



Israeli Security Trends 2006

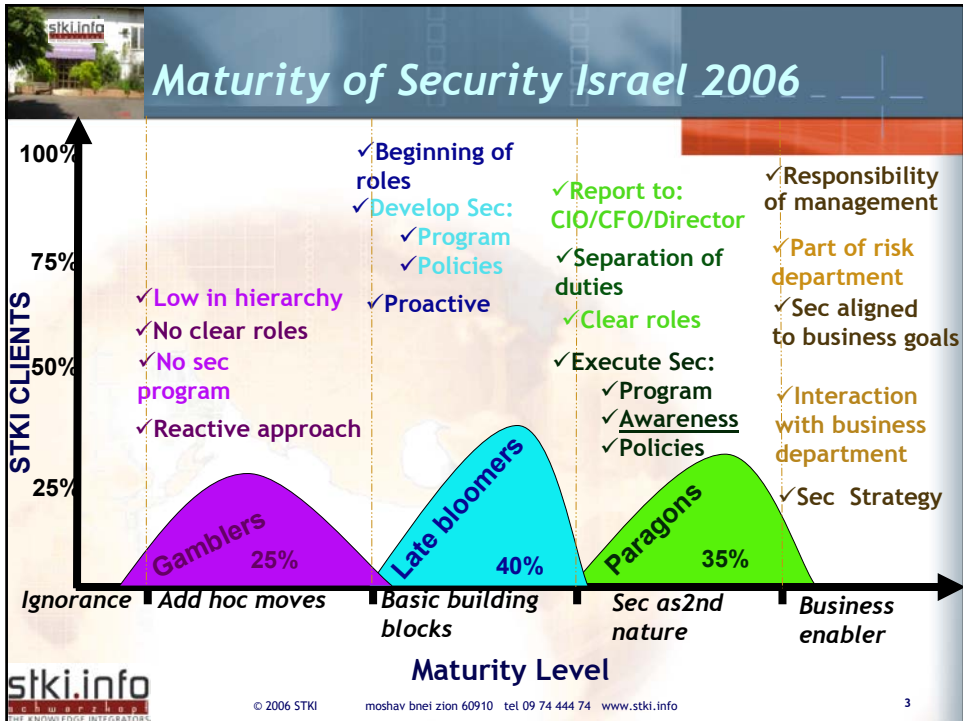
Michal Helman
Security & risk analyst
STKI
michal@stki.info



AGENDA



- ▶ Security Maturity
 - ▶ Perception, Structure Program, People
 - ▶ Compliance
- ▶ Security Management
 - ▶ Identity Management
 - ▶ Security Event Management
- ▶ Security Spending
- ▶ Web Application firewall - Latest events
- ▶ Information Leakage & End Point Admission Control



- ## Maturity of Security - Groups
- ▶ Gamblers (25%):
 - ▶ Smaller orgs
 - ▶ Non regulated sectors
 - ▶ Late bloomers (40%):
 - ▶ Larger orgs
 - ▶ Natural progression to harsh environment
 - ▶ Newly regulated (Insurance; health; SOX)
- © 2006 STKI | moshav bnei zion 60910 | tel 09 74 444 74 | www.stki.info | 4



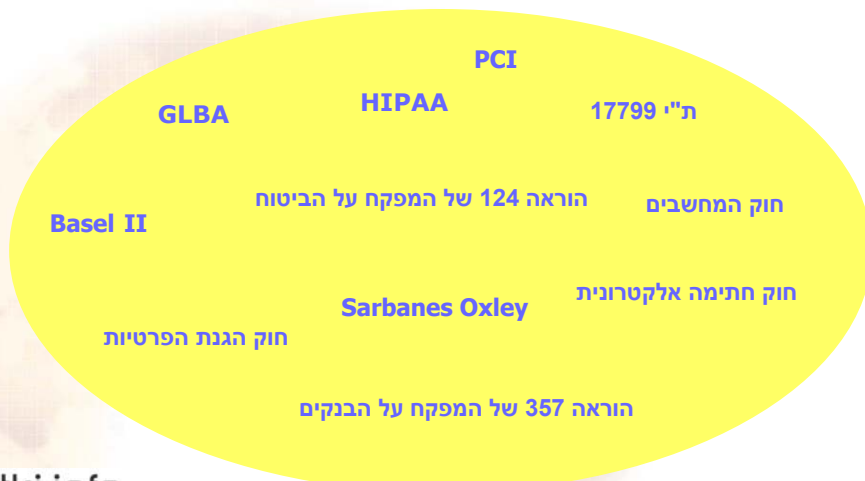
Maturity of Security - Groups

- ▶ Paragons (35%):
 - ▶ Larger orgs
 - ▶ Security oriented (Security;Financial;Hi-Tech;Telco)
 - ▶ Continuingly regulated (Financial; SOX; work abroad;health)
 - ▶ 2005 Trend - Awareness programs & initiatives



Maturity of Security - Compliance

Regulatory Environment





Maturity of Security - Compliance

- ▶ Elevates security from back office to business enabler
- ▶ Strongest trigger for security implementations (>60%)
- ▶ New segment - Compliance Sec Management
 - ▶ Orgs have earmarked resources to address compliancy issues
 - ▶ Security vendors (policy/configuration/event/identity & threat protection) with new/repositioned products that address compliancy issues



Compliance - SOX

- ▶ Designed to Improve investors confidence by making senior officers:
 - ▶ Accountable for financial report accuracy
 - ▶ Accountable for internal controls

SOX Applies to:

- ▶ US traded companies
- ▶ Governmental Companies: Agency for governmental companies (New)



Compliance - SOX

SOX Applies to:

