



## Cyber Crime, Cyber Cops : New Waves in Online Policing

Peter J Reid, CIPP  
EDS Chief Privacy Officer  
Office: 972-605-0641  
Mobile: 214-546-7089  
Email: [peter.j.reid@eds.com](mailto:peter.j.reid@eds.com)

# Cybercrime Impact

Cybercrime is a law enforcement issue

...but not only a law enforcement issue

It is also a huge issue for all public and private sector organizations

....as well as for parents and schools

# Wikipedia Definition - Cybercrime

Although the term Cybercrime is usually restricted to describing criminal activity in which the computer or network is an essential part of the crime, this term is also used to include traditional crimes in which computers or networks are used to enable the illicit activity.

Examples of Cybercrime which the **computer or network is a tool of the criminal activity** include spamming and criminal copyright crimes, particularly those facilitated through peer-to-peer networks.

Examples of Cybercrime in which the **computer or network is a target of criminal activity** include unauthorized access (i.e. defeating access controls), malicious code, and denial-of-service attacks.

Examples of Cybercrime in which the **computer or network is a place of criminal activity** include theft of service (in particular, telecom fraud) and certain financial frauds.

Finally, examples of **traditional crimes facilitated through the use of computers or networks** include Nigerian 419 or other social engineering frauds (e.g., hacking "phishing", identity theft, child pornography, online gambling, securities fraud, etc.).

**Cyberstalking is an example of a traditional crime -- harassment** -- that has taken a new form when facilitated through computer networks.

Additionally, certain other information crimes, including trade secret theft and industrial or economic espionage, are sometimes considered Cybercrimes when computers or networks are involved.

**Cybercrime in the context of national security** may involve hacktivism (online activity intended to influence policy), traditional espionage, or information warfare and related activities.

# Symantec Definition - Cybercrime

Like traditional crime, Cybercrime can take many shapes and can occur nearly anytime or anyplace. Criminals committing Cybercrime use a number of methods, depending on their skill-set and their goal. This should not be surprising: Cybercrime is, after all, simply 'crime' with some sort of 'computer' or 'cyber' aspect.

**Type I Cybercrime** has the following characteristics: It is generally a single event from the perspective of the victim. For example, the victim unknowingly downloads a Trojan horse which installs a keystroke logger on his or her machine. Alternatively, the victim might receive an e-mail containing what claims to be a link to known entity, but in reality is a link to a hostile website.

It is often facilitated by Crimeware programs such as keystroke loggers, viruses, rootkits or Trojan horses.

Software flaws or vulnerabilities often provide the foothold for the attacker. For example, criminals controlling a website may take advantage of a vulnerability in a Web browser to place a Trojan horse on the victim's computer.

Examples of this type of Cybercrime include but are not limited to phishing, theft or manipulation of data or services via hacking or viruses, identity theft, and bank or e-commerce fraud.

# Symantec Definition - Cybercrime (cont)

**Type II Cybercrime**, at the other end of the spectrum, includes, but is not limited to activities such as

- Cyberstalking and harassment
- child predation
- extortion
- blackmail
- stock market manipulation
- complex corporate espionage
- and planning or carrying out terrorist activities.

The characteristics of Type II Cybercrime are:

It is generally an on-going series of events, involving repeated interactions with the target. For example, the target is contacted in a chat room by someone who, over time, attempts to establish a relationship. Eventually, the criminal exploits the relationship to commit a crime. Or, members of a terrorist cell or criminal organization may use hidden messages to communicate in a public forum to plan activities or discuss money laundering locations, for example.

It is generally facilitated by programs that do not fit into under the classification Crimeware. For example, conversations may take place using IM (instant messaging) clients or files may be transferred using FTP.

# What is Crimeware?

The software tools used in Cybercrime are sometimes referred to as Crimeware. Crimeware is software that is:

- used in the commission of the criminal act
- not generally regarded as a desirable software or hardware application
- not involuntarily enabling the crime
- Like Cybercrime itself, the term Crimeware covers a wide range of different malicious, or potentially malicious software.

