



Emerging Security Threats



Maurizio Taffone mtaffone@cisco.com

Product Manager Security

European Markets

Agenda

- Trends in **Motivation**
- Existing threats and **Lessons from the Past**
- **New** Threats
- Coping with Threats: **Conclusions** and Recommendations

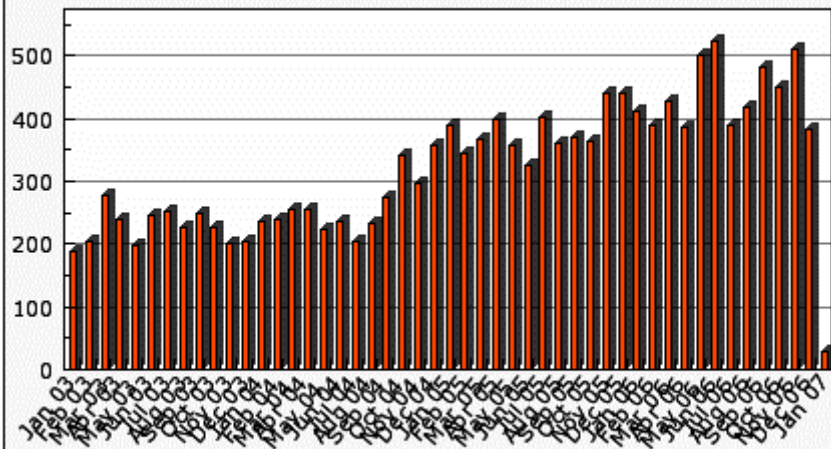
Trends in motivations



The **threat** economy

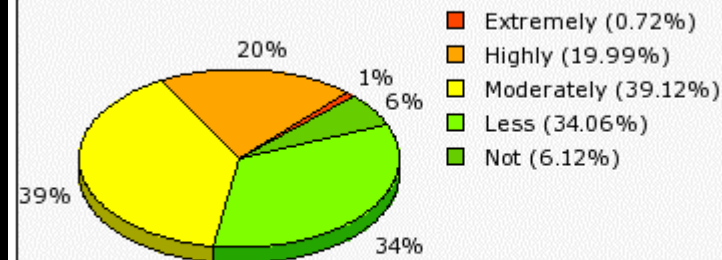
Some statistics

**Secunia Security Advisories
All Advisories (2003 - 2007)**



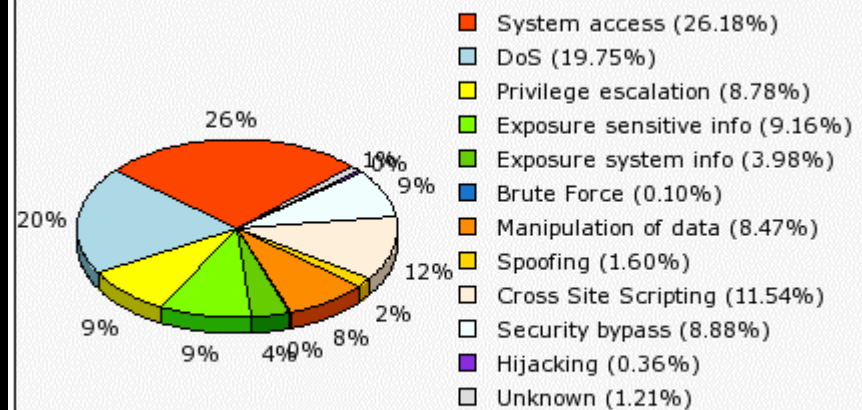
This graph was generated by Secunia.
Based on vulnerability information available at <http://secunia.com/>

