RSA CONFERENCE 2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.

Capitalizing on
Collective Intelligence

Ensuring Your 3rd Party Vendors and Partners are Secure

SESSION ID: **TECH-T07A**

Michael Gene Baker

Chief Information Security Officer
Convergys

Is your environment secure?

How do you get started?

- Vendor Management program
- Initial meeting with 3rd parties to understand their capabilities
- Do they currently support certifications?
- Credit Check – understand their financial status
- Get client references – especially from the same vertical
- Do you need a proof of concept?
- What type of your information with this 3rd party transmit, store, process or access?

Vendor Management Program

- Establishment/Improvement
- Risk Analysis
  - Is this a critical vendor for your organization?
  - Are there other vendors supporting similar activities?
- Due Diligence in Vendor Selection through RPF Process
- Documenting the Vendor Relationship
- Ongoing Supervision and Monitoring of Vendors

Due Diligence in Vendor Selection through RPF Process

- Ensure that information security has input into this process
- Ask open ended questions – not yes or no
- Consider using a framework to help with questionnaire like the SANS Institute ISO 17799 Checklist
- Once the responses are received – validate information
- Does RPF require the organization providing services to follow your information security standards?
- Always ask for more than you need

Common Topics for RPF Questions

- Information Security Program
- Policy, Procedures, Standards
- Information Classification Program
- Information Security Team Quals
- Risk Management
- Network & Infrastructure
- Antivirus Questions
- Data Network Monitoring Capabilities
- Network Security Tools
- Problem Escalation
- Backup Procedures
- Internal / External Audits
- Certification (ISO, PCI, HIPAA)
- Physical Security
- Segregation Approach
- Incident Management
- Business Continuity Planning
- Encryption Capabilities

Questionnaire Follow-up

- Set up a conference call to clarify any questions that are unclear
- Conduct an onsite pre-assessment and facilities visit
- Set up a conference call with information security organization
- Require all outstanding issues and questions be mitigated before signing the contract
- Ensure that all answers are validated in contracts and master service agreements

Documenting the Vendor Relationship

- Be Wary of Over Commitments
- Costs & Expenses – Compliance and 3rd Party Assessments
- Service Level Agreements
- Compliance of Policies and Procedures
- Incident Response and Investigations
- Reasonable Audit Notice
- Contract Relations
- Termination Clause

Ongoing Supervision and Monitoring of Vendors

- Level of Validation
- On-site visits
- Certification documentation
- External Party Assessments
  - Vulnerability Scanning
  - Penetration Testing
- Changes to Vendor Environment

Next Steps

- Get involved in the sourcing process
- Review information security portion of current contracts and master service agreements. Do they need to be changed to reflect the current risk and threats?
- For your critical vendors, establish a relationship with their information security group
- Trust but verify information you receive especially if you are relying just on self assessment questionaires

RSA CONFERENCE 2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Ensuring Your 3rd Party Vendors and Partners are Secure