Insider Access Risk – The New Security Perimeter
Greenlight Technologies Overview

- Greenlight provides business stakeholders with visibility into the financial impact of risks to the organization
  - Detective Control Monitoring
  - Preventative Policy Enforcement
  - Quantification of Access & Transaction Risk

- Strategic partnerships
  - SAP Certified Integration with SAP BusinessObjects
  - ORACLE Platinum Partner
  - CA Technologies

- SAP Premier Partner: Endorsed Business Solution
- Awarded Best Big Data Solution for SAP HANA
- Highest Possible Rating in Gartner Marketscope Report

Rapidly Expanding Customer Base
Enterprise Business Controls Platform

Policy Enforcement
Real-Time, In-Line Preventative Controls

Access Risk
Exception Based Monitoring, Insider Risk Management, Business / IT Orchestration, and Access Intelligence

Operational Performance
Business Transaction Monitoring, CFO Key Performance Indicators, Industry Regulations, and Audit Automation

Enterprise Access and Security Management
Integration: Discovery, Aggregation & Correlation
Runtime Controls Analysis

Reporting | Modeling | Rules & Analytics | Workflow | Embedded GRC / IDM

ERP | Business Systems | Legacy Applications | Custom Solutions | Cloud & SaaS | IT Systems, Servers & DB
Insider Access Risk – The New Security Perimeter
Snowden access was at system administration level
  • Got around normal user access role restrictions
  • Had the ability to move files around at will and could claim he was doing so in order to repair a corrupted drive or conduct some other maintenance operation

Snowden’s administrator account gave him the ability to log into the accounts of other users of the agency’s NSAnet computer systems – some of whom had higher security clearance than Snowden
  • Snowden would need to avoid detection by audit log analysis when changes (delete changes after the fact so period based detection wouldn’t catch)

Given the apparent lack of insider threat protection the agency had in place, they may never fully know how he did it
Insider Access Risk – The New Security Perimeter

Insider Risks Are Pervasive & Not Well Managed

Bar Chart 1: Indicators of privileged user access governance issues

- Privileged users believe they are empowered to access all the information they can view. 64%
- Privileged users access sensitive or confidential data because of their curiosity. 61%
- The organization assigns privileged access rights that go beyond the individual’s role or responsibilities. 52%
- Privileged users working from a home office have administrative or root level access rights. 33%
- Privileged users are not properly vetted or have their backgrounds checked prior to receiving their access rights. 31%
- Privileged users who leave the organization continue to have access rights for a period of time after their discharge. 17%

Ponemon Institute – 2013 Cost of a Data Breach Study
Insider Access Risk – The New Security Perimeter

CHART 2: What are the biggest operational issues around managing compliance risks that you face today?

- Monitoring employee compliance with policies: 55%
- Monitoring existing third parties: 47%
- Workforce training: 44%
- Policy/procedure management: 43%
- Audits of third parties: 39%
- Conducting internal compliance audits: 37%
- Management of internal investigations: 28%
- On-boarding new third parties: 24%
- Other: 5%

Deloitte Compliance Trends 2013 Study
Insider Access Risk – The New Security Perimeter

Impact of Misuse of Access – Fraud, Privacy Breach & IP Loss

- Embezzlement, skimming, and related fraud: 49%
- Abuse of system access/privileges: 30%
- Use of unapproved hardware/devices: 7%
- Abuse of private knowledge: 5%
- Violation of web/Internet use policy: 5%
- Violation of e-mail/IM use policy: 4%
- Handling of data on unapproved devices: 2%
- Unauthorized use of approved content: 2%
- Use of unapproved software/services: 1%
- Violation of asset/data disposal policy: 1%
- Unknown: 1%

Verizon Data Breach Investigation Report 2011
Can You Answer These Access Risk Questions?

- Do you know who has access to what information resources (applications, systems, data, cloud services) across your enterprise?

- Do you know if the access is needed based on a user’s functional role?

How confident are you that your organization has enterprise-wide visibility for user access & can determine if it is compliant with policies?

Source: Ponemon Institute - Access Governance Trends
Can You Answer These Access Risk Questions?

- Do you know if a user’s access is compliant or creates some type of risk for the business (analysis)?
- Do you know what a user specifically did with their access at any given time (fine-grained monitoring)?