However, it is important to remember that not all software used in the commission of a computer-based or computer-facilitated crime can be defined as Crimeware.

For example, while **IM client** may be used in the commission of a Cybercrime, the instant messaging application software itself is not considered Crimeware.

**FTP clients** may also be used in the commission of crimes; however, they are not considered Crimeware. Crimeware does, however, include programs which may be classified as bots, keystroke loggers, spyware, backdoors and Trojan horses.

# How technology has exacerbated Cybercrime

## Processing

Mainframe – minicomputer – desktop – laptop – pda

## Memory

KB – MB – GB – TB – PB

## Bandwidth and Internet Access

bps – kbps – mbps – gbps

## The situation today:

- Multiple PCs in the home (few are properly protected)
- High speed processors with massive storage (200+ GB)
- Wired homes and pervasive wireless connectivity
- Broadband and DSL
- Used for business (work from home employees)
- Used by children (downloading music, videos, social networking and what else)

# Storage Costs Dropping

## Information object

## How many bytes

A single text character	1 byte	
A typewritten page	2 kilobyte s (KBs)	
A short novel	1 megabyte (MB)	
The contents of a 3.5 inch floppy disk	1.44 megabytes	
A high-resolution photograph	2 megabytes	
The complete works of Shakespeare	5 megabytes	
A minute of high-fidelity sound	10 megabytes	
One meter of shelved books	100 megabytes	
The contents of a CD-ROM	500 megabytes	
A pickup truck filled with books	1 gigabyte (GB)	USB Memory Stick \$15
The contents of a DVD	17 gigabyte s	
A library floor of academic journals	100 gigabytes	
50,000 trees made into paper and printed	1 terabyte (TB)	1 TB Hard Drive <\$300
An academic research library	2 terabytes	
The print collections of the U.S. Library of Congress	10 terabytes	
All U.S. academic research libraries	2 petabytes (PB)	
All hard disk capacity developed in 1995	20 petabytes	
All printed material in the world	200 petabytes	
Total volume of information generated in 1999	2 exabytes (EB)	
All words ever spoken by human beings	5 exabytes	

# What is a Terabyte

A terabyte is:

- More than 300 feature length movies.
- 40,000 faxes.
- 15,000 CDs converted to MP3 at high fidelity.
- Enough words that it would take every adult in America speaking at the same time five minutes to say them all.

A terabyte is the equivalent of 38 miles of full file cabinets or 250 million pages of text.

GET ALL THE  
INFORMATION YOU CAN,  
WE'LL THINK OF A  
USE FOR IT LATER.



# Who is EDS?

- Electronic Data Systems (EDS) founded by Ross Perot in 1962
- Created the Outsourcing Industry
- Today ranked #2 in the outsourcing industry
- Outsourcing Services include
  - IT Outsourcing
  - Applications Development & Maintenance
  - Business Process Outsourcing
- 135,000 employees in 65 countries
- Headquarters in Plano, TX



# Why Cybercrime is a concern for EDS today

## – **We manage globally:**

- 300,000 servers; over 150 data centers and just over 3 million client desktops
- Call Centre services from 149 locations in 47 languages
- Over 15 million IP addresses
- 9 million user names & passwords

## – **We process annually:**

- Over 5 billion credit card transactions
- 500 million travel reservation transactions
- \$95 billion in U.S. Medicaid benefits for more than 20 million recipients

## – **We serve clients in every major industry and geography, including:**

- 75 of the top 100 manufacturing companies
- 250 healthcare clients in 21 countries
- 109 domestic and international air carriers
- 346 government clients in 25 countries
- more than 200 clients in 21 countries worldwide through our BPO Administrative and Transaction business units.

