

Company "O": threat assesment 2008: Current status + Plan

11/7/2007

Current State (IT security operations costs in Euro)

Step	CM	Countermeasure Name	<u>Current Risk</u> CM Cost	40.60 Step Cost	<u>Maximal Risk</u> Plan Cost	40.60 Risk
<u>1.00</u>						
	C061	No patching 3 weeks before end of quarter	0	0	0	
	C031	Oracle Enterprise Content Management	0	0	0	37%
<u>2.00</u>						
	C042	The price of reverse engineering binary code is very high (economic disincentive)	0	0	0	
	C043	Encrypt Java byte codes	0	0	0	
	C035	Destroy hard disks	2,000	2,000	2,000	
	C044	Machine software uses a license hidden with one way encryption	0	2,000	2,000	36%
<u>3.00</u>						
	C053	Perimeter, Checkpoint firewall, Aladdin content filtering	19,000	19,000	21,000	
	C052	Perimeter, incoming mail filtering, Ironport	10,500	29,500	31,500	
	C054	Host, Symantec new anti-virus licenses	25,000	54,500	56,500	
	C055	Internal, Network access control	5,500	60,000	62,000	
	C056	SOC, software and professional service to maintain	19,000	79,000	81,000	
	C057	Host, Upgrade to Symantec Endpoint Security	10,000	89,000	91,000	
	C033	Install hall cameras	20,000	109,000	111,000	
	C039	Separate payroll processing of senior manager payroll	0	109,000	111,000	
	C041	Sarbox Fraud forum audits business processes for suspected fraudulent activity	0	109,000	111,000	
	C040	SAS70 certification of payroll service provider	0	109,000	111,000	
	C051	Internal, Imperva DB firewall	7,000	116,000	118,000	
	C008	SYS, Enforce policy of downloading and deployment of latest security patches for OS, database and Web server	5,000	121,000	123,000	
	C050	Perimeter, Fidelis XPS network DLP system, policy maintenance and monitoring	9,200	130,200	132,200	

C059 Network, VPN	21,600	151,800	153,800	
C049 Perimeter, IPS, Fortigate	20,000	171,800	173,800	
C058 Outsourcing support to network security	0	171,800	173,800	
C062 Security officer	80,000	251,800	253,800	35%

Plan 2008 (IT security operations+new acquisitions in Euro)

Step	CM	Countermeasure Name	<u>Current Risk</u> CM Cost	35% Step Cost	<u>Minimal Risk</u> Plan Cost	5.90% Risk
<u>1.00</u>						
	C025	Network DLP, Monitor unusual file transfers	4,000	4,000	4,000	32.90%
<u>2.00</u>						
	C034	Training, security awareness for employees and contractors	18,000	18,000	22,000	
	C023	Network DLP, Monitor acceptable usage violations, escalate to supervisors	4,000	22,000	26,000	
	C021	Network DLP, Alert on Web postings, produce weekly security metric by department	4,000	26,000	30,000	
	C020	AUP, establish procedure and enforce for insider disclosures	2,000	28,000	32,000	28.80%
<u>3.00</u>						
	C005	IDM, login accounts should be given the minimal rights that are necessary for their functionality	20,000	20,000	52,000	25.00%
<u>4.00</u>						
	C047	Endpoint, whole disk data encryption for notebooks used by field service techs	90,000	90,000	142,000	
	C046	Endpoint, removable device control	43,200	133,200	185,200	17%
<u>5.00</u>						
	C063	Internal, Imperva DB firewall, monitor unauthorized usage of production Oracle username(s)	4,000	4,000	189,200	
	C060	IDM, single signon identity mgmt system	60,000	64,000	249,200	
	C026	Training, workplace awareness	75,000	139,000	324,200	
	C009	SDLC,Enforce security code review	50,000	189,000	374,200	7.70%
<u>6.00</u>						
	C024	Network DLP, Detect unauthorized non-proxied end points, block or permit	4,000	4,000	378,200	6.70%
<u>7.00</u>						
	C045	Implement new source control system with better control and methodology	30,000	30,000	408,200	5.90%