Disclaimer

- This talk does not contain proof of concepts, shell code, scripts or other in-depth technical details.
- The content of this talk does not reflect the opinion and security safety measures of my current or former employers.
whoami

• Working as an IT- and Information Security Specialist since over a decade, focused on Security Management, Consulting and Architecture.

• Living and working in Düsseldorf, Germany.

• upload: cissp@gmx.de

• lets start with the download...
Definition: Off-shoring and Outsourcing

Definition:

- Offshore = outside coastal waters, outside of someone’s territory, outside of a field of applications. (e.g. power generator, windmills)
- Outsource = order services by another company or spin off tasks and/or information handling to an external supplier
- Off-shore development = projects or task of a project is outsourced to fill a gap (knowledge, manpower, budget)
Plato's Cave

- The myth of the cave in Plato's allegory is about ideas, the truth and the interpretation of the real world.

- Summed up: Plato describes a group of people who are chained in a cave. These people interpret their reality and the real world only by looking at the shadows (created by the fire in the cave behind a wall).
Plato's Cave II

- Video
  „The Cave: An Adaptation of Plato's Allegory in Clay“, bullheadent
- [http://www.youtube.com/watch?v=69F7GhASOdM](http://www.youtube.com/watch?v=69F7GhASOdM)
Plato's Cave III

• Possible viewpoints:
  • Chained and see the shadows
  • Free to understand the reason for the shadows
  • Free to go outside the cave
  • Be outside the cave and see the sun, which produces shadows by itself.

• Return to the cave?
Chain Information Security?

- Based on the allegory it is necessary to understand our viewpoint, describe the Off-Shore- and Outsourcing-Situation and think about the fire, the shadows and the sun.
Level of Analogy and the Shadows

- We are the prisoners.
- The chains are our interpretation of how we should implement security in the world.
- The shadows we see are our understanding how things might be. We generate our “real world”. (result of compliance checks, results of certifications)
The Artificial Things (Objects)

- The objects (things) that cast the shadows are visible to the man in front of the wall.
- Your supplier, outsourcer or Off-Shore-partner knows that he produces a shadow.
- He knows that this shadow produces a reality for the prisoners.
- He can modify the shadow - and the result of the compliance-check!
The Fire

- The fire is the rule set of the well-known compliance- and licensing-model.
- The fire defines a standard (light) and consistent reality within the cave.
- By not knowing the real-world one or more fire(s) are burning.
- The man and the objects (things) cannot modify the fire but modify the shadows.
- Compliance check: e.g.
  - SAS 70 report (I&II), ISO 270**, Company specific guidelines and reports, Company’s maturity level, PCI DSS
The Real World I

• Outside the cave there is the real world:
  • Daylight
  • Shadows
  • Colours
• Speaking blunt:
  • information warfare & industry espionage
  • insider attacks
  • external intruders
  • 0dayz
  • vendor problems +++
The Real World II

• But there is also Good:
  • the understanding for security
  • people who would like to help
  • security evangelists.

• Even when the daylight hurts, after a process of adoption (by understanding the upper world), we realise the situation we are in.
Why Plato's Allegory? I

- We have been in the real world.
- We know the natural real objects and we understand the function of the sun.
- We have seen the daylight and know that there can be shadow.
- By thinking about and ordering off-shore development, outsourcing the IT and our information (without a concrete strategy) we knowingly chain us again deep deep in the cave.
Why Plato's Allegory? II

- We do not control the fire and need to trust the men who cast the shadows.
- We have to trust the fire makers and the persons who define the rules for the fire and the casted shadows.
- We can't change the cave.
 Lets Go into the Cave I

- Types of Off-shoring and outsourcing:
  - buy extra time-limited resources and know-how (e.g. consulting)
  - IT hosting (e.g. cloud services)
  - development
  - source out IT parts of the company (e.g. IT project management or HR ;-)
  - total IT (partnering)
Lets Go into the Cave II

• Reasons:
  • build something new on flex-men-power
  • get rid of people
  • get rid of IT (because it's no core business)
  • hidden agenda

• And always:
  • Talking about money ... like ROSI (Return on security investment) ;-)
How Does the Cave Look Like?