- ▶ Banks/credit card companies: Bank controller (New)
 - ▶ Have Implemented S.302 “Corporate Responsibility for Financial Reports”
 - ▶ Beginning of S.404 Implementations



SOX - Impact on Security

- ▶ SOX is about integrity & availability of financial reporting data
 - ▶ ITGC - “Access to program & data”
- ▶ Elevates security to a boardroom issue
 - ▶ More security programs; policies; risk assessments ...
 - ▶ Defined roles & responsibilities; separation of duties



SOX - Impact on Security

- ▶ Drive for IDM/AM projects:
 - ▶ Role based authorization; deletion of ex workers
 - ▶ Beginning of 802.1x
 - ▶ Access management
- ▶ DB/Server hardening
- ▶ Increase in Encryption for transmitted/stored data:
 - ▶ SSL – More than 60%
 - ▶ PKI – Most "Late Bloomers" + "Paragons"

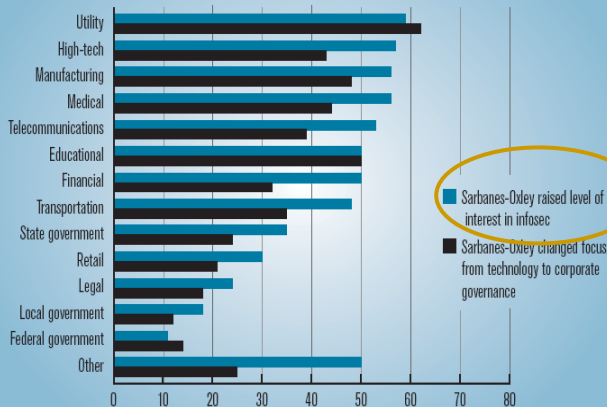


SOX - Impact on Security

2005
CSI/FBI
COMPUTER CRIME
AND SECURITY SURVEY

- ▶ "Program development"-
Secure coding
- ▶ Emphasis on physical security leads to convergence with info security

Figure 24. Impact of Sarbanes-Oxley Act on Information Security
Percentage of respondents that agree





Compliance: Regulations 357 & 124

- ▶ Sectors: Financial & Insurance
- ▶ Raises security to a BOD and CEO-level issue
- ▶ Mandates: Security program, CSO, Managerial risk assessments (MRA), Access control & strong authentication, Securing connectivity to web, BCP.



Compliance: Regulations 357 & 124

Trends

- ▶ Security programs/CSOs/MRA - Becomes the norm
- ▶ Sec Management continues - SIM/SOC; IDM/AM ...
- ▶ Increased in - Encryption; PKI; Strong authentication



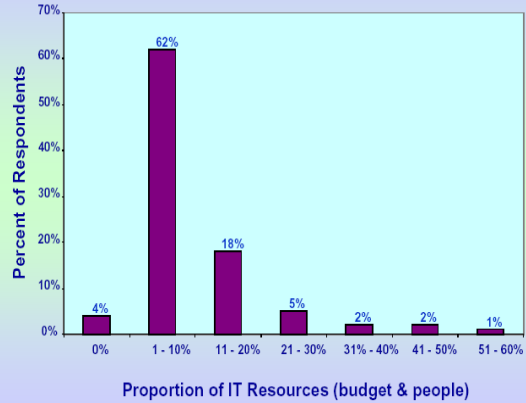


Risk & Security Spending

Butler Group
Datamonitor Company

- ▶ Users spending on risk:
2.5% - 4.5% of IT budget
- ▶ Difficult to estimate:
Security gradually becoming “invisible” - More Sec functions get embedded in network & Oss
- ▶ Risk Project Market:

IT Security Spending



2005		2006		2007
\$80	6.25%	\$85	8.24%	\$92



© 2006 STKI

moshav bnei zion 60910 tel 09 74 444 74 www.stki.info

15



Web Application Firewall (WAF)

2005/6 Activities

- ▶ Kavado Acquired by Protegrity (DB Security)
 - ▶ Provides support for Interdo - Probably for 1 more year
 - ▶ 2006 offer: Defiance
- ▶ Sanctum acquired by Watchfire
- ▶ F5 Technologies:
 - ▶ Acquired Magnifire - Basis for Trafficshield



© 2006 STKI

moshav bnei zion 60910 tel 09 74 444 74 www.stki.info

16



Web Application Firewall (WAF)

2005/6 Activities

- ▶ F5 Technologies:
 - ▶ Acquired AppShield's technology from Watchfire
 - ▶ Israeli branch offers free migration to TrafficShield
- ▶ Citrix acquires Taros: Leader in WAF
 - ▶ 2006: New player in Israel (by SCP)
- ▶ Imperva: Offers Integration into Radware (AppXcel)



WAF Israeli Market

2005 Deployments

- ▶ Kavado & Sanctum's acquisitions exploited by other players
- ▶ Confusion about replacing existing solutions
- ▶ Most deployments: Of Imperva (web; DB; web services)
- ▶ Some switch to F5
- ▶ Minority stay with Kavado
- ▶ Check Point's NGX users add Web Intelligence



WAF - Israeli Players

Company	Solution	Israeli representatives	Integrator
Citrix	Taros	SCP	Securenet; HP; Team
F5 Networks	TrafficShield	F5 Israel Networks Israel	Netvision; Artnet; 2BSecure; TrustNet; Team; Ness; NewAge; Malam; Spider; Securenet; IBM
Imperva	SecureSphere	Imperva	Ness; Bynet; NetVision; Spider; 2BSecure; We; Taldor; One/Xpert; Multi Layer Security; NewAge; Team
Protegrity	Interdo + Defiance	Kavado Israel	Protegrity support +to be determined



Management - Identity & Access Management (IDM/IAM)

