Information Security Governance & Compliance

Assessment Essentials:

Strategies for Staying Current with Technology

Douglas Brown – CISM, CISSP,
Security Solutions Architect
HP Security and Risk Management
HP Services

Instructional objectives

- Share enabling technologies taxonomy as it applies to the P^5 Model
- Familiarize one's self with common technologies encountered during security engagements
- Understand HP's security product portfolio
- Understand HP's strategy in selecting and aligning with 3rd party partners
- Know where to go for "quick" education on security tools

Agenda

- Assessing technology controls
- Technology types
- Emerging technologies
- Enabling technologies
- Applying enabling technologies
- HP security technologies
- Consultant resources
- Security technology predictions
- Breakout

Assessing Technology Controls

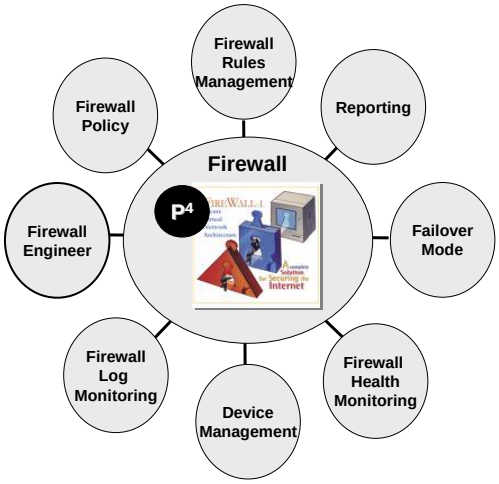
Assessing technology controls

- Role and responsibility
  - Understand technology in place to manage/mitigate threats
    - Why are they using it?
    - How are they using it?
    - How could they use it better?
  - Recognize that you won't know every technology in use
    - Clients expect us to know every single tool as an expert
    - Use probing questions to mask lack of awareness of a particular technology

Technology ecosystem

What to observe?

- What product is used?
- How is it used?
- How is it supported?
- How is it managed?
- What end products are produced?
- How is it documented?
- Is it operationalized?
- What's its success track record?
- Does the technology introduce new threats?



What drives technology decisions?

- Legal/regulatory requirements
  - SOX-compliant tools?
- Analyst reports
  - Burton, Gartner, etc.
- Previous product experience
- Aggressive sales pursuits

5/25/2007 7

Technology Types

General

- Hardware
  - Appliances
  - Firmware
  - Functionality (baked-in security)
- Software
  - 3rd party (COTS)
  - Open source
  - Primary vs. secondary applications
- Services
  - Hosted
  - Managed
  - Outsourced

Where will you encounter security products & tools?

Hardware

- Appliances
  - Stand-alone solutions
    - firewall
  - Integrated approaches
    - Firewall, IDS/IPS, content filtering
- Firmware
  - Embedded security functionality
    - HP Protect Tools
      - TPM chip
- Functionality
  - Baked-in security
    - IEEE, ISO standards
  - Bolted-on
    - Aftermarket

Software

- 3rd Party (COTS)
  - General commercial products
    - HP, Symantec, etc.
  - Open source-based COTS products
    - Guardian Digital, Inc.
  - Product assurance-rated products
    - TREP, FIPS, NIAP, DIAP Common Criteria
- Free range products
  - Freeware products
  - Shareware products

  http://www.snapfiles.com
  - Open source developed
    - Dragon, SNORT, etc.
- Primary vs. secondary functionality

OEM vs. Private Labeling

Services

- Hosted Security Service Provider (HSSP)
  - Generally single stack solution oriented
    - Secure e-mail, secure websites
      - IronPort, MessageLabs, SurfControl
- Managed Security Services Provider (MSSP)
  - Security operations centers
    - IDS monitoring, firewall rules management, SPAM filtering
      - IBM (ISS), SecureWorks, Symantec, etc.
    - Customer Premise Equipment (CPE)
- Managed Services Providers (MSP)
  - Generalist who bundles security offers from OEMs
    - AT&T, HP, BellSouth, etc.

Emerging Technologies

2007 – 2010 trends

- End-point devices, users, web applications will draw the most enemy fire
- The hardened perimeter will be replaced by more effective distributed secured control points
- Vendors will offer many reactive solutions, but customers will create more proactive, information-centric security architectures
- Organizations will spend more on privacy, but fall further behind and experience more data breaches

5/25/2007 14

2007 to 2010 trends – contd.

- Key business trends
  - Dollar signs dominate attacks
  - Compliance programs meet increasing regulatory complexity
- Key technology trends
  - "Perimeters" = strategic, business-driven, control points
  - Declaring war on the false positive
  - Information centrism – security as a core aspect of the information management lifecycle
  - Getting proactive
    - Planning, architecture, and process
      - Work with and understand the business
      - Business continuity and incident response plans
      - De-siloization: share information, share intelligence

2007 to 2010 trends – contd.

- The most successful businesses will address compliance proactively
  - Involve the legal team early and intimately
  - Think of compliance processes as core business activities, not annoying add-ons. Goal of compliance processes is to achieve:
    - **Transparency**: the organization needs to know who did what, when, and why
    - **Integrity**: the organization needs to ensure that its processes are followed faithfully and timely
    - **Accountability**: the organization's records need to have sufficient evidentiary value to allow third parties to discover facts and allocate rewards and penalties accurately
  - Include compliance in enterprise architecture
    - "control down, validate up"
  - Change compliance processes slowly; rules may change as quickly as necessary
    - discretionary rules support compliance with the business' own policies
    - non-discretionary rules support compliance with regulations

2007 to 2010 trends – contd.

