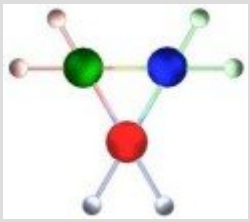
Systematizing Insider Threat mitigation

George Magklaras BSc Hons Mphil
Information Security & Network Research Group
University of Plymouth, UK



http://www.network-research-group.org/

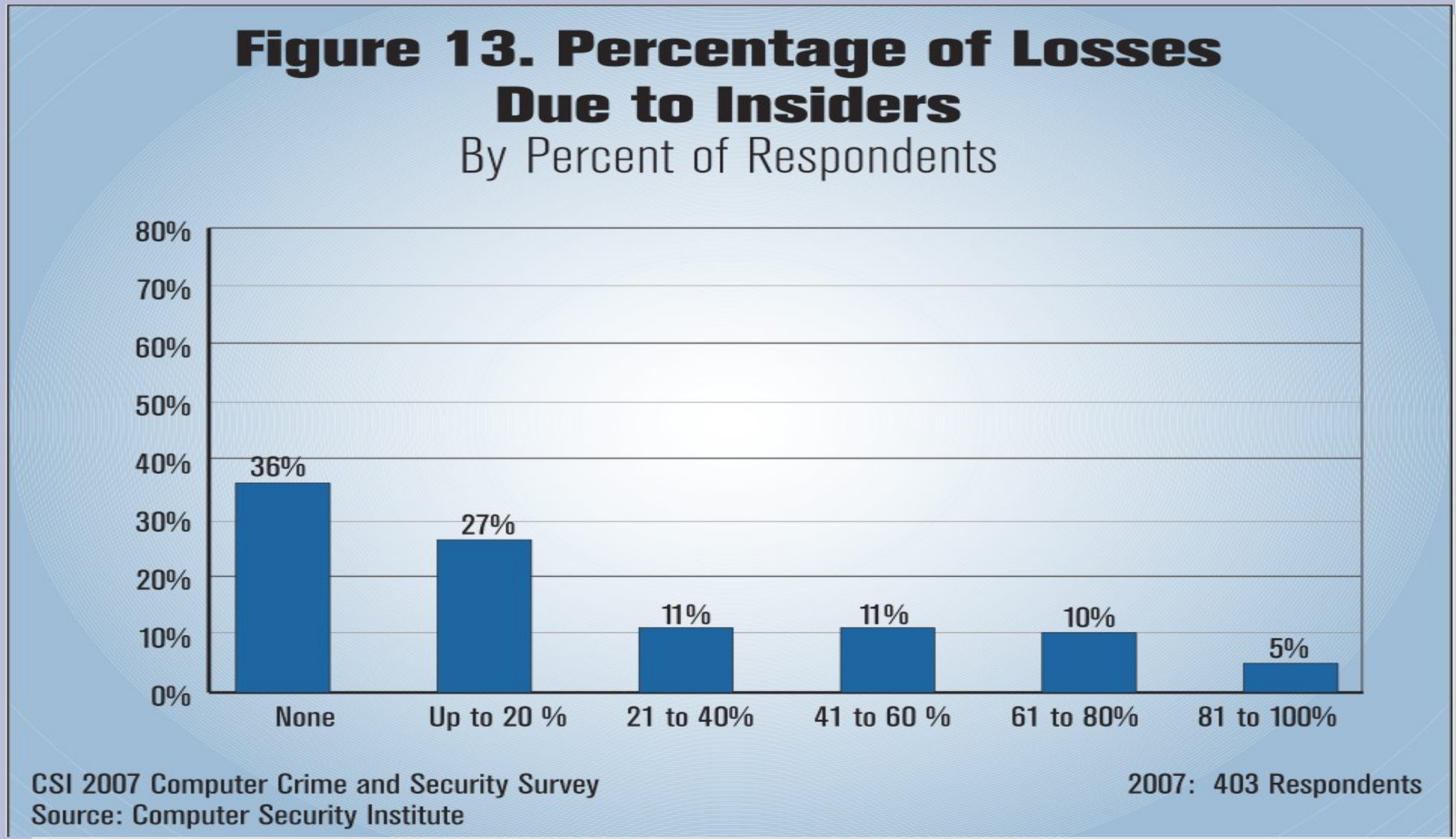
Agenda

- Basic definitions.
- Manifestation of insider threats in the real world.
- Insider threat taxonomies and frameworks
- Insider threat modeling: A system oriented view approach coupled with human factors
- Towards a repository of encoded insider threats
- Fundamental questions on insider threat modeling

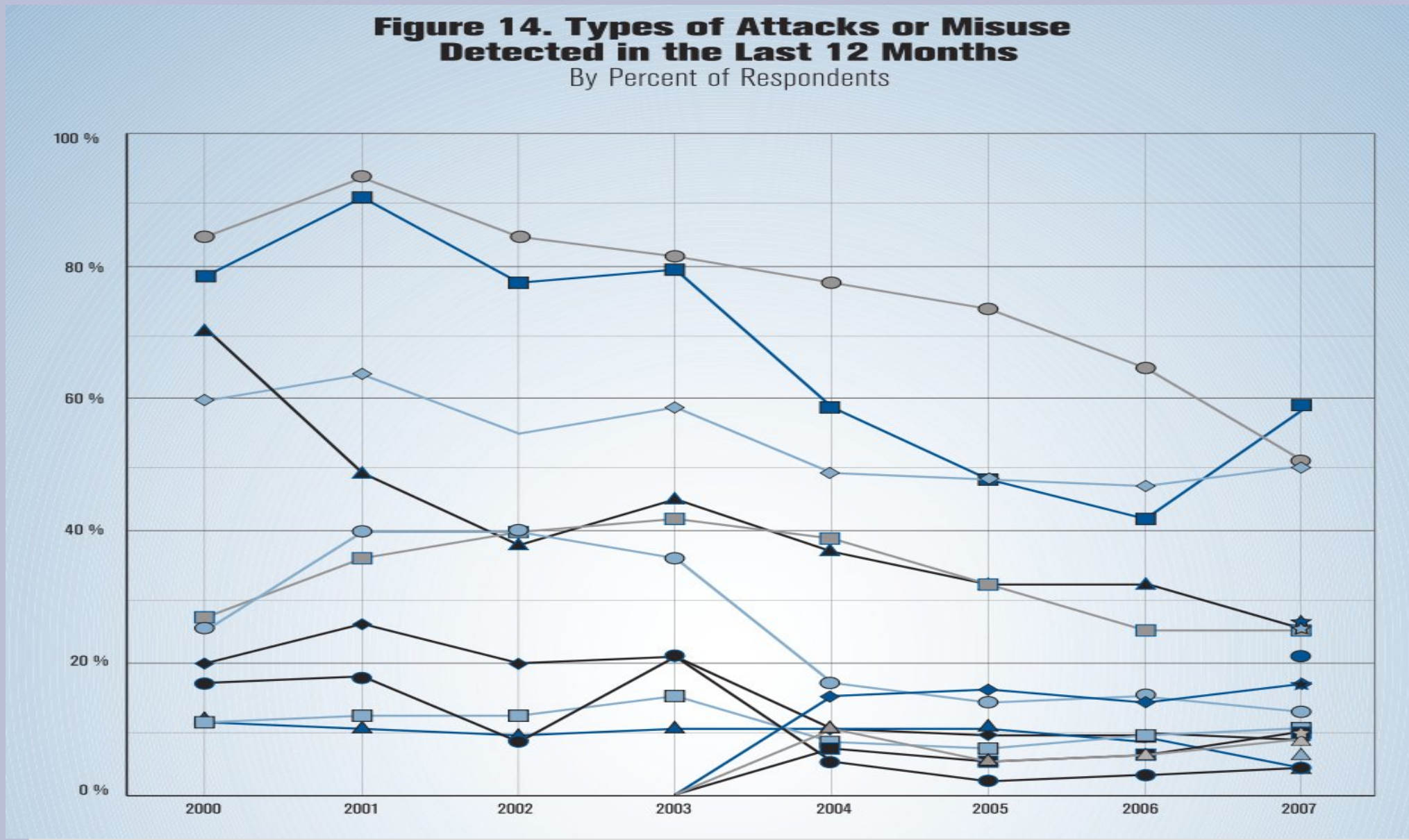
Some (boring?) definitions

- Insider: a person that has been legitimately given the capability of accessing one or many components of an IT infrastructure (hardware, software and data) enjoying effortless login by interacting with one or more authentication mechanisms.
- IT usage policy:”set of laws, rules, practices, norms and fashions that regulate how an organisation manages, protects, and distributes the sensitive information and that regulates how an organisation protects system services” [1]
- Threat: a set of circumstances that has the potential to cause loss or harm.
- To systematize: To formulate into or reduce to a system: "*The aim of science is surely to amass and systematize knowledge*" V. Gordon Childe
- Model: an abstracted physical, mathematical, or logical representation of a system of entities, phenomena, or processes.

Insider threat manifestation : source CSI 2007 survey [2]



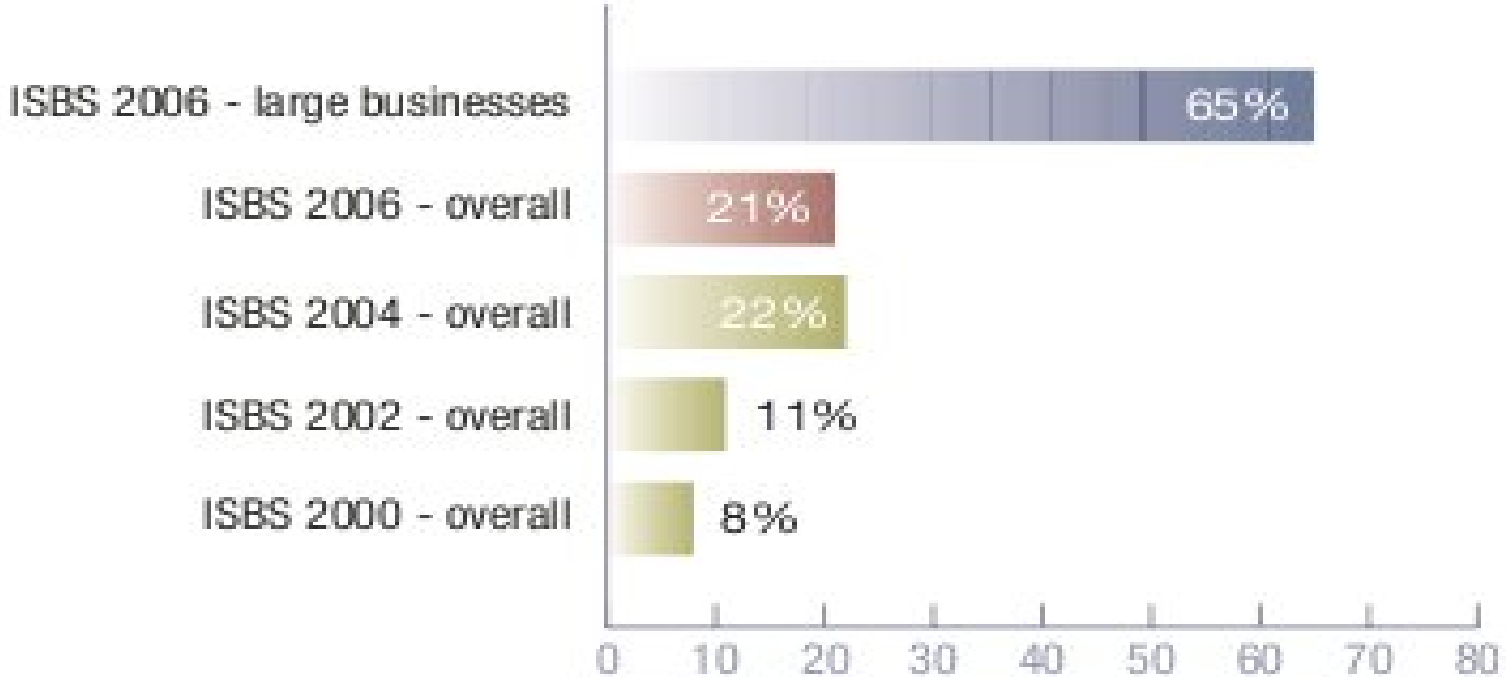
Insider Threat Manifestation (2): source CSI 2007 survey [2]



Insider Threat manifestation (3): source PwC/DTI 2006 ISBS survey [3]

How many UK businesses have suffered from staff misuse of information systems?