- ▶ **IDM/IAM** are a set of solutions used to identify users in a system and control their access to resources by associating user rights & restrictions with the established identity.
- ▶ **IDM is accomplished by** user life-cycle management, reflecting the creation, maintenance, and deletion of identities
- ▶ **IAM is accomplished by** authentication, management & enforcement of access with various levels of granularity
- ▶ **IDM/IAM Features** may also include: SSO; web SSO and strong authentication solutions (smart cards; biometrics; tokens; PKI)





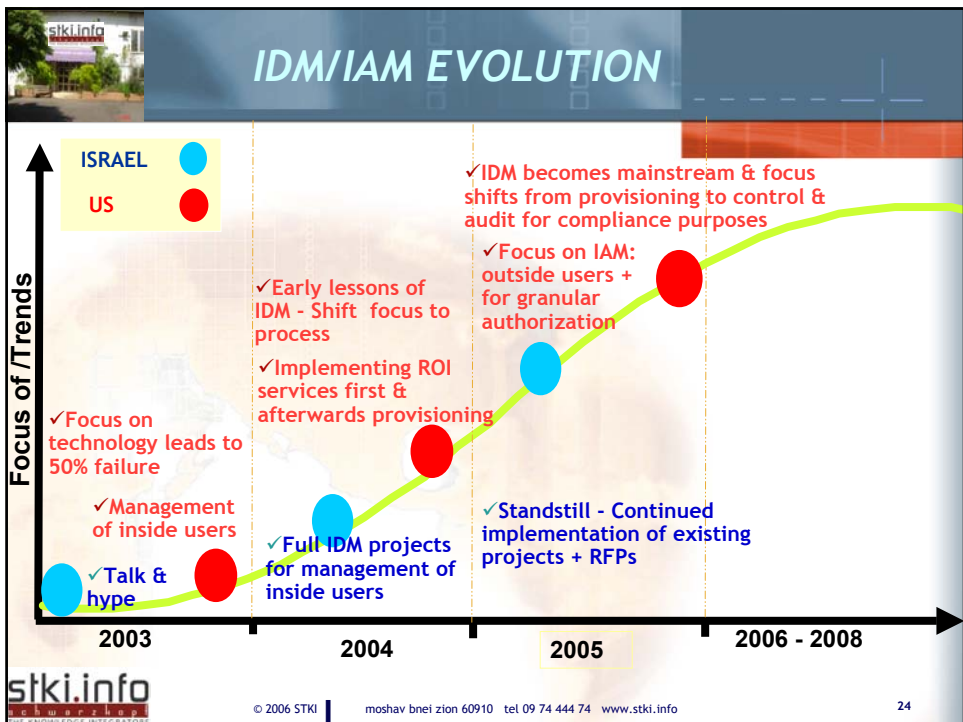
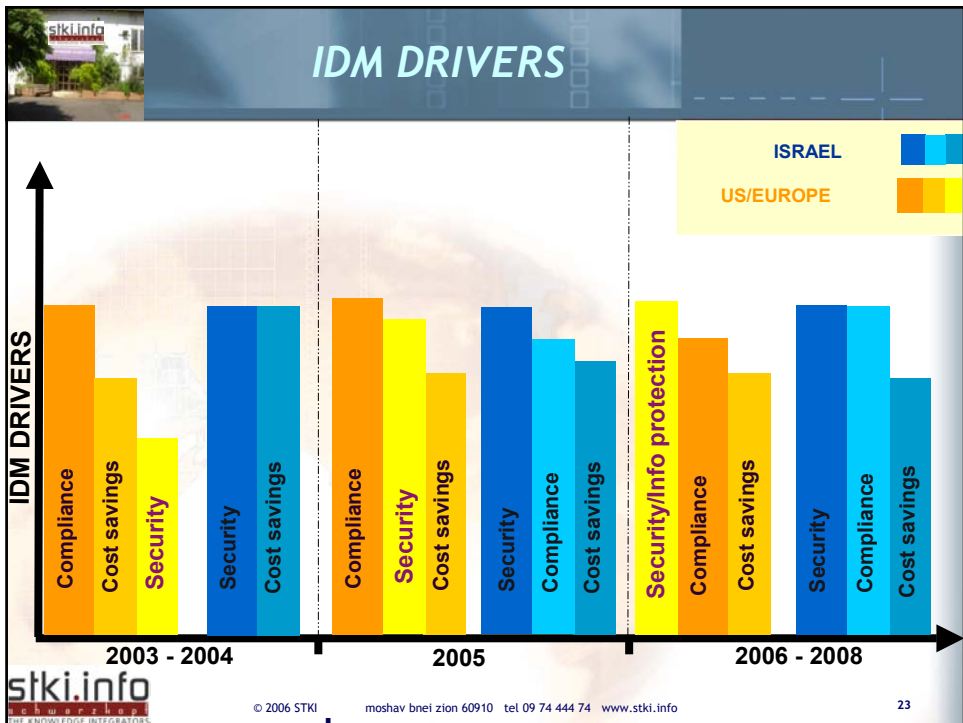
IDM - Services

- ▶ **User provisioning:** Creating, maintaining, and retiring user identities for access to IT systems and services
- ▶ **Modeling and mapping:** Using a management model (e.g., role-based) to efficiently map users to resources
- ▶ **Self-registration or self-service:** Delegating identity and editing down to individual user
- ▶ **Workflow:** Managing identity change-request approval processes



IDM - Services

- ▶ **Auditing, logging, and reporting:** Managing the necessary use of tools to track history of user life-cycle management steps, and reporting that information accurately
- ▶ **Password management:** Providing an administrative interface specifically for password policies, synchronization, and enforcement
- ▶ **Integration:** Using a “toolkit” such as a metadirectory service to link multiple identity sources together for easier updating