“A lack of internal controls, such as segregation of duties, was cited as the biggest deficiency”

ACFE - Report to the Nations on Occupational Fraud and Abuse
Assessing The Financial Impact Of Insider Access Risk
Cost avoidance

- Detect misuse of access privileges that can result in inappropriate or fraudulent transactions
- Eliminate loss of sensitive data due to insider risk
  - Average data loss impact of a data breach $3.2M in legal & notification costs as well as $3M in lost customer business (Ponemon Institute 2013 research study)
- Eliminate loss of corporate IP due to insider risk
  - Corporate IP theft is costly to the global economy: U.S. businesses alone lose upwards of $250 billion every year, according to the U.S. Trade Representative
- Eliminate regulatory fines & penalties due to access control failures
Financial Impact – Data Breach

Figure 4. Per capita cost by industry classification
Consolidated view (n=277). Measured in US$.  

Healthcare: 233  
Financial: 215  
Pharmaceuticals: 207  
Transportation: 169  
Communications: 150  
Services: 134  
Technology: 129  
Research: 129  
Energy: 125  
Hospitality: 114  
Consumer: 113  
Education: 111  
Media: 103  
Industrial: 103  
Public services: 81  
Retail: 78

Ponemon Institute – 2013 Cost of a Data Breach Study
Financial Impact - Corporate IP Loss

- Former engineer for both Intel & AMD plead guilty to five counts of fraud for the theft of sensitive Intel documents and intellectual property including information on chip design and manufacturing data.
- The value of the information was estimated at $1 billion.
  - Non-recurring engineering investment lost
  - Market competitive advantage lost
Former Goldman Sachs programmer, was found guilty on Friday by a federal jury of stealing proprietary source code from the bank’s high-frequency trading platform.

He was convicted on two counts — theft of trade secrets and transportation of stolen property.

- Software development investment lost
- Market competitive advantage lost
Societe Generale was thrown into turmoil in 2008 when a rogue trader with excessive privileges breached five levels of controls to execute a series of fictitious transactions which resulted in $7 billion loss for this French bank.
Privileged-Users

- Change to ERP system configurations & master data values a leading indicator in fraudulent transactions
- Financial impact is $120,000 per incident with more than 1/5th of cases being greater than $1 million in loss according

Association of Certified Fraud Examiners 2012 Report To The Nations
Internal Audit Helping The Business Evolve Their Insider Risk Control Monitoring
Enterprise Access Controls Challenges

- Application, data & system controls not working
  - Coarse-grained view of access (application & enterprise role level)
  - Controls correlation is a must
    - Correlate across complex transactions/business processes
    - Correlate across multiple applications that support these transactions
    - Correlate across users & their activities
  - Copy assess issues & group inherence issues
  - False-positive risks
  - SIEM & application auditing
- Business overriding controls
  - SOD
  - High-risk & temporary users
- Manual & period-based controls
Implement A Complete Control Spectrum

- Period-Based
  - Detective

- Continuous
  - Alerts

- Real-Time
  - Preventive

Operational Impact

Likelihood Of Occurrence
Insider Access Risk Continuous Detection

- Visibility to user access & risk across all applications (on premise or cloud) & fine-grained compliant user provisioning
- Continuous control monitoring of actual Segregation of Duties violations
- Manage & audit process for temporary, privileged-user & sensitive access
- Closed-loop validation of access change requests (provision & de-provision)
- Centralized policies (one authoritative rule set)
- Integrated approach across GRC, eGRC & IDM

© Greenlight Technologies. All rights reserved.
Access Risk Analysis & Real-Time Prevention

- Analysis for the financial impact of access risk
- Real-time transaction monitoring of business processes for fraud & error
- In-line preventative policy enforcement across enterprise applications
- Attribute based monitoring (conditions, variables & events)
Joiners – New User On-Boarding
- New user on-boarding triggered through HR event based on job function
- Preventive SoD policy validation against the user’s access prior to provisioning
- Automated provisioning of day one birth right access
- Entitlement level provisioning into business applications extends beyond the typical network or platform level username and password available to user’s on their first day

Movers – Access Request & Risk Analysis
- Consistent cross system access request capabilities
- Approve new access & access changes to multiple enterprise applications
- Preventive SOD policy validation against the user’s access prior to provisioning
- Automated, fine-grained provisioning across all applications

Leavers – Access Termination
- User access termination triggered through HR event
- Satisfy audit requirements to remove user accounts & application roles
- Network and platform level accounts disabled
- Business application and ERP access rights & entitlements revoked
- Manage orphaned accounts & entitlement drag for least privileges
The business should own this issue but...

Determine insider access risk monitoring
  • Period-based detection (UAR for 404)
  • Continuous monitoring (policy violations & transactions)
  • Real-time prevention (high risk activities & transactions)

Don’t get caught in the enterprise or application user role trap
  • Run rules/controls on users to their exact access permissions

Highly privileged users
  • Eliminate shared passwords for root/system administration level access
  • Require rule monitoring & auditing of all highly privileged user actions