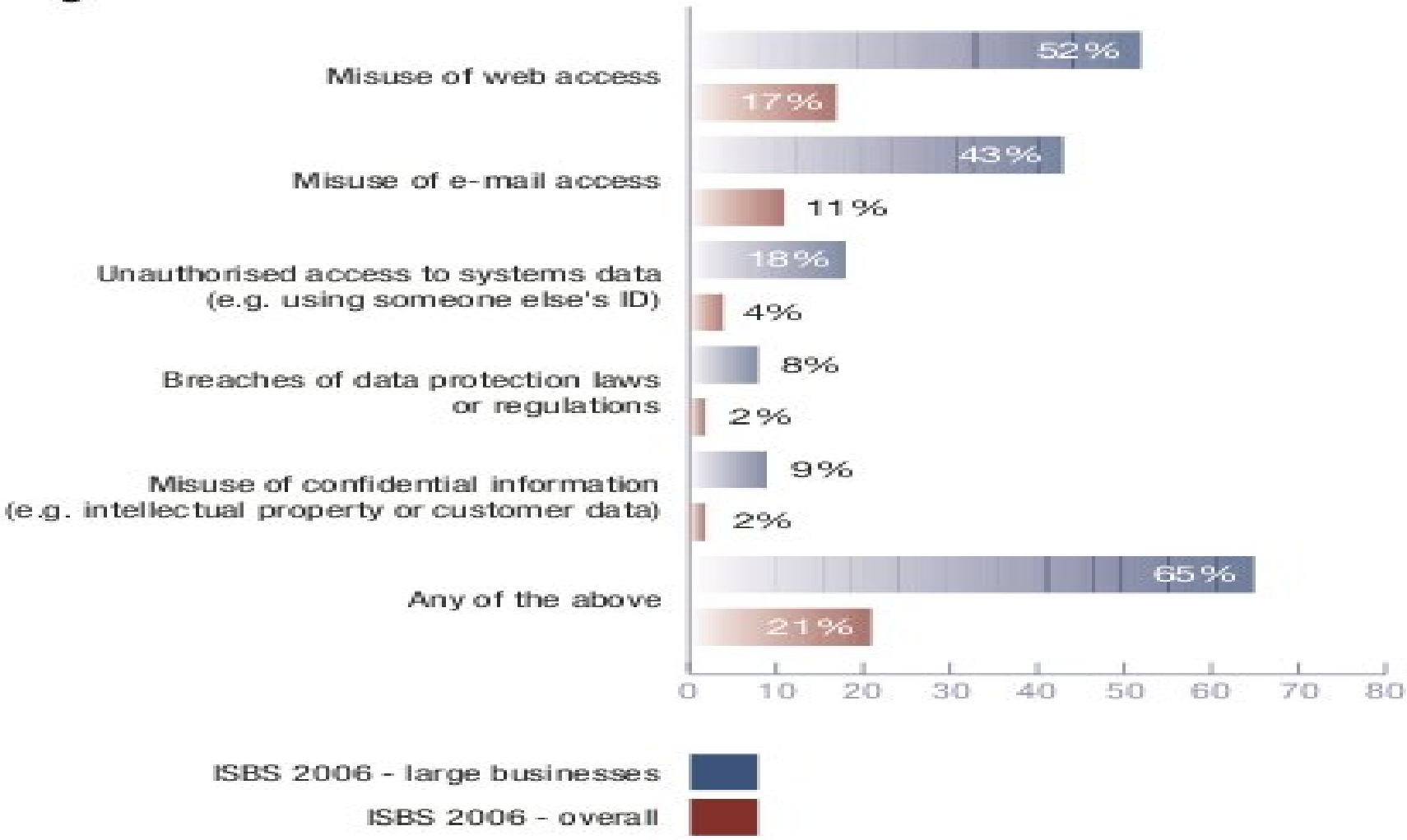
Figure 60



Insider Threat manifestation (4): source PwC/DTI 2006 ISBS survey

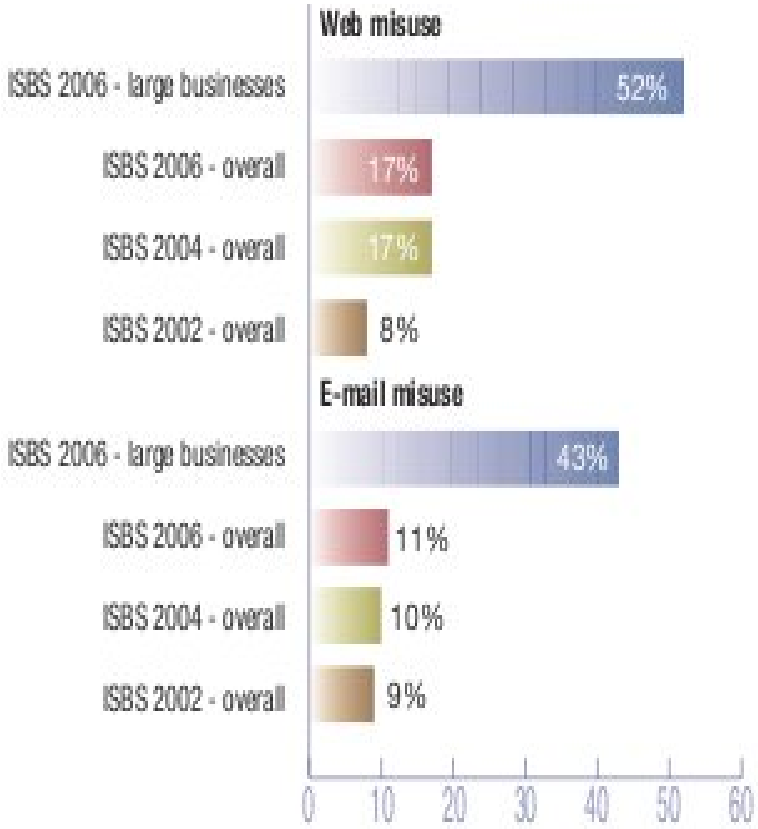
What type of staff misuse did UK businesses suffer?

Figure 61

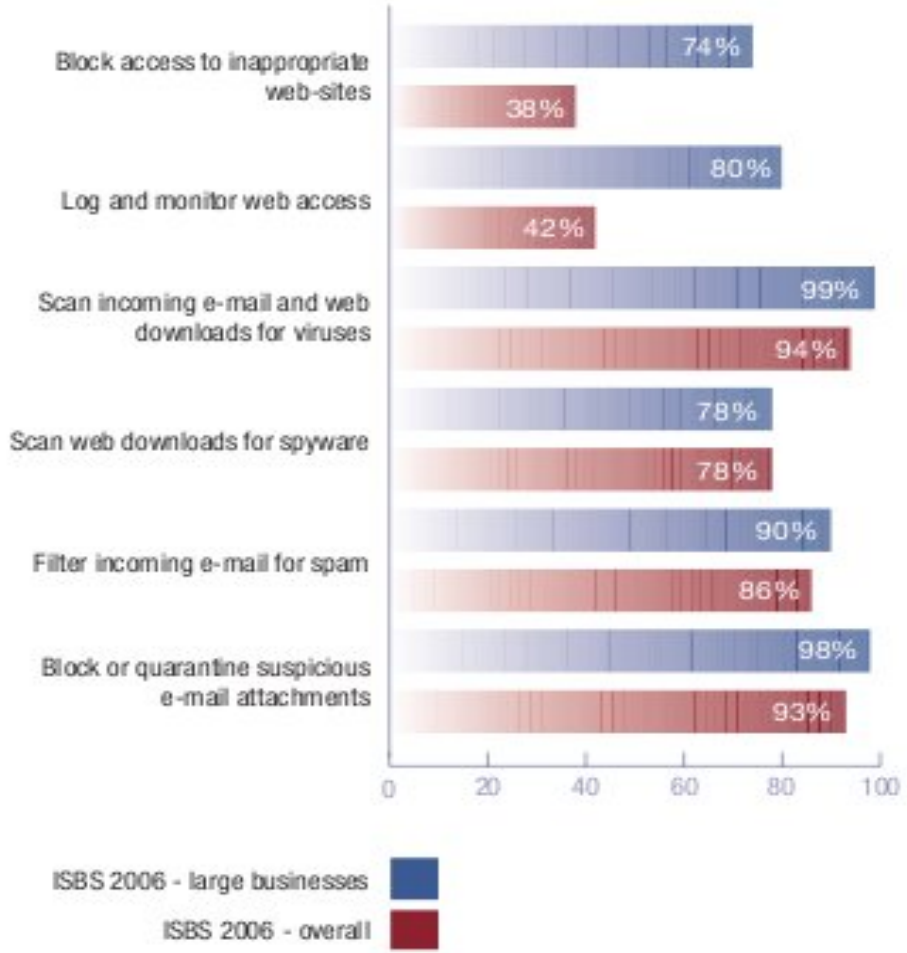


Insider Threat manifestation (5): source PwC/DTI ISBS 2006 survey

In how many UK businesses did staff misuse e-mail or web access?



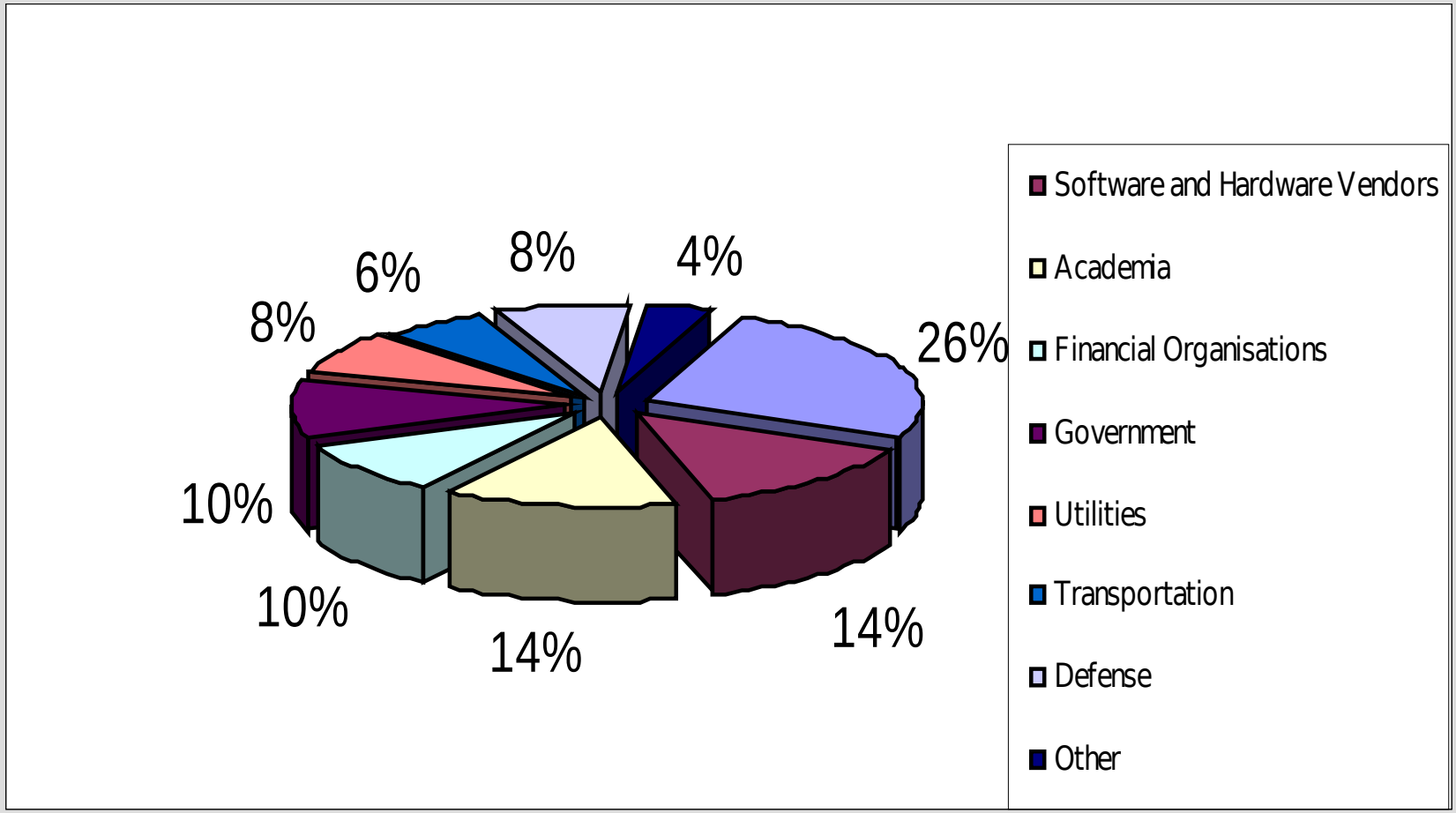
What technical controls do UK businesses have over their staff's Internet access?