# So how do we address Cybercrime?

- Employ over 2,500 security and privacy professionals worldwide
- Security Policies and Standards based on ISO 17799/27001
- Comprehensive “Defense in Depth” Security Program
  - Manage and monitor more than 2,500 firewalls and 3,000 intrusion detection systems for threats and vulnerabilities
  - Block over 4 billion “junk” mail messages from ever reaching our employees' and our clients' e-mail environments each month
  - Detect and quarantine 940,000 viruses annually
  - Protect more than 200 petabytes of data globally
  - Help secure over 1 million applications and 2.5 billion lines of code



# What else does EDS do to address Cybercrime

- Participate in Critical Infrastructure Protection initiative
- Receive feeds every 5 minutes on new and emerging threats
- Maintain an internal web site that is accessible by all employees that has current threat information; employees can sign up for periodic emails
- Have established Incident Management Process and Tools in place
- Deploying Data Loss Prevention solution to detect leakage of confidential information and intellectual property
- Looking at other tools to detect Cybercrime and other criminal activity
- Involve law enforcement whenever appropriate

**It's a matter of trust...**



**EDS removes the barriers**

Peter J Reid  
EDS Chief Privacy Officer  
5400 Legacy Drive  
Plano, TX, 75024  
Office: 972-605-0641  
Mobile: 972-983-1652  
Email: peter.j.reid@eds.com

# PWC Crime Survey

## 1.1 Companies reporting fraud (2003-2007)



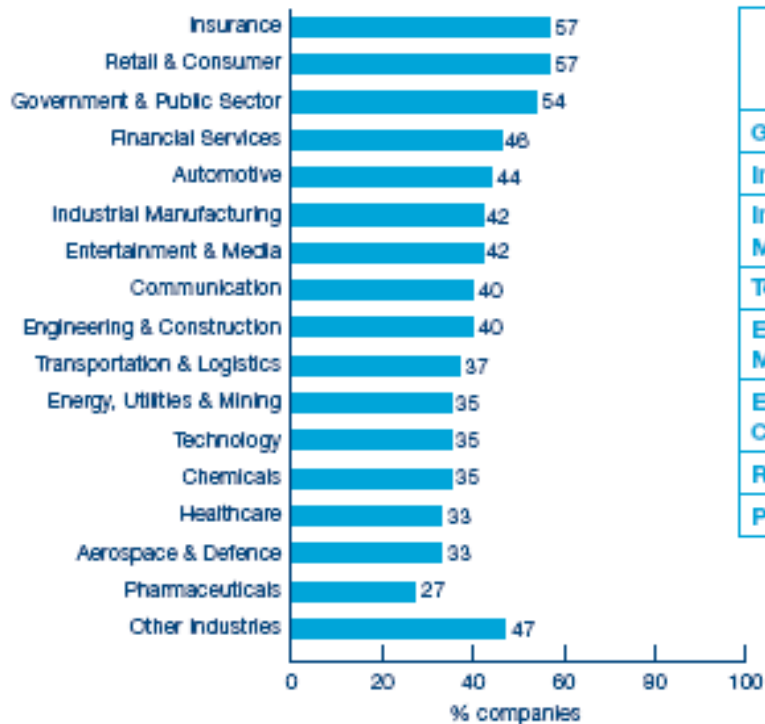
## 1.2 Companies reporting fraud, according to their number of employees



Source: PWC Survey: Economic Crime: People, Culture and Controls  
Available at [pwc.com/crimesurvey](http://pwc.com/crimesurvey)

