How Well Is Monitoring Working?

or

Death by E-mail

New York and Tampa Bay RACF User Group

20 November 2015

David Hayes

New Tools = Better Monitoring?

- Our ability to record system events and activity has never been greater
- The ability to correlate monitoring information across our enterprises is now quite significant
- Options and capabilities for communicating all those recorded system events and activities have expanded tremendously

Is our monitoring more effective?

Are Monitoring Capabilities Leveraged to Achieve Control Objectives?

- Do we have new software and hardware capabilities searching for a purpose – OR – have these new capabilities been strategically aligned with more effectively achieving our organizations' control objectives?
- Have our organizations IDENTIFIED their control objectives?
- Have the control objectives that ARE identified COMMUNICATED to the necessary stakeholders?
- New monitoring capabilities have not altered the age old questions: Do those who are tasked with the monitoring 1) know what to do in the event of an actionable situation? or 2) have the authority to act?

Observations from the Trenches

- The marketing is working – many new monitoring tools are either implemented or being planned – logging tools, SIEM – event correlation, alerting capabilities and reporting tools
- Organizations are DROWNING in logs – the sheer volume of collected monitoring data is a growing and serious problem
- It is not possible to talk to operations and staff and management anymore without them being interrupted by "alerts" on their communication devices
- The beginning of shift operational status meetings have become essential – so staff know what alerts are expected on their shift

Is Monitoring More Effective?

Mixed results:

Positive:

- Much quicker identification of system events and activity
- Problem identification and resolution more timely
- Some progress on identification of cross-platform situations that represent risk to business processes

Negative:

- Distraction of operational staff and management with new gadgets and processes that are not (yet) improving their operations/performance
- Re-direction of resources – staff and money – from existing controls