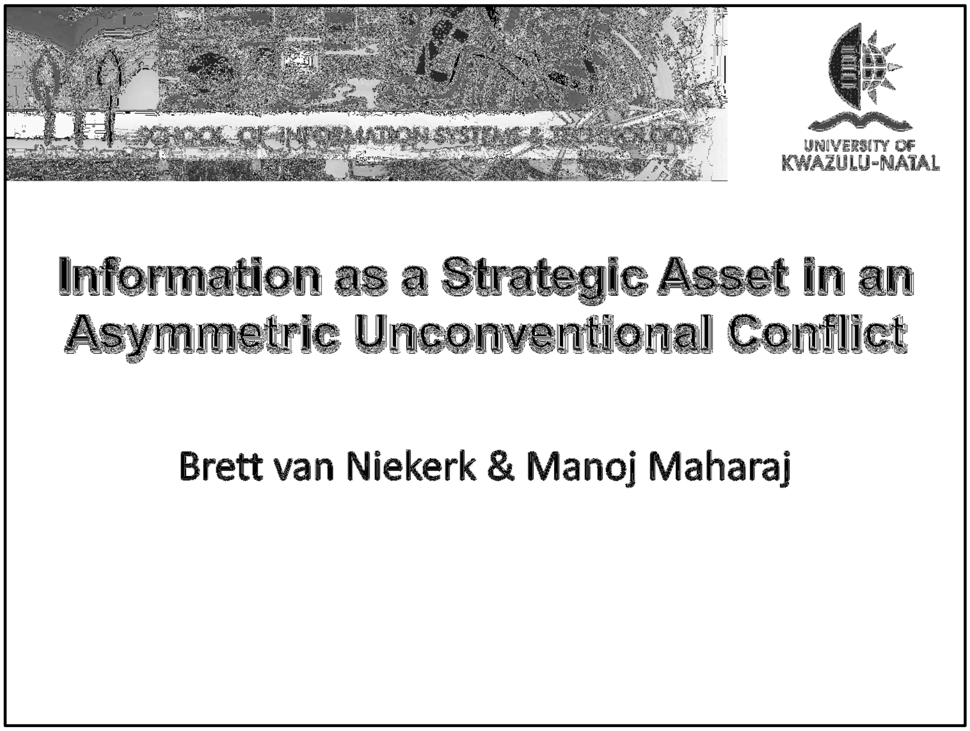
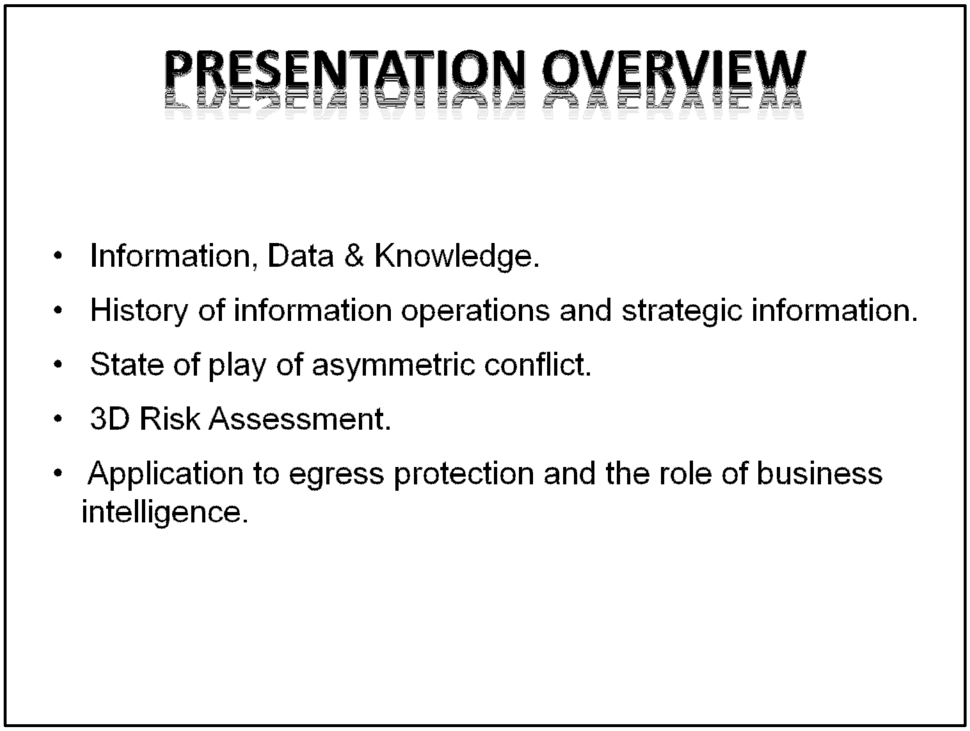