# PWC Crime Survey

## 1.6 Companies reporting fraud by industry sector

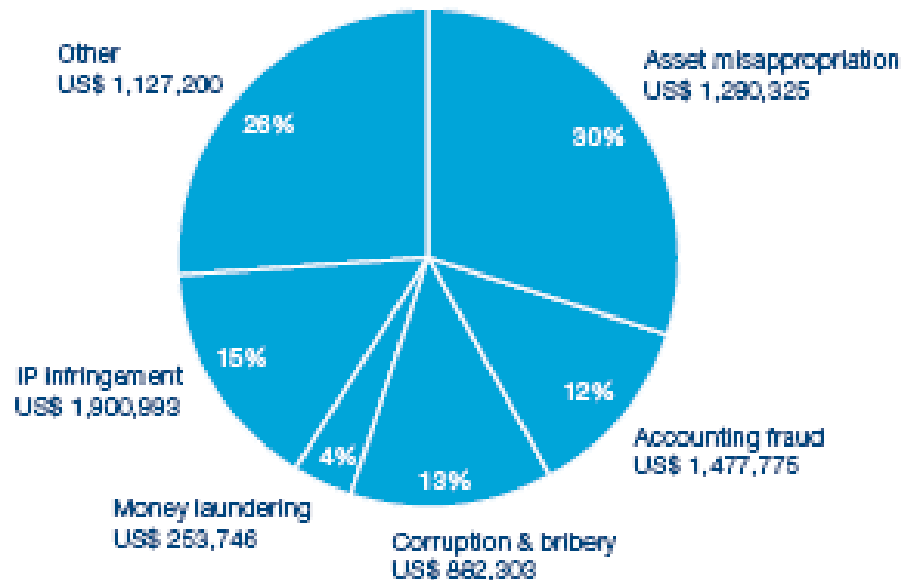


	Average direct loss (US\$)	Average management cost (US\$)	Total average cost to business (US\$)
Global	2,420,700	550,358	2,971,058
Insurance	4,476,717	1,018,114	5,494,831
Industrial Manufacturing	4,337,975	758,851	5,096,826
Technology	3,462,819	554,895	4,017,714
Entertainment & Media	3,118,516	300,862	3,419,378
Engineering & Construction	2,919,975	360,313	3,280,288
Retail & Consumer	2,605,749	481,224	3,086,973
Pharmaceuticals	2,479,047	357,251	2,836,298

Source: PWC Survey: Economic Crime: People, Culture and Controls  
Available at [pwc.com/crimesurvey](http://pwc.com/crimesurvey)

# PWC Crime Survey

## 1.8 Victimization rate combined with average loss by type of fraud<sup>8</sup>



Average loss from fraud over two years per company in 2007: **US\$ 2,420,700**

Average loss from fraud over two years per company in 2005: **US\$ 1,732,253**

Total loss reported by respondents over two years: **In excess of US\$ 4.2 billion**

Estimated total losses including the undetected losses of companies with a weaker control environment: **US\$ 5.7 billion**

Source: PWC Survey: Economic Crime: People, Culture and Controls  
Available at [pwc.com/crimesurvey](http://pwc.com/crimesurvey)