- "Run to the repository" or "data dis-aggregation"?
  - Two countervailing trends emerging at the same time
    1. E-discovery, audit evidence requirements, and explicit regulations require long-term storage and archival of data
       - Therefore, enterprises may increase information centralization in order to aid content protection and control
       - This is borne out by Microsoft's strategy with Office 12 / SharePoint
    2. On the other hand, massive amounts of ubiquitous data are created, copied, and used at disparate endpoints
       - Therefore, enterprises may tighten controls over information stored and managed on user systems and points of data extraction
       - This is borne out by acquisitions of rights management solutions and endpoint-control products; plus, aforementioned use of encryption

2007 to 2010 trends – contd.

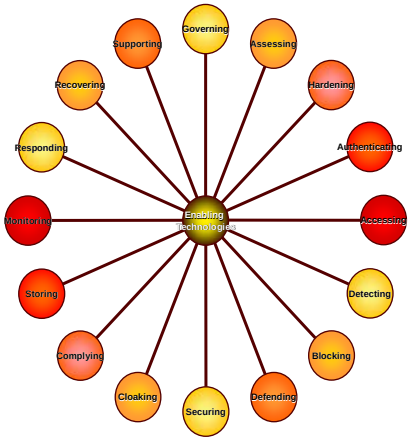
- "Content is king" (It's about the data, dummy)
  - Security teams have moved beyond simple infrastructure protection
    - "Which traffic can touch which systems?" isn't adequate
    - Goal: "Who can perform what actions on which type of information?"
  - Content protection is getting deeper and tighter
    - Deeper = more layers for prevention and detection
    - Tighter = protection closer to the useful data
  - The proactive enterprise should "seek … and find"
    - Start the process of assessing information resources: until you know what you have, information-centric protection can't work
    - Use tools, but engage the business
      - Realize that "we need data everywhere, always, forever" won't work

Enabling Technologies

OSI model defines enabling technologies

OSI Model
7 – Application
6 – Presentation
5 – Session
4 – Transport
3 – Network
2 – Data Link
1 – Physical

ISO 7498-2 Security Layer Model
7 – Authentication
6 – Access Control
5 – Non-Repudiation
4 – Data Integrity
3 – Confidentiality
2 – Assurance / Availability
1 – Notarization / Signature



OSI security layer map

OSI Layer Model:	ISO 7498-2 Security Model[1]:	Vulnerabilities:	Layer Controls:
7 – Application Layer: Specifies distributed client/server applications	Authentication	· Backdoors · Weak authentication	· Application vulnerability scanning · Secure coding standards (SDLC) · Host-based firewalls / IDS
6 – Presentation Layer: Specifies protocols for translating data format	Access Control	· Buffer overflows	· Secure coding standards
5 – Session Layer: Specifies protocols for starting and ending a communications session across a network	Non-Repudiation	· Brute force attacks · Session spoofing / hijacking	· Data-in-motion encryption · Secure FTP · Encrypted password exchange
4 – Transport Layer: Specifies protocols for end to end error control	Data Integrity	· TCP / UDP exploits · Fingerprinting / enumeration	· Firewalls · Router controls
3 – Network Layer: Specifies protocols for routing messages:	Confidentiality	· Packet spoofing · ID address/ route spoofing	· Firewalls · IPSEC · Router filtering
2 – Data Link Layer: Specifies protocols for point-to-point transmission and error control	Assurance / Availability	· Promiscuous mode sniffing · Wireless hacking / interception	· MAC address filtering · Secure network design · WEP
1 – Physical Layer: Specifies protocols for transmission of data over physical media	Notarization / Signature	· Denial of Service (DoS) · Physical theft	· Biometric authentication · Data storage encryption

Enabling technology taxonomy

Governing technologies

P⁴ Taxonomy

Description: Products or services that automate INFOSec program functions related to organizing security teams, reporting program status, training personnel, increasing awareness, and developing policies and procedures.

- Security policy builders
- On-line security training programs
- Dashboard creation tools
- INFOSec organization designer
- Security screensavers/logon messaging
- Security newsletters, posters, art

Examples

Category:	Product:	Vendor:	URL:	Resource Corner:
INFOSec Policy Builder *(Automated security policy creator / manager)*	DynamicPolicy	Zequel Technologies, Inc.	http://www.zequel.com	· **Governance Assessment Tool** - http://www.educause.edu/ir/library/pdf/SEC0421.pdf · **CERT: Governing for the Enterprise Portal** – http://www.cert.org/governance/ · **Governance Reference Desk** – **SearchSecurity.com** - http://searchsecurity.techtarget.com/topics/0,295493,sid14_tax303590,00.html?asrc=SS_CLA_303590&psrc=CLT_14 · **Google** – http://directory.google.com/Top/Computers/Security/Policy/ · **Wikipedia** – http://en.wikipedia.org/wiki/Security_awareness
Dashboard / Metrics Reporting *(Dashboard creation software)*	Dash Portal	MarvelIT, Inc.	http://marvelit.com	
Awareness Training *(On-line training system)*	SecurIT Savvy	Terra Nova Training, Inc.	http://www.securitsavvy.com	
INFOSec Organization Creator *(Job descriptions, organization structures, mission statements)*	InformationShield	Information Shield, Inc.	http://www.Informationshield.com	
Awareness Messaging *(Screen savers / logon messaging)*	Visible Statement	Green Idea, Inc.	http://www.greenidea.com/	
Awareness Messaging *(News letters, art, posters, logos)*	Various	The Security Awareness Company	http://www.thesecurityawarenesscompany.com	

Assessing technologies

P⁴ Taxonomy

Description: Products or services that determine an INFOSec program's readiness and completeness through the use of scanning, penetration, hacking, configuration, and validation tools and technologies. Assessing can be applied to every component of an INFOSec program.

