VIRUS BULLETIN 2005

EFFECTIVE SECURITY POLICY MANAGEMENT

MICHAEL D. THACKER
IBM GLOBAL SERVICES

TOPICS TO COVER

- OVERVIEW
- SECURITY POLICY BASICS
- SECURITY POLICY CONSORTIUM
- ANALYZING AND MANAGING RISK
- OBTAINING SUPPORT FOR YOUR POLICY
- SECURITY POLICY TCO/ROI
- MAINTAINING POLICY
- EDUCATION AND SECURITY POLICY
- SECURITY POLICY AND THE LAW
- WHY SPECIFIC MALWARE POLICY?

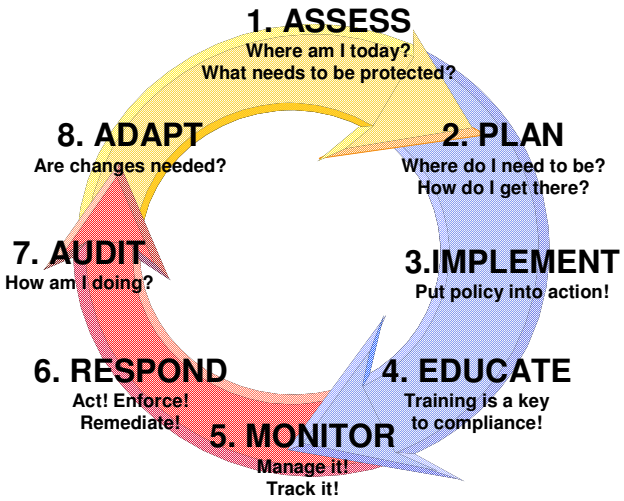
OVERVIEW

- "No one appreciates policy until it is crunch time." - Scott Sidel

OVERVIEW

- The intent of this presentation is to cover the security policy lifecycle. We will discuss policy basics and the supporting methodologies in maintaining an effective security policy.
- Security policies cover a wide area of business needs. Given the short timeframe, the goal will be to discuss the topics of security threats related to malware.

SECURITY LIFECYCLE



Security management should be a **closed loop lifecycle** of activities to continually assess, monitor, respond and adapt to a constantly changing IT environment and threat landscape which assures **continuous improvement** in the overall security posture.

SECURITY POLICY BASICS

SECURITY POLICY BASICS

- Developing and maintaining effective security policies can be difficult.

- What is a security policy?
- Why do I need a security policy?
- What is the security policy protecting? (who/what)
- How will the policy be implemented?
- How will the policy be enforced?
- How will the policy be measured? (audit/metrics)

WHAT IS A SECURITY POLICY?

- There are many opinions and definitions published for what a security policy actually is. In short, security policies define expectation and behaviors for protecting corporate assets.
- Security policies are not detailed specifics, implementation details or instructions. They are guidance.

WHAT IS A SECURITY POLICY?

- A good security policy or combination of policies, should, at a minimum, address the following:
  - a definition of information security
  - statement of management's intent to support the goals stated in the policy
  - definitions of general and specific responsibilities for all aspects of information security
  - specific security policies, principles, and standards including compliance with legal and contractual requirements; security training requirements; virus prevention and detection policy; and business continuity planning
  - guidelines for reporting security incidents

SCOPE OF SECURITY POLICY

- Security policies not only need to simply state WHAT is required, but also WHO is required to comply with the policy.
- Security policies should be written in simple, understandable terms.
- Policies are only implementation details for Processes and Procedures supporting the policies, which should contain the details of compliance.

HURDLES IN SECURITY POLICY

- Management support
- Dedication
- Expense
- Communication (Education)
- Assessment (Risk, Cost)
- Legal compliance (Law, Regulation)
- Business needs
- Cultural change

HOW MANY POLICIES DO YOU NEED?

- Not all policies are created equally!
- Some organizations are a mix of internal and external support structures. Sometimes policies do not overlap. In this case, there is a need for segmented policies.
- Implementation details are different.
- Support is different.

DISCUSSION POINT: Policy? What Policy?

- Whether on a customer premises to aid in the remediation of an incident or to transition work, when we ask for a copy of the corporate security policies we are often met with blank stares.
- Policies are rarely looked upon as tools. They are often considered INHIBITORS.
- Security policies can help prevent incidents, they help people outside of your organization (vendors, consultants) understand your requirements.

SECURITY POLICY CONSORTIUM

WHO CREATES POLICY?

- Best practices have shown that developing security policies within a collaborative group of diverse business owners is the most effective way.