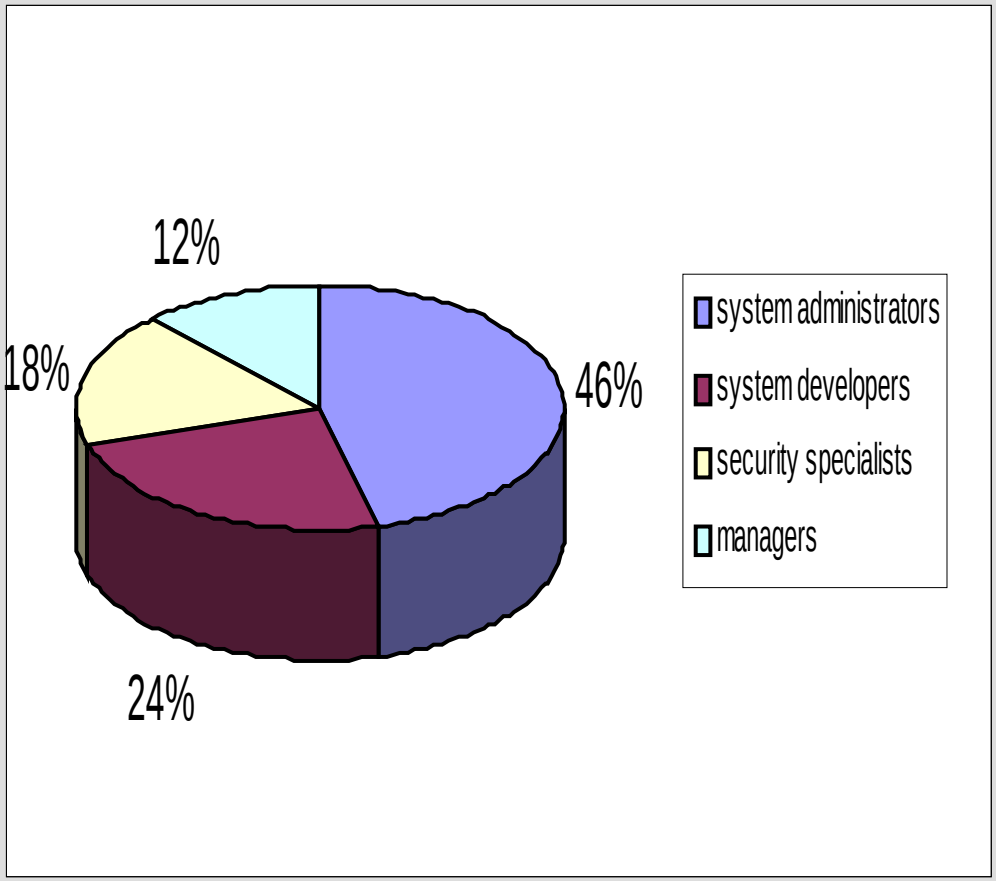
Insider Threat manifestation(6): IWAR Insider misuse survey [4]

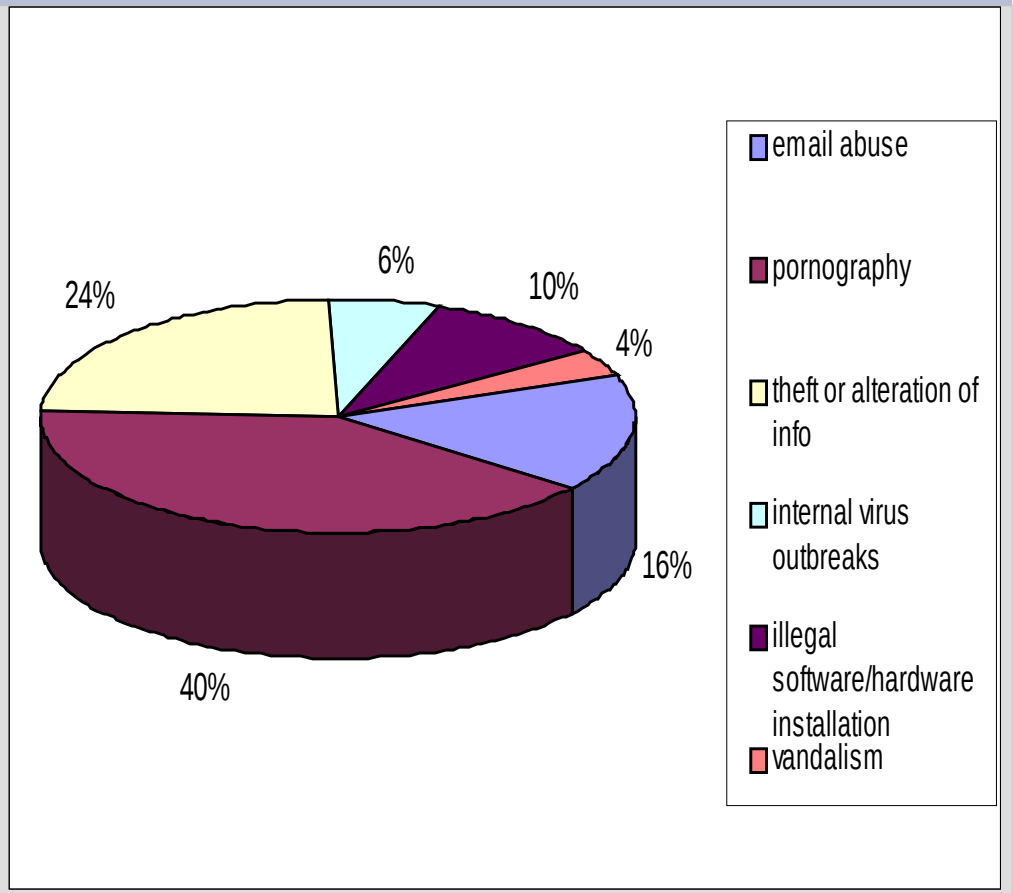
- 50 respondents from Europe (IT and Management practitioners)
- What really constitutes an insider IT misuse problem? What are the most frequent ways for a legitimate user to abuse an IT infrastructure?
- What are the most likely places in computer systems to reliably collect information about legitimate user misuse?
- Is there any indicative information about what kind of user is likely to initiate an insider IT misuse incident?

Insider Threat manifestation(7): IWAR Insider misuse survey [4]



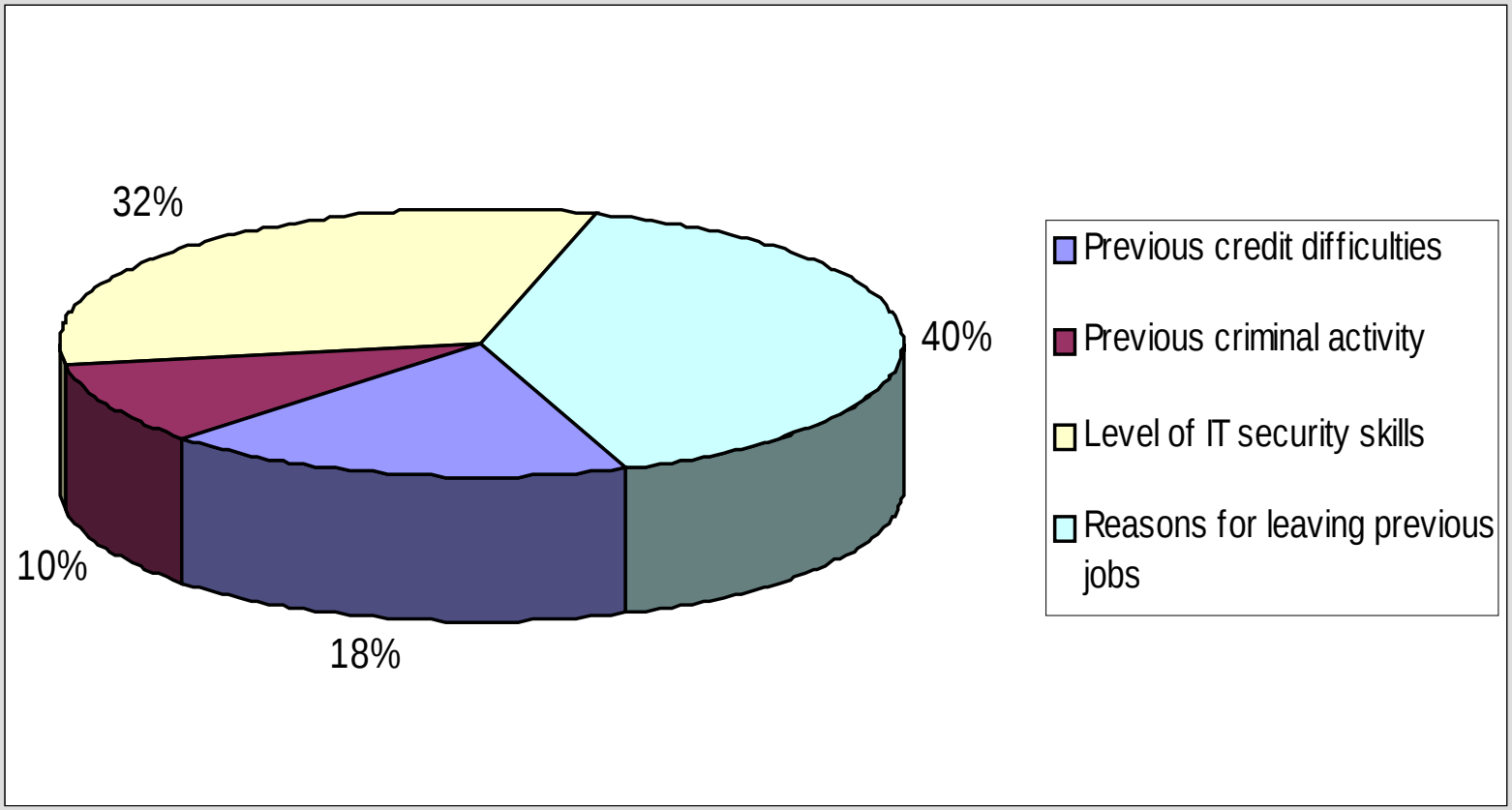
Insider Threat manifestation(8):IWAR Insider Misuse Survey [4]