- Configuration / compliance
- Code analyzers (source/binary)
- Firewall rule analyzer
- Penetration testing tool sets
- Port/network scanners
- Vulnerability scanning

Examples

Category:	Product:	Vendor:	URL:	Resource Corner:
Code Analyzer *(Review application code for security flaws and bugs)*	Fortify Suite Ounce Audit	Fortify Software Inc. Ounce Labs, Inc.	http://www.fortifysoftware.com http://www.ouncelabs.com	·**SecurityPark Research Libary: Authentication White Papers** - http://securitypark.bitpipe.com/rlist/term/Vulnerability-Assessments.html ·**Top 100 Network Security Tools** – http://sectools.org/ ·**NIST: ASSET 2.0 Self Assessment Tool** – http://csrc.nist.gov/asset/index.html ·**TechRepublic: Assessment Reference Desk** – http://search.techrepublic.com.com/index.php?c=1&q=security+assessment ·**Wikipedia** – http://en.wikipedia.org/wiki/IT_security_assessment
Firewall Rules Analyzer *(Validate and manage firewall rules)*	AlgoSec Firewall Analyzer	Algorithmic Security, Inc.	http://www.algosec.com/	
Security Configuration Analyzer *(Validate and assure adherence to configuration baselines)*	NetIQ Secure Configuration Manager	NetIQ Corporation	http://www.netiq.com	
Port Scanning *(Reconnaissance and network mapping)*	Nmap	Opensource	http://insecure.org/nmap	
Vulnerability Scanning *(ASP solution or tool for discovering and detecting vulnerabilities)*	QualysGuard	Qualys, Inc.	http://qualys.com	

Hardening technologies

P[d] Taxonomy

Description: Products or services used to make systems exceedingly difficult to compromise. Hardening includes removing or disabling unnecessary services, maintaining current patch levels, closing network ports, and using scripts to deactivate unnecessary features in configuration files.

- Hardening scripts
- Patch management systems
- Secure coding

Examples

- TCP/IP stack hardening tools
- WLAN hardening tools
- Web server hardening tools

Category:	Product:	Vendor:	URL:	Resource Corner:
Application Hardening *(Harden executables, registry entries, services, etc.)*	TSX-Protection Pack	OPSWAT, Inc.	http://www.opswat.com	·**CIS Hardening Benchmarking Tools** - http://www.cisecurity.org/bench.html ·**CERT: Secure Coding Guidelines** - http://www.cert.org/secure-coding/ ·**NSA Hardening Scripts** - http://iase.disa.mil/stigs/index.html ·**Wiki: Freeware Hardening Tools** - http://wiki.castlecops.com/Lists_of_freeware_hardening_tools ·/ ·**Wikipedia** – http://en.wikipedia.org/wiki/Hardening
OS Hardening Scripts *(Harden operating systems)*	C&I Security Practice Hardening Service	Hewlett-Packard Company	http://www.hp.com/security	
Patch Management Systems *(Ensure hardware / software is patched at most current levels)*	PatchLink Update	PatchLink Corporation	http://www.patchlink.com	
TCP/IP Stack Hardening *(Lockdown registry and configuration settings)*	Zigstack	Beyond Security, Inc.	http://xaitax.de/bin/full/zigstack_v4.rar	
WLAN Hardening *(Build and harden secure wireless networks)*	Enterprise	AirMagnet, Inc.	http://airmagenet.com	
Web Server Hardening *(Lockdown web services)*	Syhunt™ Apache/PHP Hardener	Syhunt Technology	http://www.syhunt.com	

Authenticating technologies

P[d] Taxonomy

Description: Products or services used to authenticate and grant access to users of IT assets and resources. Authentication services include access control, identity management, and entitlement/privilege management.

- Authentication (N+)
- Authorization

Examples

- Identity management lifecycle
- Entitlement management
- Role Based Access Control (RBAC)

Category:	Product:	Vendor:	URL:	Resource Corner:
Entitlement Management *(Fine grain application access based on roles and authorizations)*	Entitlement Management Solution (EMS)	Securent, Inc.	http://www.securent.net	·**Microsoft TechNet: Authentication Discussion** – http://technet2.microsoft.com/WindowsServer/en/library/78cb5d3c-d0b2-4d20-a693-fa66bde1a63b1033.mspx?mfr=true ·**Sender Authentication Working Group White Paper** – http://www.openspf.org/blobs/sender-authentication-whitepaper.pdf ·**SecurityPark Research Libary: Authentication White Papers** - http://securitypark.bitpipe.com/rlist/term/Authentication.html ·**Wikipedia** – http://en.wikipedia.org/wiki/Security_awareness
Identity Management & Account Provisioning *(Identity life cycle management)*	OpenView Select Identity	Hewlett-Packard Company	http://www.hp.com/security	
Directory Role Assigning *(Identify and assign identity roles to AD users)*	LANShield	ConSentry Networks, Inc.	http://www.consentry.com	
Role Mining & Creation *(Role Based Access Control "RBAC" modeling)*	Eurekify Sage ERM	Eurekify, Ltd.	http://www.eurekify.com	
Multifactor Authentication *(Token-based multifactor authentication device)*	ASAS	Authenex, Inc.	http://www.authenex.com	

Accessing technologies

P⁴ Taxonomy

Description: Products or services used to authenticate and grant access to users of IT assets and resources. Authentication services include access control, identity management, and entitlement/privilege management.