POLICY CONSORTIUM

- Whether you are creating policy from scratch or adapting pre-written policy, you will want a diverse group of people to review the policy.

COLLABORATION IS KEY

- Representation from all areas of the organization will give breadth and scope to the policy.
- Assembling various competencies from across the business will aid in a strategic approach to policy creation. Each business unit can provide valuable input to security policy.

AM I A TARGET?

- The entire world is connected. You may think that you have nothing others want. This is never true. Malicous attacks target not only target information, they target infrastructure.
- Example – with BotNets on the rise, how have you adapted your patching policy? Are you sure that malicous intruders are not using cycles on your infrastructure systems to propagate code, harvest information, use your bandwidth for spam or storage even.

THREE KEYS

- EFFICIENCY: Effective IT risk managers follow the 80/20 rule (Pareto's Principle) : They expend 20 percent of their resources addressing 80 percent of their risk.
- UNDERSTANDING: "What we stumble with is assessing business operations and exposure to risk, and guarding them against potentially devastating threats." - Michael Assante/Gerald Freese
- COMMITTMENT: "Defense in depth requires intimate knowledge of business drivers and continous risk assessments."
- Information Security Magazine April 2005

ASSESSING RISK

- Who VS. What
- Fully document risk
- Some risk is acceptable, and should be well documented.

CALCULATING THE COST OF RISK

1. Assign value to the information and assets
2. Estimate potential loss per risk
3. Perform threat analysis
4. Derive the loss potential per threat (i.e. ALE per threat by using the information calculated in the first 3 steps)
5. Reduce assign or accept the risk

DISCUSSION POINT: You can't block that!!

- A summary of mitigating risk and content filtering.
- One man's trash is another man's treasure.
- The Viagra incident.
- Revenue generating applications.

OBTAINING SUPPORT FOR POLICY

OBTAINING SUPPORT

- Simplicity
- Understandable
- Concrete data
- $how value!

SIMPLICITY

- Security policies should be simple.
- Avoid addressing multiple issues with one policy statement.

UNDERSTANDABLE

- Before the policy is supported, it needs to be understandable.
- Know your audience
- Speak their language, not yours.
- If the policy is confusing, it will not be effective.

CONCRETE DATA

- Support the need for implementation with factual data.
- What is at stake?
- What are the implications?
- What can be done?

SHOW VALUE

- What will the organization gain from the policy?
- Value is related to several factors
  - Productivity
  - Cost Reduction
  - Cost Savings
  - Compliance
- Management correlates value with $$$, talk their language.

SECURITY POLICY T.C.O., R.O.I.

(and other cool acronyms)

COST OF POLICY

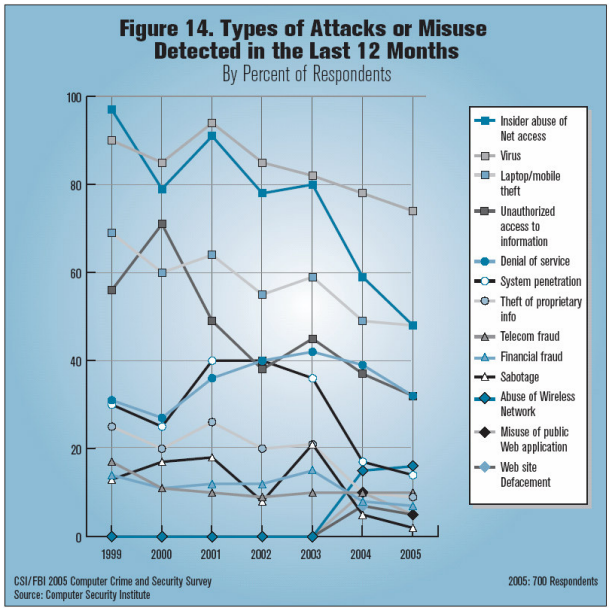
- What are the financial implications?
- R.O.I.
  - Ties performance to implementation costs. Tracks impacts.
- T.C.O.
  - Infrastructure, Education, Maintenance
- A.R.R.
  - Immediate savings, Payback