# PWC Crime Survey

## 1.10 Companies reporting significant collateral damage associated with perpetrator's position



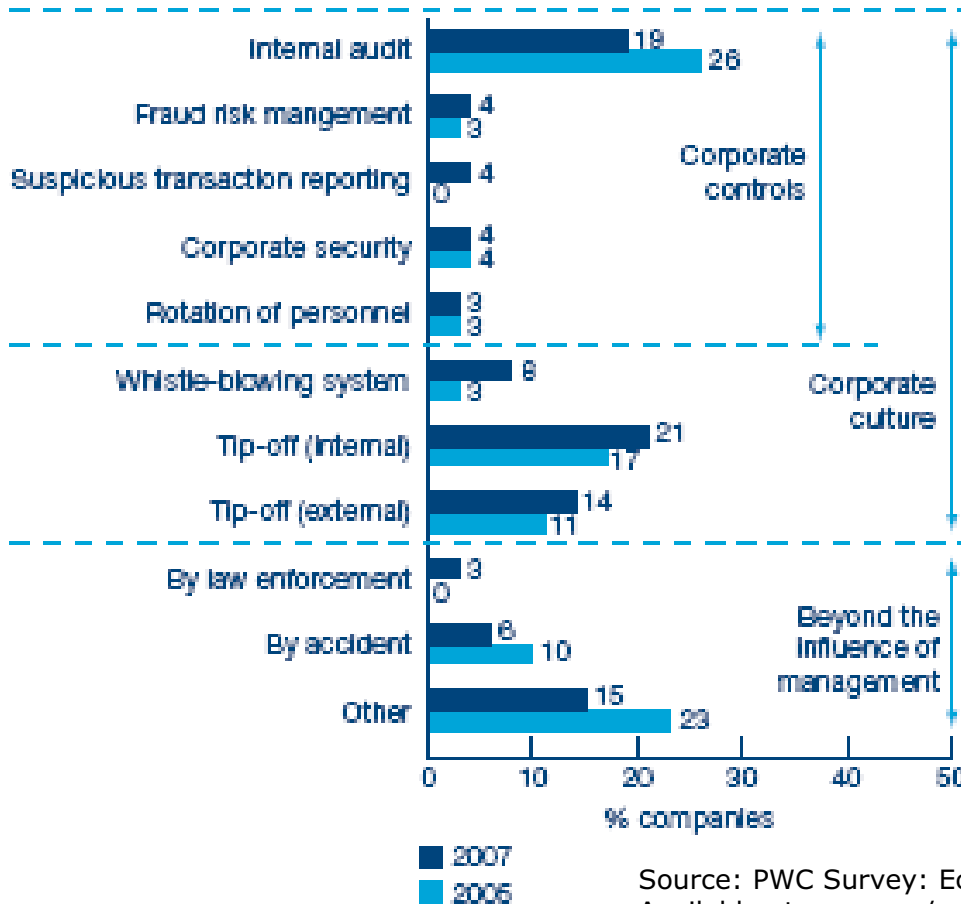
### What fraud costs

Direct losses (on average)	US\$ 3,242,095
+	
Management costs (on average)	US\$ 550,356
+	
Damage to the brand	88% cases
+	
Damage to staff morale	88% cases
+	
Damage to external business relations	84% cases
+	
Costs of dealing with the regulator	84% cases
+	
Damage to relations with the regulator	80% cases
+	
Damage to share value	9% cases

Source: PWC Survey: Economic Crime: People, Culture and Controls  
Available at [pwc.com/crimesurvey](http://pwc.com/crimesurvey)