- Card access control
- Remote access
- Single Sign-on
- Identity management lifecycle
- Entitlement management
- Role Based Access Control (RBAC)

Examples

Category:	Product:	Vendor:	URL:	Resource Corner:
Single Sign-on Access Control *(Enterprise single sign-on/reduce password access)*	v-GO Single Sign-On	Passlogix Inc.	http://www.Passlogix.com	·**BitePipe Access Control White Papers -** http://www.bitpipe.com/rlist/term/Access-Control.html ·**SecurityPark Research Libary: Authentication White Papers -** http://www.securitypark.co.uk/newsbycategory.asp?categoryid=8&title=Access%20Control ·**Wikipedia** – http://en.wikipedia.org/wiki/Security_awareness ·**ZDNet White Papers on Access Control** - http://whitepapers.zdnet.com/search.aspx?tags=access+control
Facility Access Control *(Card Access Control System)*	IdentityDefender	Lenel Systems International, Inc.	http://www.lenel.com	
Network Admission Control (NAC) *(End point scanning prior to granted access, infected end points quarantined)*	Network Admission Control (NAC)	Cisco Systems Inc.	http://www.cisco.com	
Token Access Control Devices *(Limit password use by replacing them with tokens)*	Secureid	RSA Security, Inc.	http://www.rsasecurity.com	
Single/Reduced Sign-on *(Reduced password usage and self-self password resets)*	OpenView Select Access	Hewlett-Packard Company	http://www.hp.com/security	

Detecting technologies

P⁴ Taxonomy

Description: Products or services that detect altered state conditions or violations in security policy that could lead to security breaches. Products also restrict access to unauthorized web sites, mis-configured systems, and the presence of illegal software applications.

- Illegal Web site access detection
- Configuration vulnerability detection
- File state alteration detection
- CMDB change management
- Patch level confirmation
- Greynet application detection

Examples

Category:	Product:	Vendor:	URL:	Resource Corner:
Greynet Software Detection *(Detect public IM software, adware, key loggers, etc.)*	Discovery. Dashboard	Centennial Discovery	http://www.centennialonline.co.uk	·**ESET White Papers on Threat Detection** - http://www.eset.com/download/whitepapers.php ·**Informa**tionWEEK Article on Threat Detection - http://www.infoworld.com/article/07/02/16/08TCorchsb_1.html ·**FaceTime Company: Overview of GreyNet applications** - http://www.facetime.com/solutions/greynets.aspx
Application State Changes (Detect changes to files in comparison to policy)	Tripwire Enterprise	Tripwire, Inc.	http://www.tripwire.com	
Detect Illegal/Unauthorized Web Sites	Websense Filtering	Websense, Inc.	http://www.websense.com	
Network Behavior Analysis *(Traffic monitoring yields baselines to analyze threats)*	Profiler	Mazu Networks, Inc.	http://www.mazunetworks.com	
Vulnerability Scanning Services *(Detect vulnerabilities within the enterprise that could be exploited)*	McAfee Foundstone On-Demand Service	McAfee, Inc.	http://www.mcafee.com	

Blocking technologies

P⁴ Taxonomy

Description: Products or services that block unwanted network ingress/egress attempts and intrusions. Blocking technology can drop suspicious connections, disallow traffic, and filter against Malware. Blocking can be used on inbound as well as outbound communications.

- ~~Firewalls~~
- Intrusion Prevention Systems (IPS)
- Intrusion Detection Systems (IDS)
- DDoS defensive tools
- Content filtering
- Web filtering / blocking

Examples

Category:	Product:	Vendor:	URL:	Resource Corner:
IDS & IPS *(Detect and prevent intrusions at the network or host level)*	Network Security 7100 Series	Symantec, Inc.	http://www.Symantec.com	·**Crime research Center: DoS Vs. DDoS Attacks White Paper** - http://www.crime-research.org/articles/network-security-dos-ddos-attacks/ ·**Wikipedia** – http://en.wikipedia.org/wiki/Content-control_software & http://en.wikipedia.org/wiki/Firewall & http://en.wikipedia.org/wiki/Intrusion_detection_system
Firewalls *(Allow/disallow traffic to networks and application through rules engine)*	FireWall-1	Check Point technologies, Ltd.	http://www.checkpoint.com	
Web Filtering/Blocking (Restrict access to/from URLs and block content downloads)	Barracuda Web Filer	Barracuda Networks	http://www.barracudanetworks.com	
Content Blocking *(Block outgoing content to prevent data leakage)*	GTB Inspector	GTB Technologies, Inc.	http://www.gttb.com	
DDoS Detection & Blocking *(Detect DDoS attacks and block and reshape traffic to continue operations)*	Peakflow SP	Arbor Networks, Inc.	http://www.arbornetworks.com	

Defending technologies

P⁴ Taxonomy

Description: Products or services that defend against Malware and other virulent code that could cause havoc. Common denominators for these products is their multi-purpose approach to threats by detecting and eliminating malicious code upon detection or infection.

