IT Security Teams and Managed Security Services Working Together

2006 FIRST Conference
Who am I?

Chris van Breda, CD, CISSP, EnCE
Theme for the 2006 conference

“Sharing Intelligence in Global Response” working smarter and sharing knowledge in this environment, finding ways to further our initiatives on collaborative and cooperative approaches to find solutions to the problems we face in computer and network security incident response.
The pressures of business, legislation and budgets force us all to see how we can work smarter. Unfortunately, working smarter for most management is another way of saying do more with less. Security budgets have limitations and most organizations have only increased spending when they are forced to by outside events – this could be legislation, litigation or loss of business due to security breaches.
If you’re only a one person security shop, where do you go to learn? This is an easy question to answer, just look around you. Just about anyone here will talk about security issues at the drop of a hat. If they’re like me, you’ll have trouble making them stop!

Sharing knowledge is a passion that must be spread, and that is also part of this presentation.
Whether you like it or not, you’re not the only security team out there. Also the odds are that for most of you, outsourcing some or all of your IT security will become a very real possibility. The better prepared you are, the better things will go.
Now that outsourcing some or all of your security requirements is a very real possibility, you need to find the best approach to dealing with it.
This is an INTERACTIVE session

You

Discussion

Me
Questions/Comments

Anytime
To help teams find solutions on how to effectively outsource and work with managed security service providers (MSSP).
Tutorial Overview

Review Taxonomy
Review Security Objectives
Discuss Security Influences
Where most teams are now

How and what to outsource and why
Requests for Proposals
Service Level Agreements

How to work with the MSSP
Service Reviews
How to end an agreement
Communication
<table>
<thead>
<tr>
<th>Action</th>
<th>Target</th>
</tr>
</thead>
<tbody>
<tr>
<td>Probe</td>
<td>Account</td>
</tr>
<tr>
<td>Scan</td>
<td>Process</td>
</tr>
<tr>
<td>Flood</td>
<td>Data</td>
</tr>
<tr>
<td>Authenticate</td>
<td>Component</td>
</tr>
<tr>
<td>Bypass</td>
<td>Computer</td>
</tr>
<tr>
<td>Spoof</td>
<td>Network</td>
</tr>
<tr>
<td>Read</td>
<td>Intranet</td>
</tr>
<tr>
<td>Copy</td>
<td></td>
</tr>
<tr>
<td>Steal</td>
<td></td>
</tr>
<tr>
<td>Modify</td>
<td></td>
</tr>
<tr>
<td>Delete</td>
<td></td>
</tr>
</tbody>
</table>
Incident

Attack

Event

Attackers
- Hackers
- Spies
- Terrorists
- Criminals
- Vandal
- Voyeurs
- Corporations

Tool
- Physical Attack
- Information Exchange
- Flood
- User Command
- Script or Program
- Autonomous Agent
- Toolkit
- Distributed Tool
- Data Tap

Vulnerability
- Design
- Implementation
- Configuration

Action
- Probe
- Scan
- Flood
- Authenticate
- Bypass
- Spoof
- Read
- Copy
- Steal
- Modify
- Delete

Target
- Account
- Process
- Data
- Component
- Computer
- Network
- Intranet

Unauthorized Result
- Increased Access
- Disclosure
- Corruption
- DOS
- Theft

Objectives
- Damage
- Political
- Financial
- Thrill

Ref:
http://www.cert.org/research/taxonomy_988667.pdf
Security Objectives
What are your security objectives?

Business risk perspective
Perimeter Security
Mobile Users
Internal Malfeasance
Defence in Depth
Incident Response Plan
Tracking Metrics
In most cases risk management looks pretty simple,

- Oversimplified, Risk = P \times L, where P is the probability of an event that will cause a financial loss of L.
“More than 30% of small firms are still spending less than 1% of their IT budget on security, while larger firms have significantly increased their investment in security over the past two years, spending between 4% and 5% of their IT budgets on security.”
Specifically, the FTC charged that the company failed to do the following:

- Assess risks to the information it collected and stored - both online and off-line.
- Implement reasonable policies and procedures in key areas such as employee screening and training and the collection, handling and disposal of personal information.
- Implement simple, low-cost, readily available defences to common Web site attacks or put in place reasonable measures to prevent hackers from gaining access to the company’s computer network.
- Employ reasonable measures to detect and respond to incidents of unauthorized access to the data or to conduct security investigations.
- Provide reasonable oversight for the handling of personal data by service providers such as third parties employed to process the information.
According to the complaint, a hacker exploited these failures by using a common Web site attack to gain access to the computer network. In addition, a television station found documents containing sensitive consumer information discarded in an unsecured trash bin.