- We have been outside the cave, know the “real world” and now decide (based on any decision) to order outsourcing or off-shoring.
- We sit in the cave and hardly try to interpret the shadows.
- These shadows will be our “new” “real world”.
Major Difference to Plato's Prisoners

- The prisoners (we) know that they (we) are sitting in a cave
- They (we) can (more or less) talk to the men and objects that casts the shadows
- We can change the situation!
- Result:
  - You can ask for your images and 'world- information'
  - But how? Ahhhh yes – Standards!
Of Course We Have Baselines and Standards!

• (Industry) Standards: e.g.
  • SAS 70 I&II report
  • ISO 270**
  • COBIT
  • PCI DSS
  • … and others.

• You and your partners have baselines too!
  • Company specific security guidelines
  • development guidelines
  • individual compliance checks
  • companies maturity levels
The Surrounding

• National laws:
  • local national law
  • group / company policy
  • if EU -> EU law-set
  • International non-EU law-set
  • Data-protection law EU / non-EU
  • Cross border-transfer (regulations) of (for) information
  • Cross border encryption policy / laws (e.g. limitation and definition for China, France, USA)

• Language problems

• Cultural problems
Risks and Benefits

- You are willed to put yourself in the position
- You start to over-think aspects of your (core) business, your IT, your budget - are there any risks? **We should talk about chances!**
- Confidence = trust + control
- Confidence = trust + control + acceptance of residual risks
Benefits

- You are flexible
- Your can extend and increase your know-how level
- You can extend your business by in / source out certain aspects (e.g. online-shops + delivery)
Risks – IT Partnering (total IT)

- Data loss
- Loss of control and evidence
- Loss of architectural influences
- Blending of partner’s client data (your supplier mixed up data of his clients)
Risks – Source Out (parts)

- Loss of company data
- Loss of knowledge (e.g. concerning project information)
- Loss of application and business knowledge
Risks – Support and Consulting

- Knowledge transfer
- Information loss
- Re-use of results
- Integrity and confidentiality
Risks – Development

- Intellectual property + copyrights
- Local admin rights
- Development equipment
- Data & Source code loss
- Malicious code in source code or binary
- Open source code in closed source code (license and security)
- Re-use of code snippets (more than one company)
- Information and source code flows out and into your company (… test data …)
Risks – Other Aspects

- Data exchange (transmission and connection)
- Virtual equipment used by your partner
- Intellectual property and copyright aspects
- Sub-contractors (off-shore the off-shore)

- YOU ARE THE ASSET OWNER!
- IT IS (Y)OUR REPUTATION!
Protect Your Cave!

- How to mitigate the risks?
- We know the risks
- We know we can be manipulated
Mitigation –
Strategy, Strategy, Strategy!

• It is always the same - you have to over-think what you want (to achieve) and what your target is!

• A strategy must be defined - before you handshake “the deal” at the golf course!

• The strategy must include a business strategy, an IT strategy and (!!!) an IT/Information security strategy!

• ➔ Know what you order!
Mitigation – Information Security Aspects

- Classify your business and workflow's
- Classify your data
- Asset and risk classification/analysis is necessary
- Limit access to data
- Revise your access controls
- Over-think the controls
- Know your information-flow
Mitigation – Audit and Compliance

- Develop a security guideline (based on your security strategy) to describe how you would like to proceed
- Define very clearly what you expect and what kind of evidence (result and quality) you would like to see!
- (audit proof and evidence)
- Define ways to handle incidents
- Audit by yourself (do not expect that the man casting the shadows has the same understanding of shadows)
Mitigation – Network And Connection

- Generate segregated networks / isolated networks
- Define information flow and exchange possibilities
- Over think your entry points (in-going connectivity’s, exchange of data)
Mitigation – Sourcing, Law & Regulations I

