The untapped intelligence in Australian universities

Denise Carson looks at how operational intelligence can reduce cost, increase efficiency and provide critical insights for the higher education sector

In their recent report, An agenda for Australian higher education 2013-2016 (1), Universities Australia highlights the emergence of the digital economy and new technology as the first of the four trends that are driving change in Australian higher education.

The authors go on to list increasing globalisation and the possibilities of the Asian century; economic and industrial restructuring as the nation responds to the resources boom; and the need to improve productivity with universities central to the national innovation effort.

The report also highlights that while Australia’s universities are internationally recognised for their high-quality teaching and research, and demonstrated success in attracting international students, this is not necessarily reflected in current public investment which is around two-thirds of the OECD average.

Meeting the challenge in 2014 and beyond

Gartner’s Taming the Digital Dragon: The 2014 CIO Agenda (2) states that the top technology priorities for 2014 reveal two complementary goals: renovating the core of IT and exploiting new technologies and trends.

Universities, arguably more than any other enterprise, need to ensure that their IT infrastructure is both robust and secure as well as primed to exploit emerging digital technologies, trends and preferences.

The more anticipatory they can be in regard to technology, the more creatively they can use it to gain operational and competitive advantage and deal with the challenge of escalating costs.

The power of machine data

In its 2014 CIO Agenda, Gartner highlights the “need to create the information architecture and capabilities to exploit big data” as one of the keys to renovating the core of IT.

Today, machine data represents a largely untapped source of information that can have a dramatic impact on cost reduction and operational efficiency. As shown below, there are many sources of machine data across a university and each of them provides insight into issues, usage patterns and trends.

- wired & wireless networks
- digital channels
- mobile and desktop devices
- student registration systems
- structured databases
- web and application servers
- mobile, online & legacy apps
- learning management systems
- facilities management systems
- lecture theatres and laboratories

As with most large enterprises, universities have a diverse and distributed IT environment with technology often developed in silos to address a particular requirement. This means that IT teams are often viewing machine data using tools designed to provide a view of a particular infrastructure element or process.

Operational intelligence breaks down these IT siloes and provides visibility across the whole infrastructure. This allows analysts to instantly access, tune and improve business and IT processes, identify security threats, highlight performance issues and spot emerging trends.

To build a smarter future, Australian universities need to be both highly innovative in their use of new technology and very savvy about getting the most out of their existing technology investments.


The untapped intelligence in Australian universities

Let’s take a quick look at a few areas where these sort of critical insights are already allowing decision-makers and administrators to make better decisions not just around technology but the university as a whole.

**Service improvement**

Using consolidated and centralised machine and systems data makes it far easier to track end-to-end transactions across all university systems.

For example, a major cost for a university IT department is often the service desk. An operational Intelligence approach means that service desk agents can resolve a problem without needing high level skills or extensive expertise, or needing to escalate the problem to the next level of support personnel.

A typical university student has 3 or more mobile devices. When they change a password on one, they frequently neglect to do so on the others which can mean they are locked out of student administration or learning management systems.

One Australian University’s service desk now conducts its own log search via Splunk to troubleshoot user account lockouts instead of having to escalate the issue.

This means significant time and resource savings for support staff and far quicker and more effective service to the user. The average resolution time has been reduced from 20 minutes or more to a simple two minute call.

**Security & compliance**

In a university, information security threats can happen quickly anywhere within the IT infrastructure. By gathering the relevant machine data and indexing it in a centralised repository, IT security teams gain a holistic view of a threat scenario.

This enables threat mitigation in minutes rather than the hours needed to extract and analyse many disparate log sets. In addition, real-time monitoring of incidents and attacks combined with ad-hoc reporting helps teams to be highly proactive rather than reacting long after the event.

On 18 February 2014 a massive cyber-attack struck the networks of the University of Maryland putting personal student, faculty and staff information at risk. The accessed database contained information relating to over 300,000 records including names, birth dates, university ID and Social Security numbers.

Dealing with phishing attacks was becoming increasingly resource and time intensive for one Australian university’s IT team. Compromised user accounts in particular were becoming a growing problem. Being able to more quickly recognise and respond to attacks became an overriding imperative.

