





INFORMATION SECURITY DECISIONS

Hosted by  

Proven Tactics to Guarantee Policy Compliance.

By Charles Cresson Wood, CISA, CISM, CISSP
Independent Information Security Consultant
InfoSecurity Infrastructure, Inc.
 Sausalito, California USA
www.infosecurityinfrastructure.com
 +415-289-0800; ccwood@ix.netcom.com
 InfoSec Decisions Conference 2005 - Chicago



INFORMATION SECURITY DECISIONS

Hosted by  

Why has InfoSecurity become a team effort? (1)

- **Distribution of Information & Information Technology means security work must follow**
- **Local control over Info Management & Info Systems requires alignment of intentions**
- **Reliance on Naïve users to perform jobs previously done by specialists**
- **Expanded lines of communication and increased pace of communication**



INFORMATION SECURITY DECISIONS

Hosted by  

Why has InfoSecurity become a team effort? (2)

- **Information morphs from one form to another & often only people can protect it**
- **Expanded use of non-employee workers in positions of computer related trust**
- **Information security has become a multi-disciplinary, multi-departmental, and multi-organizational function**
- **Division of labor risks sub optimization because big picture not appreciated**



INFORMATION SECURITY DECISIONS

Hosted by  

Why has InfoSecurity become a team effort? (3)

- **InfoSecurity can no longer be viewed as a one-time project**
- **Majority of losses are from insiders, and most of those unintentional (E&O)**
- **InfoSecurity Department Does Not And Cannot Wield Sufficient Power To Be In All Places It Needs To Be (Orchestration Required)**
- **An All-Volunteer Army Doesn't Provide An Adequate Defense**



INFORMATION SECURITY DECISIONS

Hosted by  

Principle of consistent application

- **Every time exception is made, security is eroded -- for maximum security, achieve consistent application (personal use example)**
- **Consistent application across users of course, but also consistent implementation of policies & other written requirements**
- **Responds to traditional adage which holds that attackers seek weakest link**



INFORMATION SECURITY DECISIONS

Hosted by  

Dangers of ignoring principle of consistent application

- **Motivation of change plummets because users see lack of management support**
- **Users excuse their own non-compliance because so many other exceptions exist**
- **Unreported exceptions proliferate because lax attitude prevails**
- **New legal exposures are created (improper termination & discriminatory treatment)**



INFORMATION SECURITY DECISIONS

Hosted by  

Pharmaceutical firm example

- **IT department issued policy about OS patch management, but R&D department existed**
- **R&D labs used software which crashed if they ran more recent OS versions**
- **Policy was out of touch with reality**
- **No risk assessment was performed prior to issuing this policy, so no clear reference point existed**



INFORMATION SECURITY DECISIONS

Hosted by  

Three areas that we will examine more closely

- **Problems with policy development**
- **Problems with policy implementation**
- **Problems with policy communication**



INFORMATION SECURITY DECISIONS

Hosted by  

Problems with policy development (1)

- **Failure to obtain sufficient management buy-in prior to issuance**
- **Insufficient legitimacy of group or individual issuing policy**
- **No broadly-scoped risk assessment completed prior to issuance**
- **Management has insufficient understanding of relevant Tradeoffs**



INFORMATION SECURITY DECISIONS

Hosted by  

Problems with policy development (2)

- **Insufficient management understanding of relevant motivational & incentive systems**
- **Failure to survey relevant laws, regulations, contracts & generally-accepted industry practices**
- **Insufficient resources devoted to tailoring policy to organization's unique environment**



INFORMATION SECURITY DECISIONS

Hosted by  

Problems with policy development (3)

- **Erroneously believing one-size-fits-all policy is sufficient**
- **Writing policies after information systems have already been placed into production**
- **Failure to differentiate between policy, guideline, architecture, procedure & standard**
- **Poor project planning & follow through**



INFORMATION SECURITY DECISIONS

Hosted by  

Problems with policy development (4)

- **Failure to regularly review/update policy in response to changed conditions**
- **Failure to monitor & report on compliance (ideally, use controls that don't require compliance checking, or that include automated compliance checking)**



INFORMATION SECURITY DECISIONS

Hosted by  

Problems with policy implementation (1)

- **Failure to tie controls defined in policy with specific business goals**
- **Unrealistic expectations that users will read & take action consistent with policy without action-forcing mechanisms**
- **Inadequate resources devoted to information security so that only squeaky wheels get greased**



INFORMATION SECURITY DECISIONS

Hosted by  

Problems with policy implementation (2)

- **Aggressive goals are established in manner which is unrealistic**
- **Policy writer fails to understand user aversion & distaste for security & policy**
- **Policy lacks more detailed supporting documentation such as procedures**



INFORMATION SECURITY DECISIONS

Hosted by  

Problems with policy communication (1)

- **Management tries to do too much all at once & users are overwhelmed & object**
- **Insufficient training is provided (InfoSec is neither instinctive nor intuitive, & management frequently assumes very high levels of user competence)**
- **Failure to define exactly what it means to be in compliance with policy**



INFORMATION SECURITY DECISIONS

Hosted by  

Problems with policy communication (2)

- **Absence of formal risk management process fostering on-going examination**
- **Management has unrealistic expectations about extent to which commercial products can be used to implement policy**
- **Management is unaware of new commercial products, so they rely on traditional manual methods**



INFORMATION SECURITY DECISIONS

Hosted by  

Sample of modern automated policy management tools

- **BindView policy development**
- **PolicyTech policy & procedure manager**
- **Polivec policy management system (PMS)**
- **Information shield information security policies made easy (by this speaker)**
- **Neupart secure Aware policy**
- **NetIQ vigilant policy center**

INFORMATION SECURITY DECISIONS

Hosted by  

Conclusion

- **Infosec is far too complex & changing too rapidly to be handled in semi-manual ad-hoc fashion where newest threat will get a new policy after a problem manifests**
- **Take more proactive stance with greater Perspective & much greater organization**
- **Automate policy development, approval, delivery, archives, & user testing**

Audience Response

Question?