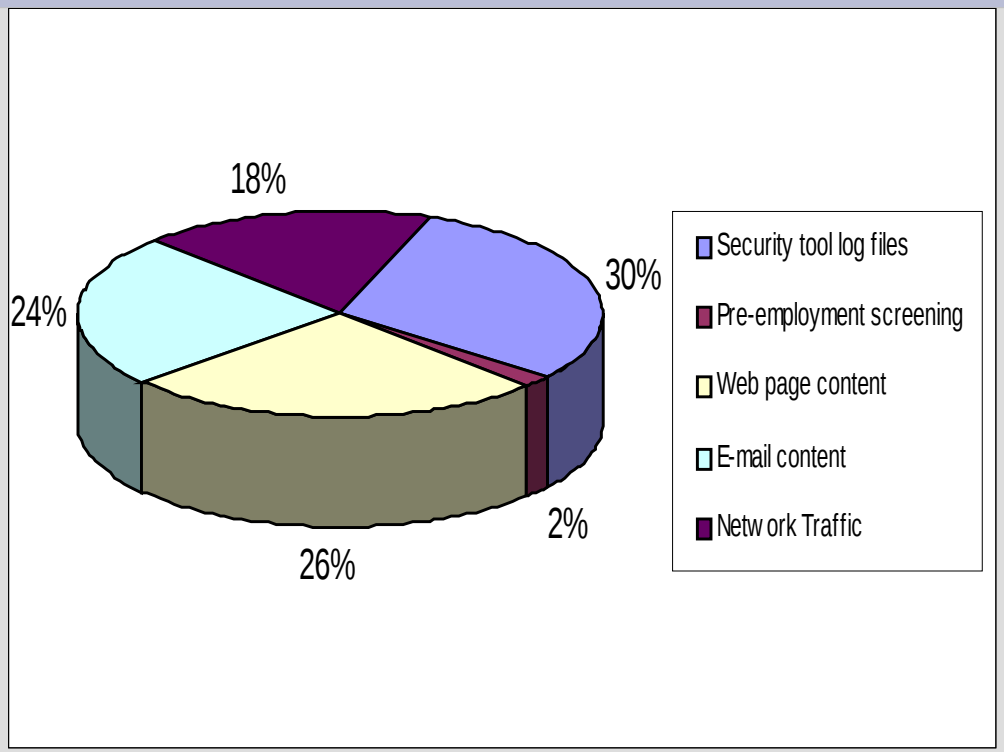
- 46% of respondents considered extensive personal usage of computing resources (IM friends, browsing food recipies, printing your son's 200 page thesis, etc) as serious IT misuse.

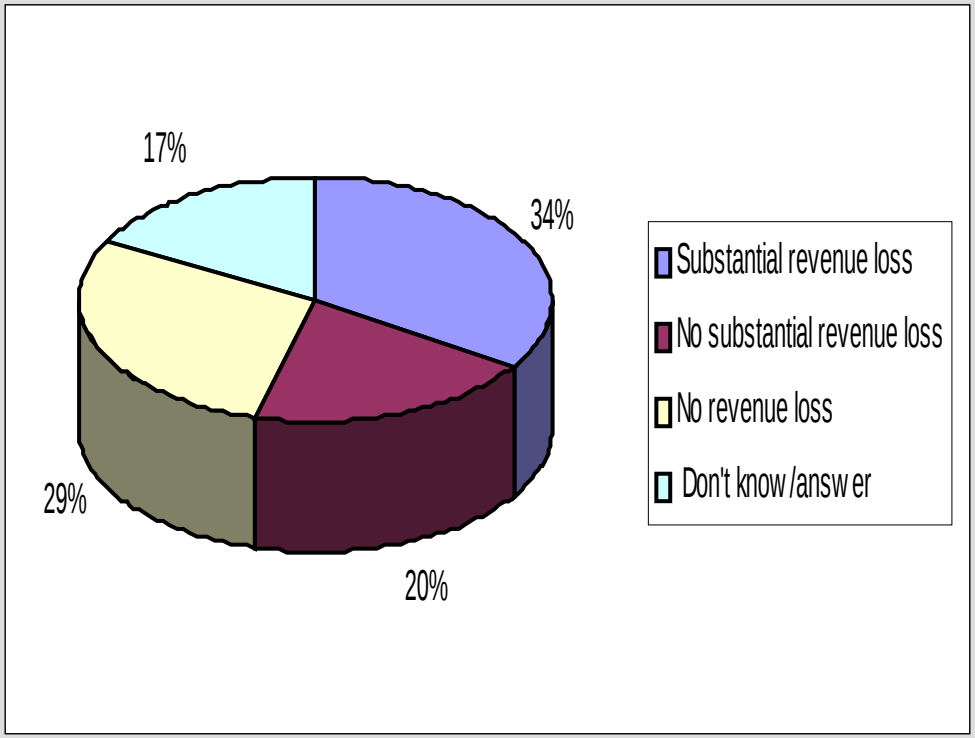
Insider Threat manifestation(9):IWAR Insider Misuse Survey [4]



- Respondents from the defense, hardware/software vendors and financial organizations were utilizing extensively strict pre-employment screening procedures.

Insider Threat manifestion (10): IWAR Insider Misuse Survey [4]





- 86% of the respondents believe that knowledgeable users (IT-wise) are more likely to misuse a system than their less knowledgeable colleagues.
- **14% believe that less knowledgeable users can create more trouble than their more knowledgeable counterparts (accidental misuse).**
- 0% did not think that IT knowledge is a threat factor.

Insider Threat Systematics: Taxonomies

- Taxonomies are vital tools that aid the conceptual understanding of a problem domain.
- Biologists and genomic researchers are trying to make sense of complex processes and large amounts of data by using taxonomies.
- Information security researchers have initially started classifying security faults:
  - *John Howard's security incident analysis [5]*
  - *SRI Neumann-Parker taxonomy [6]*
  - *Lindqvist- Jonssen's intrusion taxonomy [7]*
  - *Furnell et al Intrusion Specification taxonomy [8]*

Insider threat systematics (2): Insider threat taxonomies

- Early literature references to types of legitimate users: Anderson's discussion [9] of 'masqueraders', 'misfeasors' and 'clandestine' users.
- Tuglular's Insider misuse taxonomy [10]:
  - Incident, response, consequences
  - 'target-type-of-threat' association
  - Target ⇨ asset strategy ⇨ rule

Typical threat realization scenario

- A disgruntled head system administrator who has just been fired and *decides to take revenge by disrupting the IT infrastructure*. As a knowledgeable insider, he/she bypasses the system authentication procedure and corrupts (and does not delete entirely) certain vital database files in order to disrupt important services. In addition, the fired system administrator also deletes the database backup copies and then covers up his actions by erasing system log files.

Notable cases

- Norwich Union versus Western Provident Association:
  http://www.computerworld.com/news/2000/story/0,11280,45927,00.html

- Abdelkader Smires versus Internet Trading Systems:
  http://www.computerworld.com/news/2000/story/0,11280,45927,00.html

- University of Oslo account cracking incident:
  http://news.ists.dartmouth.edu/snms/1102.htm#30

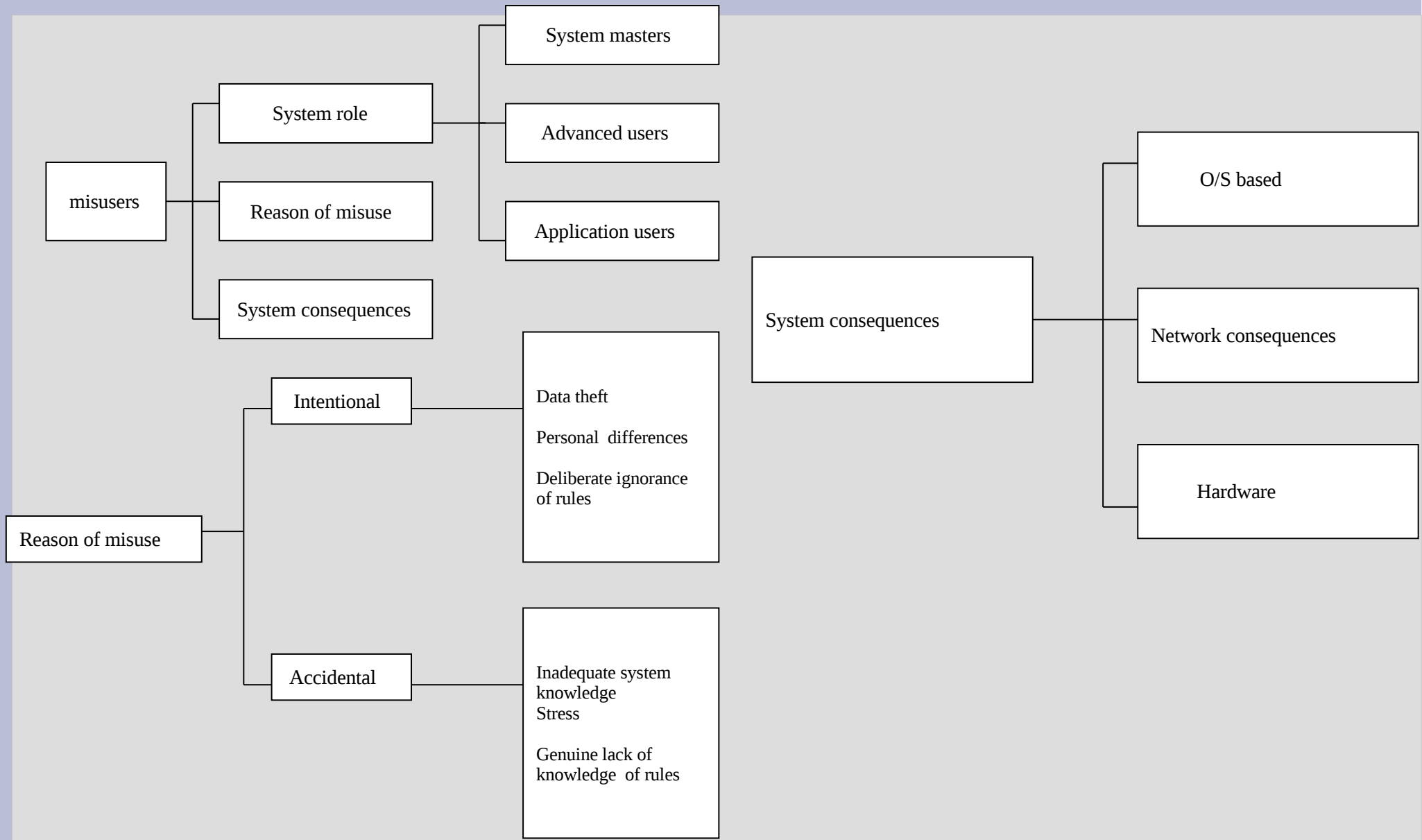
Observations:

- Insider misuse is a composite problem:
  - Human resources issues: unhappy/unloyal employees
  - Legal issues: (balancing privacy against user monitoring measures and considering when and if to litigate).
  - ➔ Technical issue (detecting and responding to insider threats (IDS/IPS), preventing insider threats)

