Outsourcing Risks

Catapulting Information Into the Unknown

The Institute of Internal Auditors
Austin Chapter Luncheon
March 16th, 2011

Brian Engle
CISO / Director of Information Security
Temple-Inland Inc.
President – ISSA Capitol of Texas Chapter

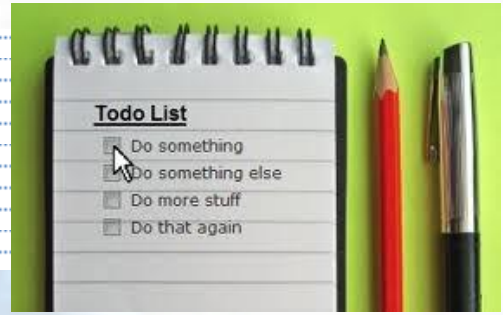
About

- The preeminent trusted global information security community
- http://www.austinissa.org
  - Monthly Chapter Meetings – numerous additional education events throughout the year

About Temple-Inland

- Low-cost, highly efficient manufacturing company focused on corrugated packing and building products
  - Containerboard – largest segment of paper market
  - Building Products – products for residential and commercial construction
- 10, 500 Employees – 82 Locations in U.S., Mexico and Puerto Rico
- $4 Billion approximate annual revenue

Agenda



- Acronym Soup and Outsourcing Types
  - The Crumbling Perimeter Wall and Other Paradigm Shifts
- Establishing Ground Zero
  - Baselines Using Frameworks and Standards
- Risk Evaluation
  - Assessing controls from the other side of the world
  - Questionnaires and Surveys
  - Identifying Deficiencies and Gaps to Standards and Expectations
  - Special Considerations
  - Vendor Provided Materials (Product Literature, SAS 70 Reports, and other assorted fairy tales)
- Dealing with the Inevitable
  - Risk Tolerance and Acceptance
  - Contractual Risk Mitigation