SCHOOL OF INFORMATION SYSTEMS & TECHNOLOGY

UNIVERSITY OF
KWAZULU-NATAL

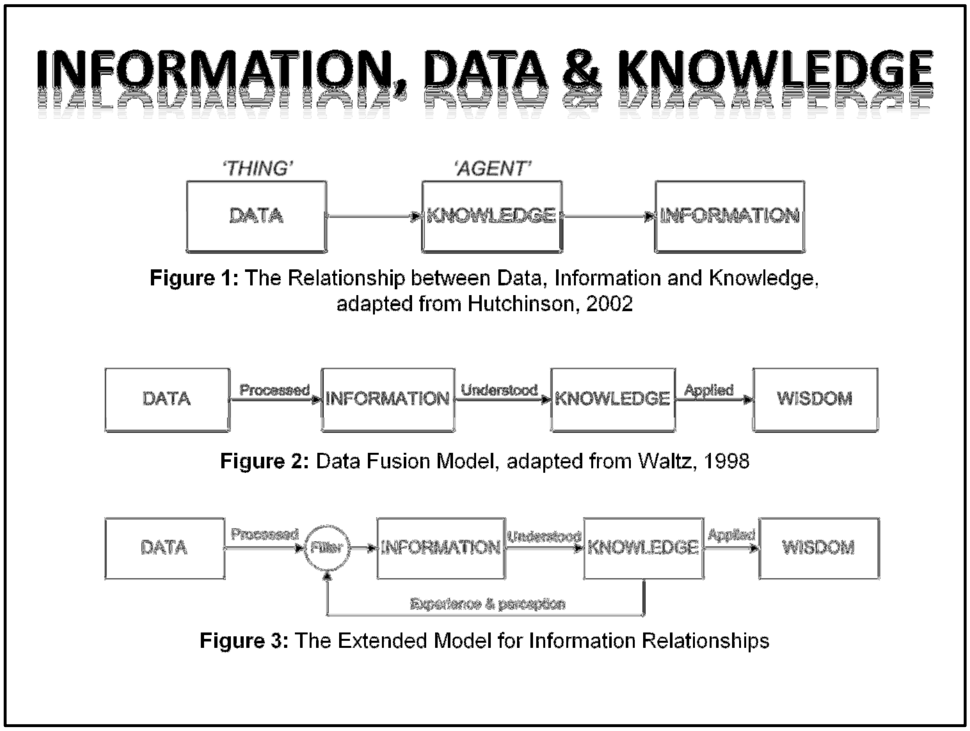
Information as a Strategic Asset in an Asymmetric Unconventional Conflict

Brett van Niekerk & Manoj Maharaj



PRESENTATION OVERVIEW

- Information, Data & Knowledge.
- History of information operations and strategic information.
- State of play of asymmetric conflict.
- 3D Risk Assessment.
- Application to egress protection and the role of business intelligence.



INFORMATION, DATA & KNOWLEDGE

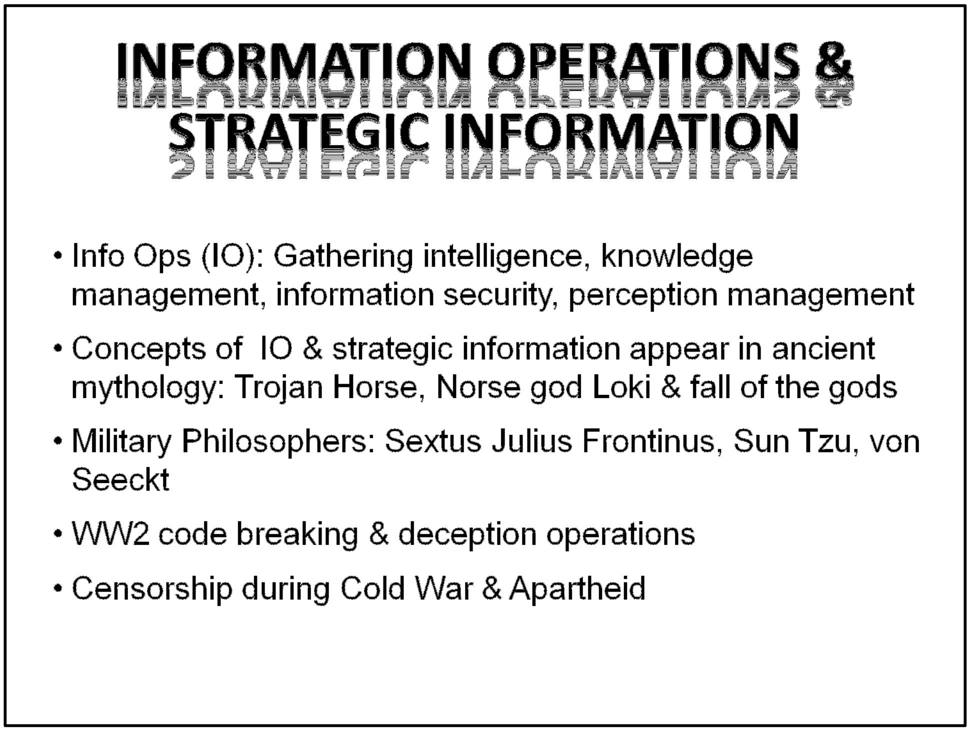
Figure 1: The Relationship between Data, Information and Knowledge, adapted from Hutchinson, 2002

Figure 2: Data Fusion Model, adapted from Waltz, 1998

Figure 3: The Extended Model for Information Relationships

Information can be seen as a collection of data that has been filtered by knowledge on the form of previous experiences and perceptions. [click] A more traditional model is that data is grouped into related sets to form information. This information is analysed and patterns emerge to form knowledge in the form understanding through the use of models and trends. This application of this knowledge can then be considered to be wisdom.

