Information Security is Information Risk Management

1. Information Risk

Technology applied to information can create three types of **risks**:

1. Information can be improperly disclosed (divulguée) -> Confidentiality
2. Information can be modified in a inappropriate way -> Integrity
3. Information can be destroyed or lost -> Availability

This will cause dollar **losses** to the information's owner. It can be:

- **direct** (reduction in the value of the information asset itself) or;
- **indirect** (service interruption, damage to the reputation, loss of competitive advantage, legal liability).

1.1 What is Risk?

Risk= Possibility of an event (called "adverse event") which will reduce the value of the business to occur.
Cost of a risk = probability of an event * consequence of the event.

1.2 Measuring Risk

A common measure of the cost of a risk is **ALE** (Annualized Loss Expectation) which is the cumulative cost of risk over a period of one year as estimated in advance.

2. Managing Risk

Four mechanisms: Liability Transfer, Indemnification, mitigation and retention.

2.1 Liability Transfer

A business can transfer liability (responsabilité) for an adverse event to another party in 2 ways:
- **Disclaimer**: Not responsible for the consequences of certain adverse events, but without specifying who will be responsible for those consequences.
- **Agreement**: Business and counter-party agree that the counter-party will be responsible for the consequences of certain adverse events.

2.2 Indemnification

A business can indemnify itself against the consequences of an adverse event. 2 major types:
- Pooling: example: insurance policies.
- Hedging: example: options.

2.3 Mitigation

2 ways of reducing the expected cost of a risk:
-Reduce the probability of the adverse event to occur by eliminate the event's causes or avoid the activity which it creates the risk.
- Reduce the consequences by taking steps to limit the damage the event causes (example: building codes that anticipate earthquakes).

2.4 Retention

If an adverse event is not very costly or not very likely to occur, a business may choose to retain the risk in 2 ways:
- Self-insure: The business set aside funds to offset (compenser) the cost of retained risks.
- Accept retained risks.

3. Information Security

Information security is a risk management discipline, whose job is to manage the cost of information risk to the business.

3.1What is Information Security?

Information security starts with policies "who should be allowed to do what" to sensitive information. The next task is to enforce the policy by deploying a mix of processes and technical mechanisms that fall in 4 categories:

- Protection measures: prevent adverse events to occur.
- Detection measures: alert the business when adverse events occur.
- Response measures: return the business to a safe condition.
- Assurance measures: validate the effectiveness of the previous operations.

The final task is an audit to determine the effectiveness of the measures taken to protect information against risk. Be careful, these operations should be done in a cycle.

3.2 What's wrong with information security?

2 reasons:

- Information security focuses on only a small part of the problem of information risk.
- It doesn't do a very good job of protecting businesses against even that small part.

3.2.1 Focus

Information security technology focuses primarily on risk mitigation by reducing the probability of an adverse event than reducing its consequences. Information security activities rarely include any discussion of indemnity or liability transfer.

3.2.2 Effectiveness

The annual FBI/CSI computer crime surveys and the CERT coordination centre annual summaries have shown substantial increases in the number of security incidents and in the dollar losses resulting from incidents in each of the past five years.

4. Quantification of information security risk

In order to quantify information security risk, and the effectiveness of the control measures, the following information needs to be collected:

4.1 Vulnerabilities

For each vulnerability, information needs to be gathered and regularly updated about the ease and frequency of exploitation, and the ease and speed of recovery from exploitation.

4.2 Incidents

The information must include what vulnerabilities were exploited and how response and recovery were handled. If unknown vulnerabilities, we must feed them back.

4.3 Losses

For each incident identified, information needs to be collected about direct monetary losses caused by the incident and about indirect losses (ex. Reputation damage, lost business)

4.4 Countermeasure effectiveness

For each incident identified, information needs to be collected about what security measures were in use at the time of incident, which security measures were bypassed, which security

measures were defeated, and how much time and effort were required to circumvent (contourner) or defeat (vaincre) the security measures in place.

5. What does the current situation look like?

- Very little information about frequency of occurrence of adverse events and about the seriousness of their consequences.
- Very little about the effectiveness of the measures we take to prevent adverse events or alleviate (alléger) their consequences.
- The people to whom these events happen have few incentives (mesures d'incitation) to report them; conversely, they have many incentives to suppress information about them.
- The system we are attempting to protect (Internet) is far too complex to be understood in detail.

Analogy with medical practice in the 19th century: Medical practitioners had a poor understanding of illness causes. The medical manual contains no information about causes, symptoms, or mortality rates of the conditions it describes; it consists entirely of lists of preparations which could be administered for each condition, with no advice on how to choose among the many options. Now we have all this information.

3 developments helped:

- Mandatory professional education and licensure of practitioners
- Systematic collection and study of public health data
- Systematic observational studies of safety and effectiveness of treatments

Let’s apply this to information risk management.

6. How should information risk be managed?

The information risk management professional will:

- require assessing the costs and benefits of all risk “treatment” options - liability transfer, indemnification, and retention as well as mitigation, detection and response as well as prevention
- Choice of “treatment” options should be based on the welfare of the “patient” which will maximized by optimizing cost of risk to the business rather than on minimizing probability of occurrence of adverse events.

Information security risk education should include financial and legal disciplines in addition to the technical disciplines taught today.

6.1 Reporting

In the future, the authors believe that information security risk assessments should focus not just on identifying risks, but also on quantifying them. Once risks are identified and quantified, the resulting data should be reported.

7. How should information risk be studied?

Information risk should be studied by an independent body with the characteristics of a public health service. This "Public Security Service" should collect from information risk management professionals, data on the prevalence of losses, the causes of losses, the effects of losses, and the effectiveness of information risk treatments.

The Public Security Service should analyze this data and publish the results of its analyses as a way to improve the state of information risk management practice, and to inform public policy decisions about information risk management.

8. How should information security technology be evaluated?

In the future, the authors believe that the effectiveness of information security technology would be most effectively evaluated by an impartial body following a process similar to the one used by the US Food and Drug Administration (FDA) to approve medical treatments for use.

8.1 Tracking and Reporting

Information risk management professionals should be required to report regularly to the evaluation body on the effectiveness of the treatments they "prescribe" to their "patients".

9. A word about the ethics of risk quantification

A review of an earlier draft of this paper questioned whether quantification of certain types of risks (particularly risks to human life and safety) in financial terms is ethically acceptable.

While the authors do not believe that every risk should be controlled using a monetary cost/benefit framework, we do believe that all risks should be quantified to the greatest extent possible, We also believe that information security risks will be poorly understood until we do a much better job of quantification of economic losses. Finally, we believe that information security countermeasures will continue to be difficult to justify in voluntary control regimes until their effectiveness can be expressed as a quantifiable reduction of economic losses.