**Secunia Security Advisories
All Advisories Criticality (2003 - 2007)**



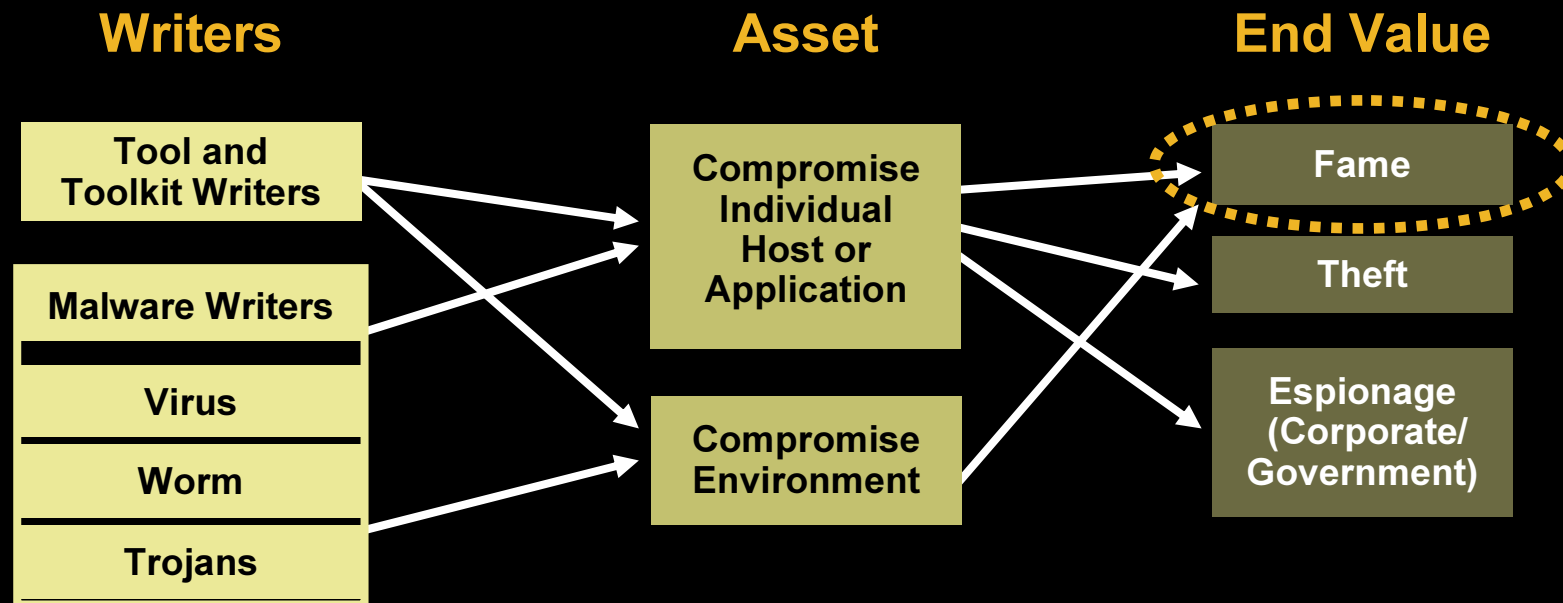
This graph was generated by Secunia.
Based on vulnerability information available at <http://secunia.com/>