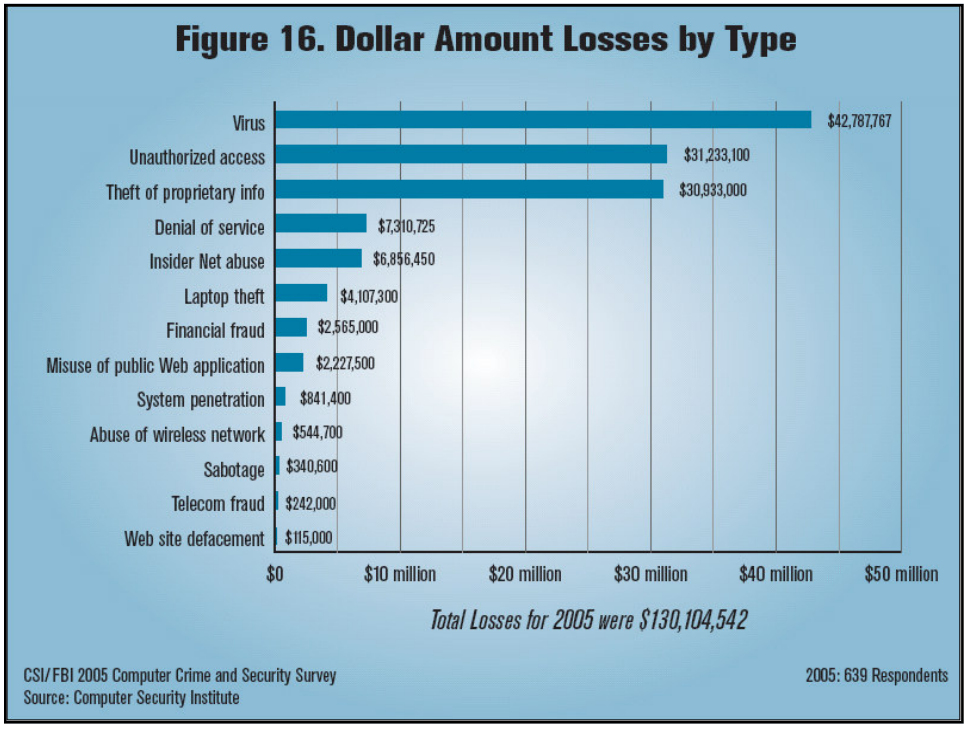
CISSP / ISO 17799 APPROACH

- Single Loss Expectancy (SLE)
  - Asset Value X Exposure Factor (EF)
  - Exposure Factor (EF) represents the percent of loss a realized threat could have on a certain asset
- Annual Loss Expectancy (ALE)
  - SLE X Annualized Rate of Occurrence (ARO)

MALWARE COSTS

- As of last year, the estimated minimum cost of the impact of high-tech crime on companies based in the U.K. with more than 1,000 employees was £2.45 billion (US$4.61 billion), the NHTCU said.
- http://www.infoworld.com/article/05/04/05/HNcybercrime_1.html





MEASUREMENTS & METRICS

MEASURING

- Metrics gathering is crucial to tracking success and failure of policy.
- How can you measure the effectiveness of policy?
  - Incidents
  - Exceptions (Risk Acceptance)
  - Education

INCIDENTS

- Security Incidents can provide valuable metrics that can aid policy owners in making needed changes.
  - System Integrity
  - Change Management
  - Response Capabilities
  - Remediation Factors
  - Technology drivers

EXCEPTIONS

- Many organizations issue exceptions or waivers for groups and/or individuals with specialized business needs.
- Documentation is key to compliance.

EDUCATION

- Who is properly trained on policy?
- Track acceptance and the saturation level of policy education.
  - Annual Validation
  - Incident reports
  - Who voices concerns

WHAT DOES THIS REALLY SAY?

- Tying risk and metrics together
- CIO Magazine polled top business executives to see what they have implemented in their security policy.
  - Network Security 55%
  - System Security 52%
- 24% of these executives do not track metrics for these policies. Only 37% measure.

POLICY COMPLIANCE

ENFORCE

- Enforce but do not inhibit productivity.
- A policy without teeth will not be taken seriously.

A CIO's PERSPECTIVE

- Dr. John Halamka (CIO, Beth Israel Deaconess Medical Center and Harvard Medical School)
- "There is no second chance if you violate trust."
- "If we don't want people to violate the policies, they have to know their boundaries."

VALIDATE OFTEN

- Repetition
- Policy Awareness and Compliance should be validated a minimum of once per year.

MAINTAINING POLICY

WHY DO POLICIES CHANGE?

- Audit results
- Security Incidents
- Regulatory compliance
- Customer and business partner requirements
- Management changes

AUDIT RESULTS

- Audits, whether internal or external, can have great impact on security policy.
- Audits help to identify
  - Gaps in current policy.
  - Gaps in our processes.
  - Compliancy issues

SECURITY INCIDENTS

- Security incidents are always crucial times to evaluate policy.
- Comparative gap analysis of policies and actions taken during incidents can reveal a great deal.