By combining these models we have the traditional data fusion model with the addition of a feedback loop that allows for the specific filtering of data by a priori knowledge. In effect this is the process of business intelligence; data and information is gathered and analysed to show trends or patterns that may be exploited by the organisation.



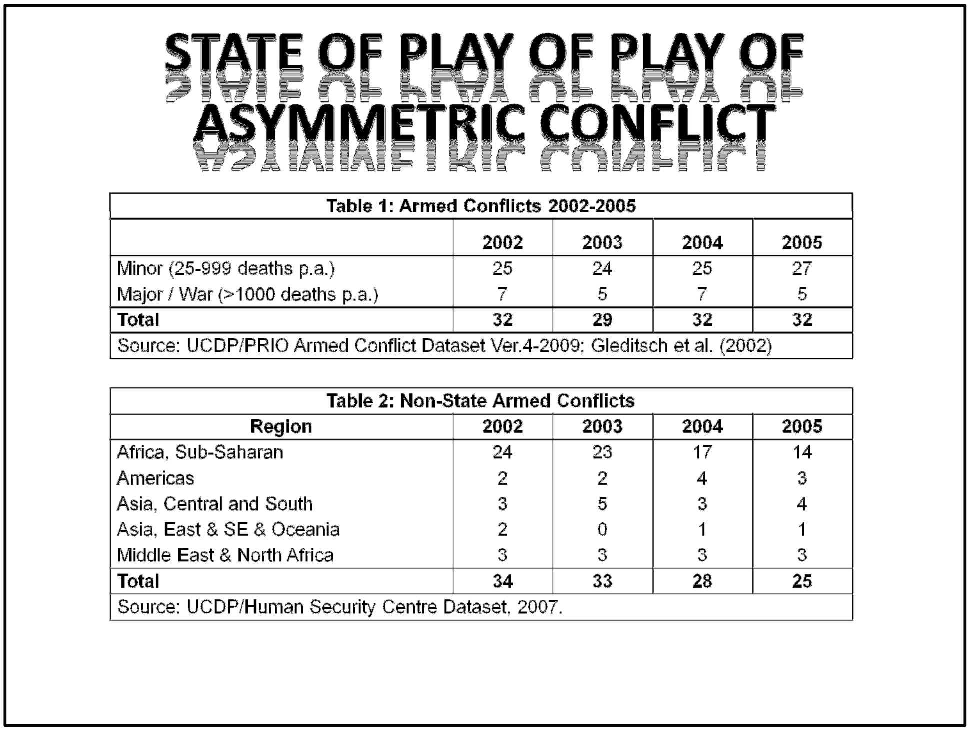
INFORMATION OPERATIONS & STRATEGIC INFORMATION

- Info Ops (IO): Gathering intelligence, knowledge management, information security, perception management
- Concepts of IO & strategic information appear in ancient mythology: Trojan Horse, Norse god Loki & fall of the gods
- Military Philosophers: Sextus Julius Frontinus, Sun Tzu, von Seeckt
- WW2 code breaking & deception operations
- Censorship during Cold War & Apartheid

Information operations is a concept that grew out of information warfare – and includes a wide variety of disciplines such as intelligence, knowledge management, and information security. Throughout history we have examples of information operations and the use of strategic information to gain an advantage over the adversary.

In mythology there is the story of the Trojan horse and the Norse trickster god, who used a insignificant piece of information in a manner which resulted in the destruction of the gods. A number of military philosophers mentioned the importance of knowledge. In WW2 there were examples of code-breaking and deception which could very well have been the difference between victory and defeat. In recent times there has been an increase in censorship from the cold war and apartheid eras to modern states.

IO appears to be a purely military concept; however it has many applications in business. Public and private organisations also need to be concerned with information and operations security and the use of intelligence and knowledge management to aid their strategic objectives. In the next few slides we will see the concpets can be applied to business.