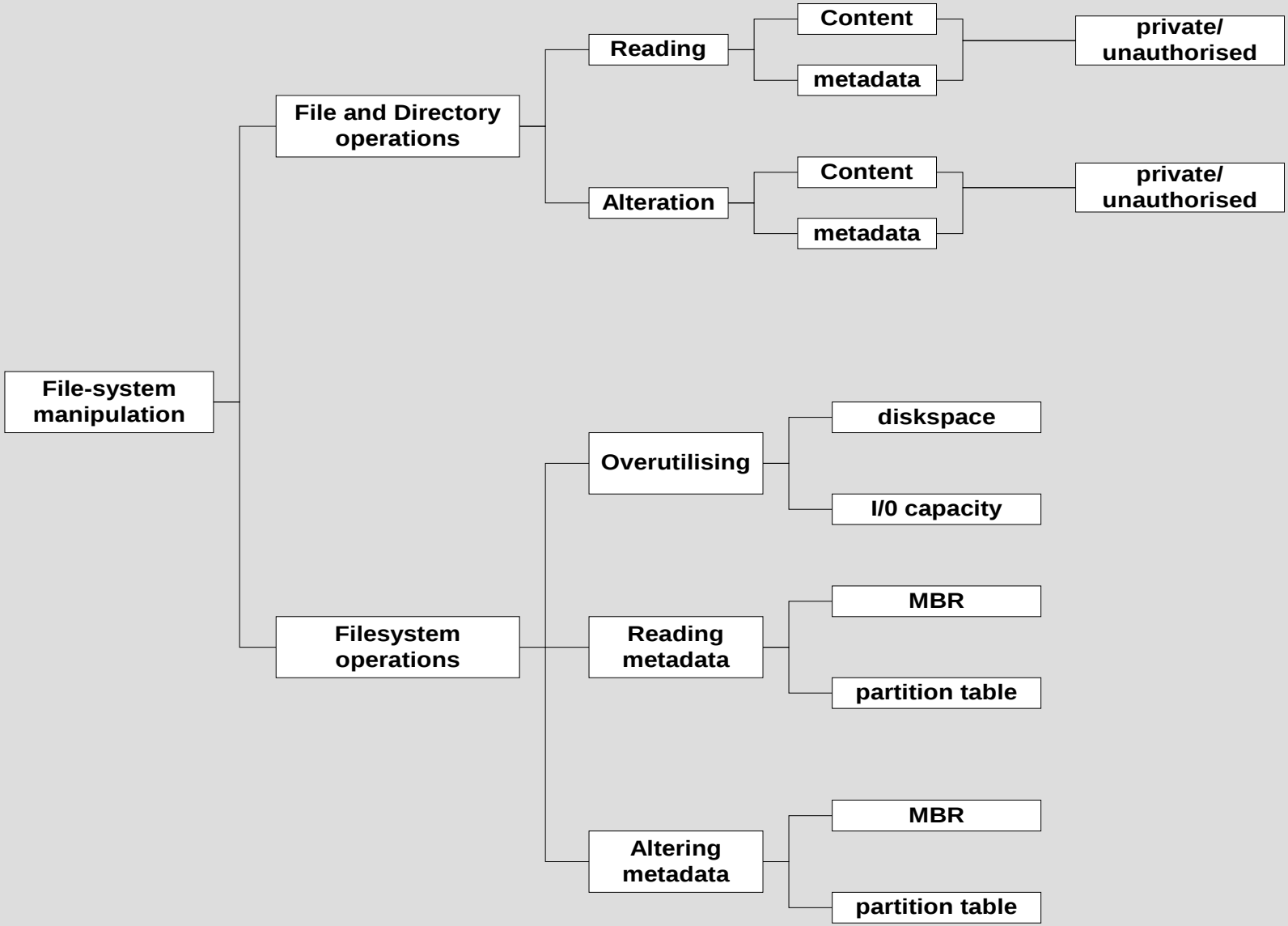
Observations (2):

- Opportunity and motive are important factors. Many taxonomies and frameworks pay attention to these two factors:
  - Inferring opportunity and motive is possible when someone focuses on how something is achieved.
  - Automated processes work best on pointing out system level consequences.
  - Insider threat prediction (IPT) is an important mitigation technique.
  - IPT requires an ability to represent events at a more system-specific level, looking at the various individual actions that achieved the result
  - Therefore, it makes sense to build a taxonomy of insider threats based on what can be easily detected at system level.

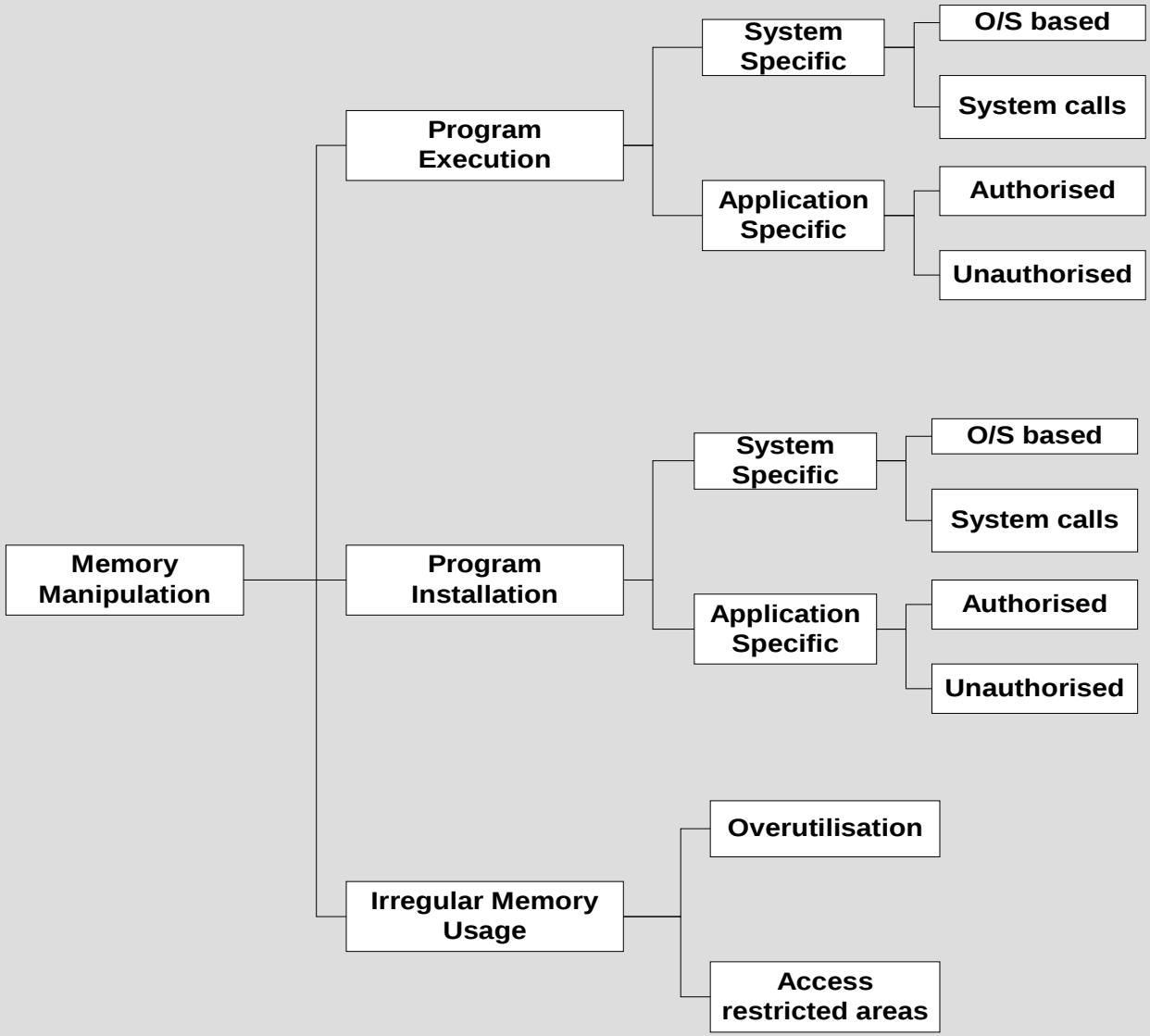
Proposed Insider Threat prediction taxonomy [11]:



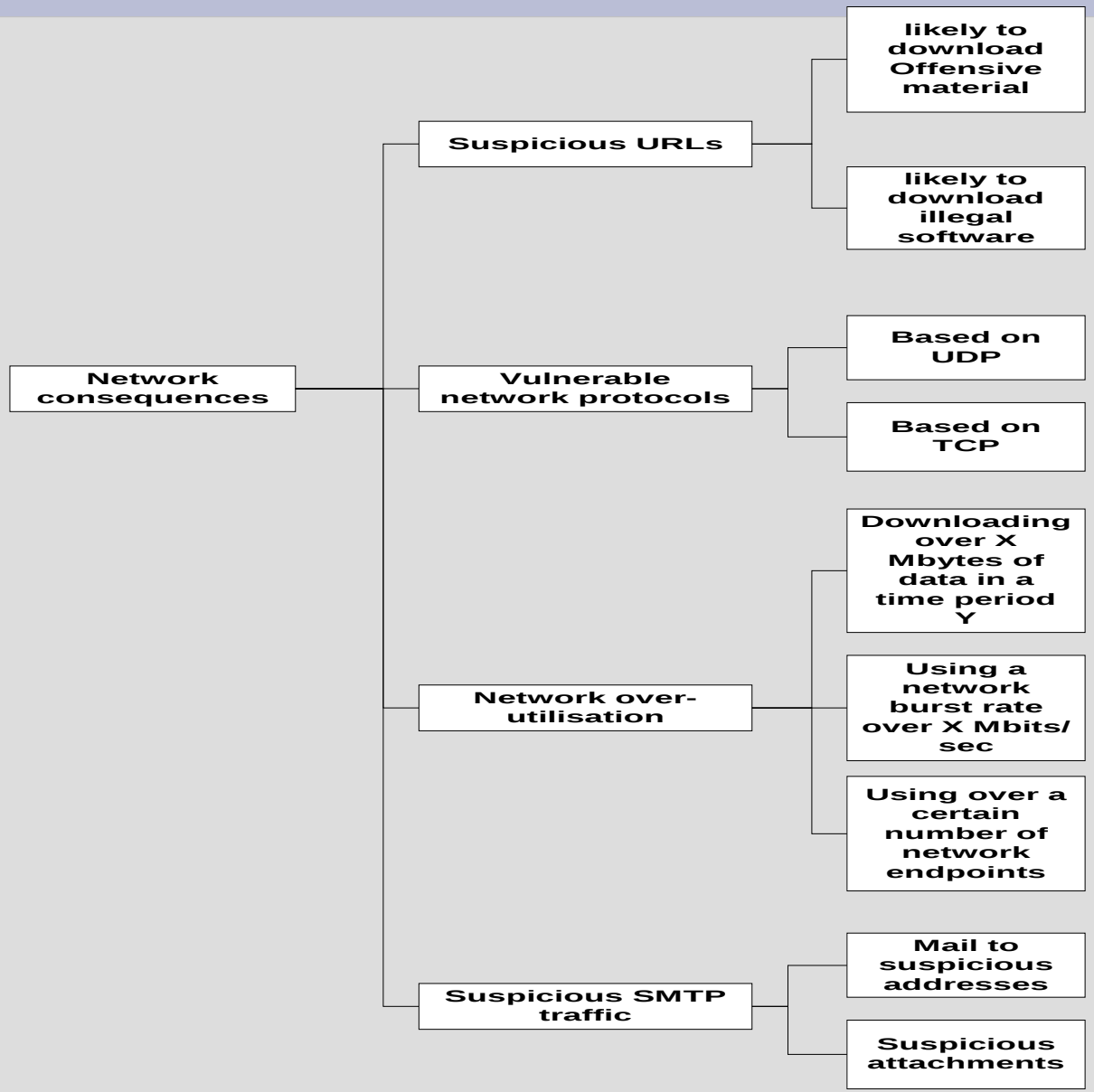
Insider Threat Prediction Taxonomy (2):OS consequences: proposed filesystem indicators [11]



Insider Threat Prediction Taxonomy (3):OS consequences: proposed memory indicators [11]



Insider Threat Prediction Taxonomy (4): OS consequences:proposed network indicators



Insider Threat prediction modeling: Wood

Wood [12] discusses a set of Insider Threat Qualifiers (ITQs) to model an insider adversary:

- Knowledge
- Privileges
- Skills
- Tactics
- Motivation
- Process

Wood does not deal with the quantification of metrics due to its introductory scope.

Insider Threat prediction modeling: Pauleo's Risk Predictor model [13]

- Human behavior based
- Incorporates risk management with elements of human behavioral science.
- Purpose: to identify employees with a higher risk of performing damage inside an organization.
- Method: Vector based modeling of events and influences that gives a numerical score for each employee. The higher the score, the higher the likelihood of threat realization by the individual.

