Managing Third Party IT Risk Effectively

Matt Plummer

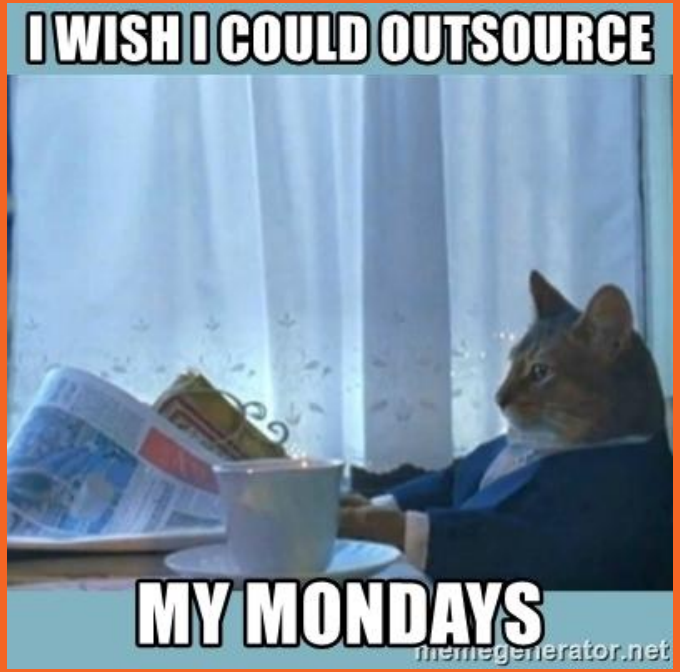
About Me

- Manager in Technology, Data & Analytics
- Specialism in Third Party IT Risk Management
  - Worked with clients across public & private sectors
  - Worked across a range of outsourcing models
  - Design and review clients' monitoring and oversight processes
  - Undertake deep dive assessments of third party processes on behalf of clients

Agenda

- What is outsourced IT?
- What are the benefits and challenges of outsourced IT?
- How can Third Party IT risk be handled?

What is outsourced IT?



Types of Outsourcing

Cloud Computing

- Software as a Service (SaaS)
  - Salesforce
  - Slack
  - Zoom
- Platform as a Service (PaaS)
  - Google App Engine
  - Heroku
- Infrastructure as a Service (IaaS)
  - AWS
  - Microsoft Azure
  - Rackspace

Onshore / Nearshore / Offshore Outsourcing

- Telecoms
- Application support
- Program Development
- Disaster Recovery
- User Administration

"Break it & Fix It"

Managed Services

- Voice over IP (VOIP)
- Data Storage
- Managed Security
- Identity and Access Management (IDAM)
- Infrastructure Management

"Proactively managed & Maintained"

The rise of Cloud Computing

- Companies are rapidly moving their **operations (75%)** and **security (76%)** to the cloud.[1]
- Worldwide end-user spending on public cloud services is forecast to grow 18.4% in 2021 to total $305 billion, up from $258 billion in 2020, according to Gartner, Inc.[2]

1. *2021 Global Digital Trust Insights Survey*
2. *https://www.gartner.com/en/newsroom*

Outsourcing - Benefits and Challenges

Why do companies outsource IT?

IT outsourcing covers a broad range of products and services. Some of the main reasons businesses outsource include:

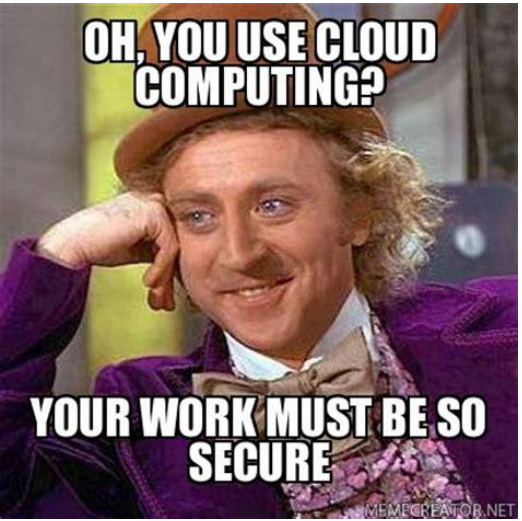
- Reduce IT Costs / lower Capital costs
- Access to specialist skills
- Flexibility
- Scalability
- Improved Resilience

Example 1 - Starting with the good news...

https://www.bbc.co.uk/news/technology-53093611

- 2.3 Tbps DDoS attack
- Roughly 500 DVD's worth of information **per second**
- 44% larger than any other attack on AWS

What are the challenges it brings?



- Small fish, big pond
- Lack of in-house knowledge - who can provide challenge?
- Coordination of multiple third parties
- Significant reliance on others to get it right
- False sense of security

Example 2 - Too big to fail?