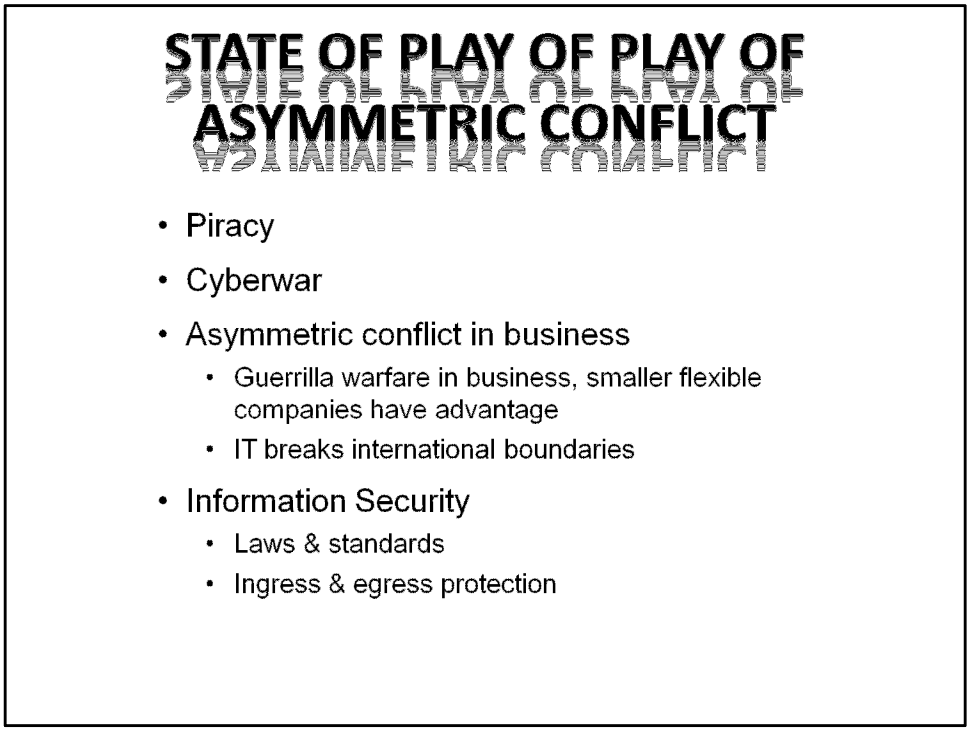
STATE OF PLAY OF PLAY OF ASYMMETRIC CONFLICT

Table 1: Armed Conflicts 2002-2005				
	2002	**2003**	**2004**	**2005**
Minor (25-999 deaths p.a.)	25	24	25	27
Major / War (>1000 deaths p.a.)	7	5	7	5
Total	**32**	**29**	**32**	**32**
Source: UCDP/PRIO Armed Conflict Dataset Ver.4-2009; Gleditsch et al. (2002)				

Table 2: Non-State Armed Conflicts				
Region	**2002**	**2003**	**2004**	**2005**
Africa, Sub-Saharan	24	23	17	14
Americas	2	2	4	3
Asia, Central and South	3	5	3	4
Asia, East & SE & Oceania	2	0	1	1
Middle East & North Africa	3	3	3	3
Total	**34**	**33**	**28**	**25**
Source: UCDP/Human Security Centre Dataset, 2007.				

What is asymmetric conflict? There is some form of asymmetry – technological, size of forces, religious fanaticism. Due to these asymmetries, unconventional conflict is usually the result, where smaller, technologically inferior forces use guerrilla warfare in an attempt to compete. In areas where there is religious fanaticism, this provides an advantage over the conventional military forces; the threat of force does not work with suicide bombers.

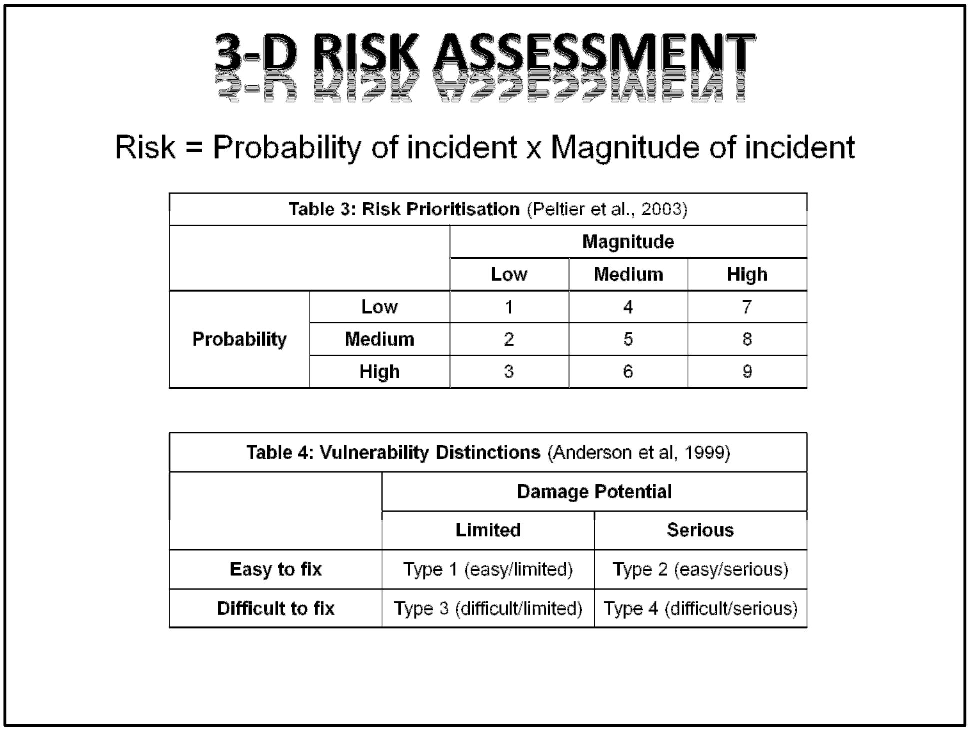
The tables on the slide show the number of armed conflicts for a 4-year period. As can be seen the number of minor conflicts far outweigh the major wars; and the vast majority of non-state armed conflict exists in Africa. Knowledge of these conflicts may aid business; they may affect transport routes or the availability of strategic minerals.



