Underground Economy report. Data Breach: Causes, Circumstances, and Remedies

Don Ng, CISSP

Enterprise Security Director, Asia Pacific

July 9th 2009

Symantec Report on the Underground Economy

Underground Economy – Key Messages

- The Underground Economy is geographically diverse and shows the ability to generate millions of dollars in revenue for cybercriminals.
- It is a self-sustaining system where tools that aid in fraud and theft can be purchased and the stolen information obtained by those tools can then be sold.
- Cybercriminals range from loose collections of individuals to organized and sophisticated groups, all with a common purpose.
- Software piracy closely reflects the retail market; software categories with the highest volume of sales are also the most heavily pirated.

Underground Economy – Key Findings

- Symantec estimates the value of total advertised goods on underground economy servers was over $276 million for the reporting period.
- The potential worth of the top seller on the UE is $6.4 million.
- The category of credit card information accounted for 31% of all advertisements for sale.
- 12% of UE servers were located in Asia Pacific & Japan.
- Desktop computer games made up 49% of software being pirated.
- In total, the approximate U.S. retail value of all tracking files observed by Symantec was $83.4 million.

Symantec Report on the Underground Economy

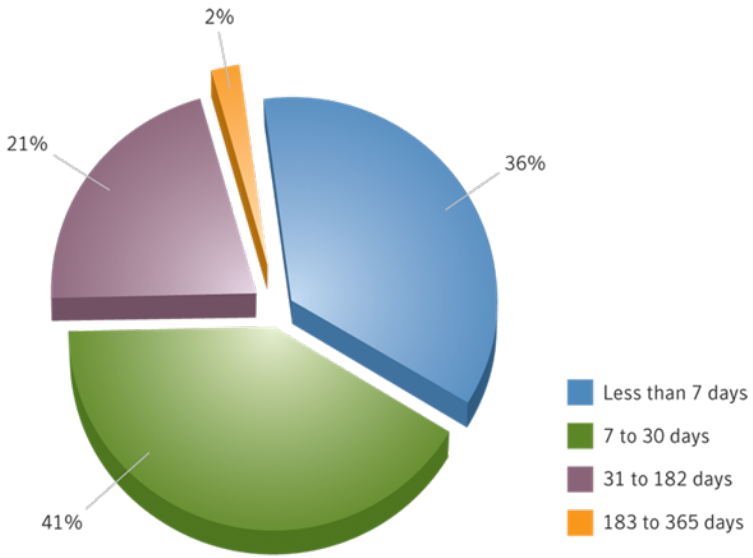
Key Facts and Figures

Cybercriminals range from loose collections of individuals to organized and sophisticated groups, all with a ***common purpose***.

Financial Gains!!!

Servers and Channels
IRC Server Lifespans

- The median average observed server lifespan was 10 days
- Servers may be abandoned by participants or shut down by owners of legitimate IRC networks
- One of the largest observed IRC server networks had approximately 28,000 channels and 90,000 users



Average server lifespan by days

The Underground Economy is ***geographically diverse*** and shows the ability to generate ***millions of dollars*** in revenue for cybercriminals.

Goods and Services
Value of Advertised Goods & Services

- Symantec estimates the value of total advertised goods on underground economy servers was over $276 million for the reporting period
- The potential worth of all credit cards advertised during this reporting period would be $5.3 billion
- Using the average advertised balance of $40,000 financial accounts would potentially be worth $1.7 billion

Rank	Category	Percentage
1	Credit card information	59%
2	Identity theft information	16%
3	Server accounts	10%
4	Financial accounts	8%
5	Spam and phishing information	6%
6	Financial theft tools	<1%
7	Compromised computers	<1%
8	Malicious applications	<1%
9	Website accounts	<1%
10	Online gaming accounts	<1%

Value of advertised goods as a percentage of total, by category

The Underground Economy is a ***self-sustaining system*** where tools that aid in fraud and theft can be purchased and the stolen information obtained by those tools can then be sold.

Goods and Services Advertised by Category

- Credit card information category ranked highest between July 1, 2007 and June 30, 2008, with 31% of sale advertisements and 24% of requests
- Credit card information and Financial accounts are relatively easy to cash out, providing immediate monetary gain

Rank for Sale	Rank Requested	Category	Percentage for Sale	Percentage Requested
1	1	Credit card information	31%	24%
2	3	Financial accounts	20%	18%
3	2	Spam and phishing information	19%	21%
4	4	Withdrawal service	7%	13%
5	5	Identity theft information	7%	10%
6	7	Server accounts	5%	4%
7	6	Compromised computers	4%	4%
8	9	Website accounts	3%	2%
9	8	Malicious applications	2%	2%
10	10	Retail accounts	1%	1%

Goods and services available for sale, by category

Goods and Services
Malicious Tools

- Malicious tools can be used to steal confidential information
- Attack kits, spam and phishing kits, malicious code, and exploits are available on the underground economy
- Exploits and attack kits had the highest average prices
- Pricing is based on supply and demand as well as the tool's capabilities