IDM/IAM Israeli Trends

Projects

- ▶ 2005 Stagnation:
 - ▶ IDM examined by orgs with little active steps
 - ▶ Standstill after the issuance of RFPs
 - ▶ Continuance of existing with virtually no new ones (Teva)



IDM/IAM Israeli Trends

Projects

- ▶ 2006 Awakening:
 - ▶ New IDM projects
 - ▶ Evolution towards WAM - Business motivation for maximum activities for clients



IDM/IAM Israeli Trends

Players

- ▶ Sun & CA position themselves as major players:
 - ▶ Successful projects this year
 - ▶ Important wins for 2006
 - ▶ Experienced partners
 - ▶ CA's leading offering for WAM



IDM/IAM Israeli Trends

Players

IBM & BMC lost their 2004 lead but improve:

- ▶ IBM:
 - ▶ TIM Express for SMBs
 - ▶ Tivoli SSO with Passlogic
- ▶ BMC acquired:
 - ▶ OpenDirectory & Calendra for better workflow
- ▶ M-Tech: Ness focuses on CA



IDM/IAM Israeli Trends

Players

- ▶ Novell:
 - ▶ Progress with IDM3
 - ▶ Continues work with Bynet & Malam
- ▶ Oracle: IDM as a strategic area:
 - ▶ Acquired: Oblix (extranet); Thor (provisioning); Phaos (development); OctetString(virtual directory)
 - ▶ Oracle Fusion IDM: Integrative solution by 2008
 - ▶ Till then: Offer current solutions



IDM/IAM Israeli Trends

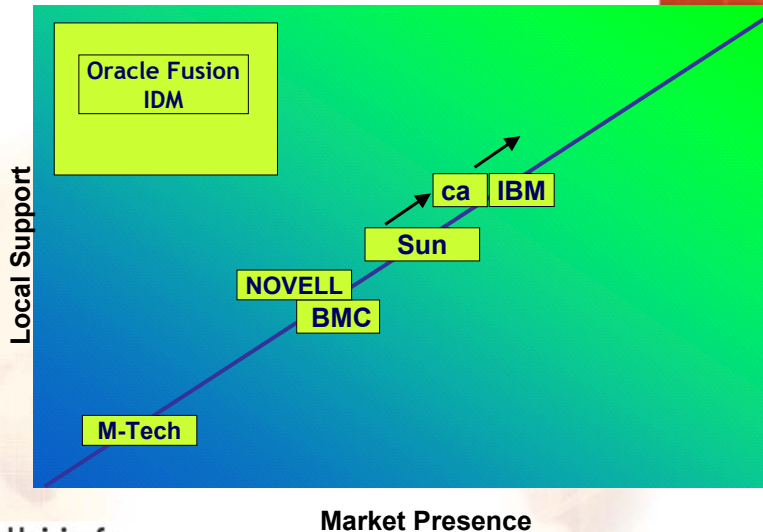


Consultants

- ▶ SECOZ- Experienced in IDM/IAM consulting projects
- ▶ PWC - Consulting experience abroad
- ▶ Comsec - 2006 - Professional services agreement for ca's projects in the UK
- ▶ Avnet; iTcon; KPMG - As part of ongoing security consulting
- ▶ Xor - Experience in integration & practical consulting




Israeli IDM/IAM Positioning 2005/6



IDM Israeli Players


Company	Solution	Israeli representatives	Integrator
BMC	CONTROL-SA	Matrix	Matrix, Xor
CA	eTrust IDM/AM suite (Netegrity)	CA Israel	Malam, Bynet, ,Datanin, Trustnet,Ness, Netcom
HP	Select Access	HP Israel	HP, Securenet
IBM	TIM/TAM	IBM Israel	IBM, Gita Technologies





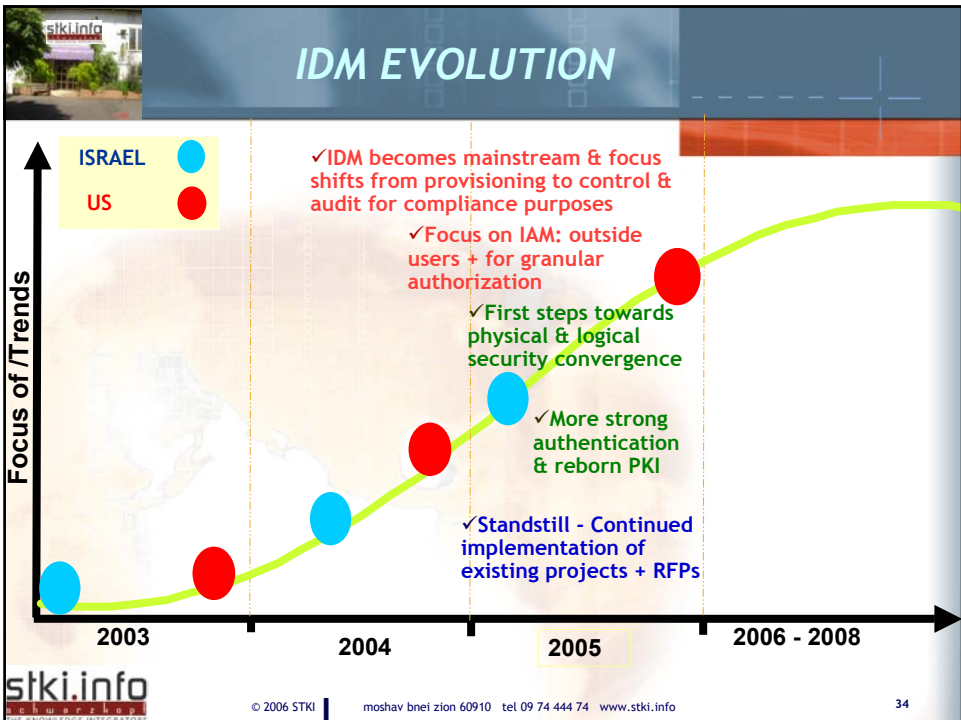
IDM Israeli Players

Company	Solution	Israeli representatives	Integrator
Microsoft	MIIS	Microsoft Israel	We, Xpert, Gita Technologies
M-Tech	M-Tech	Ness	Ness
Novell	Nsure Resources	Novell Israel	Bynet
Oracle Fusion IDM	Oracle Fusion IDM (Oblix, Thor, Phaos, Octetstring)	Oracle Israel	Gita Technologies, Xor
Sun	Identity Manager	Sun Israel	Xor, E & M, Malam