STATE OF PLAY OF PLAY OF ASYMMETRIC CONFLICT

- Piracy
- Cyberwar
- Asymmetric conflict in business
  - Guerrilla warfare in business, smaller flexible companies have advantage
  - IT breaks international boundaries
- Information Security
  - Laws & standards
  - Ingress & egress protection

Piracy: on seas – pirates use information to target shipping. Failure: tried to capture French command & control warship. Software/music/video piracy – continuously attempting to break protection.
Cyberwar: attacker unknown, sudden & distributed; for countries with high reliance on computer networks the effects of a large-scale cyber-attack can have a huge impact on the economy; the examples of Estonia on 2007 and Georgia in 2008 illustrates this. Organisations that are more reliant on e-commerce may be affected more than others.
As in guerrilla warfare, smaller businesses with less overhead and hierarchical structure are more flexible. A South African company received a large contract from the US as they were prepared to custom build lasers to the clients specifications; other companies provided a standard set of products. Using e-commerce they can compete with larger companies for niche markets in a global context. IT advances also allow organisations to distribute their operations; whereas previously all operations may have needed to be centralised. This allows companies to re-locate operations to regions where they will be better able to support the new markets. An example of this is MTN shifting some of its operations from SA to the Middle East due to the growing market in the region.
Knowledge of **information security** again is important; many organisations push security to the side, however new laws and regulations will result in the need for greater awareness and compliance; and in the future will need to be concerned with leakage of information and not just preventing viruses and spam from coming in.



3-D RISK ASSESSMENT

Risk = Probability of incident x Magnitude of incident

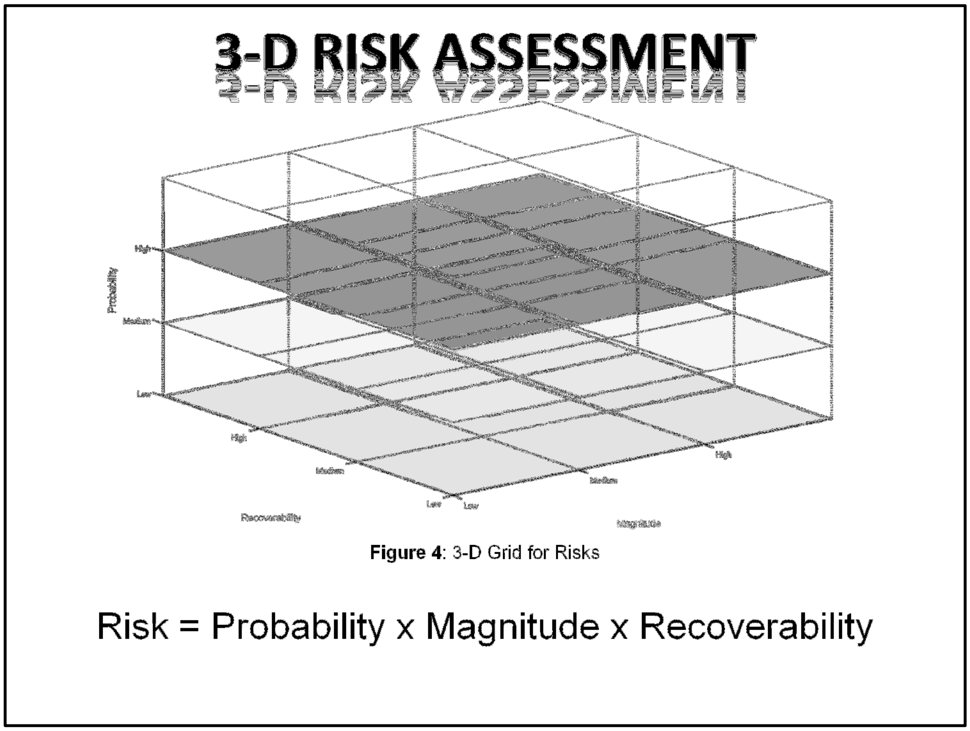
Table 3: Risk Prioritisation (Peltier et al., 2003)

		Magnitude		
		Low	**Medium**	**High**
Probability	**Low**	1	4	7
	Medium	2	5	8
	High	3	6	9

Table 4: Vulnerability Distinctions (Anderson et al, 1999)

	Damage Potential	
	Limited	**Serious**
Easy to fix	Type 1 (easy/limited)	Type 2 (easy/serious)
Difficult to fix	Type 3 (difficult/limited)	Type 4 (difficult/serious)

The basic form of risk assessment is the chance of something going wrong multiplied by how badly it will affect you. The business intelligence function can be used to estimate both the probability and impact. Usually the magnitude s expressed in monetary terms. If it is not possible to precisely quantify the probability and impact, the variables may be put into a scaled form to estimate the priorities of each risk.
A similar version may be uses the impact and the difficulty to recover from the damage to prioritize risk.