**Secunia Security Advisories
All Advisories Impact (2003 - 2007)**

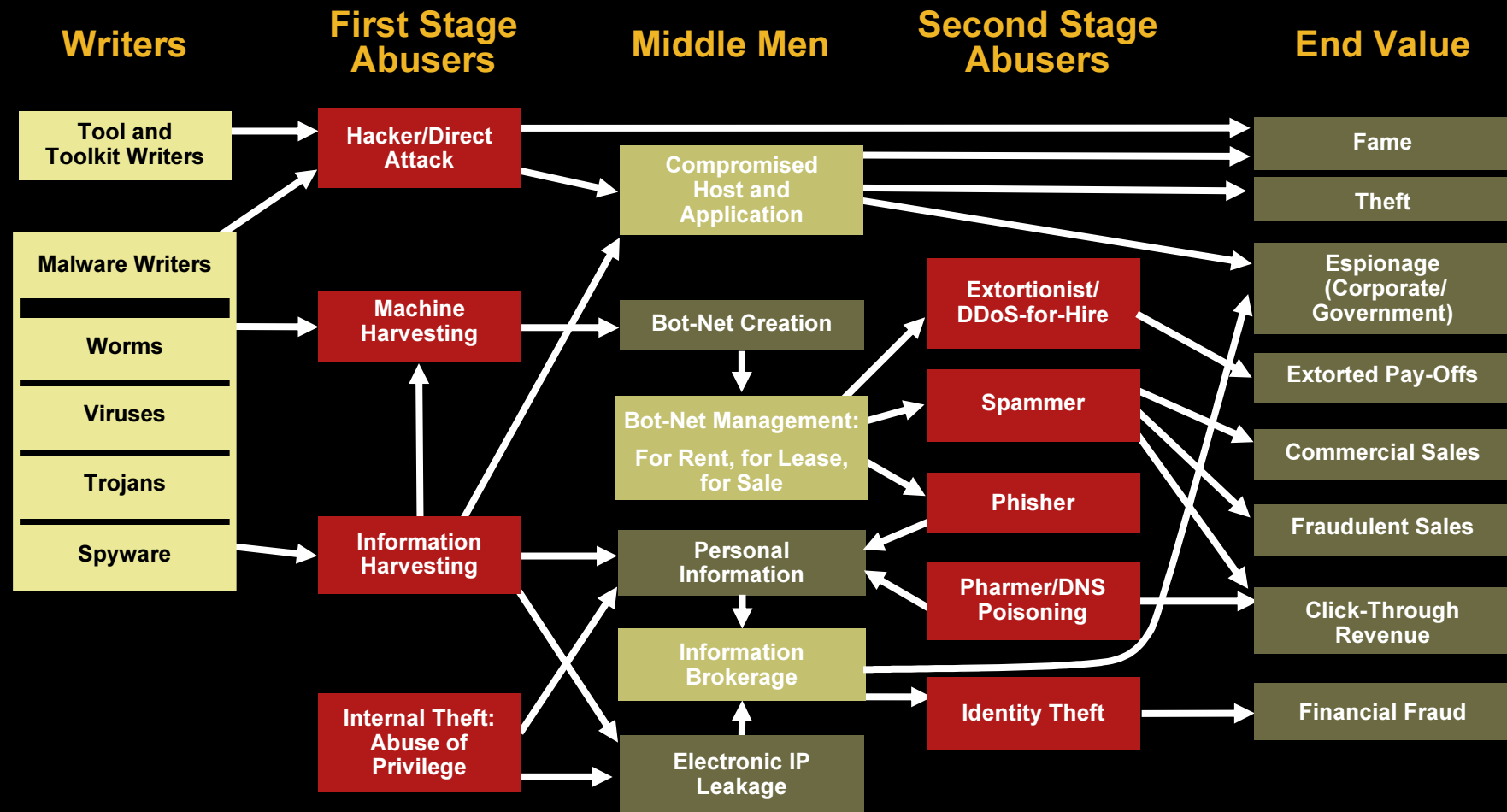


This graph was generated by Secunia.
Based on vulnerability information available at <http://secunia.com/>

Threat Economy: In the Past



Threat Economy: Today



Changing Face of Threats

- Change in **purpose**

Shift from fame to other, higher-value motivations: profit, revenge, competition

By far the strongest motivator is now profit: there's good, relatively easy money to be made by committing a computer crime or two