"Careless handling of consumers' sensitive financial information is an open invitation to identity thieves," said FTC chairman Deborah Platt Majoras. "Enforcing the laws designed to protect consumers' sensitive financial data is a priority at the FTC. This is the 13th case challenging faulty data security practices, and we will bring more cases if companies continue to fail consumers."
Influences

- Legislation
- Privacy
- Consumer confidence
- Type of Business
- Resources
- Users
- Budget
Typical Situation

- Understaffed
- Overworked
Dynamics of Incident Response

By
Johannes Wiik
Faculty of Engineering and Science
Department of Information & Communication Technology
Norway

Dr. Klaus-Peter Kossakowski
DFN-CERT Services GmbH
Germany

“A frequently identified problem is that CSIRTs are over-worked, under-staffed and under-funded.”

“Based on theory from process improvement and information from the case study, we identified that short-term pressure from a growing incident work load prevents attempts for developing more response capability long-term, leading the CSIRT into a “capability trap”.

Fundamental solutions will typically involve a worse-before-better trade-off for management. Short term the CSIRT will lower its response capability while new capability is developed.

Long term the CSIRT will get an automated response capability independent from limited human resources. Hence, it can automatically scale to future increases in workload.
Common Problems Among CSIRTs

- Frequently referenced problems in the CSIRT community are over-stretched resources and a need for continuous improvements. Killcrece et al. (2003a p. 128) refer to many such problems, for example:
  - lack of funding,
  - lack of management support,
  - lack of trained incident handling staff,
  - lack of clearly defined mission and authority, and
  - lack of coordination mechanisms.
Why and How To Outsource
Typical Security Situation

- Grown on the back of existing structure
- Lack of specific expertise
- Lack of resources/funding
- Labour legislation – no OT, long hours etc.
- Check the box attitude
- Misconceptions – we have IDS/FWs so we must be secure.
- Who accepts responsibility?
- What happens when things go wrong?
Where are you now?

- Implemented NIDS/HIDS/FWs etc
- Some logging turned on
- Might even have SIM/SIEM
- Someone gets tasked to review logs, events etc.
- 24/7 monitoring might be required
- So far you’ve managed to survive
- Workload is growing/accountability is pushed down
- Jobs on the line
- Realization you aren’t closing the gap, or you can’t continue to fund the growing resource requirement. You need options.

Are you reactive instead of proactive?
WHY OUTSOURCE SECURITY?

YOU DON’T

You’re outsourcing some operational and functional requirements the same as any other service is outsourced.

In *most cases*, the responsibility for security remains in house.

Accountability always remains in house.
How much does a 24/7 monitoring team cost?

Secure facilities
Trained resources
Proper equipment

1.1 to 1.5 million dollars for 1^{st} year.
OUTSOURCING

Identify your needs first;

- AV
- Content filtering
- Spam filtering
- IDS (HIDS/NIDS)
- IPS
- Log monitoring
- Firewall services (?)
- Do you want to own or lease (?)
Example - All You Need Retail Stores

20,000 plus users
10-15000 workstations
Mixed OS
Large geographical area
Main business – retail sales
Also provides financial services
Current situation

- Subject to legislation
- You don’t enforce AUP
- AV fairly good
- Firewalls
- Help desk
- Change management
- Small security staff
- Friction between Ops and Security
- Security review – policy/requirements
- Cost of an incident (find spreadsheet)
- Hire more staff (start-up cost of a 24/7 SOC is over a million dollars)
- Outsource to a part-time solution for after hours
- Decide what you can do well in-house and what you need help on
- Define your requirements – spend lots of time on this one
- Hire a professional service to identify your security requirements
Identify your needs

- You consider NIDS/HIDS as vital.
- You need to enforce AUP
- Spam needs to be controlled
- You need both desktop and enterprise AV
- Your most critical assets are your database servers.
- You want syslog and application monitoring turned on
- You want to be able to correlate all security device outputs (FW AV IDS SYSlog)
- You need better vulnerability monitoring and patch management.
- You need 24/7 monitoring
- You need 24/7 response
Other Considerations

- Scalability (what happens when your company doubles in size?),
- Bandwidth requirements (if your security logging is so noisy, are you causing a self inflicted DOS during peak hours?),
- Ease of use
- Interoperability – does this work well with other products?
- vendor support levels
- Product history – new or tried and tested or tried and tired?
- Independent Reviews
- Talk to others in the industry
- COST
Identify Providers that meet your needs

- Location
- Company size – size isn’t everything.
- Vendor relationships
- Existing clients
- People
- Alternate locations
- Data storage
- What services do they currently offer – avoid the “we can do that”, look for the “we do that”
- Call and talk to vendors (MSS) that you think meet most of your requirements, identify potential candidates.
- Ask vendors to come in for a meeting. Make it informal, and promise nothing. Be up front, open, and honest.
Keys to a Great Working Relationship

RFPs

SLAs
What is an RFP?