Google suffers global outage with Gmail, YouTube and majority of services affected

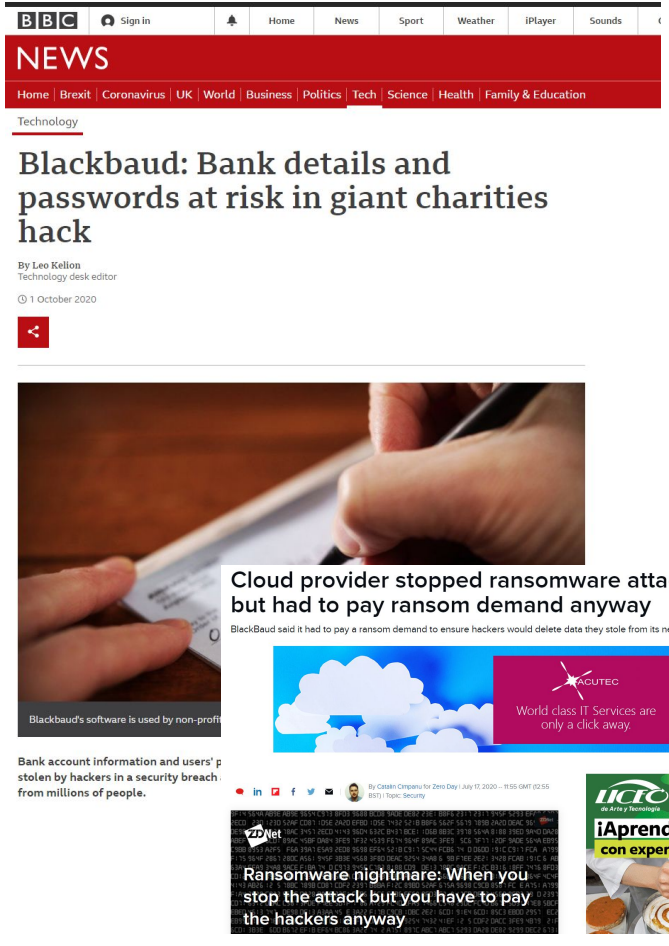
Error was due to lack of storage space in authentication tools causing system to crash

▲ The outage appears to be related to the company's authentication tools. Photograph: Denis Charlet/AFP/Getty

https://www.theguardian.com/technology/2020/dec/14/google-suffers-worldwide-outage-with-gmail-youtube-and-other-services-down

- Worldwide Outage
- Storage Quota Issue

Example 3 - Blackbaud

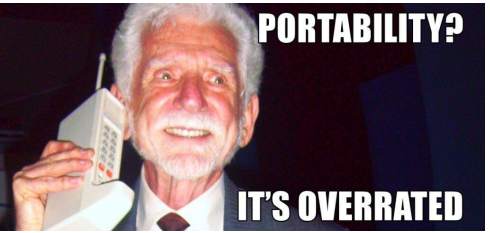


"Blackbaud: Bank details and passwords at risk in giant charities hack"

https://www.bbc.co.uk/news/technology-54370568

- SaaS provider for fundraising and relationship management
- Used across a range of industries, including:
  - Charities
  - Healthcare
  - Higher Education
- The hack occurred in May and was first disclosed to the public in July
- Affected organisations not notified as quickly as expected
- Full picture not understood for a long time

What about risks to individual organisations?



- Regulatory and compliance challenges - where is your data?
- Loss of in house skills and expertise
- Loss of transparency within IT services
- Lack of alignment between cloud services and existing services and infrastructure
- ‘Lift and Shift’ to cloud does not necessarily mitigate risk
- Lack of portability - once you’ve made the jump, how do you get out?

Example 4 - Outsourced IT Services

In house team:

- Outsourced most aspects of IT Service Management
- Relied significantly on technical knowledge of the third party
- Had limited engagement and oversight of controls and processes

Leading to:

- Out of date systems with critical security vulnerabilities
- Ineffective change management processes
- Poor quality management Information

Example 5 - Outsourced IT Services

In house team:

- Outsourced aspects of IT Service Management with robust monitoring
- Worked Collaboratively with third parties to develop strong processes
- Close oversight of third party processes

Leading to:

- Clear understanding of risk exposure & mitigating actions
- Robust processes to drive forward change
- Good quality management Information

However, this brings its own set of challenges.

Handling Outsourced IT Risk

What types of risks do we face?

Third Party IT Risks can cover a broad spectrum, including:

- Regulatory
- Financial
- Operational
- Security
- Reputational

Back to Basics - Measuring our response

Proportionate	Risk management activities must be proportionate to the level of risk faced by the organisation.
Aligned	Risk management activities need to be aligned with the other activities in the organisation.
Comprehensive	In order to be fully effective, the risk management approach must be comprehensive.
Embedded	Risk management activities need to be embedded within the organisation.
Dynamic	Risk management activities must be dynamic and responsive to emerging and changing risks

What questions should I be asking?

- What kind of data can I put out on the Cloud?
- Are there any regulatory or compliance requirements that affect me?
- Who owns the data and who has the rights to use it?
- What security measures are in place to protect my data in the Cloud?
- How do I ensure our data is appropriately segregated from other Cloud subscribers' data?
- Who is liable if things go wrong and what are the remedies?
- What recovery and continuity procedures are available in the event of a loss of Cloud service?
- What tools, procedures and support are available to migrate between Cloud providers?
- What monitoring and reporting mechanisms are available to maintain governance and oversight over the services migrated to the Cloud?
- How can we change service providers or exit the contract without incurring additional costs or exposing ourselves to risks?

Key Takeaways

- Third party IT risk needs to be managed like any other
- You’re only as strong as your weakest link
- Due diligence is good, but alone is not enough
- Even in the most well controlled environments, incidents will happen
- Failing to prepare is preparing to fail - have a plan!

Thank you for listening!

Contact Details:

E-mail: Matthew.j.plummer@pwc.com

Tel: +44 (0) 7483 440 177