REGULATORY COMPLIANCE

- Changes in the Law
- Regulatory Compliance
  - HIPAA
  - Sarbanes-Oxley

BUSINESS REQUIREMENTS

- Generically, as business changes, requirements change.
- Business processes can quickly create the need for new policy or abandoning old policy.

MANAGEMENT REQUIREMENTS

- Effective policies need management support.
- Some managers require tighter controls.

EDUCATION & THE SECURITY POLICY

SECURITY DEPTH

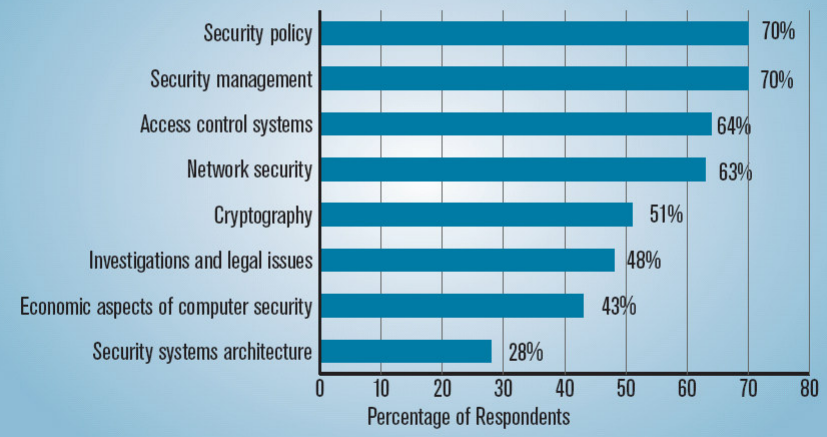
- A security policy goes far beyond the simple idea of, “keeping the bad guys out” - Chris Wan

EDUCATE YOUR ORGANIZATION

- Communicate! Who needs to know?
- A well defined and communicated information security policy serves purpose:
  - It makes clear WHAT is being protected and WHY.
  - It clearly states the RESPONSIBILITY for that protection.

Figure 20. Importance of Security Awareness Training

Percentage of Respondents Identifying as Important

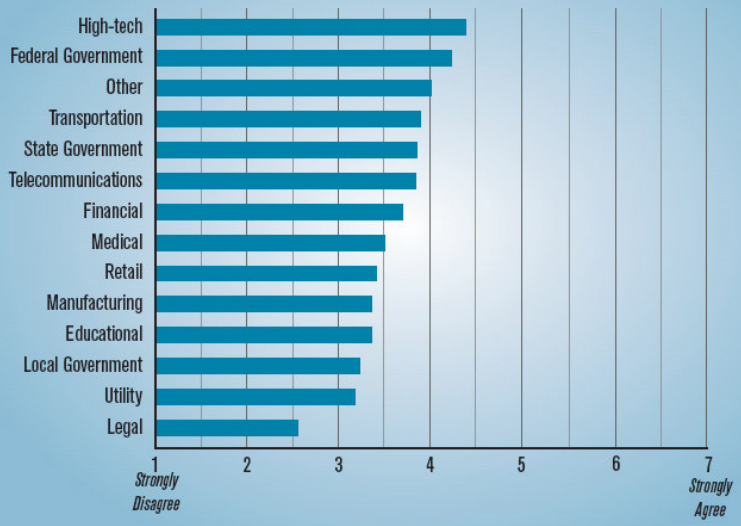


CSI/FBI 2005 Computer Crime and Security Survey
Source: Computer Security Institute

2005: 694 Respondents

Figure 19. Organization Invests the Appropriate Amount on Security Awareness Training

Mean Values Reported on a Seven-Point Scale



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

2005: 698 Respondents

SECURITY AWARE

- Education of security policy helps to create a security conscience culture, which can be your most effective asset.

- Threats
- Confidentiality
- Integrity
- Responsibility
- Availability

DISCUSSION POINT: Virus security website and computer based training

- Use your policy as the educational tool.

- Create automated learning.

- Information availability.

- Centralized information hubs.
  - Disseminate and Collect data

SECURITY POLICY and THE LAW

COMPLIANCY

- Know the law and how it affects your policies.
- Many organizations are either being forced by customer requirements or other regulation to comply with information security laws.
  - Privacy
  - Information Protection
  - Information Disclosure

SECURITY POLICY AND THE LAW!