- Change in **expected behavior**

Less noisy

More sophisticated

More variants, smaller scope of each

Old and **unresolved** threats

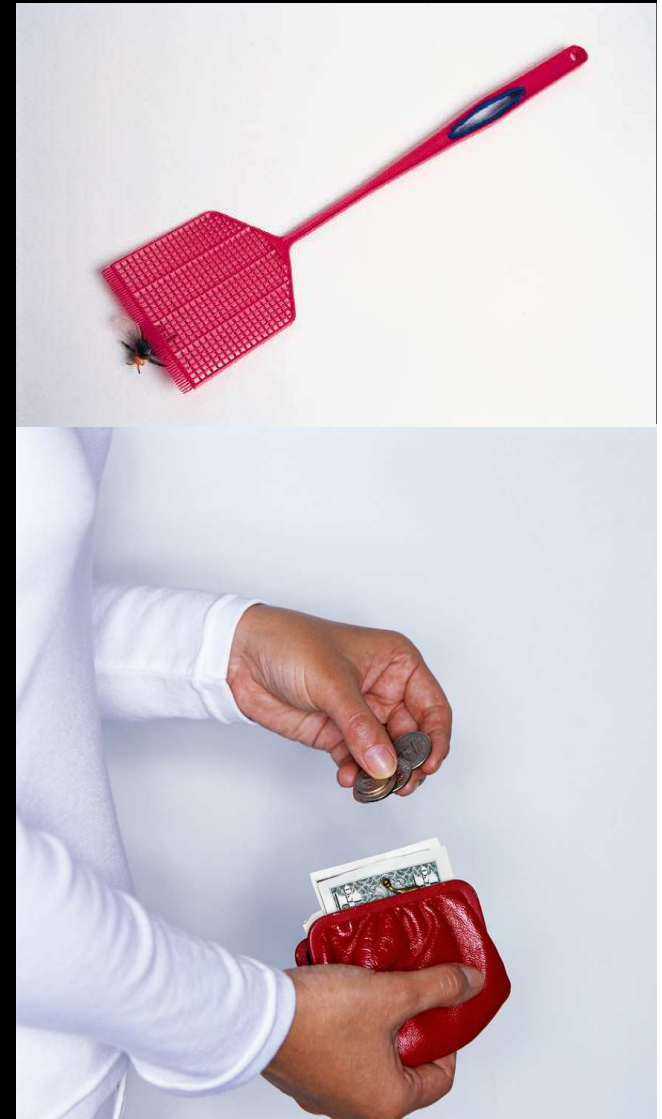


Old (and Unresolved) Threats

- Worms and Viruses
- Botnets
- Spam
- Spyware
- Phishing, Pharming, and Identity Theft
- Application Security

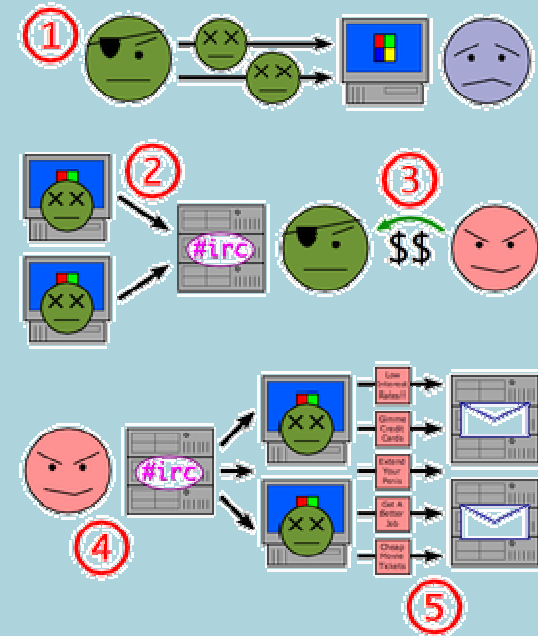
Threats to Your Users: Worms and Viruses

- **2006** - Not a big year in worms and viruses...Why?
- Opportunity shrinking
- Motivation changing



Resurgence of Botnets

- **Botnet:** a collection of compromised machines running programs under a common command and control infrastructure
- **Building the Botnet:**
 - Viruses, worms; infected spam; drive-by downloads; etc.
- **Controlling the Botnet:**
 - Covert-channel of some form



Using a Botnet to Send Spam

1. A botnet operator sends out viruses or worms, infecting ordinary users' Windows PCs
2. The PCs log into an IRC server or other communications medium
3. A spammer purchases access to the botnet from the operator
4. The spammer sends instructions via the IRC server to the infected PCs—
5. ...causing them to send out spam messages to mail servers

Source: www.wikipedia.org

What About Spyware?

- **Still a major threat**

 - Drive-by downloads still a major source of infestation

 - Image-based vulnerabilities in particular enable this (WMF and jpg vulnerabilities are good examples)

 - However, confusing or misleading EULAs still a problem

- **A Trojan by any other name—**

 - Spyware is increasingly indistinguishable from certain classes of virus

 - Nasty race condition: sheer number of variants makes it very difficult for technology solutions to hit 100% accuracy at a given moment

- **Rise of intelligent spyware**

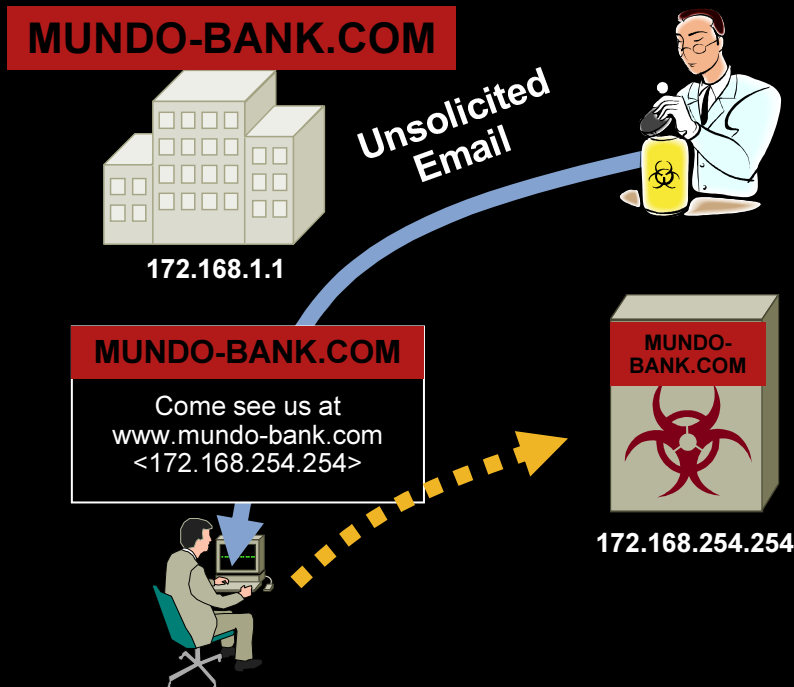
 - Directed advertising is more valuable than undirected