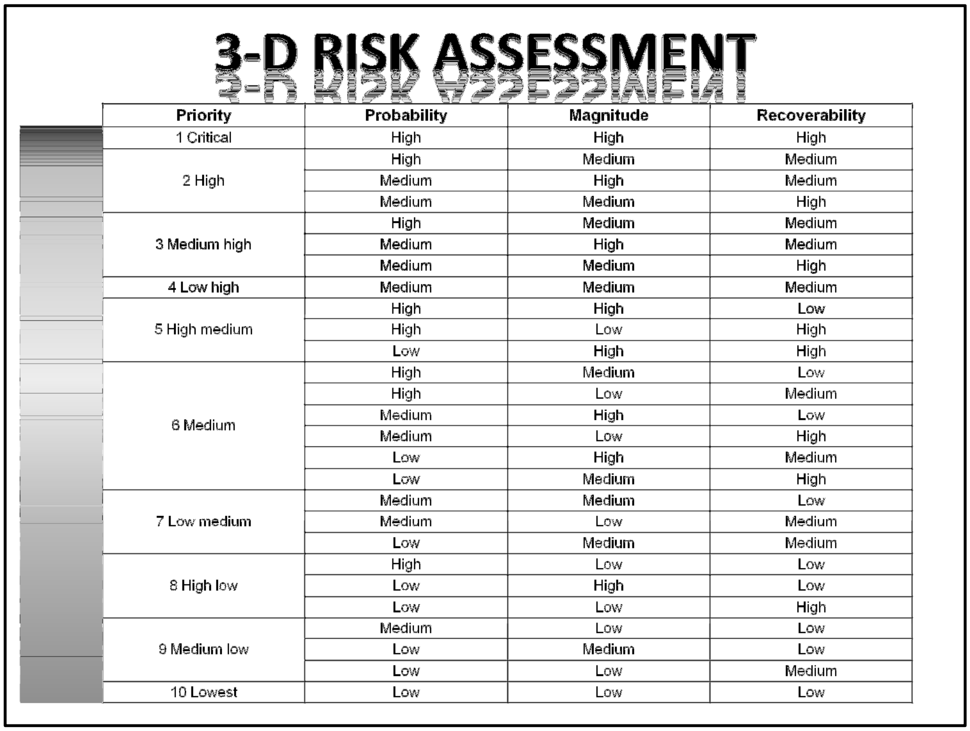


3-D RISK ASSESSMENT

Figure 4: 3-D Grid for Risks

Risk = Probability x Magnitude x Recoverability

If we combine the 2 risk models, we get a ‘3D’ variant of the risk assessment. This is just an example; the variables might change; a rating for vulnerability could be used in place of either the magnitude or recoverability terms. By using scaled metrics of 1-5 for low-high, the risks can then be prioritised as follows....

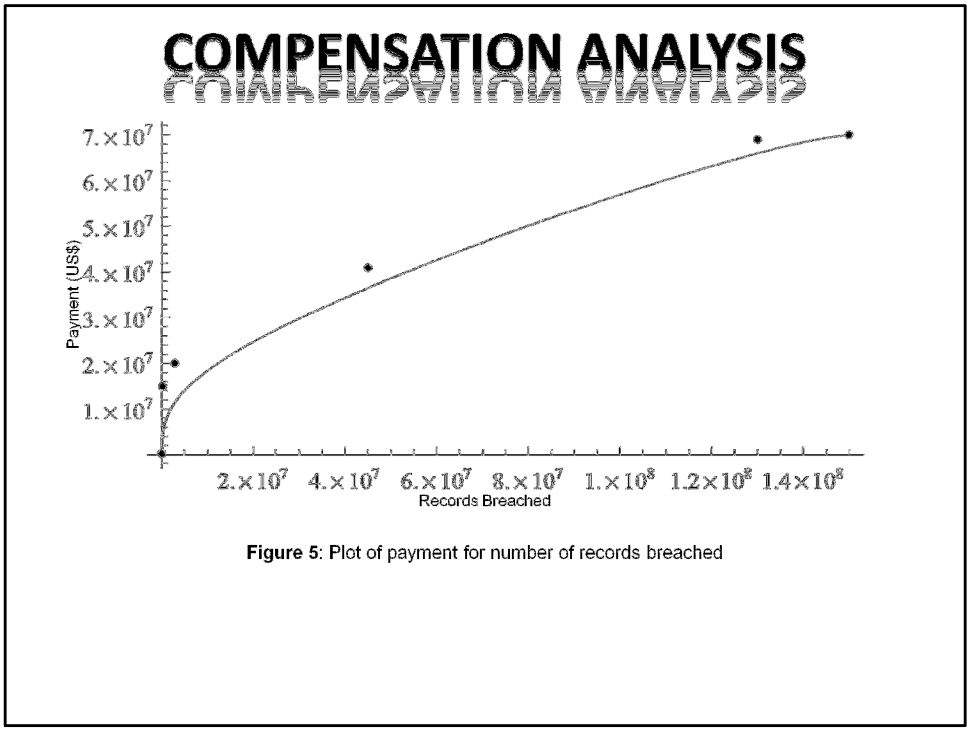


3-D RISK ASSESSMENT

Priority	Probability	Magnitude	Recoverability
1 Critical	High	High	High
2 High	High	Medium	Medium
	Medium	High	Medium
	Medium	Medium	High
3 Medium high	High	Medium	Medium
	Medium	High	Medium
	Medium	Medium	High
4 Low high	Medium	Medium	Medium
5 High medium	High	High	Low
	High	Low	High
	Low	High	High
6 Medium	High	Medium	Low
	High	Low	Medium
	Medium	High	Low
	Medium	Low	High
	Low	High	Medium
	Low	Medium	High
7 Low medium	Medium	Medium	Low
	Medium	Low	Medium
	Low	Medium	Medium
8 High low	High	Low	Low
	Low	High	Low
	Low	Low	High
9 Medium low	Medium	Low	Low
	Low	Medium	Low
	Low	Low	Medium
10 Lowest	Low	Low	Low

The table is in the paper, so I wont spend too much time on it; the left hand column effectively groups the outcome into the same values; providing a scale of 1 to 10 of risk priorities. The max value is 125 (5 x 5 x 5), min val is 1 (1 x 1 x 1).