© 2006 STKI | moshav bnei zion 60910 | tel 09 74 444 74 | www.stki.info

33





Strong Authentication - Reborn Public Key Infrastructure (PKI)

2005
CSI/FBI
COMPUTER CRIME
AND SECURITY SURVEY

Smart Cards use Increased to 42%

- ▶ Vendors Landscape: Microsoft is dominating
- ▶ Sectors: Financial; Security; Health; Telco; Governmental
- ▶ Projects: Tehila; Magna; Bursa; Batei mishpat; Mapalei; Police...

Drivers

- ▶ PKI/Smart cards/Biometrics mature:
 - ▶ Infrastructure (login time = seconds)



© 2006 STKI

moshav bnei zion 60910 tel 09 74 444 74 www.stki.info

35



Strong Authentication - Reborn PKI

Drivers

- ▶ PKI/Smart cards/Biometrics mature:
 - ▶ Experienced integrators (Bynet; Gita; Securenet; Xor)
 - ▶ Price (free CA from W2K)
 - ▶ Biometrics more wide spread for convenience reasons-Improvement will follow



GDF ↓ .15 HJK ↑ 1.25 RTY ↓ 1.23 IOP ↑ .05 BNM ↑ 12.0 XCV ↑ .20 QEW ↓ .65



Convergence with physical security

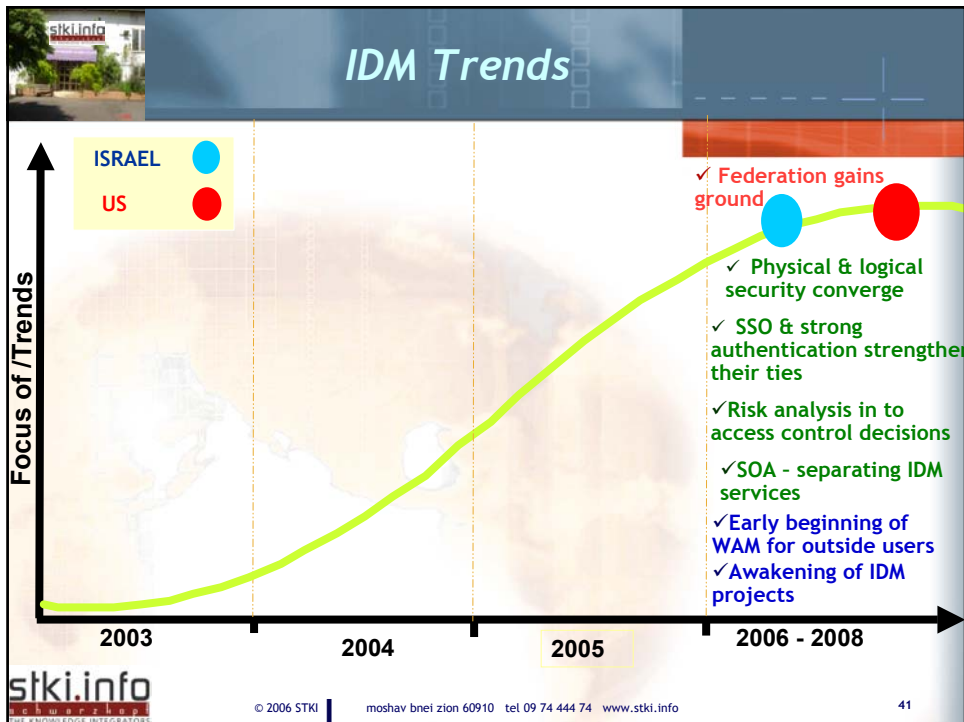
- ▶ Groups: Paragons
- ▶ Sectors: Financial; insurance; security; telco
- ▶ Drivers:
 - ▶ Maturation of security - Move outside of IT
 - ▶ Regulations & enhanced security
 - ▶ Cost saving



Convergence with physical security

Market Examples

- ▶ Technological convergence at different levels:
 - ▶ Smart “ID/employee” cards for logical/physical access
 - ▶ Correlating logical access with physical presence
- ▶ Ad hock cooperation: Awareness campaigns; IDM projects...
- ▶ Structured cooperation



Management - Security Event/Information Management (SIM)

Drivers

- ▶ Complexity & heterogeneity: Need for better & real-time awareness of internal & external threats for better mitigation
- ▶ Compliance: Need to monitor systems and report on security policy & compliance
 - ▶ 357: From “business transactions log saving” for accountability to - SIM Implementations
 - ▶ SOX- Monitoring business applications/transactions

Footer: stki.info | © 2006 STKI | moshav bnei zion 60910 tel 09 74 444 74 www.stki.info | 42

Management-SIM

SIM tools

- ▶ Aggregate & normalize data from many sources
- ▶ Core value is correlation for better assessment