- Anti-virus software
- Anti-SPAM software
- Anti-Spyware/adware
- Malware elimination
- Threat management appliances
- Unified threat management tools

Examples

Category:	Product:	Vendor:	URL:	Resource Corner:
Anti-Malware (scan for viruses, worms, spyware and Trojans entering through Web-based backdoors)	Blue Coat ProxyAV 2000	Blue Coat Systems, Inc.	http://www.bluecoat.com	·**Wikipedia** – http://en.wikipedia.org/wiki/Malware
Anti-Virus (Virus scanning, detection, quarantine, and removal)	InterScan Enterprise SuperSuite	Trend Micro Incorporated	http://www.trendmicro.com	
Anti-Spyware *(Detection, blocking, and removal of Spyware)*	Windows Defender	Microsoft Corporation	http://www.microsoft.com	
Threat Management Appliance *(Gateway multi-threat detection reflection tool)*	Astaro Security Appliances	Astaro AG	http://www.astaro.com	
Unified Threat Management (Appliance that includes virus, SPAM, pop-up, Malware prevention)	Symantec Gateway Security 5600 Series	Symantec, Inc.	http://www.Symantec.com	

Securing technologies

P⁴ Taxonomy

Description: Products or services that automate INFOSec program functions related to organizing security teams, reporting program status, training personnel, increasing awareness, and developing policies and procedures.

- Encryption solutions
- Content protection
- Secure messaging tools
- Privacy preserving technologies
- Data Loss Protection (DLP)
- Virtual private networks

Examples

Category:	Product:	Vendor:	URL:	Resource Corner:
Data Loss Protection (DPL) *(Prevent malicious loss of confidential data)*	Onigma	McAfee, Inc.	http://www.mcafee.com	·**SearchSecurity.com: Data Loss** - http://searchsecurity.techtarget.com/tip/0,289483,sid14_gci1229761,00.html ·**Ziff-Davis Buyer Guide: DPL** - http://content-management.webbuyersguide.com/buyingadvice/2266-wbgcontentmanagement_buyingadvice.html
Data-in-Motion Encryption *(Encrypt data transmission behind the firewall)*	EpiForce	Apani Networks, Inc.	http://www.apaninetworks.com	
Digital Certificates *(Bind entities together through trusted paths/connections)*	Extend SSL	Verisign, Inc.	http://www.verisign.com	
Digital & Enterprise Rights Management (DRM & ERM) *(Securing document individually or enterprise wide)*	Windows Rights Management (WRM)	Microsoft Corporation	http://www.microsoft.com	
Virtual Private Networks (VPN) *(Securing network connections and data outside the firewall)*	Cisco VPN SUite	Cisco, Inc.	http://cisco.com	

Cloaking technologies

P⁴ Taxonomy

Description: Products or services used to hide or make invisible network services and/or devices in order to prevent them from being detected by hackers. Cloaking can also include impersonation of identities to further mislead attackers.

- IP stealth technology
- Static cloaking
- Dynamic cloaking
- Network cloaking
- Load balancing
- Server masking /anonymizing

Examples

Category:	Product:	Vendor:	URL:	Resource Corner:
Anonymizing *(Removing identifying details from web servers)*	servermask	Port80 Software, Inc.	http://www.Port80software.com	·**SecurityITWorld.com Article** – http://security.itworld.com/nl/security_strat/11142006/ ·**Wikipedia** – http://en.wikipedia.org/wiki/Security_through_obscurity
IP Stealth Technology *(Make Internet devices invisible to hackers)*	AlphaShield Enterprise	AlphaShield Inc.	http://www.alphashield.com	
COM Security Capability (Determines what identity the client projects toward the server during impersonation.)	Clocking (COM)	Microsoft Corporation	http://msdn2.microsoft.com/en-au/library/ms683778.aspx	
Network Cloaking (Strips internal network information in the returned traffic)	Sidewinder G2 Security Appliance	Secure Computing Corporation	http://www.securecomputing.com	
Load Balancing *(Obscure the fact there are multiple servers by making them appear as one)*	BIG-IP	F5 Networks, Inc.	http://www.f5.com	

Complying technologies

P⁴ Taxonomy

Description: Products used to report or present the state of an organization's standards and regulatory compliance state. Approaches range from sophisticated interactive dashboards to business intelligence engines that extract compliance-related data for reporting.

- Compliance dashboards
- Compliance management
- Compliance reporting
- Compliance demonstration/proof
- Compliance testing
- Compliance attestation

Examples

Category:	Product:	Vendor:	URL:	Resource Corner:
Compliance Dashboard *(Dashboard view of policy, identity, standards, and risk compliance state)*	Compliance IQ	SailPoint Technologies, Inc.	http://www.sailpoint.com	·**eWEEK Compliance Desk reference** - http://www.eweek.com/category2/0,1874,1639143,00.asp ·**IT Compliance Institute** - http://www.itcinstitute.com/ ·**IT Compliance.com: Portal for IT Compliance Issues** – http://www.itcompliance.com ·**Google** – http://directory.google.com/Top/Computers/Security/Policy/ ·**Wikipedia** – http://en.wikipedia.org/wiki/Compliance_%28regulation%29 **Wikipedia** – http://en.wikipedia.org/wiki/Compliance_%28regulation%29
Compliance Management *(Compliance standards database mapped to control remediation and audit reporting)*	Brabeion Compliance Center	Brabeion Software Corporation	http://www.brabeion.com	
Compliance Reporting *(Business intelligence engine to extract attribute information related to regulatory compliance)*	iWay	Information Builders, Inc.	http://www.iwaysoftware.com	
Compliance Demonstration *(Map technical controls to regulations and report on status)*	Bindview	Symantec, Inc.	http://www.Symantec.com	
Compliance Testing *(Control testing and tracking)*	OpenPages GCM	OpenPages, Inc.	http://www.openpages.com	