Where you identify your requirements in detail
You ask who can meet your requirements, in detail
It leads to an SLA and a contract
All You Need Retail Stores, is soliciting proposals from firms that are able to render professional and monitoring services in the area of IT Managed Security Services.

Proposals must address all of the services described in the detailed Scope and Deliverables section.

All You Need Retail Stores intends to make a single contract award to the most responsive and responsible firm earning the highest score. This procurement is open to eligible firms that meet the qualification requirements.
All You Need Retail Stores is a national retail chain with 2000 stores and 10000 employees over varying geographical areas. All You Need Retail Stores provides a wide range of consumer goods through a distributed warehouse system and has supply arrangements with around 1000 vendors, both nationally and international. 

All You Need Retail Stores also has its own credit services division and offers clients a wide range of financial services.

All of our stores, warehouses are connected by a network consisting of .................(high level overview)
All queries concerning this RFP must be directed only to the following:

- NAME
- Phone/FAX
- Email
## RFP Schedule

<table>
<thead>
<tr>
<th>Event</th>
<th>Date</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFP Released</td>
<td>15 June 2006</td>
<td></td>
</tr>
<tr>
<td>Questions from interested parties</td>
<td>NLT 30 Jun 2006</td>
<td>4 PM</td>
</tr>
<tr>
<td>Proposal Due Date</td>
<td>NLT 30 Jul 2006</td>
<td>2 PM</td>
</tr>
<tr>
<td>Interviews (three best)</td>
<td>15 Aug 2006</td>
<td></td>
</tr>
<tr>
<td>Validation Audit (best only)</td>
<td>NLT 30 Aug 2006</td>
<td></td>
</tr>
<tr>
<td>LOI Issued</td>
<td>1 Sep 2006</td>
<td></td>
</tr>
<tr>
<td>SLA Finalized</td>
<td>30 Sep 2006</td>
<td>2 PM</td>
</tr>
<tr>
<td>Contract Award Date</td>
<td>1 Oct 2006</td>
<td></td>
</tr>
<tr>
<td>Proposed start of services</td>
<td>1 Dec 2006</td>
<td></td>
</tr>
</tbody>
</table>
The term of the resulting agreement is expected to be 36 months with the possibility of 2 one year extensions and is anticipated to be effective from December 1, 2006 through November 30, 2009.

The agreement term may change if All You Need Retail Stores makes an award earlier than expected or if All You Need Retail Stores cannot execute the agreement in a timely manner due to unforeseen delays. The resulting contract will be of no force or effect until it is signed by both parties. The Contractor is hereby advised not to commence performance until all approvals have been obtained. Should performance commence before all approvals are obtained, said services may be considered to have been volunteered if all approvals have not been obtained.
RFP – Bidder questions

- How and until when can potential bidders ask questions?
RFP - Decision criteria

- (lowest cost, best services etc)
- *Pass a mandatory third party audit before contract awarded*
- *Give them the audit details.*
- *Failing a third party audit will nullify any LOI and All You Need Retail Stores will be free to contact the next most qualified bidder and continue the contract process with them.*
RFP - Deliverables

- **Functional requirements**
  - What services
  - 24/7/365 monitoring of ….
  - Reports

- **Non Functional Requirements**
  - Supports the business requirements

- **Technical Requirements**
  - Failover
  - Clustering
  - Reporting

- **Support and Maintenance**
  - Expectations
Requirements Review

- 24 x 7 x 365 monitoring.
- Identification of events, attacks, and incidents.
- Reporting of events, attacks, and incidents.
- Containment recommendations on attacks and incidents.
- Triage performed on attacks and incidents.
RFP Steps- part 1

- Overview
- Background
- Contact Information
- Schedule
- Term
- Questions
- Decision Criteria
- Deliverables
What Information you want