Event →

- ▶ Focus on establishing a clear process
 - ▶ Choosing the technology - decision plays a minor role

stki.info
THE KNOWLEDGE INTERPRETER

© 2006 STKI moshav bnei zion 60910 tel 09 74 444 74 www.stki.info 43

SIM - Israeli Trends

Adopters

- ▶ Israeli market: Early adopters
- ▶ Features: Large orgs, regulated, complex infrastructure
- ▶ Groups:
 - ▶ 2005 - Paragons
 - ▶ 2006 - Late bloomers
- ▶ Sectors:
 - ▶ 2005 - Telco, financial & governmental
 - ▶ 2006 - Insurance, security & health

stki.info
THE KNOWLEDGE INTERPRETER

© 2006 STKI moshav bnei zion 60910 tel 09 74 444 74 www.stki.info 44



SIM - Israeli Trends

Security Operation Center (SOC)

- ▶ No structured SOC:
 - ▶ Requires large resources
 - ▶ Focus on technological deployment
- ▶ 2005:
 - ▶ Leveraging help desk and network controllers with escalations to CSO
 - ▶ No 24x7: Security team reviews periodically & responds



SIM - Israeli Trends

Adopters - SOC

- ▶ 2006: Richer & larger orgs - Paragons will focus on process:
 - ▶ Dedicated SOC team: reviews, responds & follows-up
 - ▶ SIM “clients” (InfoSec, physical sec, fraud, risk): respond & SOC team follows-up





SIM - Israeli Trends

Deployments & Players

- ▶ 2005 & 2006: Market continues to be busy
- ▶ CA (SCC): 2005 with 5 new projects; 2006: 6 more; Total of 17 deployments
- ▶ Arcsight: 8 deployments
 - ▶ We Consulting represents eIQ for SMBs
- ▶ IBM (Micromuse) acquired Gaurded.Net (3 deployments)
 - ▶ Ness focuses on CA



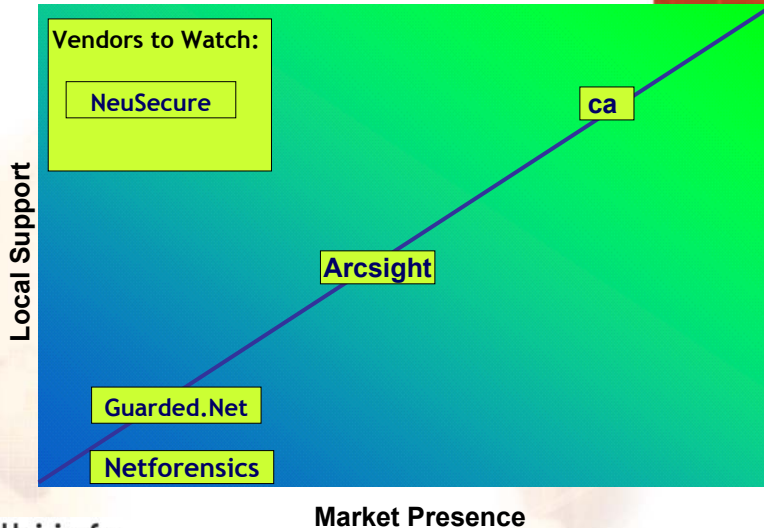
SIM/SOC Israeli Consultants

- ▶ SECOZ - Experienced in SIM/SOC consulting projects
- ▶ IPSEC - SIM/SOC consulting projects
- ▶ PWC - Consulting experience abroad
- ▶ Comsec - 2006 - Professional services agreement for ca's projects in the UK
- ▶ ITcon; Avnet - As part of ongoing security consulting





Israeli SIM Positioning 2005/6



SIM - Israeli Players

Company	Solution	Israeli representatives	Integrator
ArcSight	ArcSight	We Consulting	We Consulting
CA	eTrust Security Command Center	CA Israel	Malam, Bynet, Datanin, Trustnet, Ness, Netcom
IBM acquired Micromuse	NeuSecure (as part of Tivoli)	IBM	Head On + to be determined





SIM - Trends

- ▶ Small market: Around \$250m during 2005; Expected growth to \$600m in 3 years
- ▶ Fragmented: No real dominator:
 - ▶ Leaders: CA, ArcSight, netForensics, Intellitactics, e-Security and Network Intelligence



SIM - Trends

- ▶ Fragmented:
 - ▶ Expected consolidation as market matures
- ▶ 2006-7: Consolidation with Endpoint security solutions to identify and act promptly on specific endpoint threats (netForensics & InfoExpress)





Information Leakage (IL)

Drivers

- ▶ Regulations demand for:
 - ▶ Strong protection of sensitive info
 - ▶ Notification of compromised data
- ▶ Non compliance may result in:
 - ▶ Substantial fines, civil lawsuits & executive liability



Figure 1: Recovery Cost Averages



2005: Data breach announcements resulted in the notification of more than 50 million customers



Information Leakage (IL)

2005

CSI/FBI
COMPUTER CRIME
AND SECURITY SURVEY

Drivers

- ▶ Loss of investor and customer confidence & damage to brand name & company's reputation

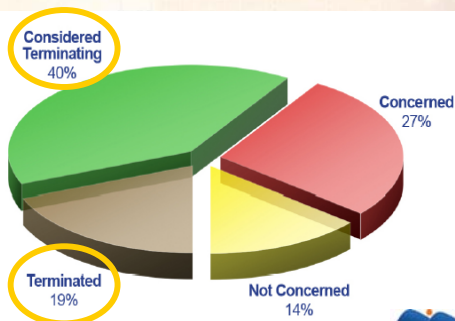
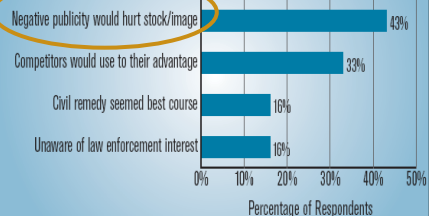