Insider Threat prediction modeling: Pauleo's Risk Predictor model [13]

$$R_x * I = x_x$$

$$S_x * E = y_x$$

$$x_x + y_x = z_x$$

$$z_x * I = R_{x+1}$$

$$(i=1->m)\Sigma R_{x+1} = Score_{x+1}$$

$$Slope_{time\_y} = (Score_{x+1} - Score_x)/time\_y$$

m=number of influences, n=number of events, I=Influence matrix (mxm), E=Event Matrix (nxm), R_x=Response Vector (1xm), S_x=Stimulus vector (1xn), x_x=Interim Response Vector, y_x=Interim Stimulus Vector, z_x=Interim Stimulus Response Vector, R_{x+1}=new Current Response Vector, time_y=time period of interest, Scorex+1=numerical representation of employee level of risk, $Slope_{time\_y}$=scores versus time period of interest

Insider Threat prediction modeling: Gonzalez [14]

Suggests a system dynamics method focusing on a number of ITQs based on:

- Human behavior factors (as in Schultz)
- Organizational administration aspects: resources dedicated to data security, number of reported incidents/revenue lost.
- Temporal basis of modeling: What is a good time window to monitor for assessing properly various metrics that might need longer detection periods?
- Historical behavior of certain ITQs: certain patterns can be observed/distinguished?

Insider Threat Prediction Model: Schultz [15]

$$Xe = (\Sigma W_i X_i) + C = W_1.X_1 + W_2X_2 + W_3X_3 + \ldots + W_NX_N + C$$

X1...XN → quantified Insider Threat indicators (examples: verbal behaviour in email)

W1...WN → Weights of the respective Threat indicators

C → Arithmetic constant

- meaningful errors
- correlated Threat indicator patterns

Insider Threat Prediction model: Magklaras and Furnell [11]

- Based on the proposed insider threat taxonomy.
- System oriented approach:
  - Threat qualifiers that have to do with email behavior, documenting stress and other personal events for an employee are good intelligence but not always feasible due to:
    - Technical reasons (external encrypted email accounts)
    - Privacy concerns: In some countries, keeping employee data on health/personal details is questionable practice from a legal and ethical point of view.
- The need for an effective but less intrusive set of threat qualifiers is very relevant.

Insider Threat Prediction model: Magklaras and Furnell [11]

$$EPT = \sum F_{ITPQA} \Rightarrow$$

$$EPT = F_{attributes} + F_{behavior} \Rightarrow$$

$$EPT = C_{role} + F_{accessrights} + F_{behavior}$$

$$F_{accessrights} = C_{sysadm} + C_{criticalfiles} + C_{utilities} + C_{physicalaccess}$$

$$F_{behavior} = F_{sophistication} + F_{fileops} + F_{netops} + F_{execops}$$

$$(6,6,6,6,6,12,18,18,20) = (WC_{role}, WC_{data}, WC_{hardware}, WC_{sysadm},$$

$$WC_{utilities}, WF_{sophistication}, WF_{fileops}, WF_{execops}, WF_{netops})$$

Insider Threat Prediction model: Magklaras and Furnell [16] sophistication metrics

$$F_{sophistication} = F_{breadth} + F_{depth}$$

$$F_{breadth} = \Sigma ni/c$$

n -> Number of unique applications per session,

c-> number of sessions

$$\mathbf{F_{breadth} = Wmax, \text{ if } (\mu_{ordinary} < x \leq \mu_{advanced})}$$

$$\mathbf{F_{breadth} = Wmax/2, \text{ if } \mu_{novice} < x \leq \mu_{ordinary}}$$

$$\mathbf{F_{breadth} = Wmax/3, \text{ if } 0 < x \leq \mu_{novice}}$$

Insider Threat Prediction model: Magklaras and Furnell [16] sophistication metrics

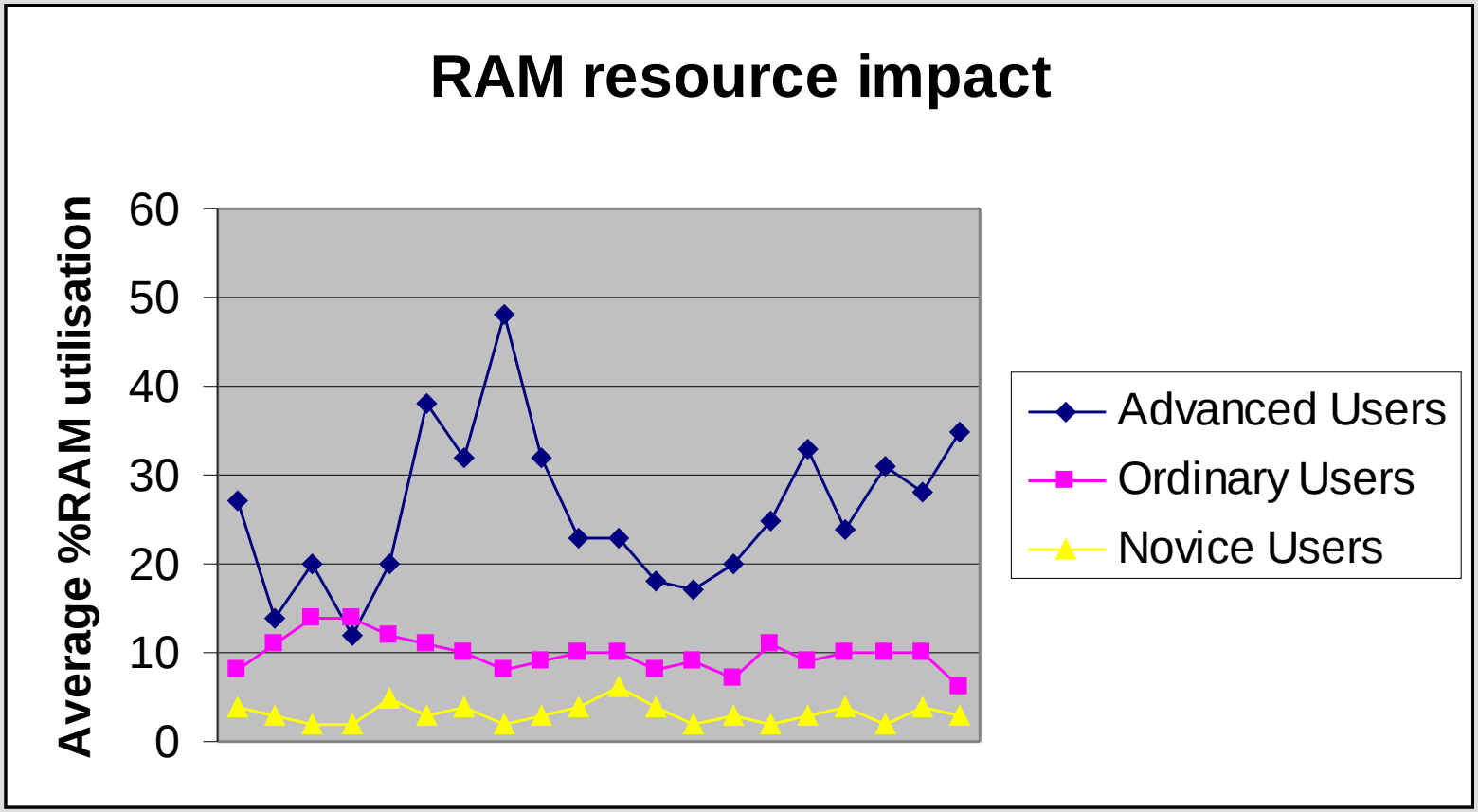
$$F_{depth} = F_{appscore} + F_{resourceutil}$$

$$F_{depth} = (S_{app1} + S_{app2} + \ldots S_{appn})/n + S_{CPU} + S_{RAM} + S_{simapps}$$

n -> Number of executed applications

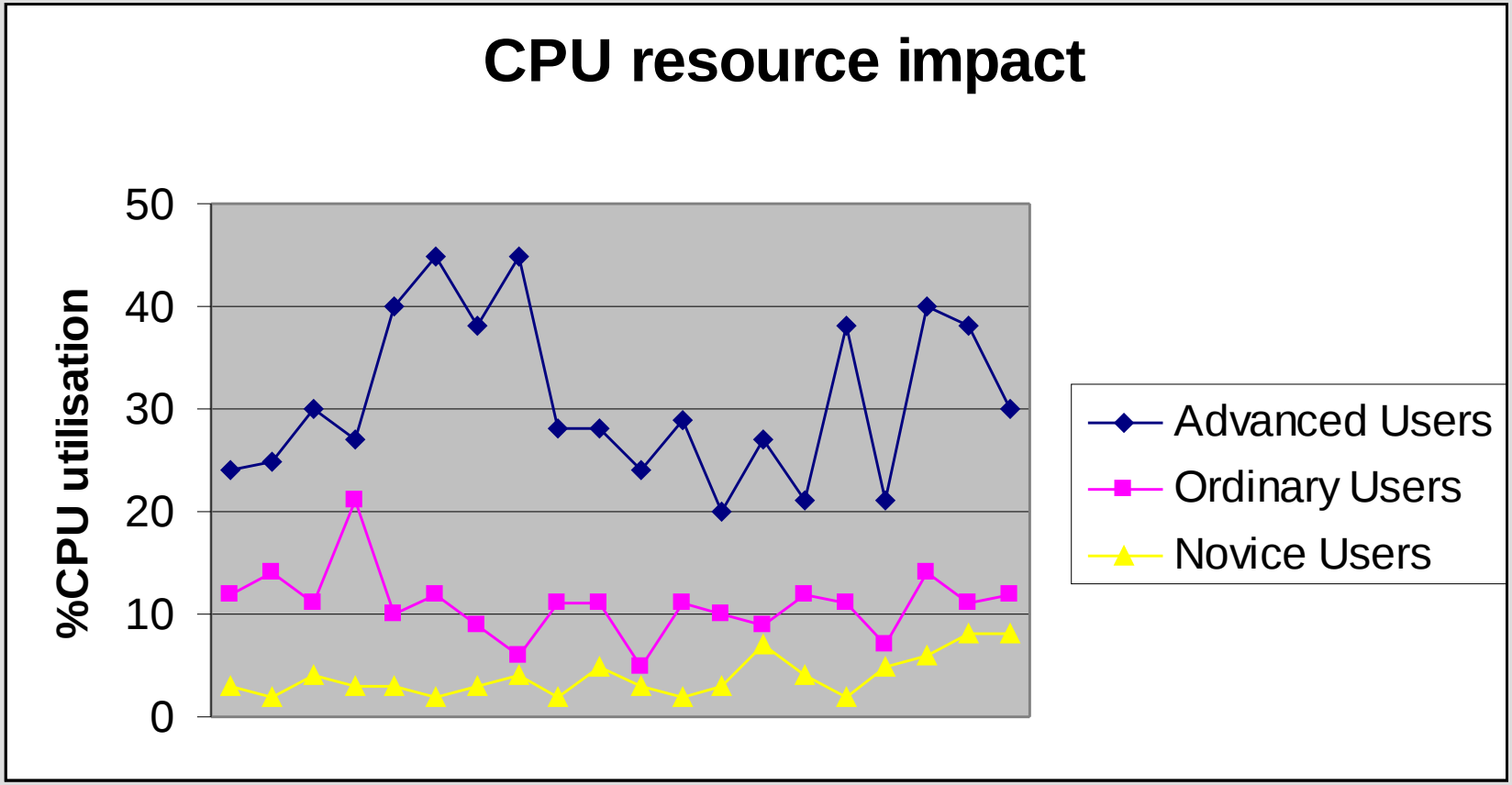
$$\mathbf{S_{CPU/RAM/simapps} = Wmax, \text{ if } (\mu_{ordinary} < x \leq \mu_{advanced})}$$
$$\mathbf{S_{CPU/RAM/simapps} = Wmax/2, \text{ if } \mu_{novice} < x \leq \mu_{ordinary}}$$
$$\mathbf{S_{CPU/RAM/simapps} = Wmax/3, \text{ if } 0 < x \leq \mu_{novice}}$$

Insider Threat Prediction model: Magklaras and Furnell [16] sophistication metrics



