Building and protecting the IT architecture of the future

Rapid advances in technology have brought about new challenges in the fields of cybersecurity, compliance and regulation. **Peter Morrison**, Strategy and Architecture, BP (Singapore), explains why large businesses should consider hiring an IT architect, and identifies the challenges in using technology to monitor misconduct, prevent market manipulation and mitigate a range of risks

Energy Risk: Is it useful for large trading organisations to have an IT architect? What value can it add to have an experienced person in such a role?

Peter Morrison: It's absolutely useful to have an IT architect. A large trading organisation will use a mix of vendor-supplied and in-house software, and is sure to run an in-house or managed service technical team of some size. The role of the architect in such organisations is to direct the construction or configuration of software in such a way that the organisation as a whole can operate well into the future after the initial project is concluded. Counterintuitively, this means the architect may impose decisions that slow down projects. The value of such decisions cannot always be gauged from the scope of the individual project. It may be that the program or portfolio benefits from a more reusable component or the organisation benefits from having software that is simpler to maintain and doesn't require continual IT involvement to make configuration changes. It is the job of the architect to identify and defend these decisions, which is why this experience is so important.

Peter Morrison

Energy Risk: When different systems are used in the same organisation, how can management be certain it is accurately monitoring its key risks?

Peter Morrison: Organisations tend to follow Conway's law, which states, approximately, that the structure of systems reflects the structure of organisational communications. To use an example, in a trading organisation the market risk system is almost always distinct from the credit risk system because these two control functions usually have distinct organisational silos, joined together at the level of the chief risk officer (CRO).

This is not necessarily a bad thing; the profession of risk management is about identifying, partitioning, monitoring and mitigating risk categories. To be sure that management is accurately monitoring key risks, we must look at the organisation reporting to the CRO and create roles with cross-cutting concerns. Briefly, let's look at operational risk, obsolescence risk, vendor risk, integration risk and compliance risk.

An operational risk function should identify business processes that either lack adequate controls or aren't backed by software that supports the process. Part of the remit of this group is simplification, but this must be balanced against compliance risk where certain parts of a process must be performed by distinct groups and may not be combined. A software obsolescence group should identify and prioritise systems that are at risk of becoming obsolete and secure funding for upgrades. By definition, obsolescence risk arises long after the initial implementation project has been closed. End of serviceable life is a constant pressure on organisations with a large IT footprint. A vendor assurance group should have the responsibility of monitoring and mitigating risks associated with vendors of systems and infrastructure. Integration risk covers the interfaces between systems, customisations and infrastructure touchpoints.

A number of these risk categories sit in the IT space, and are often managed by groups distinct from the CRO structure. The chief information officer (CIO) therefore has authority delegated from the board to manage those risks. One of the risks – not so easily categorised, but commonly faced in IT – is the risk of 'solving the same problem' more than once, with the consequent overspend on projects and ongoing operational expense incurred. The role of an architecture group will usually include accountability for this risk.

Energy Risk: What is your approach to vendor risk management and the key criteria you apply when evaluating vendors?

Peter Morrison: There are a number of risks to consider when using vendor-supplied systems; the most obvious is the risk that you will choose a vendor and they will somehow go out of business. The challenge in this area is that often the risks are opposed – if you choose a solid vendor to mitigate abandonment risk, then you instead face stagnancy risk where the vendor is so solid it doesn't rapidly change its systems to keep up with a changing environment. Or, if you go with a nimble vendor, you risk the cost of an upgrade schedule that doesn't match your organisation's preference. If you go off-the-shelf, you risk changing your business practices to fit the operation of the system, but if you pay for customisations you risk an increased maintenance fee and more expensive upgrades. Truly, this is a challenging space to be in. When evaluating vendors, the key is to get agreement on the balance you are seeking; accordingly, this means reaching agreement on the many risks that you will choose to accept instead of mitigate. The business environment can change rapidly, so set triggers to activate a risk review. Put simply – know what you are getting into.

Energy Risk: How has your organisation had to adapt its IT systems to deal with the influx of new regulation over the past few years?

Peter Morrison: The pace of regulatory change has certainly picked up over the past few years. Added to this is the particular lens that regulators use to look into trading organisations – a viewpoint that supersedes any internal system structures and often requires information to be captured at the trade execution point and preserved right through to the settlement of a trade (for example, the best execution regulations), regardless of how many systems are involved in the trade life cycle. The trading company within BP is affected by regulation but, as a trading company that exists largely to hedge genuine physical exposure, it is exempted from some of the conditions.

Concentrating on BP as a specific example, much of the regulation covering the trading company is about reporting of activity. Fortunately, this is an area in which there is plenty of expertise and no shortage of data – everyone understands how to produce a report. The challenge is making sure we have collected the right data in a timely fashion. This occasionally means we need to go all the way back to trade capture and add fields right there that will propagate through the various trade systems and eventually be output on to an activity report. Adding fields all the way through a trade life cycle pipeline raises integration risks, of course, which must be managed appropriately.