Monitoring technologies

P⁴ Taxonomy

Description: Products or services that monitor the continuous state of hardware, software, or events related to security. Monitoring can be applied as a managed services or as an enterprise solution where agents are used to monitor security appliance states and events.

- Security event monitoring
- Compliance monitoring
- Facilities monitoring
- Threat monitoring & reporting service
- Managed service security monitoring
- Access & event log monitoring

Examples

Category:	Product:	Vendor:	URL:	Resource Corner:
Access and Event Logging *Monitor logs for security alerting and compliance purposes)*	LogLogic ST & XT	LogLogic, Inc.	www/loglogicom	·**BizForum White Paper on Security Monitoring** - http://www.bizforum.org/whitepapers/bluelance-1.htm ·**Project Lasso – Global Logging Standards** - http://www.loglogic.com/logforge/#
Facilities Monitoring *(CCTV, HVAC, Alarm Surveillance and Monitoring)*	OnGuard	Lenel Systems International, Inc.	http://www.lenel.com	
Security Intelligence Service *(Security Threat Monitoring)*	iDefense Security Intelligence Service	VeriSign, Inc.	http://www.verisign.com	
Managed Security Services *(Outsource IDS/IPS, Firewall, Content, Log Monitoring)*	Managed Service Services	LURHQ SecureWorks, Inc.	http://lurhq.com	
Terminal Server Monitoring *(Records server session activity)*	RecordTS	TS Factory, Inc.	http://www.tsfactory.com	
Security Event Management *Correlate and aggregate security events for analysis)*	nFX	netForensics, Inc.	http://www.netforensics.com	

Supporting technologies

P⁴ Taxonomy

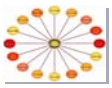
Description: Products or services that directly or indirectly support the operationalization of security technologies. Products are aligned to the ITIL Framework and include change management, configuration management, problem management, and other.

- Asset management
- Change control
- Configuration management
- Problem management
- Release management
- Service level management

Examples

Category:	Product:	Vendor:	URL:	Resource Corner:
Identify and Inventory IT Assets	OpenView Asset Center	Hewlett-Packard Company	http://www.hp.com	·**HP Software Listing** - http://h20229.www2.hp.com/ · **Wikipedia** – http://en.wikipedia.org/wiki/OpenView
Open and Track Service Tickets Related to Security Issues	OpenView Service Desk	Hewlett-Packard Company	http://www.hp.com	
Monitor Security Appliances for Health Status	OpenView Operations	Hewlett-Packard Company	http://www.hp.com	
Ensure Security Appliances/Devices are Patch Correctly	OpenView Configuration Management Patch Management	Hewlett-Packard Company	http://www.hp.com	
Ensure Security Appliances/Devices are Configured Correctly	OpenView Configuration Manager Inventory Manager	Hewlett-Packard Company	http://www.hp.com	
Maintain Security Attributes in Application Profiles	OpenView Configuration Manager Applications	Hewlett-Packard Company	http://www.hp.com	

Storing technologies – Group 1



P⁴ Taxonomy

Description:

-
-
-
-
-
-

Examples

Category:	Product:	Vendor:	URL:	Resource Corner:

Responding technologies – Group 2

P⁴ Taxonomy

Description:

Examples

Category:	Product:	Vendor:	URL:	Resource Corner:

Recovering technologies – Group 3

P⁴ Taxonomy

Description:

Examples

Category:	Product:	Vendor:	URL:	Resource Corner:

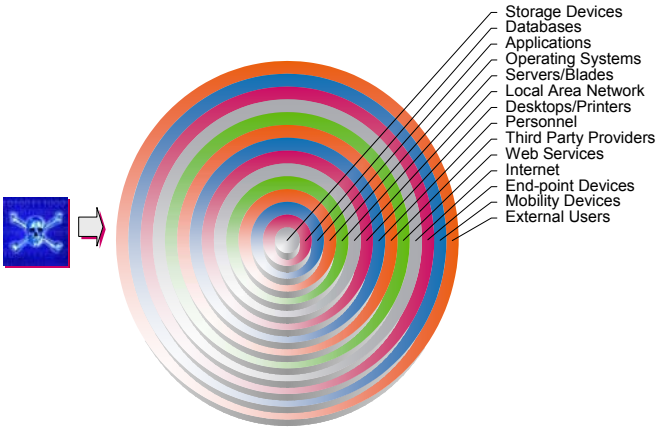
Summary

- Key business trends
  - Dollar signs dominate attacks
  - Compliance programs meet increasing regulatory complexity
- Key technology trends
  - “Perimeters” = strategic, business-driven, control points
  - Declaring war on the false positive
  - Information centrism – security as a core aspect of the information management lifecycle
- Getting proactive
  - Planning, architecture, and process
    - Work with and understand the business
    - Business continuity and incident response plans
    - De-siloization: share information, share intelligence