Figure 5: Customer Turnover Impact



Figure 22. Reason Organization Did Not Report the Intrusion to Law Enforcement

Percentage of Respondents Identifying as Important



CSI/FBI 2005 Computer Crime and Security Survey
Source: Computer Security Institute

2005: 423 Respondents



Information Leakage (IL)



Drivers

- ▶ Expanding perimeter due to the constant change in the corporate environment:
 - ▶ Blurred boundaries between insider & outsider: Network access to: consultants, outsourcers, business partners, customers, and other visitors
 - ▶ Mobility of information:
 - ▶ Employees work from: home, cafe's, clients' sites ...
 - ▶ Use of laptops for both inside & outside the org

Checkpoint current strategy: Focus on Internal Security



Information Leakage (IL)

Drivers

- ▶ Expanding perimeter due to the constant change in the corporate environment:
 - ▶ Mobility of information:
 - ▶ Use of detachable devices: USB; CD; corporate & self-owned smart phones & PDAs
 - ▶ Extensive use of email, messaging (IM) and P2P, inside & outside the org
 - ▶ The rise in sophisticated social engineering, ID thefts and phishing attacks



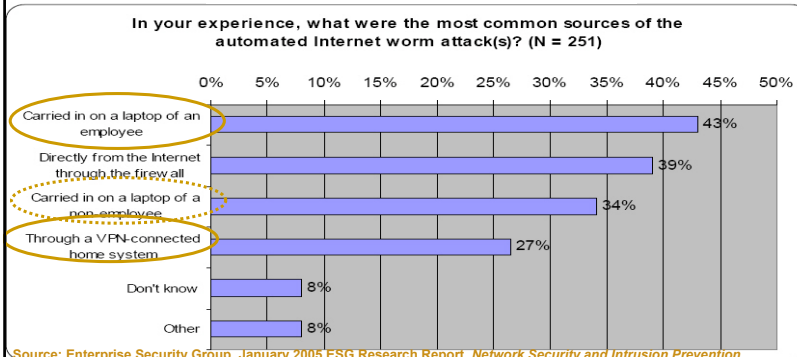
Information Leakage (IL)



The Internal threat

2005 Losses from insider abuse: \$6,856,450

- ▶ 70% of info leaks are unintentional or accidental - “Oops syndrome”, Trojan affair
- ▶ 80% of all security-related losses come from internal parties



Types of incidents & sensitive info

Sector	Sensitive Content	Information Leak Incident & related (prevented) damage
Government/ Financial	Financial statement; Business reports	<ul style="list-style-type: none"> ▶ Secretary had mistakenly sent classified customer integrated into a document template ▶ Cost: Reputation damage, violations of SOX rules
Teleco	Customer data; Marketing plans	<ul style="list-style-type: none"> ▶ Customer records sent to Russia ▶ Legal actions taken against employee connected to fraud network
Teleco	Customer Data; Business plans	<ul style="list-style-type: none"> ▶ Customers credit cards information distributed without encryption ▶ Internal user had intentionally leaked marketing information to competitors ▶ Cost: PCI violations, marketing program ruined
Teleco	Marketing plans; Business plans	<ul style="list-style-type: none"> ▶ Marketing information was sent by insiders to their next employer ▶ Cost: Marketing program ruined



Information Leakage - Controls (ILC)

▶ Type of ILC will depends on:

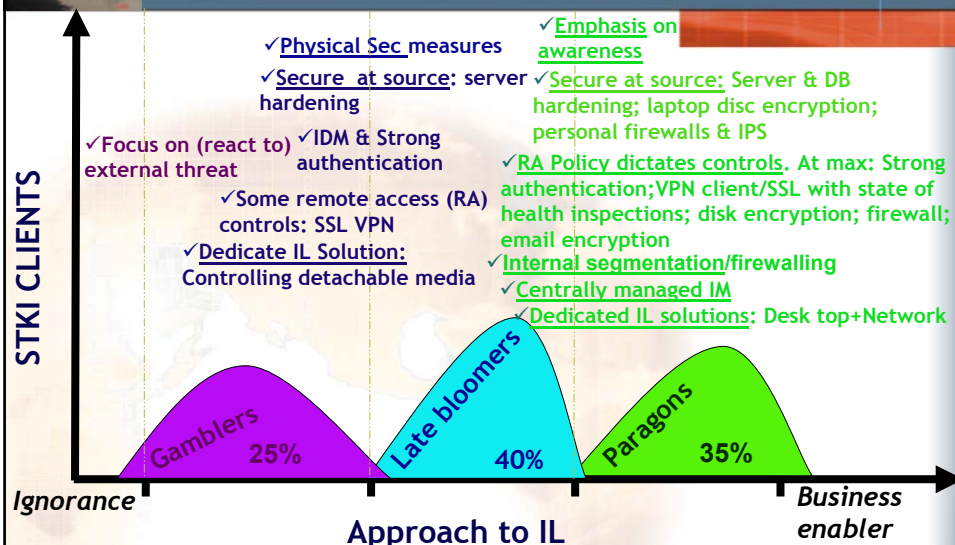
▶ Where:

- ▶ Is the info stored? Servers, DBs in LAN, laptops, disk on keys, smart phones...
- ▶ Is it accessed from? Home, café, clients site...

- ▶ Channel of delivery: Email (Orgs; free web mail IM, fax, HTTP, FTP, P2P...