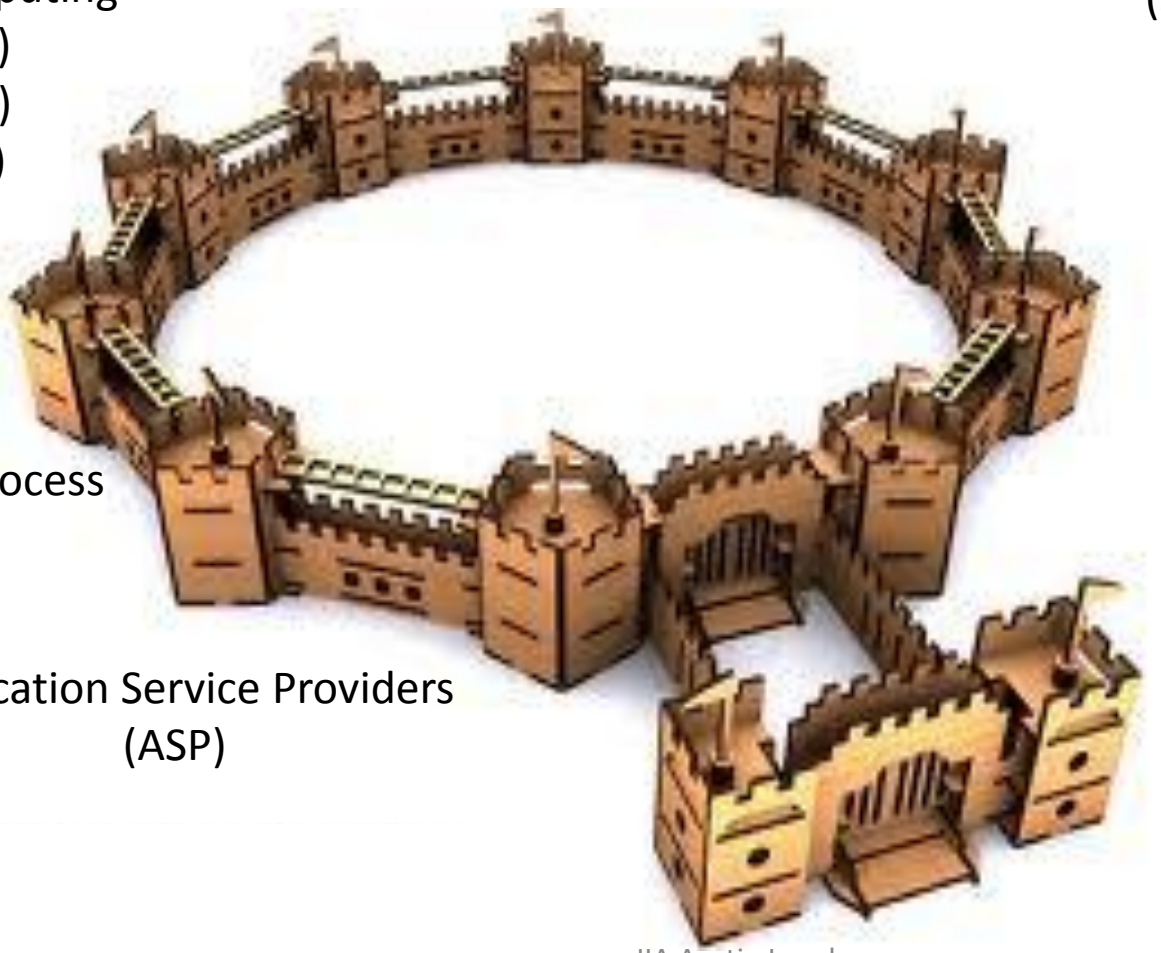
Outsourcing Business Drivers

Outsourcing Types

Application
Development and Testing

Cloud Computing
(SaaS)
(PaaS)
(IaaS)

Personnel
(Security Guards)
(Call Centers)
(General Labor)



Manufacturing
Operations

Business Process
(BPO)

Product
Design

Application Service Providers
(ASP)

Security Services
(MSSP)
(Penetration Tests)

The Crumbling Perimeter Wall

Outsourcing Risks

Some Old…

- Unauthorized Access
  - Insider
  - External
- Availability Threats
  - Denial of Service
- Fraud and Theft
  - Insider
  - External
- eDiscovery

Outsourcing Risks

Some new…

- Seizure of Infrastructure
- Vendor Viability
- Liability
- International Laws
- Import / Export Considerations

Desired State and Acceptable Conditions

First, define the desired outcome.

Security > Current or Required State

Security = Current or Required State

Security < Current or Required State

There will always be tradeoffs, usually at the sake of security.

Define a Reference Point

Start with a framework…

- COBIT
- ISO 17799 or ISO 27001
- COSO
- FISMA
- NIST
- ITIL

…to derive your policy and standards…

…then evaluate the outsourcing arrangement to see how they measure up.

Assessing from a World Away

Broad Risk Criteria

Broader Company Considerations

- Policies and Standards
- Governance
- Ethics and Business Conduct
- Information Security Management
- Personnel Security (Awareness, Responsibilities)
- Third Party Vendor Management
- Compliance and Legal Requirements
- Insurance

Specific Assessment Criteria

Business Continuity, Backup and Recovery

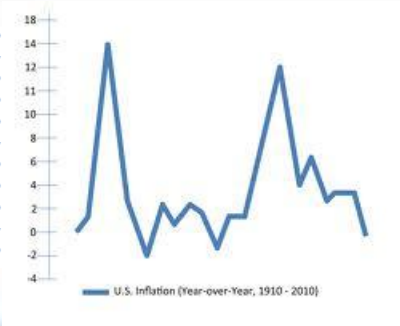
- Recovery time objectives
- Redundant data centers
- Mirrored data environments
  - Last test of recovery capabilities
- Media handling and security
  - Encrypted backup tapes
  - Secure destruction of retired media
  - Offsite storage

Specific Assessment Criteria

Data and Software Exchange

- Securely transmitting information
- Secure email communications
- Consider ongoing data transmissions as well as any bulk import information loads at onset
- Escrow of application code
- Secure destruction of information
- Record retention considerations

Specific Assessment Criteria



Changes, Enhancements and Modifications

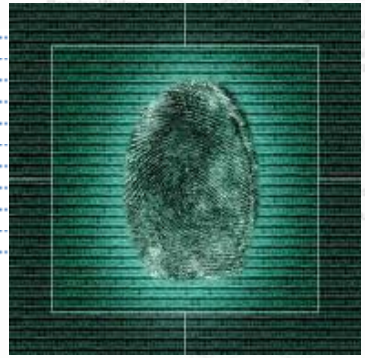
- Change management and revision control
- Development methodology
- Segregation of duties to prevent unauthorized changes
- Rate of change
  - Impact to personnel (training)
  - Mitigation of vulnerabilities
  - Impact to availability