Attack Kit Type	Average Price	Price Range
Botnet	$225	$150–$300
Autorooter	$70	$40–$100
SQL injection tools	$63	$15–$150
Shopadmin exploiter	$33	$20–$45
RFI scanner	$26	$5–$100
LFI scanner	$23	$15–$30
XSS scanner	$20	$10–$30

Attack kit prices

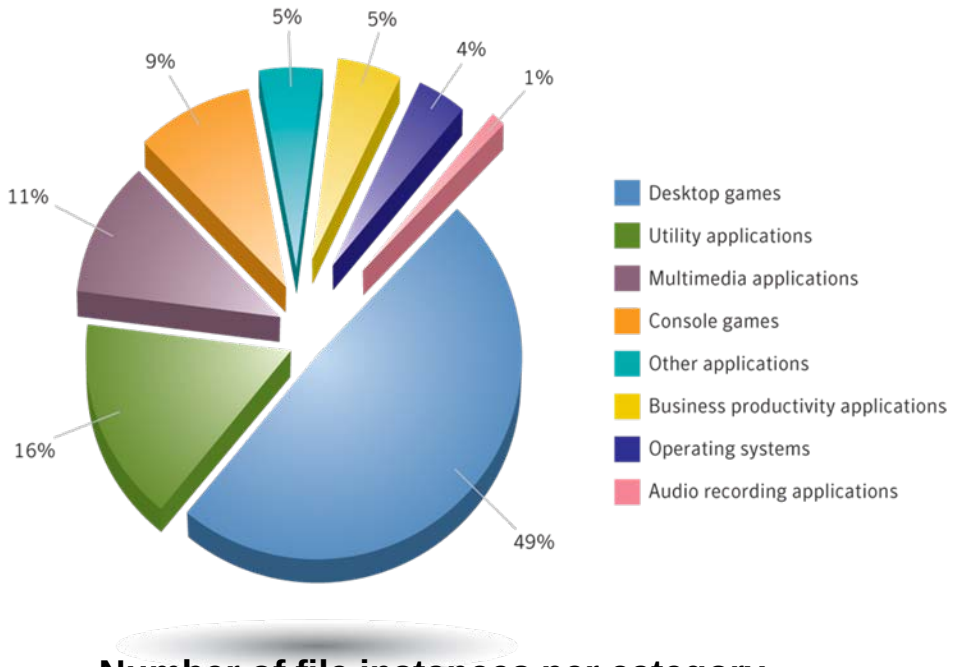
Exploit Type	Average Price	Price Range
Site-specific vulnerability (financial site)	$740	$100–$2,999
Remote file include exploit (500 links)	$200	$150–$250
Shopadmin (50 exploitable shops)	$150	$100–$200
Browser exploit	$37	$5–$60
Remote file include exploit (100 links)	$34	$20–$50
Remote file include exploit (200 links)	$70	$50–$80
Remote operating system exploit	$9	$8–$10

Exploit prices

Software piracy closely reflects the retail market; software categories with the highest volume of sales are also the most heavily pirated.

Piracy
File Instances by Category

- Desktop computer games were the most frequently seen tracking files by a significant margin, accounting for 49% of all file instances observed
- Retail sales of desktop games are among the highest of any category
- Number of tracking files for software tends to increase when a new release is available



Number of file instances per category

Piracy
Financial Effect on Business Sectors

- The total approximate value of all categorized tracking files observed by Symantec was $83.4 million
- Multimedia software accounted for approximately $53 million
- While there were more desktop game file instances the lower total value was due to a lower average price

Rank	Category	Approximate Value	Percentage of Total Value of Categories	Price Range of Software	Percentage of File Instances
1	Multimedia applications	$53,098,000	65%	$40–$8,000	11%
2	Business productivity applications	$8,671,000	11%	$400–$700	5%
3	Desktop games	$8,062,000	10%	$50	49%
4	Audio recording applications	$2,992,000	4%	$250–$700	1%
5	Utility applications	$2,573,000	3%	$20–$230	16%
6	Operating systems	$2,237,000	3%	$100–$220	4%
7	Other applications	$2,152,000	3%	$30–$600	5%
8	Console games	$1,286,000	0%	$35–$60	9%

Approximate dollar value of file instances observed

Enterprise Mitigation

- To help prevent loss of confidential data that could be used in identity fraud, enterprises should:
  - Implement database encryption
  - Limit access to databases including use of least privilege
  - Employ secure communications channels to transfer sensitive information
  - Ensure that endpoint security measures are in place to prevent confidential information from being copied to portable media such as USB devices and compact discs

