The IT Risk Environment and Data Analytics

Parm Lalli, Director, Sunera LLC

Michael Kano, Senior Manager, Sunera LLC

Professional Strategies – S23

About Your Speakers

Parm Lalli, CISA, ACDA

Parm is a Director with Sunera and leads the national data analytics practice. Parm has over 15 years of data analytics, audit, and controls experience with Sunera and other IT consulting firms. This experience includes leading multiple data analytics and CCM initiatives; installing, implementing, and configuring ACL Audit Exchange; and being involved in work on IT general controls, application controls, internal audit, IT risk assessment, process improvement advisory, operational audit, Sarbanes-Oxley Act (SOX), and National Instrument 52-109. Parm has also been involved in conducting vulnerability assessments and penetration testing for clients. Parm has a great deal of experience with CAAT's tools, performing data analytics, and developing Continuous Controls Monitoring applications for many different business processes. He has over 15 years experience with ACL Software. Parm is a Certified Information Systems Auditor (CISA) and ACL Certified Data Analyst (ACDA).

Michael Kano, ACDA

Michael is a Senior Manager with Sunera's national data analytics practice. Michael has 20 years of experience in data analytics and internal audit with organizations in the USA, Canada, and Kuwait. He has 20 years of experience with ACL software, including 8 years as the leader of ACL Services Ltd.'s global training team. He is an ACL Certified Data Analyst (ACDA). Prior to joining Sunera, Michael spent four years with eBay, Inc.'s internal audit team as Manager, Audit Analysis. He was tasked with integrating data analytics into the audit workflow on strategic and tactical levels. This included developing quality and documentation standards, training users, and providing analytics support on numerous audits in the IT, PayPal, and eBay marketplaces business areas. Michael also has 7 years of experience with Arbutus Software, and has managed the transition to Arbutus from other data analysis tools. He is a proficient user of Tableau, Microsoft Access, and Teradata SQL Assistant.

OBJECTIVES

- Raise awareness of the contribution data analytics can make to mitigate risks in IT
- Identify key risk areas that can be tested with data analytics tools
- Describe data analytics tests for key high-risk areas
- Demonstrate continuous control monitoring

AGENDA

- Why data analytics for IT?
- Risks to mitigate
- Specific risk areas
- DA tools
- Proactive security monitoring

WHY DATA ANALYTICS FOR INFORMATION TECHNOLOGY?

2014 Data Breach Statistics

- $3.8 million per organization*
- $154 per record*
- Increases in
  - Cyberattack frequency
  - Remediation costs
  - Business impact
  - Detection/escalation costs

**IBM/Ponemon 2015 Cost of Data Breach Study*

The Environment

- High-risk area
- Abundance of data
- Multiple platforms/formats
- Complex
- Decentralized
- Proliferation of unencrypted devices

DA enables…

- High-frequency automated testing
- Development of metrics
  - Operational performance
  - Call centers
  - Cybersecurity
- Close to real-time monitoring/reporting of risks
- Comprehensive overview

Output

- Dashboarding of trends/metrics
- Drill-down capabilities for supporting data
- User-friendly formats

RISKS


ISACA
Trust in, and value from, information systems
San Francisco Chapter
CyberSizeIT
SF ISACA FALL CONFERENCE
NOVEMBER 9-11, 2015
HOTEL NIKKO-SAN FRANCISCO

Risks

- Unauthorized activity
- Loss of revenue
- Data corruption
- Data leakage (accidental)
- Data theft (intentional – internal or external)
- System downtime
- Loss of confidentiality
- Erosion of process integrity
- Decreased performance
- Malfunctioning hardware

RISK AREAS


ISACA
Trust in, and value from, information systems
San Francisco Chapter
CyberSizeIT
SF ISACA FALL CONFERENCE
NOVEMBER 9-11, 2015
HOTEL NIKKO-SAN FRANCISCO

Key Risk Areas

- Access
- Change logs
- Segregation of duties
- Change management
- Physical access
- General Computer Controls/ITGC
- Application controls
- Improper user of company assets (Policies)

Access

- Elevated access review
- Usage of Admin/Super user accounts
- Compare access to position description
- Compare to previous review results
- Flip flop access privileges
- Segregation of duties
- Access to contractors
- HR payroll records vs Active Directory user listing

Change Logs

- Review major changes
- Identify change/reversion ("flip-flop")
- Frequency distribution by individual or department
- Audit logs for application and database changes

Change Management

- Compare to ITAF standards
- Proper categorization
- UAT results
- Test all environments to ensure proper change management (Dev, Test, Prod)
- Use DA tools for Code Review
- SOX controls for Vendor Master / Customer Master changes

Physical Access

- Review entries/exits to data centers (who)
- Review entry times vs exit times (duration)
- Cross-reference with HR data for departing employees
- Compare against logs for suspect events
- Review temporary access passes for approvals
- Review failed attempted access logs

General Computer Controls/ITGC

- Configuration vs Policies
  - Default accounts
  - Passwords
  - Inactivity
  - Failed logins
  - Time out settings
- Security
  - Firewall configuration settings/changes

Application Controls

- Password settings
- Account settings
- Time out settings
- User access reports (compare time periods)

Compare all of the above with policies and procedures

Applications

- Active Directory
- UNIX
- Mainframe
- Oracle
- Other Databases
- HRMS

PROACTIVE SECURITY MONITORING

DA Tools for IT

- Standard data analytic tools
  - ACL, Arbutus, IDEA
- PowerShell
  - Scripts to access Active Directory
  - Run through EXECUTE & RUN commands
  - Creates CSV (or other formats) files to import into above tools
- Forensic Software for data examination (emails)
- Cyber Security tools

Proactive Security Monitoring 1

- **Login Velocity** – logging into multiple assets from a single source
- **Previously Unseen Origin** – Remote logging in from a location not previously seen
- **Previously Unseen Process** – Identify a previously unseen process running on critical machines
- **Impossible Traveler** – logging in from different locations that can not be achieved through normal travel means
- **Cross User Login** – same user account being logged on to multiple assets at the same time

Proactive Security Monitoring 2

- **Non-Badged User Login** – identifying when an on-site login does not have a corresponding badge entry into the building
- **Proxy Beaconing** – looking for machines reaching out to uncommon domains and IP's
- **Timewheel** – identifying machines performing beaconing during hours of the day when the user or system isn't typically active.
- **Snowflake** – analysis to find process/software that has not been seen in the environment before, across the fleet
- **Concerning Connections** – assess network data to automatically generate network maps from which undesired, or unexpected, connections can be identified.

The End

- Questions / Comments?

Contact Information

For additional information on Sunera's services, visit our website at **www.sunera.com** or contact:

Parm Lalli
Director
(949) 204-4550
plalli@sunera.com

Michael Kano
Senior Manager
(604) 602-7119
mkano@sunera.com