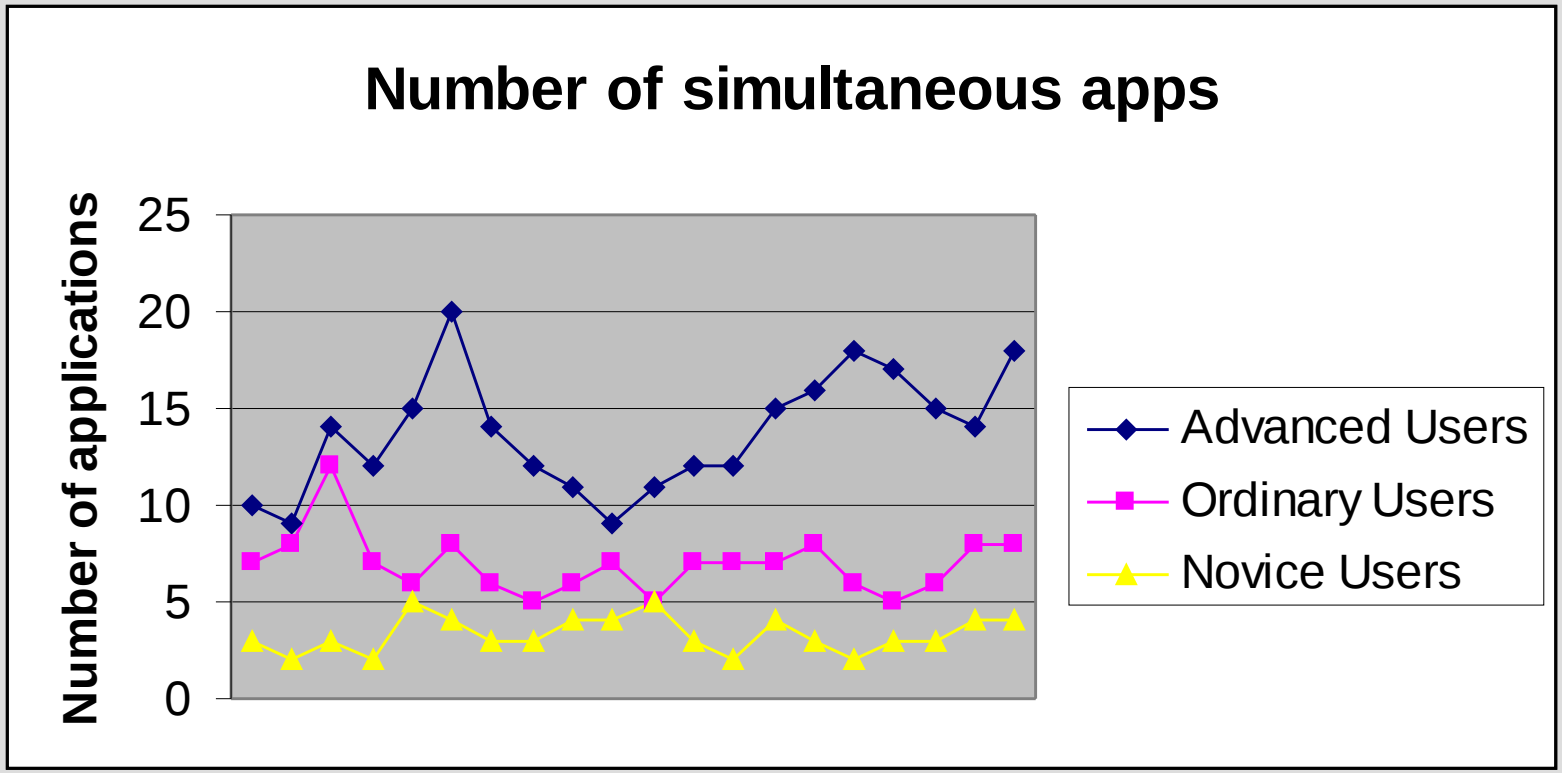
	Advanced	Ordinary	Novice
Arithmetic mean	26	9.85	3.25
σ	8,813	2,033	1,118

Insider Threat Prediction model: Magklaras and Furnell [16] sophistication metrics



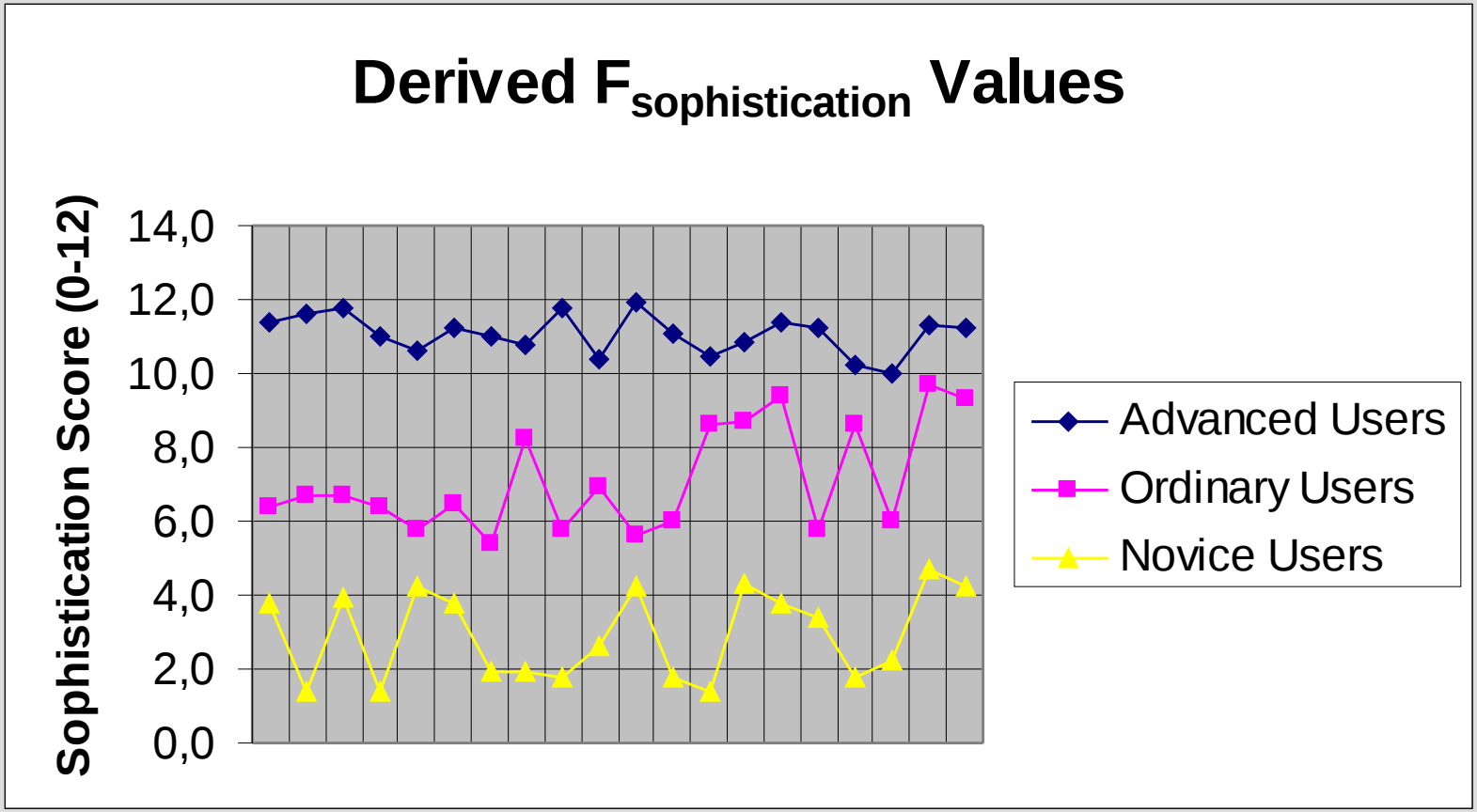
	Advanced	Ordinary	Novice
Arithmetic mean	30,9	10,95	3,95
σ	7,986	3,316	1,959

Insider Threat Prediction model: Magklaras and Furnell [15] sophistication metrics



	Advanced	Ordinary	Novice
Arithmetic mean	13	7	3
σ	3	1	1

Insider Threat Prediction model: Magklaras and Furnell [16] sophistication metrics



Insider Threat Prediction model: Magklaras [17]: File and net signatures

$$\mathbf{F_{fileops}=Weight_{Ffileops}\ t/n,\ with\ t \leq n}$$

n=number of statements in the signature

t=number of true statements in the signature

$Weight_{Ffileops}$=Weight Matrix value for $F_{fileops}$

$$\mathbf{F_{netops}=Weight_{Fnetops}\ t/n,\ with\ t \leq n}$$

n=number of statements in the signature

t=number of true statements in the signature

$Weight_{Fnetops}$=Weight Matrix value for $F_{neteops}$

Insider Threat Prediction model: Magklaras and Furnell: execop (command) signatures

```
outer_ loop:    for (i=0 i<=m i++) {

                    if(sizeofAsignature!=0) {

                        inner_ loop:for (j=0 j<=n j++) {

                            if(Alegitimate[i] == Asignature[j]) {

                                number_of_matches++

                                left shift Asignature by one element

                                                    }

                                    }

                                    } else {

                return (100 * (number_of_matches/n))}
```

Insider Threat Prediction model: Magklaras and Furnell: ITPM engine internal representation of signatures

#Header

ipaddress, targetos,day,month,year

usercategory,reason,keyword1,keyword2,keyword3

WC_{role},WC_{sysadm},$WC_{criticalfiles}$,WCutilities,$WC_{physicalaccess}$,$WF_{sophistication}$,$W_{Fileops}$,$_{WFnetops}$,$WF_{execops}$

#Fileops

FileStatement1, FileStatement2, FileStatement3, …., FileStatementn

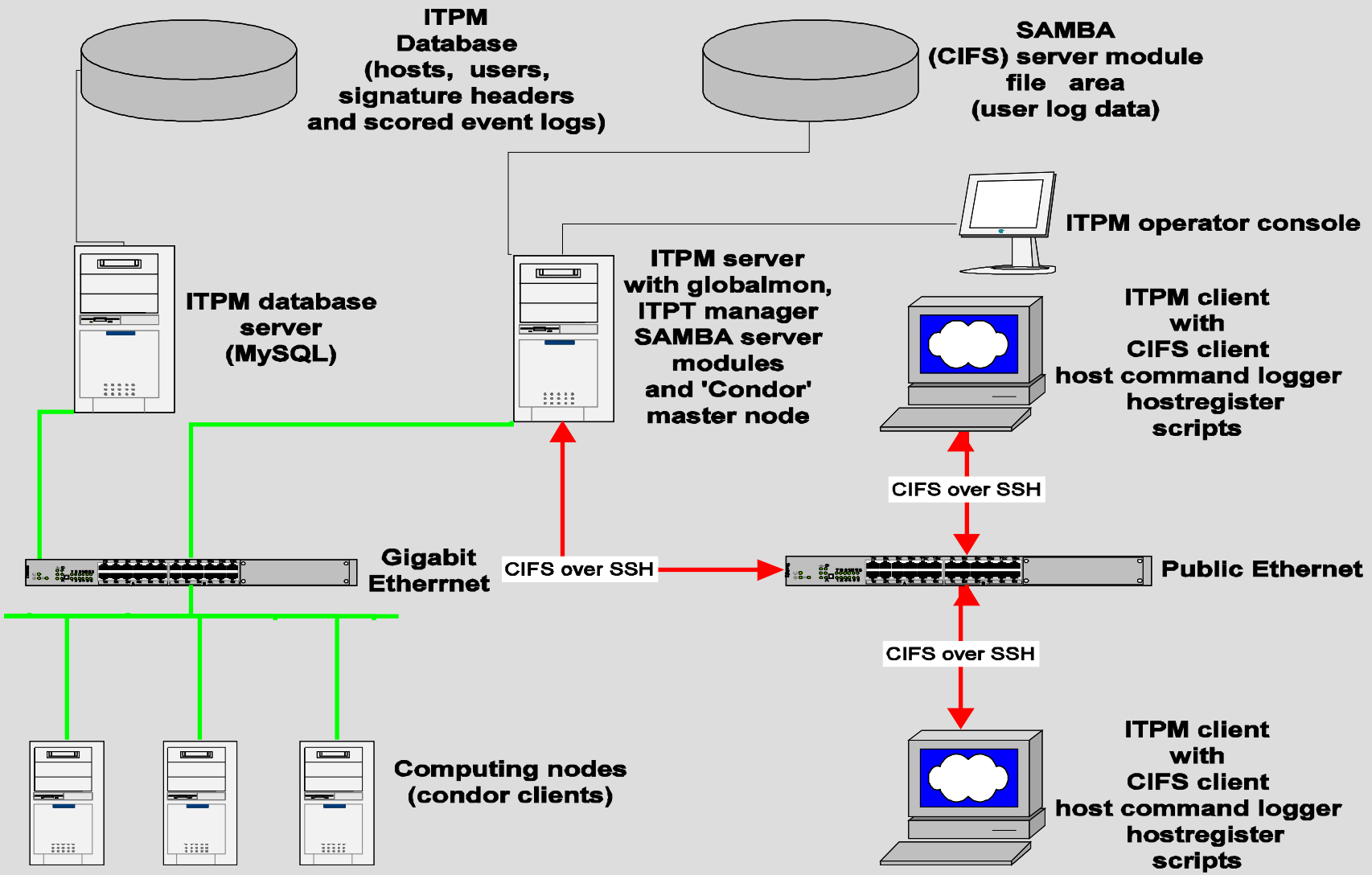
#Netops

NetStatement1, NetStatement2, NetStatement3, …., NetStatementn

#Execops

seq_xCcommandcodeArguments#seq_{x+1}CcommandcodeArguments…-##8#

ITPM architecture [17]