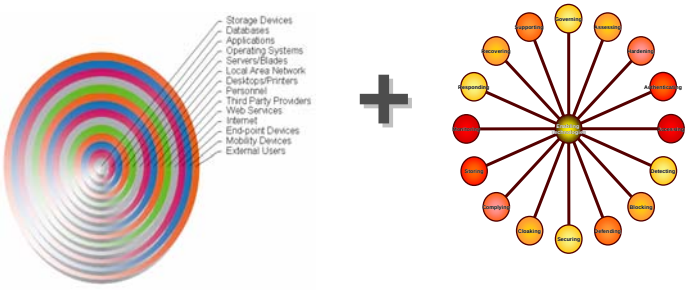
Applying Enabling Technologies

Enabling technologies discovery

1. What are the threats?
2. Where do the threats originate?
3. What are the likely impacts?
4. What is most vulnerable?
5. What could be exploited?
6. What should be protected?
7. Who would be most affected?

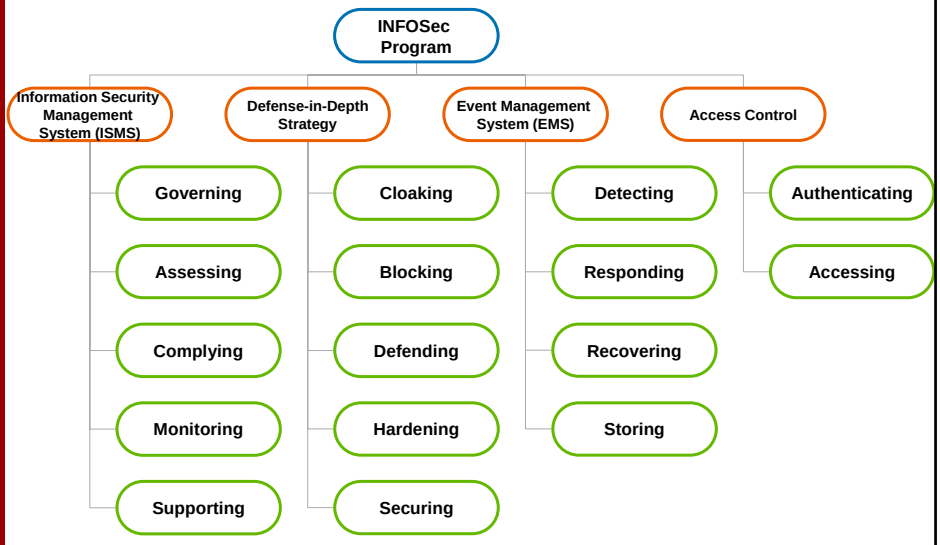


Enabling technologies planning

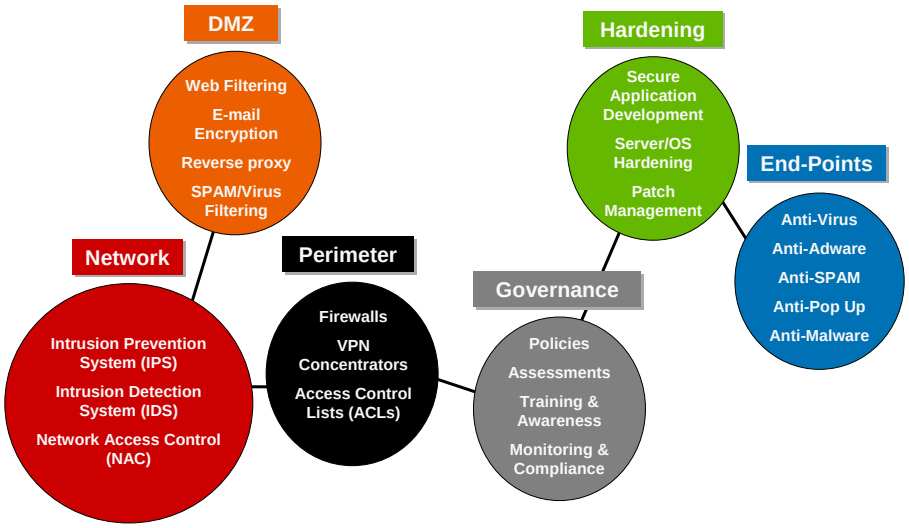


1. How do we govern our assets?
2. How do we assess our readiness?
3. Where do we harden our infrastructure?
4. Where do we restrict access?
5. How do we authenticate access/entitlements?
6. How do we detect that we're under attack?
7. Where can we block threats?
8. How do we defend against attacks?
8. How do we secure our infrastructure?
9. How can we make ourselves invisible to attackers?
10. How do we comply with regulations?
11. What data requires retention?
12. How do we monitor our controls and readiness state?
13. How we respond to security breaches?
14. How do we recover from security incidents?
15. How do we support our controls to be more effective?