Consumer Mitigation

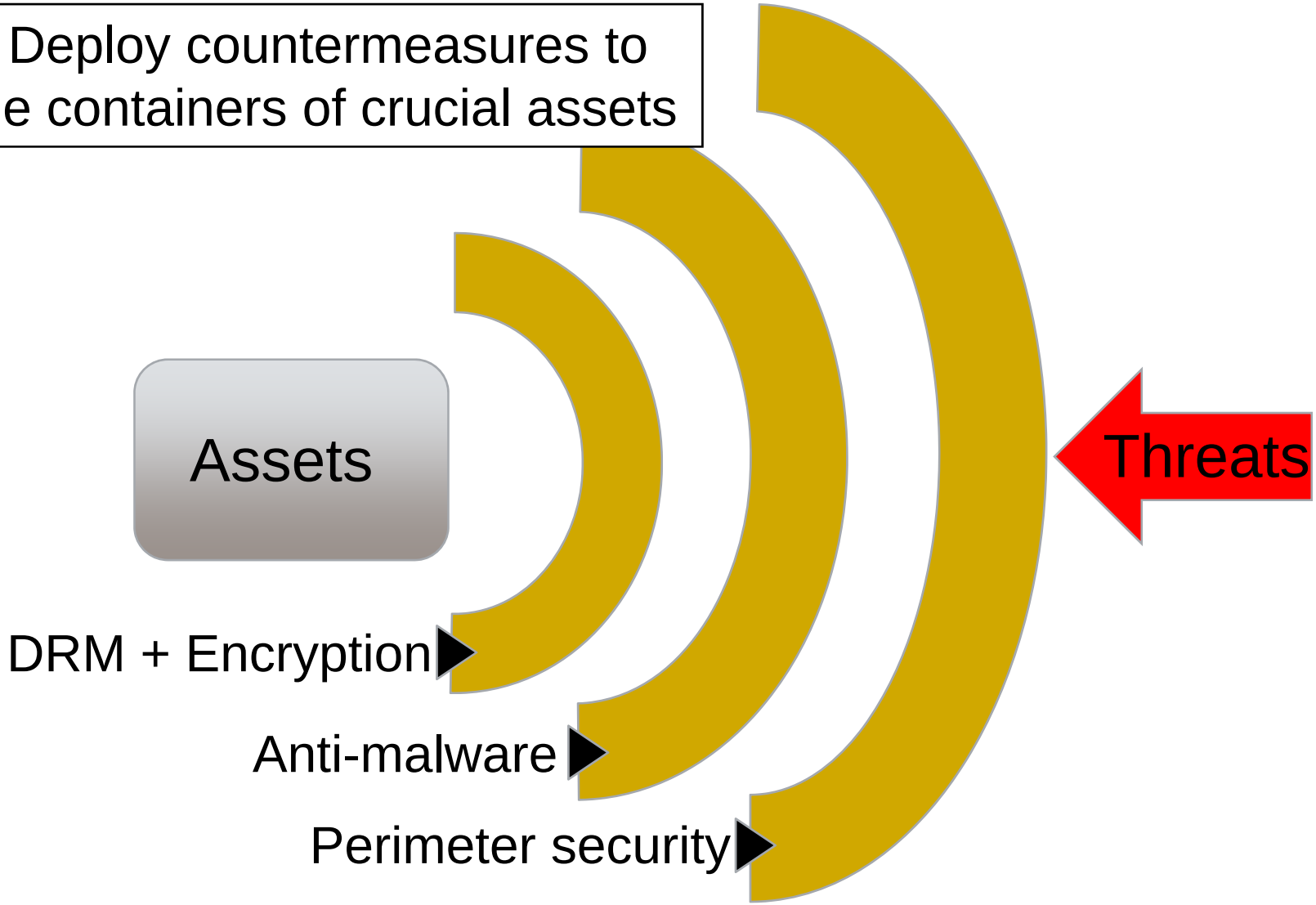
- To help prevent the loss of confidential information that could be used in identity fraud, consumers should:
  - Employ email filtering solutions to help block fraudulent messages such as those used in phishing attacks
  - Use defense-in-depth strategies like antivirus software, firewalls, and anti-phishing toolbars
  - Limit the amount of sensitive personal information stored on their computers
  - Utilize strong passwords and change them on a regular basis
  - Do not store online account credentials using the Web browser's "remember password" feature