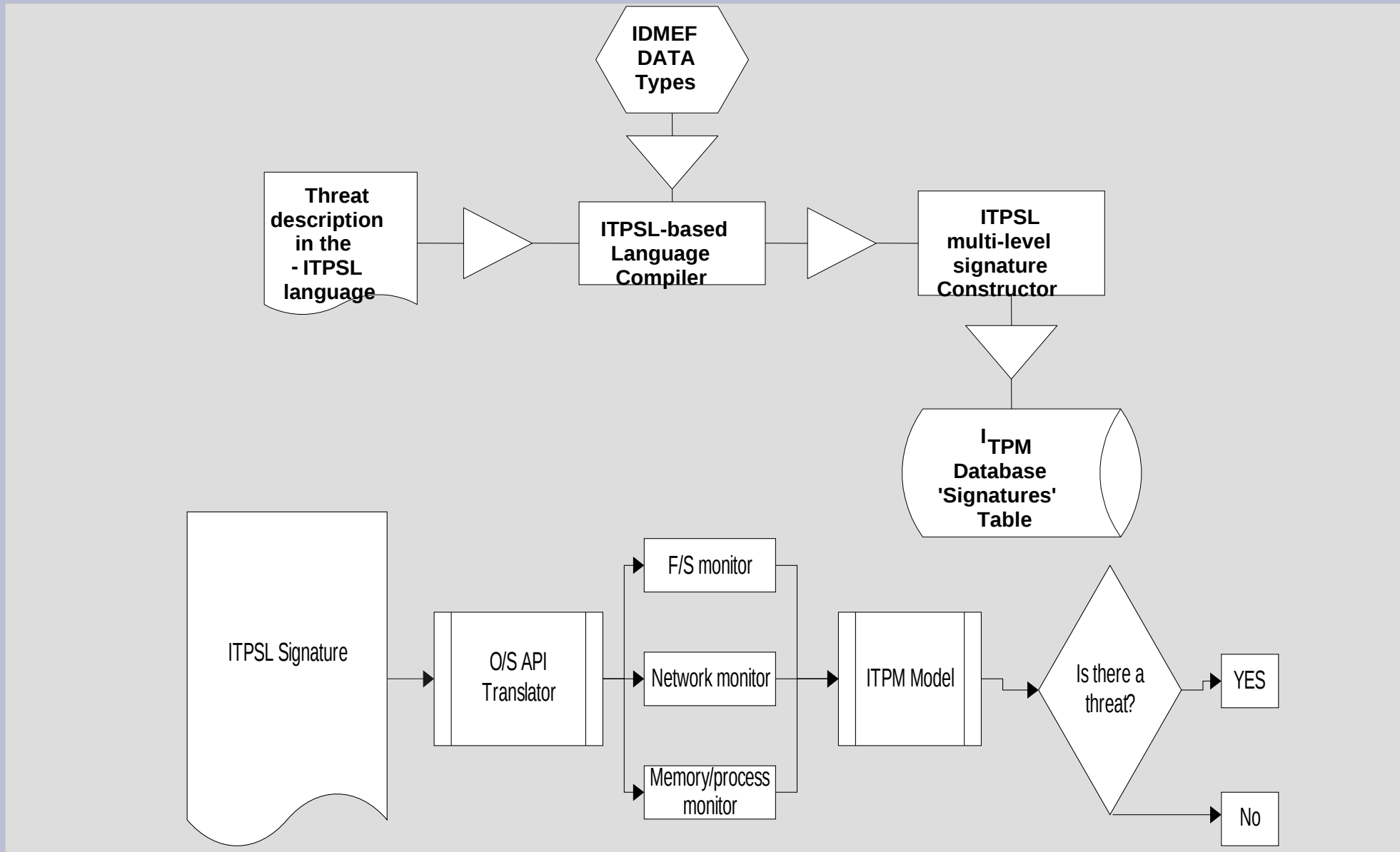
The Insider Threat Specification Language (ITPSL) [18]:

- Taxonomies give us a better understanding of the problem domain.
- Models apply the understanding to threat realization scenarios.
- A specialized language to express threat scenarios using system level parameters in a standardized way is an important tool that:
  - Will help professionals (sys/security admins, forensic professionals) express an insider threat incident in a discrete number of steps.
  - Builds an insider misuse threat case repository that can assist in threat mitigation (know the threat, know its signs -> predict it)

Insider Threat Specification Language (ITPSL): Magklaras and Furnell [18]

- the abstraction of the domain, which involves the removal of all the unnecessary details of the environment;
- the systematic categorisation of the necessary (abstracted) details into language semantics;
- the process of engineering the developed semantics into software.
- Refinement by building case repositories and testing them against live infrastructures.

The Insider Threat Prediction Specification Language (ITPSL) [18]:



The Insider Threat Prediction Specification Language (ITPSL) (3):

- An external Domain Specific Language (DSL) approach is followed.
- Semantics are based on XML markup.
- Should have the ability to represent decision theoretic information.
- Not tied to the ITPM but could facilitate other insider threat prediction frameworks.

The Insider Threat Prediction Specification Language (ITPSL) (4):

```
<itpslbody>
      <AND|OR|XOR|as_a_result_of>
          <AND|OR|XOR|as_a_result_of>
              <filestatements> ....</filestatements>
              <execstatements>....</execstatements>
              <netstatements>...</netstatements>
          </AND|OR|XOR|as_a_result_of>
          <AND|OR|XOR|as_a_result_of>
              <filestatements> ....</filestatements>
              <execstatements>....</execstatements>
              <netstatements>...</netstatements>
      </AND|OR|XOR|as_a_result_of>
      </AND|OR|XOR|as_a_result_of>
</itpslbody>
```

The Insider Threat Prediction Specification Language (ITPSL) (5):

```
<itpslbody>
      <AND|OR|XOR|as_a_result_of>
          <AND|OR|XOR|as_a_result_of>
              <filestatements> ....</filestatements>
              <execstatements>....</execstatements>
              <netstatements>...</netstatements>
          </AND|OR|XOR|as_a_result_of>
          <AND|OR|XOR|as_a_result_of>
              <filestatements> ....</filestatements>
              <execstatements>....</execstatements>
              <netstatements>...</netstatements>
      </AND|OR|XOR|as_a_result_of>
      </AND|OR|XOR|as_a_result_of>
</itpslbody>
```

The Insider Threat Prediction Specification Language (ITPSL) (6):

```
<itpslheader>
    <signid> 69754c2b65627a098d02eb6244e40e69 </signid>
    <signdate>
        <year> 2007 </year>
        <month> 08 </month>
        <day> 25 </day>
    </signdate>
    <ontology>
        <reason> intentional </reason>
        <revision> 1.0 </revision>
        <user_role> ordinary_users </user_role>
        <detectby> multi </detectby>
        <weightmatrix> (d,d,d,d,d,d,d,d,d) </weightmatrix>
        <os> linux </os>
        <threat>   (“peer-to-peer”,   “p2p”,   “installation”,”azureus”)
</threat>
[ <synopsis> “This signature estimates the threat of installing and using
the azureus p2pclient” </synopsis>]
    </ontology>
</itpslheader>
```

References:

[1] Caelli, W., Longley, D. and Shain, M. (1991), Information Security Handbook, Stockton Press.

[2] Richardson R. (2007). “2007 CSI COMPUTER CRIME AND SECURITY SURVEY”, Computer Security Institute, URL: http://www.gocsi.com/index.jhtml

[3] PriceWaterHouseCoopers portal (2006). “DTI Information security breaches survey 2006”,Technical Report,URL: http://www.pwc.co.uk/eng/publications/dti_information_security_breaches_survey_2006.html

[4] Magklaras G., Furnell S. (2004). “The insider misuse threat survey: investigating IT misuse from legitimate users”m Proceedings of the 5th Australian Information Warfare & Security Conference, Perth Western Australia, 25-26 November 2004, pp. 42-51

[5] Howard, J. (1997), “An Analysis of Security Incidents on the Internet 1989-1995”, PhD Thesis, Carnegie Mellon University, Pittsburgh, Pennsylvania, USA.

[6] Neumann P., Parker D. (1989), ’A summary of computer misuse techniques’, In Proceedings of the 12th National Computer Security Conference, Baltimore, USA, pages: 396-407.

[7] Lindqvist U., Jonsson E. (1997),”How to systematically classify Computer Security Intrusions”, Proceedings of the 1997 IEEE Symposium on Security and Privacy, May 4-7, 1997, IEEE Computer Society Press.

References (2):

[8] Furnell S., Magklaras G., Papadaki M., Dowland P. (2001), 'A Generic Taxonomy for Intrusion Specification and Response', Proceedings of Euromedia 2001, Valencia, Spain, pages: 125-131.

[9] Anderson, James P., 'Computer Security Technology Planning Study 2. ESD-TR-73-51, Bedford, MA: Electronic Systems Division, Air Force Systems Command, Hanscom Field,October 1972.

[10] Tuglular T. (2000), "A preliminary Structural Approach to Insider Computer Misuse Incidents', EICAR 2000 Best Paper Proceedings: pages 105-125.

[11] Magklaras G., Furnell S. (2002), "Insider Threat Prediction Tool: Evaluating the probability of IT misuse", Computers & Security, Elsevier Science Ltd, Vol. 21, No. 1, pages: 62-73.

[12] Wood B. (2000). "An insider threat Model for Adversary Simulation", SRI International, Research on Mitigating the Insider Threat to Information Systems - #2: Proceedings of a Workshop Held by RAND, August 2000.

[13] Pauleo A., "Mitigating Insider Threat using Human Behavior Models", Master's Thesis, US Air Force Institute of Technology, AFIT/GCE/ENG/06-04

[14] Schultz, E.E. (2002). "A framework for understanding and predicting insider attacks", Computers & Security, vol. 21, no. 6, pp. 526-531.

References (3):

[15] Melara, C., Sarriegui, J.M., Gonzalez, J. J., A. Sawicka, D.L. Cooke, (2003), “A System Dynamics Model of an Insider Attack on an Information System,” in Proc. of the 21st International Conference of the System Dynamics Society, New York, NY

[16] Magklaras G., Furnell S. (2005) “A preliminary Model of End User Sophistication for Insider Threat Prediction in IT Systems”, Computers & Security, Volume 24, Issue 5, August 2005, Pages 371-380.

[17] Magklaras, G. (2005), An Architecture for Insider Misuse Threat Prediction in IT Systems, MPhil Thesis, School of Computing, Communications and Electronics, University of Plymouth, UK.

[18] Magklaras G., Furnell S., Brooke P. (2006), “Towards an Insider Threat Prediction Specification Language, Information Management & Computer Security, vol.14, no.4, pages 361-381.