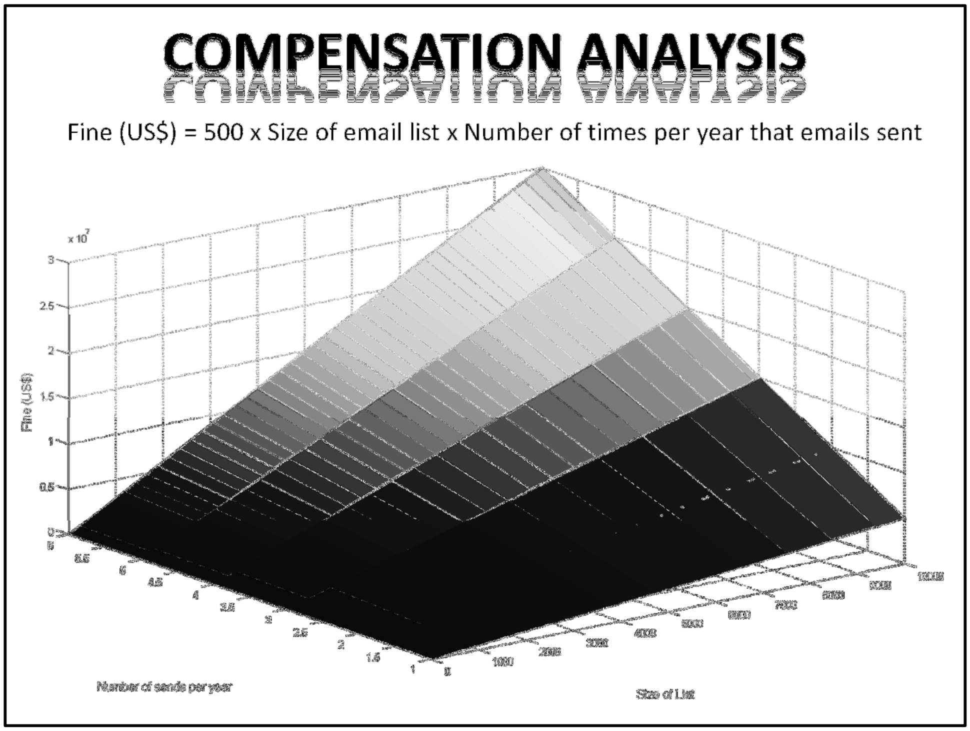
That was an example of using scaled metrics to estimate the risk prioritisation. The next 3 slides will give an example of using open sources of information to generate models and patterns that may be used to estimate the magnitude of impact more precisely. The case of data breaches is used; which also illustrates the need for egress protection. Many organisations focus on preventing spam emails and viruses from entering the network and dont configure their systems to prevent outgoing spam; this could impact on the business. I witnessed to examples in industry: a single computer was participating in a denial of service attack; the resultant data flow shut down the external internet access; the second was a single email address was sending spam, resulting in the organisations emails being blacklisted. There are now laws which may hold companies liable for participating in an attack or sending unsolicited emails.



COMPENSATION ANALYSIS

Figure 5: Plot of payment for number of records breached

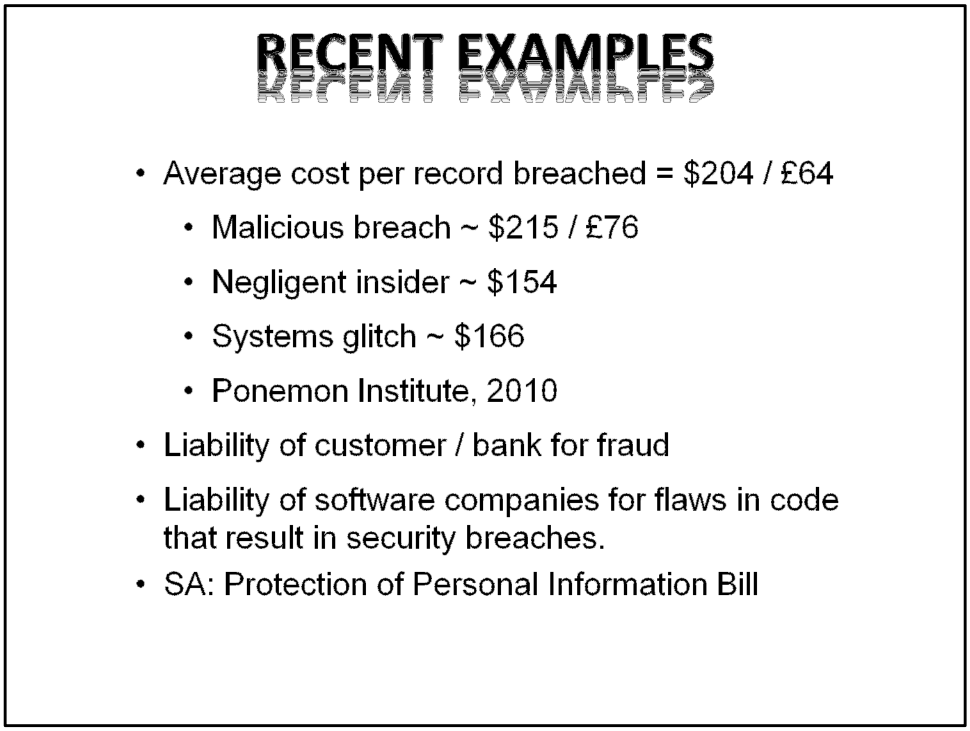
Court cases related to data breaches in the US were analysed; a spline curve was fitter to six points with a seventh artificial limit at 70million US$ - the graph is the resultant curve. With more points as more data becomes available, the more accurate the curve will be; but you can get an estimate of the compensation an organisation will be required to pay due to the number of records that were compromised.