Agenda

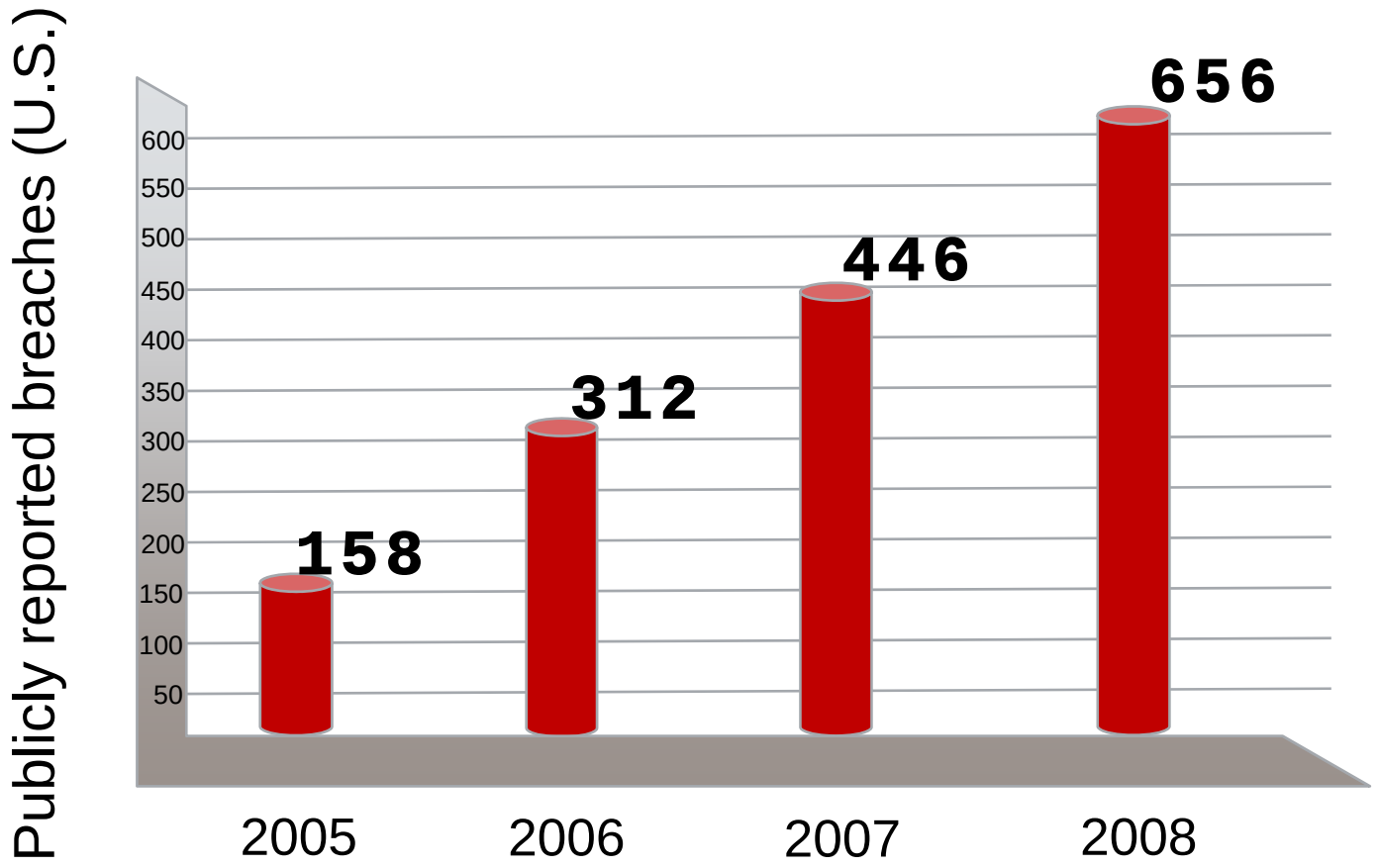
- What's wrong with security today?
- Data breach: causes and circumstances
- Examples of breach stopped by Symantec
- Managing risk factors for breach

Mission statement of traditional security

Mission: Deploy countermeasures to protect the containers of crucial assets



High breaches rates pose a question



If traditional approaches work **why** are breach rates so high?