- Legality in the Media
  - http://in.tech.yahoo.com/040427/137/2csgs.html
  - http://www.computerworld.co.nz/news.nsf/NL/5D897F828DC204C3CC256E35006C95AE
  - http://news.bbc.co.uk/2/hi/technology/3256814.stm
  - http://spamnews.com/blog/spamNEWS/archives/2004/04/employees_could_sue_over_porn_spam.html
  - http://www.gammassl.co.uk/topics/time/RTPs.html
  - http://www.fcw.com/article89361-06-27-05-Print

DISCUSSION POINT: "Help, Help, I'm being repressed!"

- Spam, specifically pornography and related unsolicited advertisements over the past years have created needs for security policy.
- Organizations can be sued for not protecting assets (infrastructure, employees, etc).
- Many employers have been successfully sued for not taking appropriate actions.

SPECIFIC MALWARE POLICY

QUOTABLE EXPERTS!

- In a recent article in Information Security experts tell us straight up! (September 2005)
- "Trust no one" – Mikko Hypponen (F-Secure) goes on to say, "Ultimately, we all have to take responsibility for our actions, and only we can rely on ourselves to get that done."
- "Risk management needs to be multifaceted" – Eva Chen (Trend Micro)
- "Don't be complacent" – Sara Santarelli (MCI)

MALWARE POLICY

- Malware IS everywhere.
- Adapt policy to educate users and set expectations and responsibilities.
- Security Conscience Culture – The Best Defense!

MALWARE POLICY

- Email (Mass Mailers, Phishing, Spam)
- File Transfers
- External Media
- Instant Messaging
- Mobile Devices
- Internet Browsing
- Patching
- System Security (password, av, firewall)
- Incident Reporting

DISCUSSION POINT: How the Malware got there, How the Malware stayed!

- It never surprises me.
- Environments with old malware
- Customers that keep getting re-infected.

TESTING AND ANALYSIS: THE ART OF INTELLIGENCE

MALWARE TESTING

- For most organizations the practice of testing and/or use of malicious code should be discouraged.
- We have seen several cases where customers have used live malware to test current or new product sets.
- While the practice may seem reasonable, it can lead to unfavorable results, including outbreak.

MALWARE TESTING

- IF your organization accepts the risk of live malware testing, be sure that you have strict policy in place to enforce control and compliance.
- Strict Access
- Segmentation
- Policy and Code of Conduct
- Training
- Handling and Containment strategies
- Due Diligence in Security

SUM IT UP!

SECURITY POLICY

- First Steps:

- Review what you already have.
- Identify business requirements.
- Identify the threats related to those requirements.
- Identify specific policies.
- Create.
- Implement.
- Gather metrics.
- Review and audit.
- Rinse, Repeat.

LEARNING FROM MISTAKES

- Those who cannot learn from history are doomed to repeat it. - George Santayana

ASSESS YOUR POLICY NEEDS

- Why do you need a policy?
- What needs protecting?
- How do you protect it?

PLAN OUT YOUR POLICY

- What are the risks and benefits?
- What can you prove?
- Who will need to be involved in the policy creation?
- How will you gain management support?

IMPLEMENT YOUR POLICY

- Policy provides a FOUNDATION on which to interpret and resolve any conflicts that might arise later.

MONITOR YOUR POLICY

- Change control
- Compliance
- Integration

RESPOND TO YOUR POLICY

- Enforce - The lack of a well defined security policy and supporting program may result in the organization's inability to identify, and take disciplinary action against an individual or group of individuals who violate security policies or commit a crime.

AUDIT YOUR POLICY

- Poorly defined or ambiguous policies can put the organization and its information assets at unnecessary risk.
- Continuously assess risk.

ADAPT YOUR POLICY

- Listen to those directly affected by policy
- Update your policy

SIMPLICITY IN POLICY

- Policies are the business tools that all users can/should understand.
- Policies should be simple.
- Policies should be straight forward.
- Repetition in moderation
  - Policies for malicious code should be referenced often. (Email, File Sharing, External Media, etc).

IMPLEMENTING SUCCESS

- Experience shows that the following factors[1] are critical to the successful implementation of information security within an organization:
  - *Security policy, objectives and activities that reflect the business objectives*
  - *An approach to implementing security that is consistent with the organizational culture;*
  - *A good understanding of the security requirements, risk assessment and risk management;*
  - *Effective marketing of security to all managers and employees;*
  - *Distribution of guidance on information security policy and standards to all employees and contractors.*
  - *Providing appropriate training and education;*
  - *A comprehensive and balanced system of measurement which is used to evaluate performance in information security management and feedback suggestions for improvement.*

- [1] BS7799-1:1999 Part 1: Code of practice for information security management.

THANK YOU!