IT Infrastructure / The Larger Frame: Risk Management: 2017-09-28

One of an intermittent serious of (2) hour round-table discussions on topics relevant to IT Infrastructure at non-profit biomed research institutes.

Attendees:
Allen Institute, Benaroya Research Institute, Center for Infectious Disease Research, Fred Hutch, Omnigroup, UW Genomics

Notes from Stuart Kendrick http://www.skendric.com

Conscious & Shared

- We are striving for Conscious & Shared choices around Risk (typically a mix of Mitigation and Acceptance).
- This requires conversations upwards, downwards, sideways.
- The time & effort & education it takes to have these conversations – Managing Expectations – is hard, harder, for example, than managing IT systems
    - Repetition is the key to learning
    - Reconfirm shared understanding: Review outstanding risks with audience periodically (e.g. "Last year, we accepted this risk – shall we do the same this year?" If you get a new boss, make reviewing the risks which their predecessor accepted an early conversation)
    - Beware of over-simplification: including complexity can sometimes help the audience grasp / engage on the topic
    - Sometimes, your audience may push back with "I don't want to know; you're the IT expert; you solve it"
        - Or, "Stop: I don't have time to be educated. What I want is: (a) your recommendation, (b) your willingness to stake your job on that recommendation".
        - One attendee notes that he has offered to his management the following around the risk of cryptoware: "We have implemented, with the funding you have provided, sufficient protections that I claim we can recover from a cryptoware infection without paying the ransom. If I am proved wrong, then I believe the cost should come from my salary."
- Use Incidents to contribute to communication
    - Service disruptions
    - Near-hits, e.g. "Last week, we tore through two of our three data protection mechanisms, i.e. had our final barrier to data loss failed, as the first two did, then we would have lost data."
- Leverage other forums
    - e.g. some biomed institutes are covered by regulation, which incurs processes around IT security related to protecting personal information. Use this forum to talk about risk of data loss – not strictly 'security' related, but hey.
    - e.g. we sys admins typically spend substantial staff time maintaining archaic / fragile pipelines; this translates into spending indirect dollars, which can translate into conversations with Finance and even CFO & COO around where indirect $$ are going (and thus into the risks involved with the existing archaic / fragile pipelines).

- Beware of Normalization of Deviance, e.g. our nervous systems become accustomed to threat and quit firing around them. The examples are legion:
    - Space Shuttle / O-rings routinely pushed beyond specification
    - Institute firewall doesn't block malware: just a NAT box
    - Living & doing business on the Ring of Fire (e.g. Seattle)
- Expect gradual progress … sometimes very gradual! – in terms of Conscious & Shared

Quantifying Risk

- Ideally, we can quantify the cost of the risk (e.g. 1mil / year), the likelihood (e.g. 10% / year), and the cost of mitigation (e.g. 10K/year), and thus make a business case – in this example, one could easily make the case for spending 10K/year in order to mitigate a 10% per year chance of a 1mil cost.
- However, interesting risks tend to carry intangible costs, e.g. reputational damage. Intangibles make the conversations, and judgement calls, hard.
- And, typically, quantifying is hard, so we tend to end up with the subjective 'Low / Medium / High' instead.

Misc

- Quadrant 2 Risks: High Impact / Low Likelihood risks are hard to handle. To make matters worse, they typically tend to cost a lot to mitigate. Our most experienced risk manager typically sees his audience engage and discuss such risks but has yet to see his audience implement concrete steps around them.
- Some risks are easy for the audience to visualize, e.g. fire, earthquake, flood; audiences will tend to engage on these. That's too bad. Because plenty of other risks are more important (i.e. Impact x Likelihood produces a larger value) – the IT space is full of these (IT stuff tends to be hard to visualize – those bits are pretty small).

Comments from Bob Robbins http://www.rj-robbins.com/

Another aspect of risk management to be aware of: Risk management as a tool in intra-organizational political battles.

One could attack the HR department by claiming that they were failing to protect the organization against the risk of lawsuits from employees.

One could attack the finance department by claiming that they were failing to protect the organization against the risks associated with (A) inadequate insurance, (B) bad financial investments, (C) dangerous loan provisions, etc.

One could attack the facilities department by claiming that they were failing to protect the organization against the risks associated with, say, major earthquakes.

The options for criticizing the IT department by claiming that they were failing to protect the organization against IT-associated risks are very large. In this case, the ability of the IT department to

respond to these allegations is, I think, more difficult than for the other departments. The reason is, all of management can probably produce some level of understanding regarding the risks associated with human-resources practices, with financial positions, and with building construction and maintenance. However, the majority of management cannot produce anything vaguely approximating a decent mental model regarding IT risks and mitigation. Plus, new IT-related risks pop up probably at least an order of magnitude, if not more, frequently then do new risks arise in the other areas. Finally, if the organization is defrauded out of millions of dollars because a member of the finance-department staff falls for a phishing attack, was that damage caused by a failure of the IT department to protect against IT-related risks, or by a failure of the finance department to protect against staff-ignorance risks?

It is also worth noting that efforts to mitigate IT-related risks almost always involve methods that are diametrically opposed to efforts to achieve either convenience or cost effectiveness, or both.

Bottom line, to avoid the opportunities for inter-departmental political battles AND to achieve better risk management, institutions would do well to adopt an approach to risk management that does away with any departmental-based conceptualization (i.e. finance risks, IT risks) and instead insists upon considering all risks to be institutional risks.

For example, from an IT technical perspective, it would be almost trivially easy to implement and deploy an email system that had virtually zero risk from toxic attachments or from fishing attacks or from pretty much any other kind of email-associated malware.

All you would have to do is to go back to some ancient UNIX-based, text-only email system that prohibited attachments. There would be no outbound links to support phishing and no attachments to deliver malware. There would, however, be a major adverse effect on the convenience and effectiveness regarding the use of email by staff in all other, non-IT departments.

I am emphasizing the problems for non-IT staff, because most IT staff could figure out how to use other technologies to distribute or acquire files, to connect with other remote resources, or to accomplish any of the tasks rendered convenient through email attachments and links.

More generally, all efforts to make information technology more friendly and more usable by non-IT professionals simultaneously makes that technology more dangerous. This is an inescapable fact with regard to the way IT works. It is especially true, and even more inescapable, when the information technology in question is connected to a network, and then on to the wider Internet.

Should this increased risk be considered the fault of the IT department, or should this increased risk be recognized as deriving from the insistence of non-IT staff that they be permitted to use information technology without being required to understand it?
==========