A successful project has resulted in Splunk applications being used to trigger alerts on certain types of events. By reducing response time, IT security is now able to contain these events far more effectively. A single Splunk search dashboard displays any number of current security events including phishing attacks, high volume email traffic, account-related events such as password attacks and anomalous log-on events. The business outcome is ensured uptime and service continuity through catching unknown threats and new zero-day attacks.

Universities must meet multiple regulatory requirements such as Payment Card Industry Data Security Standard (PCI DSS) and PCI and HIPAA. Operational Intelligence mitigates risk to the university through cost-effective security and compliance based on accurate and complete data auditing and regulation visibility. Incident investigation is reduced from hours to minutes directly impacting the bottom line and dramatically reducing the risk of regulatory non-compliance.

**Preventing network abuse**

On the typical campus, the potential for users to abuse network resources is very high. A classic example is the use of the network for downloading non-learning related content, which results in a massive strain on network resources and consumes large and unpredictable blocks of time for IT staff.

Other examples include the illicit use of printers, which has major cost implications and the use of laboratories and equipment for unapproved or illegal purposes. By analysing data that has been correlated from a broad set of sources, patterns of abusive activity can be detected as they are actually happening.

The University of Texas at Austin is a top-ranked state research university and the flagship of the University of Texas System, which includes nine academic universities and six health science centers. Operational Intelligence technology has helped automate the identification and response to malware threats, helping to control outbreaks and reduce or eliminate escalations.

“Searches that used to take ten minutes can now be done in seconds with Splunk. When an analyst has to do that several times per day, the savings add up. More importantly, Splunk software helps us identify and create signatures for new threats and deploy those signatures much faster.”
Capacity Planning

Operational Intelligence can be used in university environments to help pinpoint devices that need replacement by identifying devices of a given type, as well as by location and department.

One University reused sets of log data that were originally collected for security purposes to better manage asset replacement in this way.

Regular reporting has also helped to improve operational visibility across the university’s entire infrastructure through analysing dynamics around teaching space usage and device utilisation.

Understanding a particular department’s computer pool usage by analysing logs from specific workstations enabled the IT and procurement teams to tailor a hardware upgrade to meet future requirements and saved considerable costs in the process.

BI vs OI

Put very simply, business intelligence or BI provides historical data which can be used to make future decisions. With OI or operational intelligence the data is continuous, directly linked to events as they occur so that decisions can be made proactively. It is helpful to think of them as complementary as in some ways OI was developed to answer questions that BI was not designed to ask.

A subset of OI is Digital Intelligence which is particularly useful to Universities as it enables real time visibility, analysis and insight across digital channels. This is particularly relevant for web sites as they are a critical element of successful student acquisition and enrolment campaigns.

Roadmap to Mature Operational Intelligence

Where to start?

The journey of transforming machine and systems data into Operational Intelligence typically starts in the IT department with root cause analysis use cases. It then travels all the way to university leaders and campus administrators using it for real time business insights to support international competitiveness, research and innovation.

Phase 1 typically involves capturing, storing and searching the data to reactively find the root cause of important events.

Phase 2 takes place when proactive machine data monitoring and analysis occurs to detect exceptions before they have an impact on the campus, its faculty, students and staff, systems and service operations. This phase often sees the data being used to provide other types of business intelligence and insight related to emerging trends.

Phase 3 sees the machine data being used to measure KPIs and service levels as well as providing more holistic, overall visibility into student and faculty behavior and overall university performance.

Phase 4 reaches a stage of maturity where business, machine and systems data are correlated and combined to detect trends and patterns and to predict outcomes. This level of Operational Intelligence provides views that support real time decision-making across enrolment, administration, research, and learning.
UXC Connect and Splunk
UXC Connect has partnered with Splunk since early 2013 to offer Operational Intelligence to customers across a number of vertical industry sectors including Government, Education and Mining, Oil & Gas. Our partnership makes machine data accessible, usable and valuable to our customers. Our solutions offer our clients the freedom and flexibility to ask questions and receive answers in real time, helping them to unlock the largely untapped value in the massive streams of data generated across their organisation.

About the author
Denise Carson is Practice Manager, Enterprise Mobility & Operational Intelligence at UXC Connect. An industry authority on the strategic business use of disruptive technology, she runs regular CXO roundtables across Australia. Having written many papers on this topic and published in key industry reports, such as Deloitte Access Economics’ Mobile Nation – the Economic & Social Impacts of Mobility, Denise is passionate about helping Australian business and government get the very best out of emerging technology.