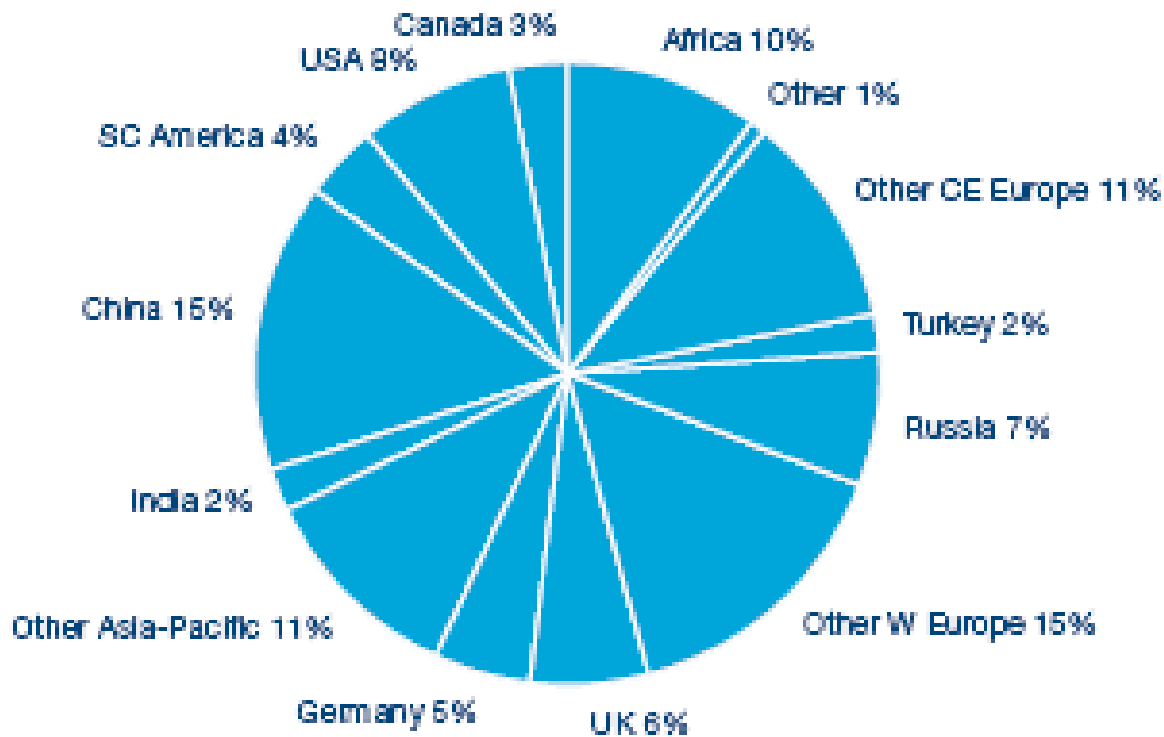
# PWC Crime Survey

## 1.11 Detection methods<sup>10</sup>



# PWC Crime Survey

## 1.14 Regions from which foreign perpetrator was operating



Source: PWC Survey: Economic Crime: People, Culture and Controls  
Available at [pwc.com/crimesurvey](http://pwc.com/crimesurvey)

# PWC Crime Survey

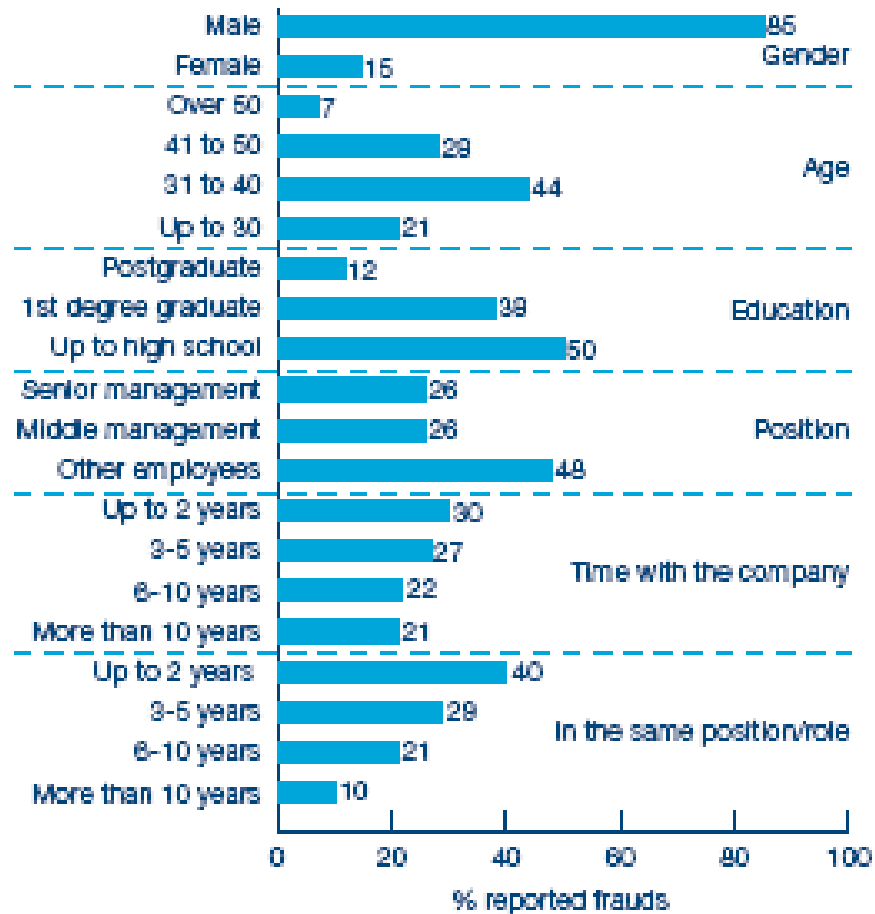
## 1.15 Reasons cited by companies to explain why fraud was committed (multiple answer)



Source: PWC Survey: Economic Crime: People, Culture and Controls  
Available at [pwc.com/crimesurvey](http://pwc.com/crimesurvey)

# PWC Crime Survey

## 1.16 Profiling the fraudster



Source: PWC Survey: Economic Crime: People, Culture and Controls  
Available at [pwc.com/crimesurvey](http://pwc.com/crimesurvey)