Data Breach: Causes and Circumstances

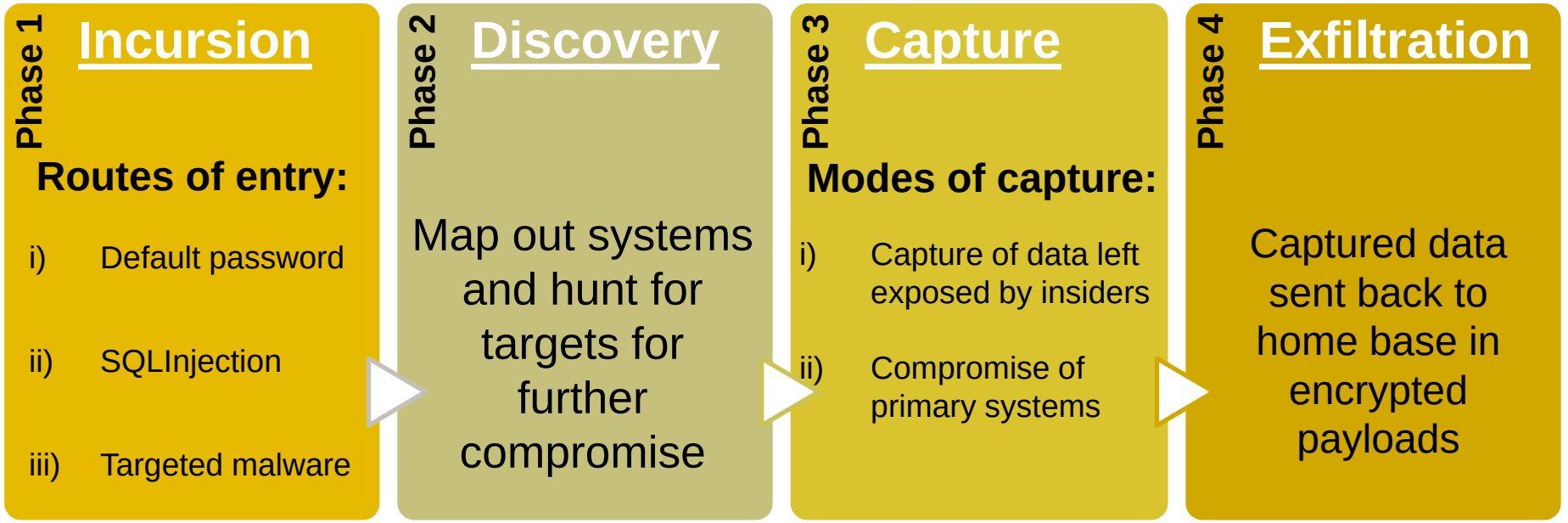
Data Breach Threat Agents

Hackers and malware

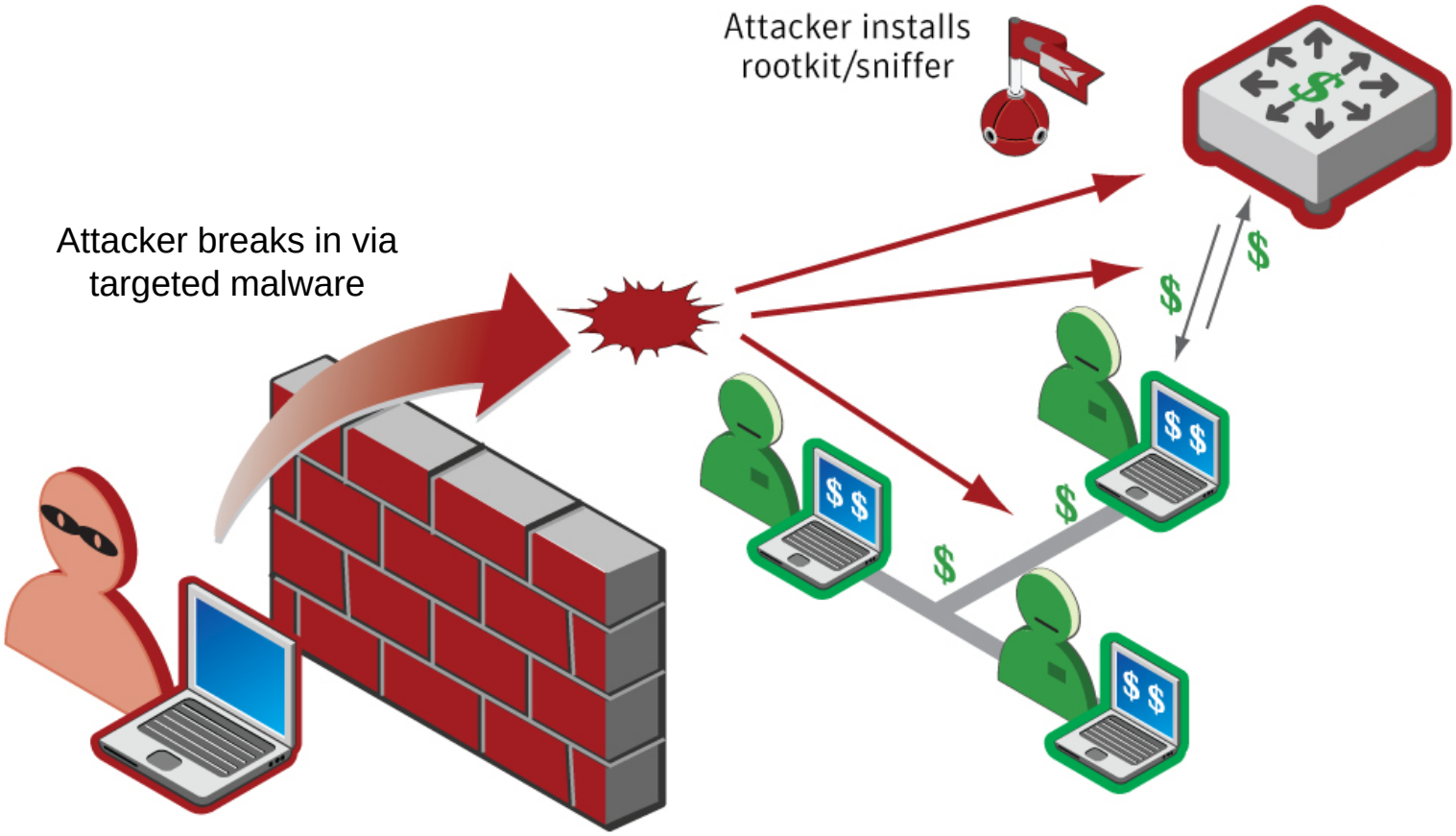
Well meaning insiders

Malicious Insiders

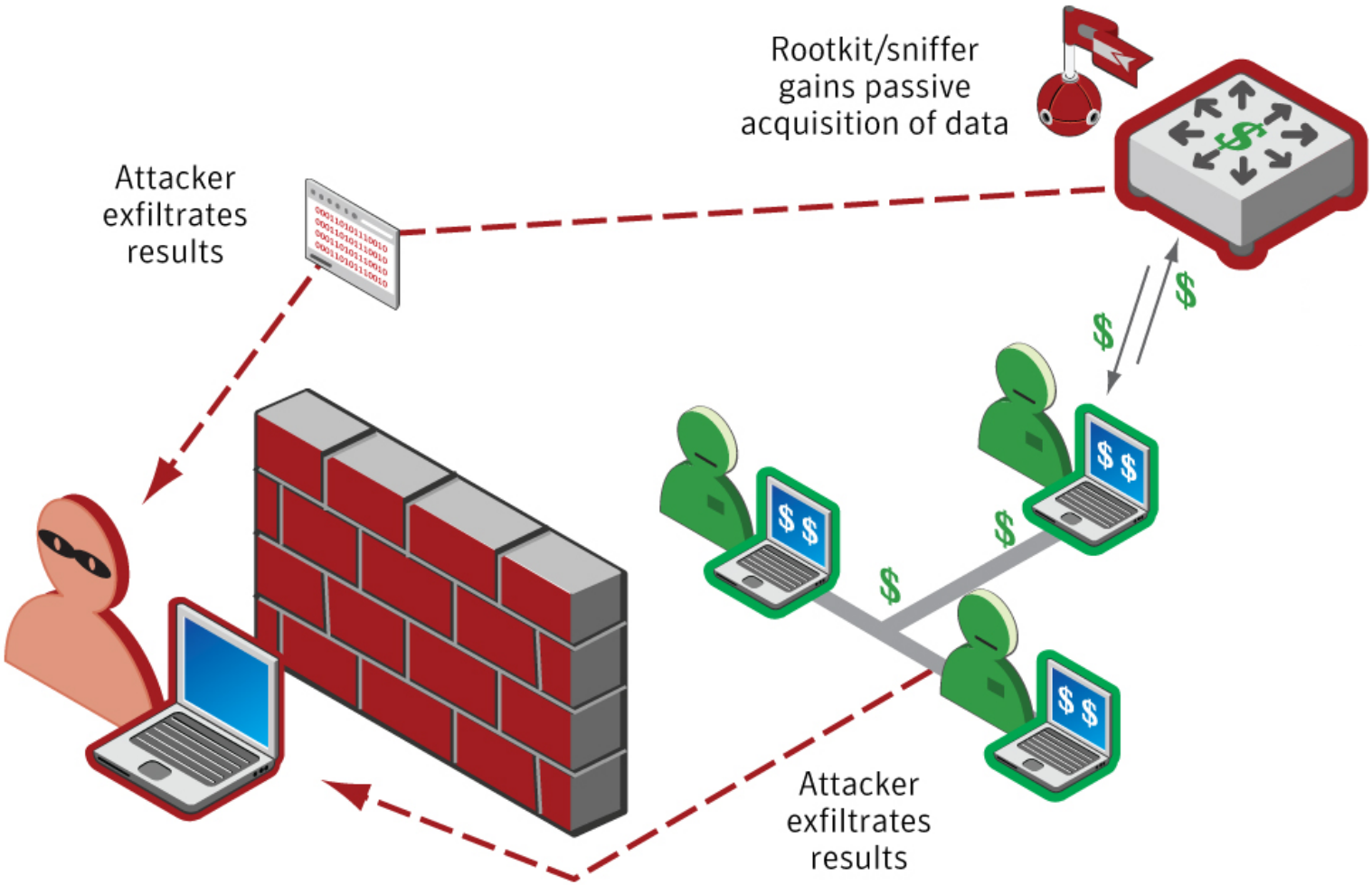
Summary attack tree: hacker breach



Incursion and Discovery



Capture and Exfiltration



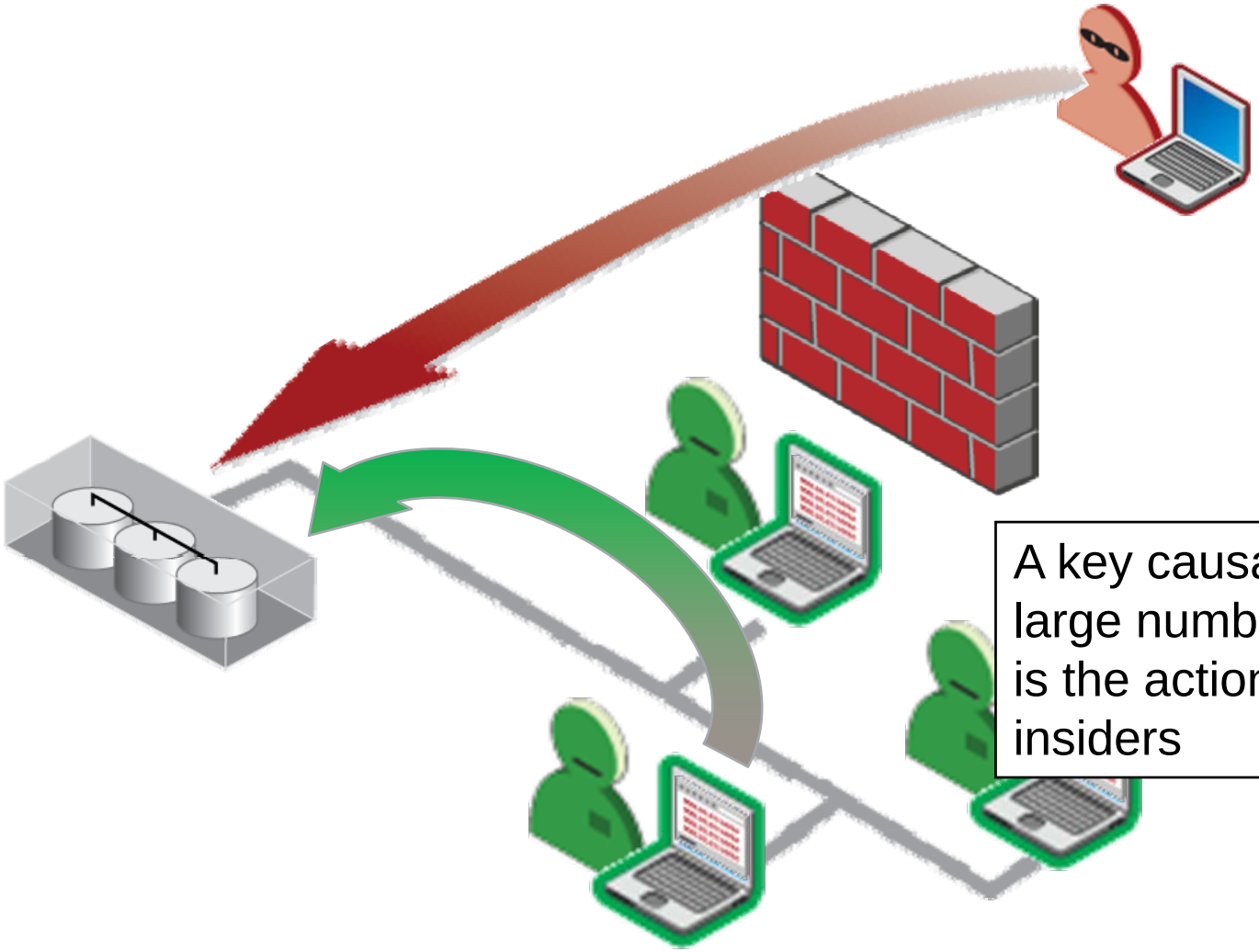
Data Breach Threat Agents

Hackers and malware

Well meaning insiders

Malicious Insiders

Well Meaning Insiders



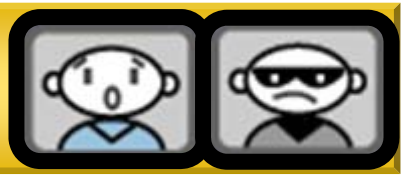
A key causative factor in a large number of breach cases is the action of well-meaning insiders

Well meaning insiders enable hackers

(*) Data targeted by hackers is confidential data that the victim organization did not know was stored there

Source: "Verizon Data Breach Investigation Report: 2009"

Well meaning insider data breach

Insiders and Hackers  *vs.* Major Federal Agency

- **SETUP**
  - Agency detected traffic going outbound to a known hacker site
  - Knew they were in trouble, but needed us to help them know how much
- **WHAT WE DID**
  - Symantec DLP found the original target of the hacker's efforts
  - A software development team had copies of this employee data
- **RESULT**
  - Internal data spill event is now under control
  - DLP is instrumental in the cleanup

