



**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



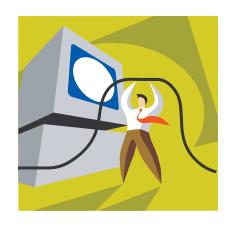
# Organizational Gap

#### **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



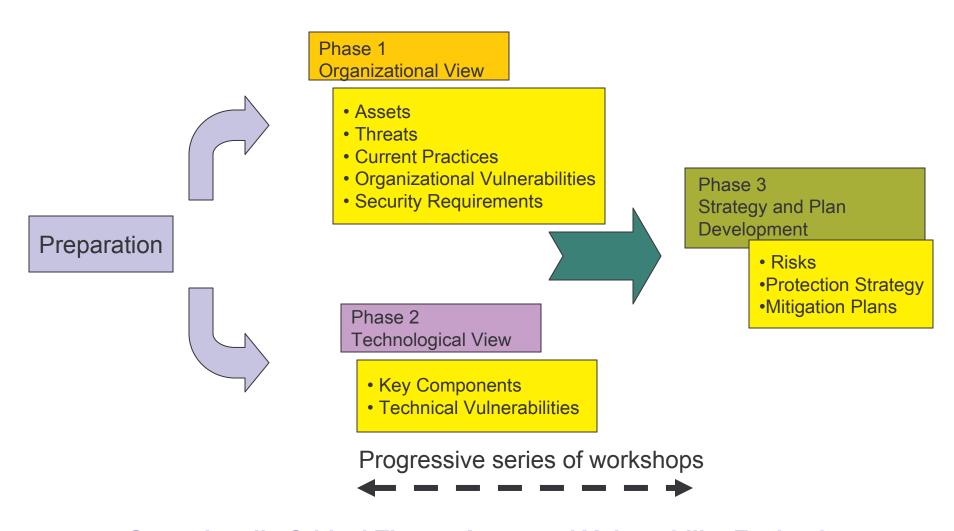
# Conducting OCTAVE

- •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

Step 11	totoro con	19 1 11901	cal Access	<u> </u>	0.4	ер	25			$\vdash$		Step	27			(	Ste	20										Ste	20	
Asset	Access	Actor	Motive	Outcome		ep ipac		الم												ooti	00	Λ roc	20			$\vdash$		App		
ASSEL	Access	ACIOI	IVIOLIVE	Outcome	1111	ipac	LV	alu	28	$\vdash$		Probability Value Confidence					Sec		y Practice Areas Strategic					000	rotio	$\rightarrow$	App	Uat	111	
					⊬	-	₩		⊬	$\vdash$	-	value	COI	IIIGE	ence	-	-	-	Sui	alec					Ope	eratio	mai	-	$\dashv$	
					Reputation	Financial	Productivity	Fines	Safety	Other			Very Much	Somewhat	Not at All		1. Security Policies		3. Asset Classification			6. Comm. Management	7. Access Control	8. Sys. Development	9. Continuity Mgmt.	10. Compliance		Accept	Defer	Mitigate
				disclosure	М	M		M	-	Ī		М	_	X	$\Box$			-	1,	Ì			·	,,,	-			Ť		<u> </u>
			accidental	modification		М				П		L		Х	П													)	x	
				loss, destruction		М			П	П		L		Х	П													)	x	_
		inside		interruption	М	М	Н	М				L		Χ														)	X )	X
				disclosure	М	M	L	M	$\vdash$	Н		L		Х														+	7	X
Loan			deliberate	modification		Н				П		L		Х	П															X
Proc.	physical			loss, destruction		M						M		Χ																Χ
System				interruption	М	М	Н	M				L		Х														$\Box$		X
				disclosure		Н		M				L			Х														7	X
			accidental	modification		М				Ш		L			Х													X	$\perp$	
				loss, destruction		М				$\Box$		L			Х															X
		outside		interruption	M	М	Н	M				L			Х	_											-	$\Box$	7	X
				disclosure		Н		M				L		Χ															<u> </u>	X
			deliberate	modification		M						L		Χ														X		
				loss, destruction		M						L		Χ																Χ
				interruption	M	M	Н	M		$\Box$		L		Χ																Χ



## 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