- Define security issues in the Request For Proposal (RFP)
- Avoid promises; do it, fix it!
- Bind externals with a concrete contract
- Revise and verify your sourcing strategy
- Check your sourcing and ordering process
Mitigation – Sourcing, Law & Regulations II

- Define non-negotiable contract-parts which contain
  - intellectual property
  - copyright
  - local / national law
  - data protection law
  - penalty aspects
  - direct links to your security guideline
Mitigation – Development and Architecture

- Work on your virtualisation concept
- Over think and revise the local admin concept
- Run security and quality checks on the source code
- Specify controls and audit's in development
Who can help? Outsource the Outsource!

- Why get dirty hands? Ask professional support for offshore development and IT-Outsourcing!
- Companies offer full engagement, services and consulting to support your outsourcing.
- Supporter-Managed ODCs vs. Client-Managed ODC
Who can help?  
Outsource the Outsource! II

Example: Achievo’s professional services team provides in-depth research on locations, including city proles that cover:

- Transportation
- Local talent pool
- Long-term client strategy
- Infrastructure
- Political and economic environment
- Culture, lifestyle and living conditions
- Consult Consult Consult
- Location Location Location
- +++

<table>
<thead>
<tr>
<th>Catalog</th>
<th>Service Items</th>
<th>Client Managed ODC</th>
<th>Achievo Managed ODC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Facility</td>
<td>Furniture maintenance</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Management</td>
<td>Computer maintenance</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td></td>
<td>Network equipment</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td></td>
<td>Conference / other equipment</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>IT &amp; IP</td>
<td>Internet and intranet</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Protection</td>
<td>Physical security</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td></td>
<td>Data security and back-up</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td></td>
<td>Disaster recovery</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Software maintenance</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td></td>
<td>Intrusion detection</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Antivirus</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td></td>
<td>Document management</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operations</td>
<td>Accounting support</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Support</td>
<td>Procurement support</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td></td>
<td>Timesheet and billing</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td></td>
<td>Administrative support</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td></td>
<td>Legal support</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Staffing, HR and Training</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Recruiting and hiring</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td></td>
<td>Labor contracts</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Orientation and training</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td></td>
<td>Retention program</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Salary, insurance, benefits</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Specific talent pool maintenance</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Process and</td>
<td>Process management</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Project</td>
<td>Project management</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Management</td>
<td>Quality assurance management</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Communications management</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Communications management</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Source Code management</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure: [Achievo ODC services menu](http://www.achievo.com/upload_file/Achievo-Offshore-Development-Center-Brochure-2009-01-19-EN.pdf)
Who can help?
Outsource the Outsource! III

• As-is-situation:
  Business \(\rightarrow\) (orders) \(\rightarrow\) IT

• New situation:
  Business \(\rightarrow\) (orders) \(\rightarrow\) IT + Outsourcer / Supplier / external partner

• “Supported” situation:
  Business \(\rightarrow\) (orders) \(\rightarrow\) IT + Outsourcing-supporter \(\rightarrow\) (orders) \(\rightarrow\) Outsourcer/Supplier/external partner

• This helps! ;-)

• BTW: Ramp up-service offered … but no shut down service.
Conclusion and Summary

- You are responsible for your business; even when you are ordering a contractor.
- You know what the real world looks like.
  - Return to the fire? Return to the cave?
- By ordering real-world images casted in the cave, high endeavours have to be made!
- To stay in the cave you have to invest in protecting mechanisms!
- It is required to do a comprehensive analysis before starting with this topic.
Questions?

• Thank you for your attention
• Any questions?

BTW: Do you do offshore banking? ;-)
Merry Christmas!

Links, Information, Sources

- http://www.offshoringtimes.com/Pages/2006/offshore_news496.html
- http://www.platon42.de/caveanalogy.html
- http://www.capurro.de/plato.html