



Top 10 Challenges in IS Security Management (According to One Guy)

www.assuraconsulting.com

Today's Objectives



- Discuss the challenges “in the trenches”
- Open dialog about security management challenges and some solutions
- Lively discussion
- Disclaimer: Based on my experiences – YMMV

Question: What *is* IS Security Management?

Let's Examine the Premise

- Is information systems security important?
- Why or why not?



Challenge 1: “Why Should I Care?”



- Lack of understanding on their part
- Lack of clear communication on our part
 - Too technical
 - Cannot adequately articulate risk, probability and impact
 - Trying to prove a negative
- It all comes down to making a business case
 - How is it relevant to the organization?
 - How is it relevant to me?

Challenge 2: Security Practitioners Shoot Themselves in the Foot

- Risk avoidance vs. risk management
- The “no” squad
- Hyper-control vs. training, delegation and accountability for risk decisions
- Levying requirements on managers without training
- Poor/boring training
- Platitudes instead of admitting “yep, they got us: we don’t know”

“That hurt,
maybe this one
won't be so bad”



Prime Motivators for Security as a Management Priority

1. Forward thinking (rare)
2. We got hit (more frequent)
3. Regulatory compliance (most common)



“There are no atheists in foxholes.”
-- Ernie Pyle

Challenge 3: Vague/Conflicting Legal Requirements

- Lots of “what” but very little “how”
- Example: FOIA vs. e-Discovery vs. document destruction schedules
- “You” are on the hook if you get it wrong
 - Data breach
 - Audit finding
 - Legal action/sanction
- **The good news:** most privacy/security-focused standards/regulations say approximately the same thing

“First thing we do, let’s kill all the lawyers.”
- William Shakespeare

Get out of jail free?

- **Due care:** “That care which an ordinarily prudent person would have exercised under the same or similar circumstances.” (Black’s Sixth Edition)
- **Due diligence:** Carrying out the activities necessary to implement due care.
- The only way to disprove negligence
- But still at the whim of the courts (including the court of public opinion)



Challenge 4: Implementing Security to the Standard/Regulation



- False sense of security
 - Motivation on the attacker's part
 - Lack of imagination on our part
 - Sometimes you miss the forest for the trees

Compliance != Security

Challenge 5: Passive Risk Management

- Assessments that gather dust
- No ownership of risks
- No active risk management
- Are risks always negative?



Challenge 6: Culture



- We want a friendly, inviting work atmosphere and security shows a lack of trust
- We can't inconvenience our employees/customers
- I don't want to be rude (i.e., challenging strangers)
- I don't want to rock the boat (if I bring up security issues)
- Denial of Insider Threat
 - Our people would never do that!
 - We don't have anything worth stealing

Challenge 7: Competing demands

- Security managers have operational responsibilities (and not enough time to do security management)



Challenge 8: Duplicative Efforts



- Physical Security/Life Safety
- IT Security
- Business Continuity/COOP
- Financial Controls (e.g., COSO IC-IF, SOX, OMB A-123, ARMICS)
- **What do all of these have in common?**

Challenge 9: Incorporating Security Into System Development

- Lack of formal SDLC
- Lack of SDLC that incorporates security
- Lack of secure coding practices/training
- Source code reviews are time consuming, expensive and difficult (flaws in the human “computer”).
- Automated tools are imperfect (tools are programmed by humans)
- Disconnect between development and security

```
01522 Private Function CleanUpLine(ByVal sLine As String) As String
01523     Dim lQuoteCount As Long
01524     Dim lcount      As Long
01525     Dim sChar       As String
01526     Dim sPrevChar   As String
01527
01528     ' Starts with Rem it is a comment
01529     sLine = Trim(sLine)
01530     If Left(sLine, 3) = "Rem" Then
01531         CleanUpLine = ""
01532         Exit Function
01533     End If
01534
01535     ' Starts with ' it is a comment
01536     If Left(sLine, 1) = "'" Then
01537         CleanUpLine = ""
01538         Exit Function
01539     End If
01540
01541     ' Contains ' may end in a comment, so test if it is a comment or in the
01542     ' body of a string
01543     If InStr(sLine, "'") > 0 Then
01544         sPrevChar = ""
01545         lQuoteCount = 0
01546
01547         For lcount = 1 To Len(sLine)
01548             sChar = Mid(sLine, lcount, 1)
01549
01550             ' If we found "" then an even number of " characters in front
01551             ' means it is the start of a comment, and odd number means it is
01552             ' part of a string
01553             If sChar = "" And sPrevChar = "" Then
01554                 If lQuoteCount Mod 2 = 0 Then
01555                     sLine = Trim(Left(sLine, lcount - 1))
01556                     Exit For
01557                 End If
01558             ElseIf sChar = "" Then
01559                 lQuoteCount = lQuoteCount + 1
01560             End If
01561             sPrevChar = sChar
01562         Next lcount
01563     End If
01564
01565     CleanUpLine = sLine
01566 End Function
```

Challenge 10: Third Parties



- Breaches aren't your fault, but they're still your problem
 - Lack of security requirements in acquisitions
 - Lack of integrated processes with key vendors
 - Where's our stuff? (Positive control over assets and data)
 - How is data retention/destruction handled?

Wrap-up



- Security as a discipline is relatively young
- There are still a lot of problems to solve
- Security practitioners have to do better to communicate with users, management and auditors
- Progress is *evolutionary*, not *revolutionary*



Contact Information: Name: Joshua Cole
Telephone: 804-672-8714
E-mail: joshua.cole@assuraconsulting.com