Enabling technologies hierarchy

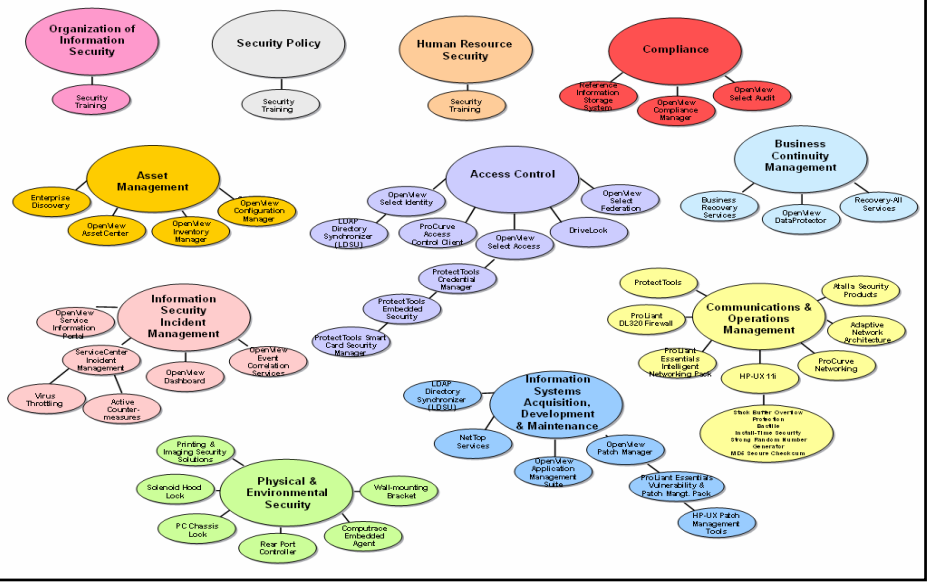


Enabling technologies relationships



HP Security Technologies

Examples of HP enabling technologies by ISO domain



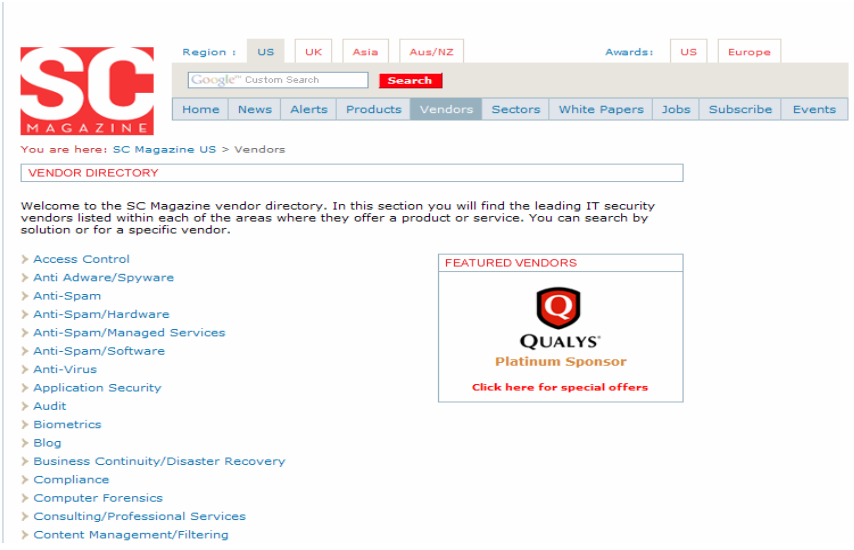
HP security technologies

- OpenView Suite for Security
  - Select Identity
  - Select Access
  - Select Audit
  - Select Federation
  - Compliance Manager
  - Service Desk (Key component of ITSM/ITIL)
  - Network Node Manager (NNM) for Security Operations Center (SOC), Network Operations Center (NOC)
  - … and much more
- ProtectTools Security Software Modules
  - http://practices.know.hp.com/C0/Defense%20and%20Security/Defense%20and%20Security%20Library/IT%20and%20network%20infrastructure%20(horizontal)%20solutions/IT%20Security/HP%20ProtectTools%20Security%20Solution.html

HP security technology partners

Security Staff Resources

Security product vendor directory



5/25/2007 50

Security tools resources

Vendor White Papers

Founded in 1998, Bitpipe, Inc. (www.bitpipe.com) created an online network of IT and business Web sites and pioneered the concept of creating multiple distribution channels for vendor-created content.

Mega Security Links

http://www.cccl.net/pandl/pandl.html

HP Deployed Security Products

http://it-ea.corp.hp.com/app/product.aspx?list=category

Microsoft TechNet Security

http://www.microsoft.com/technet/security/default.mspx

Security Tools Portal

http://sectools.org/

Encyclopedia of Tools

http://en.wikipedia.org

Threats drive technology choices

- Vulnerabilities tracking sites:
  - CERT
  - Bugtraq
  - Cisco
  - HP
  - Microsoft
  - RedHat
  - SuSE
  - Vulndev
  - Securiteam
  - Neohapsis
  - ISS X-Force
  - National Infrastructure Protection Center
  - CVE
  - VU# Database
  - Security Tracker

Security Technology Predictions

Top-10 security product predictions

1. The rise of 3S will merge security, systems, and storage management disciplines
2. Managed threat environments will offer criminals more scalable attack platforms
3. NAC will absorb mature content management products
4. OS authors & Service Providers will assimilate consumer security products
5. Consumer authentication will emerge as a new enterprise market

IDC
Analyze the Future

Top-10 security product predictions

6. Physical & IT security will start to converge within large enterprises
7. Anti-virus and anti-spyware technologies will gradually disappear as standalone consumer products, but not brands
8. Vulnerability testing for application code will become a growing part of the SDLC
9. Security will get better, but more annoying
10. Compliance will be recognized as a new class of vulnerabilities

IDC
Analyze the Future