

Managed Security Services

Best Practices and
Issues



Cygnos I.T. Security Services Include:

- | **Complete Security Solutions**
- | **Placement & Outsourcing**
- | **Audits & Assessments**
- | **Planning and Architecture**
- | **Prevention and Detection**
- | **Business Continuity & Disaster Recovery**
- | **Management and Education**

Presentation Overview

1. MSS Market Review
2. Service Offerings
3. When does an MSS fit?
4. Selecting an MSS
5. Benefits and Risks
6. Best Practices

1. MSS Market Review



MSS Marketplace

- I MSSP marketplace is young: 3 years old (SC magazine, Sep 2002)
- I Growth in the marketplace from USD\$140mil to \$170*billion* by 2005 (global infosecurity briefing)
- I Estimated losses exceeding one trillion in 2000 due to security incidents (same source)

2. MSS Service Offerings



MSS Overviews: What can they do?

- | Product evaluation and selection
- | Managed Firewalls (33%), VPNs
- | Intrusion Detection (19%)
- | Virus Scanning
- | Web-site security assessments
- | Content inspection and monitoring
- | Secure Messaging Services
- | Security Log Consolidation
- | Security Design Services (23%)

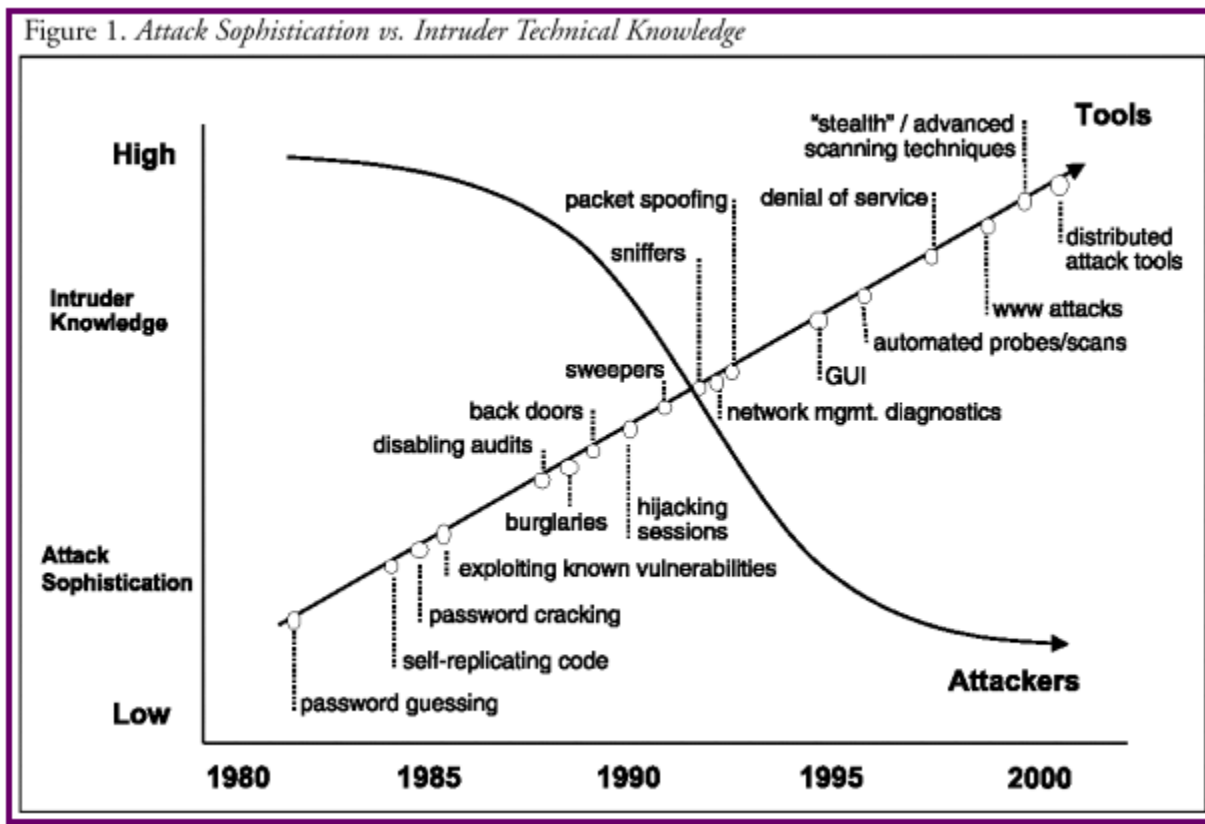
3. MSS: The attractions



Reasons to Outsource

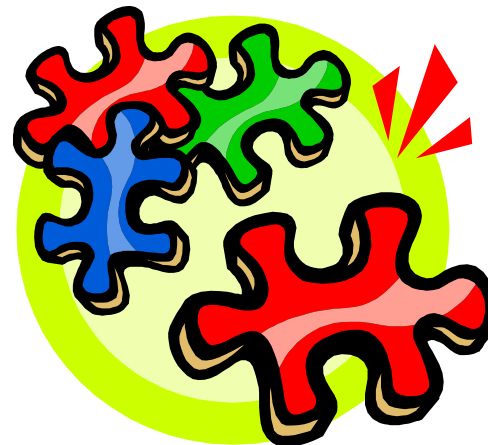
1. Sophistication of hackers increasing
2. More complicated countermeasures
3. Core competencies to manage, evaluate, deploy and integrate security solutions don't exist internally
4. MSS's are informed on current developments
5. MSS's can lower overhead costs more quickly
6. Lack of internal resources

Attack Sophistication



Increasing Complexity of Countermeasures

- Firewalls
- Anti-virus scanners
- Intrusion Detection Systems
- Central Logging
- Incident Handling and Response
- Hardening Measures
- System Integrity Checks
- Password Policies
- Enforcement
-



And... They must all work together!

Expert Resource Availability

- I How easily available are security staff, and what does it takes to keep them onboard?
 - Policy makers
 - Pen Testers
 - Forensic Experts
 - Firewall Experts
 - IDS Architects
 - Etc...

4. Selecting an MSS



Questions to ask of an MSS

- | Understand and Apply Client Security Policy
- | Understand Client Business and its Security Needs
- | Breadth of Offering
- | What is the representative Client Base?
- | Solid reference accounts
- | What can they monitor and manage

Understand and Apply Security Policy

- | Show Me Your Policy
- | Security is based on Policy articulating business protection requirements
- | MSS must be capable of articulating prevailing policies and standards and of reflecting them in proposed protection measures