ILCs used by Israeli Orgs





Dedicated ILCs - Network based

- ▶ Traditional content filtering tools for outbound content:
 - ▶ SCM packages: Symantec/ McAfee; CA; Trend...
 - ▶ Very limited effect

Network Dedicated ILCs

- ▶ Proxy/Sniffer near firewall
- ▶ Market largest growth in 2005 & is expected to multiply to \$40M (or more) in 2006



Dedicated ILCs - Network based

Evaluation Parameters

- ▶ Recognize unstructured on top of structured data (fingerprint)
- ▶ Cover maximum network channels (email;HTTP;IM;fax...)
- ▶ Accuracy: For minimum false positives/negatives
- ▶ Reporting & audit - For compliance
- ▶ Scalability: Shouldn't affect performance





Dedicated ILCs - Desktop



- ▶ Secure Delivery - Encryption of DOK; Laptops; PDAs...
 - ▶ Players (Enterprise level management) - Reflex Magnetix; M-systems (M-Trust)Utimaco;Pointsec; Aliroo; Securewave (2006)

Controlling Detachable Devices (CDD)

- ▶ Monitors & bocks info leakage from DD
- ▶ Based on agents installed in to operating systems (kernel)

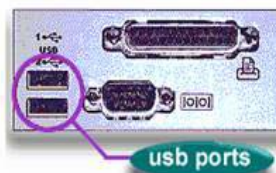
60% of sensitive data is stored on unprotected end points



Controlling Detachable Devices

Evaluation Parameters

- ▶ Granularity level (file; user...)
- ▶ Anti tampering
- ▶ Scalability
- ▶ Directory integration
- ▶ Audit & reporting
- ▶ Real time operation
- ▶ Mobile user support





Dedicated ILCs - Israeli Market

- ▶ 2005 - Increase in deployments which will continue in 2006

Adopters

- ▶ Late Bloomers: DD ILCs ((Security & army obligated to lock)
- ▶ Paragons: Also Network based

Network based Vendors

- ▶ PortAuthority (Vidious) - 7 implementations
 - ▶ Blocks Faxes & internal email IL



Dedicated ILCs - Israeli Market

Network based Vendors

- ▶ Fidelis - 3 implementations
- ▶ Onigma (2) - Overall blocking (email... + DD)

Desktop based vendors

- ▶ ControlGuard:
 - ▶ Largest installed base (More than 15)
 - ▶ Integration with CA's SCC & OEM with M-Systems





Dedicated ILCs - Israeli Market

Desktop based vendors

- ▶ Securewave: Encryption of downloaded files & full disk (end of 2006)
- ▶ Safend - Chosen by financial orgs. Promising roadmap
- ▶ Reflex Magnetics: Established company; Also does DOK Encryption
- ▶ Devicelock (Ecora) - Hardly a player
- ▶ Lambda (Sentinal) - Closed



ILCs - Established Vendors

- ▶ Microsoft:
 - ▶ Vista - Better control over DD in GPO
 - ▶ Rights Management Server (RMS):
 - ▶ Allows users to build access and distribution rights into documents and email messages
 - ▶ Not viewed as a full blown IL solution - Mainly for email inside org
 - ▶ More pilots & some deployments



ILCs - Established Vendors

- ▶ CA - eTrust integration with ControlGaurd

CDD As part of End Point Admission Control (EPAC):

- ▶ Symantec: Sygate blocks DDs
- ▶ Check Point: As part of Integrity by next year
- ▶ McAfee: As part of NAC by next year



EPAC - Israeli Market

- ▶ 2005: Beginning of 802.1x implementations
 - ▶ Requires authentication for network access
 - ▶ More PKI than User name & Password
 - ▶ Migration isn't easy: Switch, radius, CTA agent, architecture...



EPAC - Israeli Market

Orgs compliment with EPAC packages:

- ▶ State of health inspections
- ▶ Policy enforcement: Block, Quarantine, VLAN for patching
- ▶ Personal IPS & Firewall & application firewall
- ▶ ILC for DDs (Sygate; 2007)



EPAC - Israeli Market

EPAC Packages - Deployed Solutions:

- ▶ Symantec (Sygate) - Most deployed
- ▶ Check Point (Integrity/ZoneLab)
- ▶ McAfee (NAC): Doesn't require 802.1x
- ▶ 2006-8: Growing migration to 802.1x will accelerate EPAC deployments



Information Leakage - Trends

- ▶ 2005: Emphasis on blocking due to compliance requirements
- ▶ 2006-2007:
 - ▶ Controlling IL for internal email (Port Authority for Lotus; Exchange)
 - ▶ Expected integration between Network & Desk Top ILCs

Forecast



Information Leakage - Trends

2006-2008 - Expected Integration of ILCs with:

- ▶ End point security packages (Symantec; McAfee; CA)
- ▶ Secure email solutions for automatic encryption routing or quarantine (PGP & PortAuthority)
- ▶ IDM solutions- preventing sensitive info leakage from trusted insiders
- ▶ Network security offering - Additions to NAC...
- ▶ SIM Solutions (CA's SCC with ControlGuard)

Forecast



IL Controls - Israeli Players

Company	Israeli Representative	Solution	Coverage	Integrator
Control Gaurd	Control Gaurd	End Point Access Manager	Host	One; Spider; 2BSecure; ArtNet; CoreBiz; ICT
Ecora	Integrity	DeviceLock	Host	Integrity
Fidelis	Fidelis - Dany Liberman	Fidelis datasafe	Network	Fidelis + to be determined
Onigma	Onigma	Onigma	Network + Host	To be determined



IL Controls - Israeli Players

Company	Israeli Representative	Solution	Coverage	Integrator
Reflex Magnetics	BeSecured	Disknet Pro	Host	Team; Trustnet; 2BSecure; SecondWave Solutions
Safend	Safend	Safend Protector	Host	Xor
SecureWave	TrekIT	Sanctuary platform	Host	Ness; We; NewAge
Vidious	Vidious	PortAuthority	Network	Bynet; Netvision; We; Comsec



Thank You!