Specific Assessment Criteria

Security Reviews

- Ongoing Internal Analysis as well as Independent, Third Party Analysis
  - SAS 70 Audits (Type 1 vs. Type 2)
  - PCI-DSS Audits
  - Static Source Code Analysis
  - Application Vulnerability Analysis
  - Penetration Testing
  - Overall Vulnerability Assessment

Specific Assessment Criteria



Physical and Environmental Security

- Equipment Protection from Environmental Hazards
  - Power, Humidity, Temperature, Fire
- Secure Areas
  - Unauthorized physical access
  - Surveillance, guards, escorted visitors
  - Access logs and authorized access reviews

Specific Assessment Criteria

Protection from Malicious Software

- Malware Prevention Systems
- Incident Detection and Response
- Intrusion Prevention
- Introduction of vulnerabilities from third party, outsourced development

Specific Assessment Criteria

Access Controls

- Authorization for access
- Deactivation
- Periodic Access Reviews
- User Registration, Provisioning, De-provisioning and ongoing maintenance
  - Segregation of Duties
- Access Logs (retention, review, alerting)

Specific Assessment Criteria

Authentication

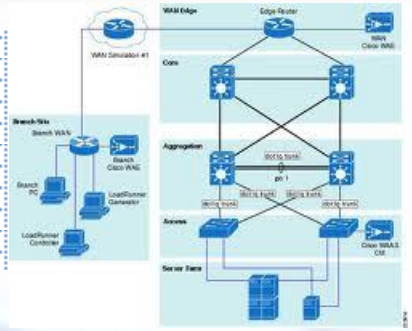
- Password Expiration
- Password Complexity
- Password Uniqueness
- Initial Password Changes
- User ability to change password
- Limit access from specific sources (IP limits)
- Support for multi-factor authentication

Authentication Special Consideration

Federated Identity Management and Single Sign-On Solutions

- Outsourced applications typically require their own login ID
- Authentication parameters that are not synchronized to internal IDs are problematic for users
- Credential issues include Password Sloth and the temptation to use poor password security

Specific Assessment Criteria



Application Architecture

- Logical separation of client instances
- Physical separation of client instances
- Database integration
- Application component tiers
- Encryption and authentication between tiers
- ***Maintenance utilities***

  (Bulk Imports and Data Fixes)

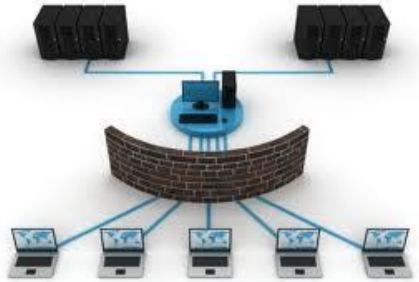
Specific Assessment Criteria

Application Security

- Input Validation
- Injection Flaws
- Insecure Object References
- Cross-Site Scripting
- Cross-Site Request Forgery
- Error Handling

Check out OWASP.org for much more.

Specific Assessment Criteria



Network Architecture

- Network segregation and compartmentalization
- Network Access Controls
- Firewall implementation and upkeep
- Port restrictions
- Intrusion Prevention System implementation and upkeep
- External connection requirements
- Network monitoring
- VPN

Other Materials

Vendor Materials (Propaganda)

- Security Summaries
- Internal White Papers
- Marketing Materials
- Website
- User Guides

Other Data Sources

- Project meetings
- Interviews
- Request For Proposal (RFP) responses
- Vendor presentations
- References

Contractual Mitigation

- SLAs
- Exit Strategies
- Return of Information upon request
  - for any reason, not just at contract expiration or breach
- Requirements for Third Party Evaluations
  - Include requirements for providing reports with sufficient detail
- Ongoing monitoring

Dealing with Risk

- Data Classification
- Elusive factors
  - Impact
  - Probability
  - Motivation
- Hidden Costs
  - Acceptance
  - Mitigation
  - Transference

Audit Considerations

- Have outsourcing arrangements been risk assessed?
- Is the process repeatable, and are there sufficient auditable artifacts?
- Have risks been addressed, mitigated or accepted?
- What cascading risks are present? Who has accepted those?

Questions?

Thank You!

Contact Info:

BrianEngle@templeinland.com

Brian.Engle@gmail.com