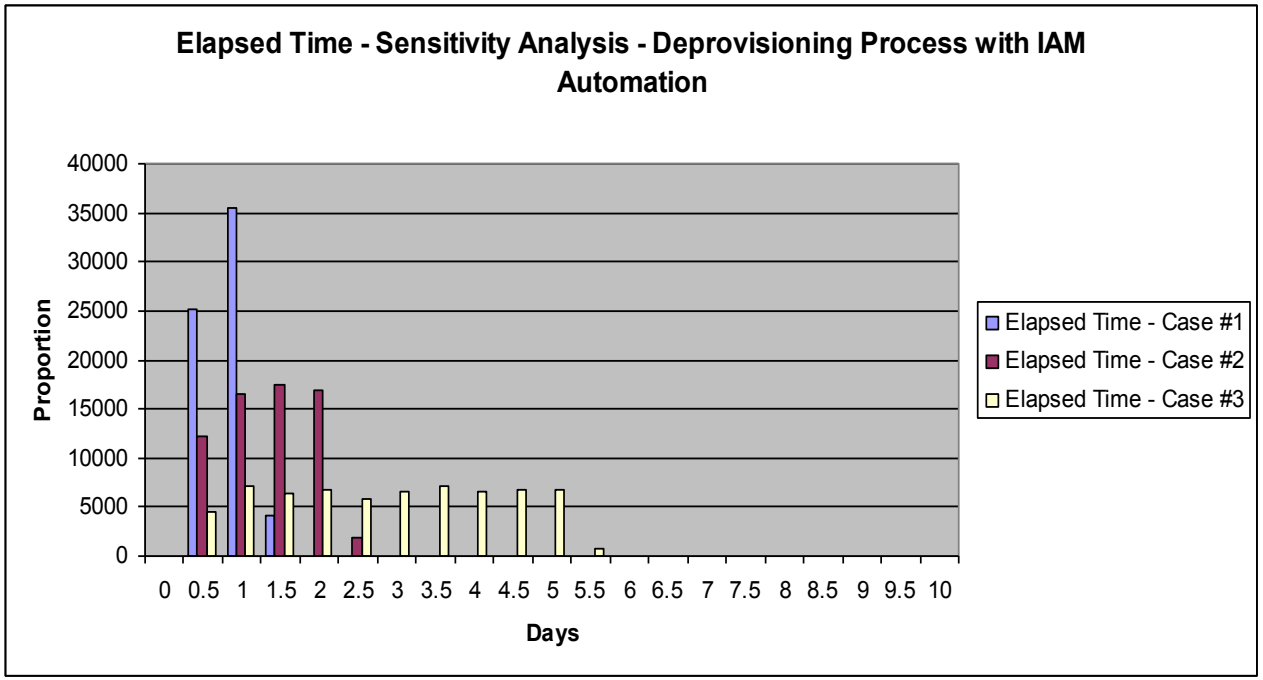
© Copyright 2010 Hewlett-Packard Development Company, L.P.

RESULTS FOR CRM DEPROVISIONING WITH IAM AUTOMATION

Assumptions
- Usage of Automated HR Notification (with some delays)
- Automated Removal of Accounts

Sensitivity Analysis for "Elapsed Time To Begin Deprovisioning"
(Duration of this Step)

- Case #1: 1 day
- Case #2: 2 days
- Case #3: 5 days



 © Copyright 2010 Hewlett-Packard Development Company, L.P.

IAM CASE STUDY - FINAL REMARKS

- Our case study was successfully completed in 3 months and produced a full Security Analytics Report, followed by a presentation of our findings to the customer
- Based on input received from the customer, Security Analytics helped them to ground the analysis of their risks and explore the implications of making investments or modify their policies
- It provided the decision makers with scientific evidence to support their decision making process in order to address current risks and improve their current access management processes
- Additional actions might be taken by the customer to refine their current access policies to mandate more specific constraints and goals

© Copyright 2010 Hewlett-Packard Development Company, L.P.

OUTLINE

- Addressed Problem
- Risk Assessment and Decision Support for Security Policies
- Approach: Security Analytics
- Case Study on Identity and Access Management (IAM)
- Conclusions

© Copyright 2010 Hewlett-Packard Development Company, L.P.

CONCLUSIONS

– We presented our work on Security Analytics to Provide Risk Assessment ad Decision Support to Strategic Decision Makers when Dealing with their Strategic Security Policies

– Probabilistic modeling and simulation tools have been used to explore the risk exposure of an organization at the operational level and the implications of specific security policies. What-if analysis was carried out to explore decision options

– We described how this methodology has been successfully used in a case study, in the space of user access management, jointly carried out with a customer and how this informed potential investments and policy changes

© Copyright 2010 Hewlett-Packard Development Company, L.P.

Q&A

© Copyright 2010 Hewlett-Packard Development Company, L.P.