 - More sophisticated spyware matches user-gathered data with directed advertising

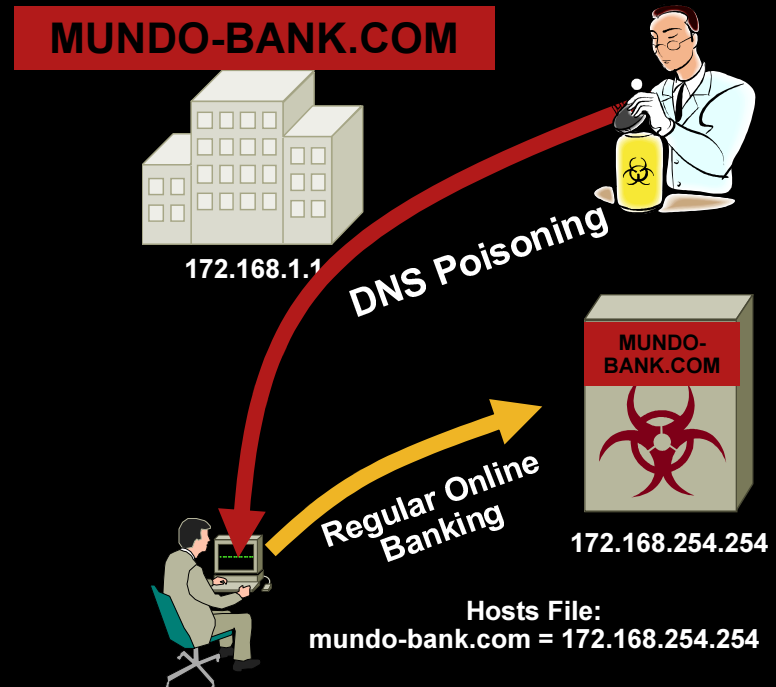
 - Bot-based spyware is also more valuable, as it can be updated over time

Phishing, Pharming, and Identity Theft

PHISHING



PHARMING



- Identity theft continues to be a problem
- Phishing scams growing in sophistication every day
- Protecting your users: implement some technology, but don't forget user education!!

- If you're a target:
 - Consider "personalization" technologies (e.g. user-chosen images on a webpage)
 - Support identified mail initiatives, like DKIM

Example: Hybrid Threats

Combination Attacks involving Viruses and Phishing

As an example of phishing, please note that some of our customers reported receiving the following pop-up screen while logged on our secure site. The pop-up screen is known to be a hoax and contains the following information:

Approximate date of the hoax: 3/29/2006 - present

Title of Pop-Up Box : Security Measures [see below]

Information Requested: Social Security Number, Mother's Maiden Name, Date of Birth

Security Measures

We are currently performing regular maintenance of our security measures

Please fill in the correct information for the following category to verify your identity.

SSN:

Mother's Maiden Name:

Date of Birth: / / MM/DD/YYYY

Please note that this fraudulent activity may be the result of a computer virus and is not a part of the American Express website. If you received this pop-up box, your computer may have this virus. The use of both anti-virus software and a firewall to protect your PC is strongly recommended. For more information, please [click here](#).

If you received this pop-up box and entered your information, please contact American Express by calling the number on the back of your card.

Application Security: Port 443 Problem

- We've "solved" the port 80 problem
 - Port 80 problem: everything rides on port 80, as it's universally open outbound
 - However, that gives rise to:
- **Port 443 problem**: encrypted port 80 problem
- How do I enforce policy over the encrypted tunnel?
 - Service use enforcement**: P2P file sharing; instant messaging; outbound information conduits
 - Acceptable use monitoring**: anonymous proxies, redirects, etc. to get around URL Filtering
 - Malware scanning**: cannot scan objects—email, IM, web downloads
- Note the corollary (and less discussed) problem of port 22 (SSH)

New threats



New Threats

- RFID Threats
- Service-Oriented Architectures
- Voice over IP Threats
- Device Proliferation and Mobile Devices
- Outsourcing
- Distributed Workforce
- Connected Home

New Threats in Application Security: XML and Service Oriented Architectures

What is an SOA?