- | MSS must be capable of discerning:
 - Variations in security requirements (law enforcement, regulatory, compliance, fraud detection...)
 - Countermeasure types (detective, preventative, deterrent, corrective, etc...) and their situational applicability to your business

Understand Client Business and its Security Needs

- | Beware of “one size fits all” approach
- | Offer modularized solutions
- | Can MSS adapt as fast as your network changes?
- | Is resident or local expertise a requirement?
- | Ability to understand relationships, reporting lines, and responsibilities
- | How well suited are MSS incident handling practices to your needs – how easily they lend themselves to integration with your incident handling capabilities

What to look for?

MSSP should be able to:

- | Define security policies
- | Offer Business Continuity Services
- | Assist in analysis and appraisal
- | Offer modularized solutions
- | Create simplicity for a single-source solution!

5. Benefits and Risks



Benefits

Business Advantages

- | Potentially lowered costs of ownership
- | Risk Transference
- | Competencies for complex initiatives
- | Lowered Staffing and HR requirements
- | 24/7/365 service availability

Technical Advantages

- ü Optional ownership of security technology
- ü Lowered effort to manage/maintain equipment

MSS Outsourcing Risks - Overview

1. How secure is the MSS
2. Interpreting client business requirements
3. Access to sensitive information and assets
4. Incident Handling
5. Baselines and Tuning: defining parameters
6. The Black Box - The Weakest Link Paradigm
7. Technical Implementations: IDS, Perimeter..
8. Risk Management: Could risks or costs increase?

Out-Sourcing: How Secure is MSS?

- | Are they “paranoid” enough?
- | Must maintain an advanced security posture compared to most secure client
- | How insulated from your competition is your network?
- | MSS Staff Security - clearance, and accreditation
- | Third party audits

Operations Procedures

- I Do they maintain sound procedures – to name a few concerns:
 - How are signatures qualified and updated?
 - How are monitoring devices updated?
 - IDS testing handling and co-ordination
 - How are evidential records handled?
What are their change and configuration management practices?
 - Vulnerability Tracking Practices – Do they have any?

Access to sensitive information and assets

- I Alerts and Logs are more than just that
 - Useful in mapping the network
 - Useful in figuring your security posture
- I Visibility of your IT assets to MSSP's network
 - And, potentially to hackers and/or competition

Incident Response Handling

How are alerts communicated?