Energy Risk: The introduction of mandatory trade reporting has been an important new development for energy trading firms in the past few years. What do you see as the best strategies, from an IT perspective, for dealing with all of the new reporting rules?

Peter Morrison: The first thing to realise is that regulators in different jurisdictions have requirements that often converge to become quite similar, but over a long period of time (in IT terms). There is a natural tendency to write a completely bespoke solution for the first regulator that mandates a particular report, then to attempt to clone it with tweaks for the second regulator, and then to wring one's hands and bemoan the cost of doing it all a third time when the next region settles on its requirements. The observation is that it takes approximately three attempts to construct a properly reusable solution in the IT space, and it is approximately three times as difficult to build a reusable solution as it is to build a bespoke one.[1] The best strategy therefore is to simply accept that you're going to do things about three times before producing a genuinely reusable framework.

Energy Risk: Should trading organisations use technology to monitor for potential signs of misconduct or market manipulations by their traders? What do you see as the biggest challenges in the field of trade surveillance technology?

Peter Morrison: Trading organisations should definitely use technology to monitor for potential signs of misconduct or market manipulation. This is not only to identify actual misbehaving staff – which is the sharp end of the stick, so to speak – but also to enable compliance staff to guide traders and other market-facing staff before allegations of misconduct can even be laid. The simplest technology is to record communications and to openly tell the traders and market-facing staff that communications are being recorded. This has two outcomes: first, it provides a reference should there be any dispute; second, it provides a constant reminder that communication is not just between a trader and a counterparty, but with a large potential future audience of auditors, compliance officers, trading managers and lawyers. This tends to ensure that communication is kept sober and professional; it is when people forget this that lapses tend to occur.

There are other technological avenues to monitor behaviour, and the currently booming field of data science offers numerous techniques, such as clustering and anomaly detection, to connect otherwise unrelated data sets. These techniques can and should be applied, even in scenarios that produce occasional false positives, for the 'reminder' effect that the behaviour of an employee operating while representing the company is, effectively, the behaviour of the company itself, and that the company can and will monitor it.

These technologies are not without challenges. The most obvious headache for recording is the use of non-recorded technologies. Calls from desk telephones can be recorded centrally, but almost everyone has a smartphone, and the number of messaging apps available is growing on an almost daily basis. What is the appropriate response to this? Is it technological or managerial? How strict should the constraints be? In the field of data science, the challenge is not about accumulating data, that's the easy part. Rather, the difficulty is how to pose the right questions to be answered by the data provided. There is often an absence of positives to compare with – compliance officers work night and day to ensure that there is a never a 'market manipulation' event, but from the point of view of data scientists, such an event would provide excellent training data for a monitoring system.

Energy Risk: What are your thoughts on the use of open-source software? Do you think it makes sense for firms to migrate from closed-source vendors to platforms built on open-source technology?

Peter Morrison: Open source has revolutionised the world of software. By commoditising ever more complex components, the open-source movement has enabled huge advances in technology, at the cost of enormous disruption to the industry. It is difficult to emphasise enough just how extraordinary the change has been over the past 30 years. Today you can use a free web browser to connect to a cloud provider and spin up a free virtual server using a free operating system, download a set of free technologies and create something to unleash upon the world. Developers everywhere can access vast libraries of technology to solve the specific problem they are having that day and move on. Productivity has exploded (by some measures). Also, typically an entire class of problems to do with licensing just goes away when adopting open source.

Enthusiasm aside, there are still considerations before committing to open source. New products appear, seemingly overnight, and the pace of adoption causes them to rapidly become ubiquitous, but do those products solve the problems your current closed-source (or in-house) system solves? Have those products run up against the corner cases that your organisation has encountered previously? Is the profile of the current adopters similar to that of your organisation? It would be foolish for a large company to hastily abandon, for example, an enterprise messaging bus feeding a critical core transaction pipeline because something new has stormed the market. Critical middleware takes time to evaluate.

The counter-argument to maturity/robustness concerns is that, because a popular open source package can reach such a large audience of both adopters and developers, closed-source commercial software with its more limited client list and access to developers can find itself outpaced, out-innovated and, eventually, just out. Robustness tends to follow popularity.

Energy Risk: What measures do you take to address cybersecurity in your company? Does it make sense to engage independent security reviewers from out-of-house?

Peter Morrison: Cybersecurity is a key concern at BP. There are certain companies, which, by their very nature, attract attention and oil companies are right up there because they are big political and economic targets.

To address this, the digital security function has an organisational structure that has authority delegated right from the CIO level and a remit to examine every aspect of IT at the company. As a consequence, some areas where other industries are already well advanced, such as adoption of cloud technology or the development of mobile applications, have been entered more cautiously and in a strong partnership with digital security specialists.

[1] *Atwood, Jeff (2013),* The Rule of Three, *http://blog.codinghorror.com/rule-of-three*