Best practices in Supply Chain Security

Providing C-Level Executives with an Internal Checklist to Set Service Level Agreements, Performance Metrics, Certifications, and How to Trust-but-Verify that the Vendor Solutions are Reliable, Secure & Compliant

How weak is Your Technology Supply chain?

Discussion Leader: Theresa Payton,
Former CIO of the White House,
Chief Advisor and CEO of Fortalice®, LLC
Don’t be the next newspaper headline:

From GCN.com: “Treasury shuts down 4 cloud-hosted Web sites after infection... Malicious code appears to have come from servers in Ukraine”
Bad Events Re-Define Brands: Do you want to be Tylenol or BP?

1. RISK SCORECARD
2. RISK VS. REWARD
3. BRAND & COMPLIANCE MANAGEMENT
Overview

- Strong Process
- Contracts & Contract Audits
- Reliability
- New “Insiders”
Executives Often Ask:

- How have other executives overcome security concerns?
- What do we need to look for in an outsourced solution to address security issues?
- What “best practices” can we leverage?
  - Vendor assessments / Contract Language
  - Metrics / Certifications to require
  - Service Level Agreements / Trust but verify ongoing
Is It My Data or Yours?

- When there is litigation, do their lawyers fight before releasing your data or just hand it over?
- When you “break up” what are their sanitization policies so you get your data back and they don’t have the digital footprints?
- Does your industry prevent you from storing sensitive data outside a specific geography?
Take Away – Checklist
7 Security Checkpoints

- Information Security
- Identity Management
- Endpoint and Server Security
- Gateway and Network Security
- Web and Application Security
- Physical and Personnel Security
- Security Management
- Intellectual Property, Customer Information, and Financial Transaction Security
<table>
<thead>
<tr>
<th>Take Away – Checklist</th>
<th>Vendor Management Best Practices</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓ Chain of Custody</td>
<td>✓ Persistent Protection</td>
</tr>
<tr>
<td>✓ Least Privilege</td>
<td>✓ Compliance Management</td>
</tr>
<tr>
<td>✓ Access</td>
<td>✓ Code Testing and Verification</td>
</tr>
<tr>
<td>✓ Separation of Duties</td>
<td>✓ Trusted and Vetted Staff</td>
</tr>
<tr>
<td>✓ Tamper Resistance</td>
<td></td>
</tr>
<tr>
<td>and Evidence</td>
<td></td>
</tr>
</tbody>
</table>

Fortalice
Assess Core Functional Areas

- Data Map
- Data Protection Policies (INOFSEC & Compliance)

Vendor Contract Considerations

- International
- Vendor & Internal Maturity
- Business Continuity
- Operations
- Regulatory and Compliance
Take Away – Checklist
Contract Negotiations

- Trust but Verify
- Visibility & Traceability
- Logs
- Encrypted Transmission
- Audits
- Legal Controls
- Data Masking
Certifications = Security?

- Lack of a widely accepted “Good Housekeeping Seal of Approval” has led to organizations to ask companies for certifications.
- SAS 70 TYPE II
- PCI
- ISO
- CISSP for Staff
Take Away – Checklist
Internal Questions

- How do you handle “chain of custody”?
- Do you have full visibility into your suppliers’ suppliers?
- Rating “reasonable security protections”
- Data Map – all targets are not the same
- IP

Fortalice
Take Away – Checklist Internal Considerations

- Do you mandate certifications?
- Do you accept certifications as the final source or do you still require an assessment?
- How are your initial assessments conducted?
- What control measures do you have in place to insure that the vendor stays in compliance with your terms?
Best Practices

- See http://www.sharedassessments.org/

Mandated contract language

Risk assessment checklist

Do you have the ability to do a risk vs. reward tradeoff analysis?
How do you keep up with your vendor’s capabilities and performance?
Emerging Trends

- Companies leveraging a cyber-intelligence technology service provider to scour the Internet for potential vendor security issues.
  - These services could include: broad search and detection; contextual cross-analysis of URLs; multilingual; incident detection and response; data dilution capabilities (feeding the attackers false data); and analytics.
- Industry groups coming together to do certifications and best standards
Group Exercise

- Share 1 best practice
- Share 1 area of concern
- What items on the checklist will you check first?
Let’s Keep the Dialog Going!

Please Reach Out to Me:

- Twitter: @FortaliceLLC
- Web: www.FortaliceSolutions.com
- Facebook: Fortalice-LLC
- Email: TP@FortaliceSolutions.com
- CBS WBTV: WBTV.com Protecting Your Cyberturf