- | Who gets to know of incidents at their end
- | How is it communicated back to the client
- | What about the forensic dimension?
 - Log consolidation and upkeep
 - Log disposal practices
- | What if the MSSP is attacked?
 - Full disclosure may be required

The Black Box - The Weakest Link Paradigm

- I You are as secure as the weakest link. Your security is:
 - A function of MSSP's security posture, and
 - A function of other clients' security posture
 - Is your competition being served by same MSSP
 - I Is the risk acceptable anyways
 - What assurances do you need?
 - I Will the MSSP grant you access to perform spot audits on their network?
- I Third party dependencies that may impact your as well as *their* business!
 - Ex. DoS may bring down their alerting capability ... Guess whose turn is next?
 - Do they subcontract some of their obligations?

Technical Implementation

- | Trustworthiness of the products in use
- | How trustworthy is the solution in use?
 - Scope of vision
 - Vulnerability to evasive attacks
 - Vulnerability to intelligence gathering
- | The risk of adversely impacting existing infrastructure – security and/or otherwise

6. Managing Your Risks



Reasons not to Outsource

1. Costs: Return on expenditure may exceed benefits
2. Sensitivity: Information assets are simply too valuable to outsource
3. Suspicion: lack of confidence in MSSPs
4. Immature Market
5. Fear of MSSPs going out of business
6. Fear of losing internal head-counts
7. Proprietary: Systems or processes are highly customized within the organization

Managing Your Risks

- | MSS is not a “hands-off” approach!
- | Create an MSS management team
- | Work closely with an MSS to ensure they understand your:
 - Business Requirements
 - Security Policies
 - Reporting and Response Needs
- | Service Level Agreements
- | Incident Handling and Response

Managing Your Risks – cont'd

- I How healthy is the MSSP. Factors to consider:
 - Certification, accreditation and licensing (if applicable)
 - Ownership
 - Past performance – both short and long term
 - Liability and insurance
 - Support infrastructure
 - Profitability and Lifespan

Managing Your Risks – Staffing Issues

- I Assess rate of MSS' staff turnover, and impact on:
 - Quality of service
 - Increased potential for attacks from “disgruntled” employees
 - Increased potential for breach of confidentiality
 - I Read their employment contract – may even go as far as full disclosure of terms of employment
- I Ensure that the MSSP is willing to develop the skills that are of particular applicability to your environment requirements

Managing Your Risks – cont'd

- I Availability to respond to emergencies
 - Local expertise if needed
- I Did we mention “impact of third party dependencies”?
 - Asses them carefully

Managing Your Risks – Cultural Issues

- I Cultural and Political Sensitivities:
 - Internal sensitivities (mainly due to matters being handled by external provider)
 - Privacy and confidentiality assurances
- I Consequently:
 - Need to involve your staff
 - Incident Handling and Response Policy must be provisioned to cater for cultural, and political sensitivities as well as legal issues.

Risk of Escalating Cost

- | Big does not mean better
- | Constant management intervention = \$\$\$
- | Will the contract involve high maintenance overhead?
- | Does the cost of dealing with an MSS exceed the value of the assets you are protecting?

Preparation

- I What does a company need to do in preparation to dealing with an MSS?
 - Business expectations
 - Risk Analysis and Management
 - Establish working management groups
 - Policies
 - Awareness Programs

Now that the Contract is Signed

Next Steps

- | Third party assurance audit ... before you cut the ribbon
- | Routine audits, and penetration testing
- | Spot audits
- | Test Change and Configuration Management Practices

Now that the Contract is Signed

Next Steps – cont'd

Regular meetings:

- Update on outstanding vulnerabilities and related issues
- To confirm understanding and appreciation of your needs
- To confirm their performance in meeting their contractual obligations
- Perform regular disclosures, if required
- Review of MSSP costs

Now that the Contract is Signed Next Steps – cont'd

- I Perform Regular Risk Assessments:
 - Culture changes
 - Network changes
 - Changing business requirements
 - Changing hacker methodologies and/or attacks
 - Etc...
- I How will outsourced solution be retrofitted to provision for emerging needs?

Conclusion

- | Outsourcing is a viable option, only if you:
 - Do your home work, first – no one will do it for you
 - Understand and successfully translate your understanding of your needs into precise measurable performance requirements
 - Manage your risk
 - Keep your MSSP on their toes, and YES the most effective way is routine third party audits
 - | Audit means audits including pen tests