



Information Security Solutions



Company

HQ in California, Locations in Australia, Ireland, UK

- Criteria Solutions must fit this framework:
 - People orientation
 - Information security is not a technical issue
 - Concentrate on information, not systems
 - System perspective tends to reduce emphasis on security issues outside of the systems, but this is where many security occurrences take place
 - Offer a logical, repeatable methodology
 - Standards based, process focus
 - Exist within the environment, support regulations
 - Work with the existing technology already in place



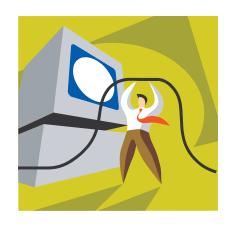
Organizational Gap

Information Professional

Business Planning Budget Research







Technology Professional

Hack Points
Communication
System Administration
Network Support



Gaining Control

- The security focus must be expanded.
 - Organizational and IT focused.
 - Inclusive of policy, practices, procedures.
 - Proactive rather than reactive.
 - Continuous process.
 - Based on organization's risk factors.



Dynamics of elements involved





Solutions

- Risk Assessment using the OCTAVE™ methodology – can be combined with ISO 17799
 - Enables you to effectively communicate critical information security issues
 - Provides a foundation for future security improvements
- Portal creation for security departments
 - Web sites for policies, information gathering, user registration
- Cryptographic infrastructure implementation
 - Addresses remote access, WLAN, file encryption, email security issues



Risk Assessments

OCTAVE

- Operationally Critical Threat, Asset and Vulnerability Evaluation
- Developed at the Software Engineering Institute of Carnegie Mellon University
- The same organization that manages CERT, the worlds first and best known computer incident response team



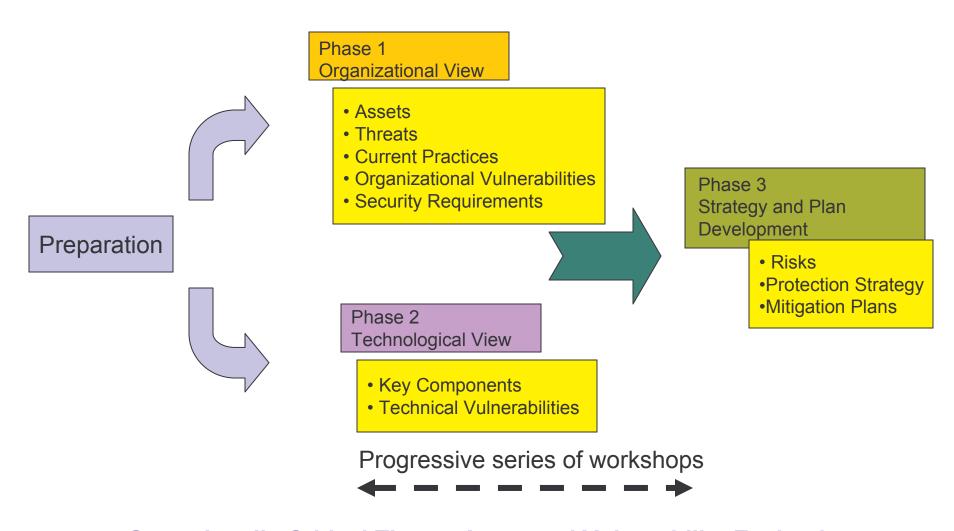
Conducting OCTAVE

- •An interdisciplinary team composed of:
 - Business or mission-related staff
 - Information Technology staff





OCTAVE Process



Operationally Critical Threat, Asset and Vulnerability Evaluation



Risk Assessment Worksheet

Human A	Actors Usir	ng Physi	cal Acces		Т					Τ	Т																		
Step 11					St	ер	25					Step	27			Ste	p 29	•									Ste	р 3	0
Asset	Access	Actor	Motive	Outcome	lm	Impact Values						Probability				Security Practice Areas						as					App	roa	ch
												Value	Cor	nfide	ence			Str	ate	gic				Ope	eratio	onal			
					Reputation	Financial	Productivity	Fines	Safety	Other			Very Much	Somewhat	Not at All	1. Security Policies	2. Org. Security	3. Asset Classification	4. Personnel Security	5. Physical Security	6. Comm. Management	7. Access Control	8. Sys. Development	9. Continuity Mgmt.	10. Compliance		Accept	Defer	Mitigate
				disclosure	M	M	ī	M	1	Ť	\top	М	Ĺ	X	\vdash	·	-	Ü	7	77			-	0,					X
			accidental	modification		М			T	T	1	L		Х	П												\exists	Х	
				loss, destruction		М						L		Х	П													Х	
		inside		interruption	М	М	Н	M			\perp	L		Х														Х	X
				disclosure		М		М				L		Х															X
Loan			deliberate	modification		Н						L		Χ															X
Proc.	physical			loss, destruction		М						M		Х	Ш														Χ
System				interruption	М	М	Н	М	┡	╀	\vdash	L		Х	Н													\blacksquare	Χ
				disclosure		Н		М				L			Х														Χ
			accidental	modification		М				┸	┸	L			Х												Х	Ш	
				loss, destruction		М			\perp	\perp	\perp	L			Х												\dashv		Χ
		outside		interruption	М	М	ļΗ	М	_	1	\vdash	L			Х												\blacksquare	\dashv	Χ
				disclosure		Н		M	L	t		L		Х															X
			deliberate	modification		М		_				L		Χ													Х		
				loss, destruction		M		М				L		Х													\Box		Χ
				interruption	M	М	Н	М	L			L		Χ															X



Outputs of OCTAVE

Protection Strategy



Defines organizational direction

Mitigation Plan



Plans designed to reduce risk

Action List





Near-term action items

- Enables you to effectively communicate critical information security issues
- Provides a foundation for future security improvements
- Positions your organization for compliance with data security requirements or regulations





Global standard for information security management systems

- Impruve incorporates regulatory and legal compliance for your industry
 - FDA (Life Sciences)
 - GLBA, Basel 2 (Finance)
 - HIPAA (Health Care)
 - Sarbanes-Oxley



Portals for Security Departments

Impruve provides both the content and technology to:

- Publish security policies
- Gather information
- Consolidate incident reporting
- Can be combined with other Impruve solutions
 - Risk assessment surveys
 - Certificate registration and distribution



Technology

- Developed cryptographic solutions using Microsoft Windows 2003 Certificate Authority. Supporting the following applications:
 - Wireless Lan (WLAN)
 - VPN, to secure devices and remote access
 - SSL, both server and client
 - File encryption
 - Email security
 - Digital signatures



Conclusion

Impruve - Risk, Policy, Technology

- Using the latest solutions developed by the top researchers in the area of information security
- References appropriate best practices and requirements
 - ISO 17799
 - GLBA
 - HIPAA
 - Sarbanes-Oxley
- Deployed by experienced information security professionals CISSP's, trained and licensed by CERT