- Interlinked system of services, communicating with a standard methodology (XML, SOAP, etc) – “Web services”
- Enables “systems of systems”; tying together disparate backend application systems into a cohesive whole

Major Security Considerations:

- Directly exposes the application tier to external entities for the first time
- Security concerns involve both *access control* problems (based on strong or weak identity credentials), as well as *new attack types* (“X-malware”, “X-DoS”, etc)
- Enables new security capabilities for integrity and confidentiality: field-level encryption services; document signing; content transformation services, etc.
- Not “new” this year per se, but starting to hit critical mass

New Threat: Voice over IP Threats

Gartner Group Sums It up Best:

- “The hype surrounding VoIP threats has, thus far, outpaced actual attacks”

Thoughts on Why:

- **Opportunity:** well understood business risk is promoting integration of security technologies in voice deployments
- **Opportunity:** limited pool of technical experts on voice within attacker community
- **Motivation:** no well-established business model driving financial incentives to attack

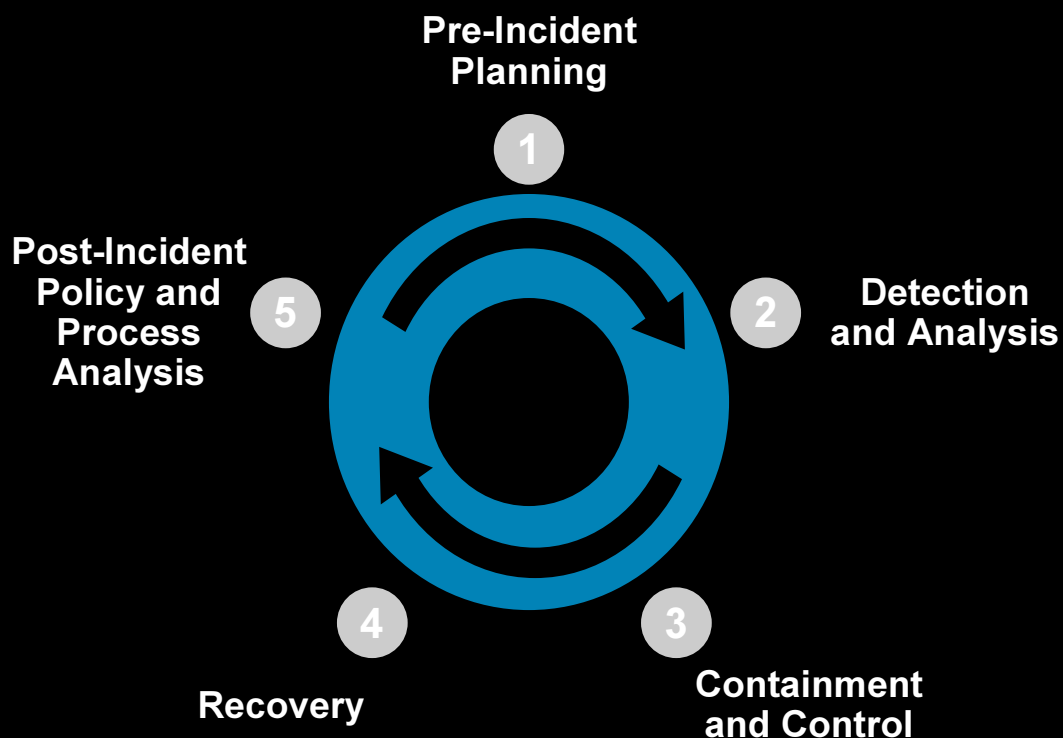
Coping with Threats



Conclusions and Recommendations

Incident Response Basics

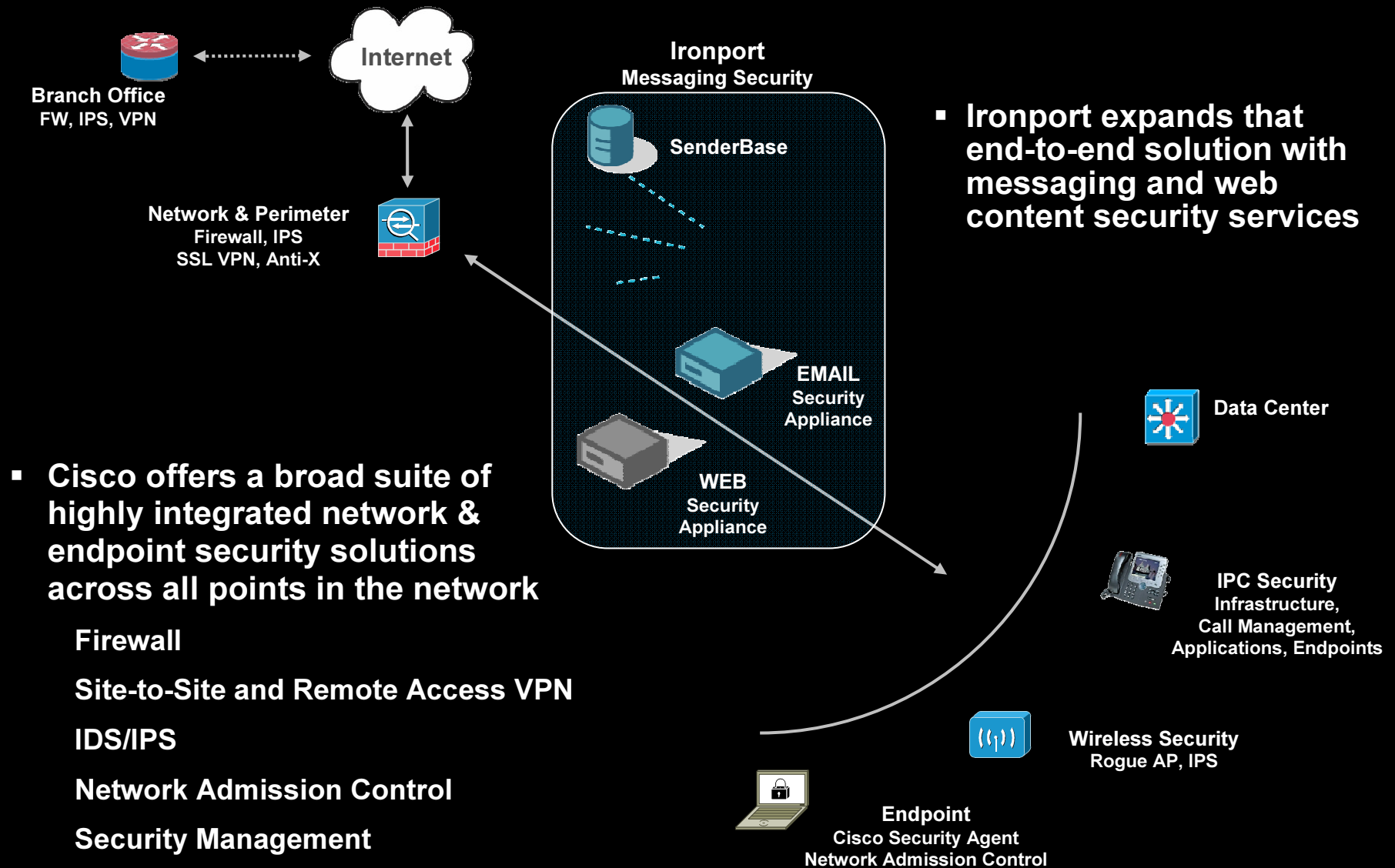
Incident Response Life Cycle



- Most important step: **Step 1**
- Second most important step: **Step 5**
- Most commonly skipped step: **Step 1**
- Second most commonly skipped step: **Step 5**
- *There's a message in here somewhere...*

Adapted from reports at www.gartner.com and www.securityfocus.com

Filling in the Cisco Security Solution



Cisco Agreement to Acquire Ironport Systems

- **Market**

- Cisco expanding from \$5B Network Security market into adjacent \$2.0B Messaging Security market

- **Market Position**

- Ironport is Messaging Security Market Leader

- **Products and Technology**

- Ironport Messaging Security Solutions built on:
 - High-performance Appliances
 - Ironport Messaging Security Services: SenderBase[®] (Anti-Spam, Content Filtering, etc.)
 - Partner Services: Anti-Virus, URL Filtering, etc.