COMPENSATION ANALYSIS

Fine (US$) = 500 x Size of email list x Number of times per year that emails sent

Similarly; the fine that can be expected for spam emails can be estimated with the equation; the reference can be found in the paper. The surface is the fine for various values of email list and frequency of distribution; sending 10000 emails 6 times a year will result in a fine of 30million US$.



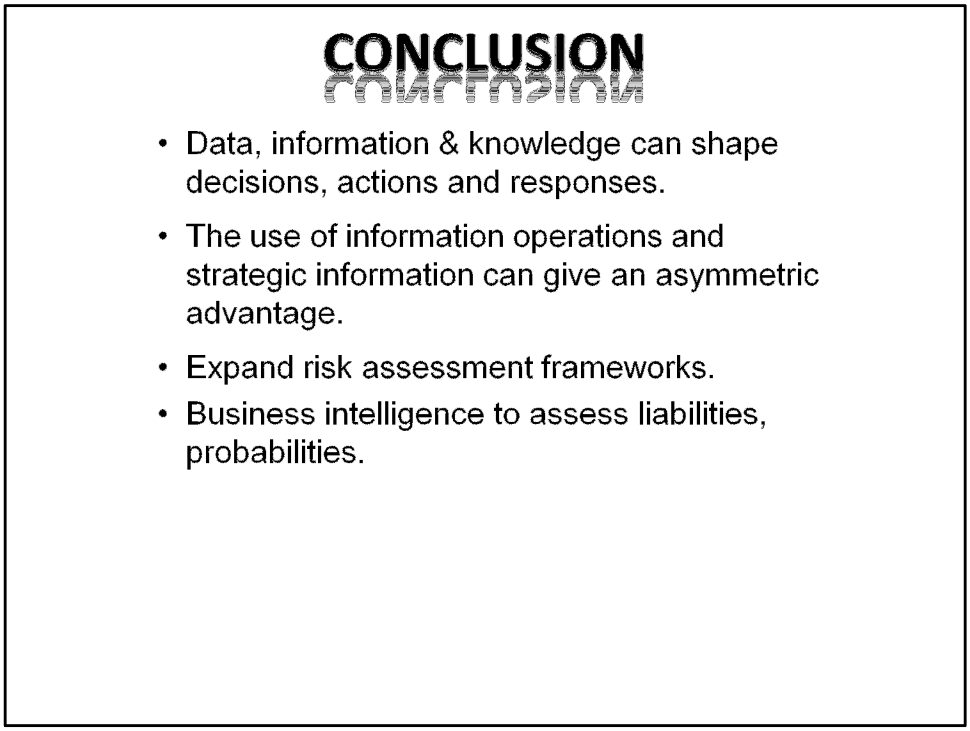
RECENT EXAMPLES

- Average cost per record breached = $204 / £64
  - Malicious breach ~ $215 / £76
  - Negligent insider ~ $154
  - Systems glitch ~ $166
  - Ponemon Institute, 2010
- Liability of customer / bank for fraud
- Liability of software companies for flaws in code that result in security breaches.
- SA: Protection of Personal Information Bill

Using open source information may be advantageous due to the amount of research that is published on the internet; an example given here is the Ponemon Institute investigating the implications of data breaches; this report goes into more detail giving average cost for various ways which the data was breached. It is also possible to find lists of the top cyber threats, or analyse data from some Computer emergency response team websites.

Currently there is a court case which may ultimately determine who is will be considered liable for phishing attacks; the customer of the bank. There is also a drive to make software vendors liable for security flaws in their code that result in data breaches.

In South Africa, the new Protection of Personal Information Bill may result in similar legal proceeding. This bill, combined with the new cybersecurity policy (1st draft released end of feb), which calls for compliance to regulations and standards, may see South African organisations hard pressed to secure their data records.



CONCLUSION

- Data, information & knowledge can shape decisions, actions and responses.
- The use of information operations and strategic information can give an asymmetric advantage.
- Expand risk assessment frameworks.
- Business intelligence to assess liabilities, probabilities.

To conclude, the use of data, information & knowledge can shape the decisions and actions of organisations; the effective use of information operations and strategic information can provide an asymmetric advantage over competitors.

Risk assessment frameworks can be expanded and modified; and business intelligence may be used to assess liabilities and incident probabilities. Examples were given for the case of data breach liability; which can then be used to determine the need for egress protection.

SCHOOL OF INFORMATION SYSTEMS & TECHNOLOGY

UNIVERSITY OF KWAZULU-NATAL

Thank you.

Questions?

Brett van Niekerk	Manoj Maharaj
991160530@ukzn.ac.za	maharajms@ukzn.ac.za
+27 (0)31 260 8521	+27 (0)31 260 8023