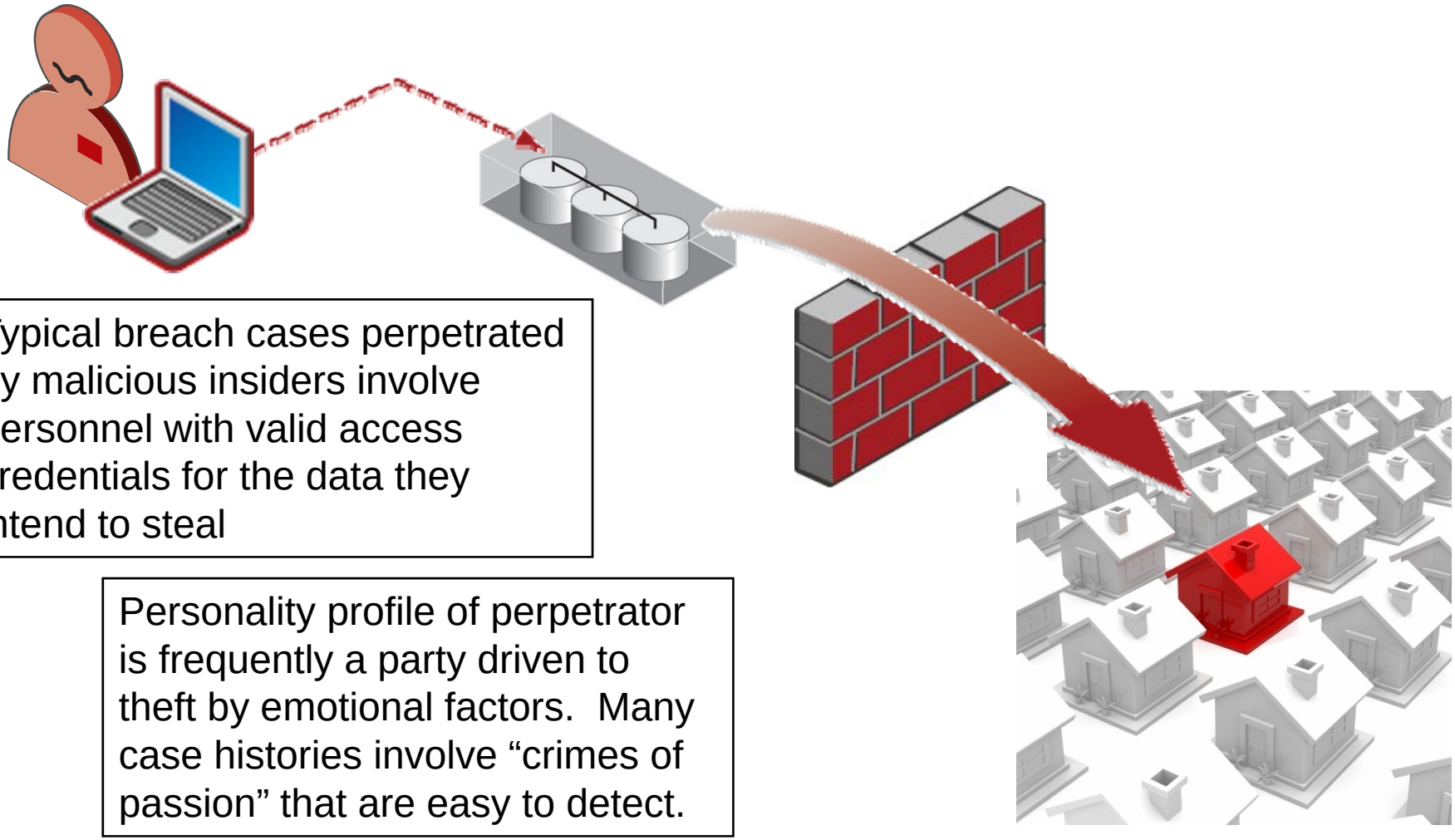
Data Breach Threat Agents

Hackers and malware

Well meaning insiders

Malicious Insiders

Malicious Insiders



Typical breach cases perpetrated by malicious insiders involve personnel with valid access credentials for the data they intend to steal

Personality profile of perpetrator is frequently a party driven to theft by emotional factors. Many case histories involve “crimes of passion” that are easy to detect.

Malicious insider data breach

Malicious insiders  *vs.* Leading Savings and Loan

- **SETUP**
  - After RIF rumors, employees decided to start stealing data
  - Over 12 sales people tried to email customer data out the door
- **WHAT WE DID**
  - Symantec DLP blocked numerous attempts at theft that day
- **RESULT**
  - We stopped a dozen theft attempts cold
  - DLP is now considered “mission critical” with this customer

What Hackers Target

Poorly Protected Infrastructure

Poorly protected information

Lack of IT Policies

Poorly Managed Endpoints

Enterprise Security Strategy

Secured Infrastructure

Information centric

Risk Based and Policy Driven

Operationalized

Symantec Security Portfolio

Symantec Protection Suites

Data Loss Prevention Suite

symantec™

Control Compliance Suite

Altiris Management Suite

In conclusion

- How do I know if I am at risk? Answer these questions:
  - Do I know if there are signs of incursion into my perimeter?
  - Where is my data? Where is it going?
  - Are my critical internal systems well defended?

Questions?