- Vendor company information
- Company background/history
- Quick overview of services and capabilities
- Management or key personnel bios
- Contact information
- Vendor’s proposed solution
  - Basic summary of the solution
  - Solution methodology/process
  - Development plan
  - List of tasks
  - Timeline
- Details on proposed solution
  - Original ideas – strategy, creative, etc.
  - Features and functionality
  - Options and add-ons
  - Scalability
  - Technical requirements
  - Preliminary design compositions (voluntary)

Proposed budget
Cost of services
What Information you want - continued

- Required 3rd party costs
- Support and maintenance
- List of deliverables
- Ownership
- Proposed Project Team
- Vendor references
- Show examples of previous work
- Provide client references
- List awards/accolades and special certification
Next Steps

- Have both legal and procurement departments (if they exist) review the RFP.
- If they are not available, have it reviewed both by somebody on your team and an outside source.
- Put it out for bid, be realistic and give at least 6-8 weeks for response, maybe more if the RFP is very long.
Review Responses

- Form your evaluation team before the cut-off date
- Score the proposals against your criteria
- Reject the ones that failed the mandatory requirements
- Narrow the field (3 is a good number)
- Interview the bidders
- Make a decision
Final Bidder review

- Don’t sign a contract yet
- Do the audit – if they fail, go to the next bidder
- Sign a Letter of Intent based on an acceptable SLA
- Don’t be pressured into signing a contract yet, there’s still a lot of work ahead.
Service Level Agreements

- Based on the bidders response plan, work out a *detailed* SLA
- Why?
SLA Steps

- Define your terms and how you will monitor them.
- Spell out how the agreement will be monitored.
- Cover best- and worst-case situations.
- Make the penalties fit.
- Demand continuous improvement.
- Designate an SLA Manager.
- Ensure understanding of the SLA by both parties.
- Review any draft SLAs internally.
- Does a legal review sound like a good idea?
Final Thought on SLAs

- Provider Attitude
  “If we have a breach on our network, we don’t have to tell you. Its our network!”
Final Steps – or not?

- Sign your contract
- Manage the SLA
What outsourcing does for you

- Reduce costs?
- Pooled experience
- Unlimited resources (if money is no object)
- Compliance issues
- Containment Recommendations
- Separation of Duty
What your outsourcing does NOT do for you

- Absolve responsibility
- Incident Response
- Fix all your security problems
- Is not an “authoritative” partner
- Vulnerability Management
- No Guarantees
Your responsibilities

- Why would MSS be a fit in your organization?
- The right solution for your needs
- PDAR
- Communication
- Information Sharing
- Job Security
- Network Knowledge – Critical asset identification
- Definitions (security events)
- Feedback
- Contract/SLA oversight
Incident Response together

- Communication
- Planning
- PDAR – together
- Issue Resolution
- Process evolution
Working with your MSSP-Communication

- Get to know their team members, have a face to face meeting
- For the first month, have daily or weekly conference calls
- Invite their team members to come over and see your team first hand
- Talk to the provider client service manager at least monthly
Working with your MSSP-Planning

- Plan incident scenarios
- Talk through an incident using actual data
- Keep contact information up-to-date, both yours and theirs, confirm it at least monthly
- Plan tests, both with and without notice but don’t overdo it
- Handle problems and issues at the lowest level possible
Working with your MSSP-PDAR

- **Work together**
  - Prevent
  - Detect
  - Analyze
  - React

- **If your provider doesn’t drive you crazy in the first month or two, they aren’t doing their job**
  - Why?
Working with your MSSP-Issues

- Resolve at the lowest level possible, but don’t hesitate to escalate
  - Remember, you’re paying for the service

- Keep it professional
  - Don’t scream and shout
  - Keep to the facts

- If you can’t resolve it, involve senior management (both sides)
Working with your MSSP-Evolution

- Times and technology change
- You may be able streamline your own processes
- See if your provider has recommendations
- Keep track of what you could have done better or major issues you have
When Things Go Wrong- Termination

- In the contract and SLA address
  - If the provider goes out of business, how will your data be protected/returned
  - If you’re not happy, what will it cost you?
  - If at the end of the contract term, you do not want to renew
    - Provide for monthly extensions
    - Provide for turn-over/transition to new provider
Review

- Communicate on the same level
- Identify your needs in advance
- Write a detailed RFP
- Choose the right provider
- Write a clear SLA
- Manage the service
- Communicate
Questions or Comments

Contact Information
Cyberklix Inc.
Chris van Breda, CD, CISSP, EnCE
220 Laurier West, Suite 560
Ottawa ON K1P 5Z9
(613) 230-5693
chrisv@cyberklix.com