Quantifying Information Risk and Security

Conducting risk assessments and the calculation of a return on investment (ROI) on information security is challenging. ISACA’s Risk IT framework defines IT risk as “The business risk associated with the use, ownership, involvement, influence and adoption of IT within an enterprise.” That said, managing risk requires predictions, assumptions and guesses.

COBIT® 5 for Information Security addresses governance issues that were missing in previous publications, standards and good practices. While it provides many indicators and suggested metrics, quantifying information security in business terms remains difficult.

The impact of security events on the business relies on knowledge of incidents, the IT systems and services that are essential to support business processes, and the assessment of the impact of their malfunctions on business operations. Acquiring such knowledge relies on business process owners—they are the only ones who can assess and quantify the operational, financial and regulatory impact of disruptions. The impact on reputation remains hard to calculate with any accuracy.

A well-developed business impact analysis (BIA) should reflect how business operations are impacted and how time affects such impact, as this is rarely a linear function. A 10-minute service interruption may have a negligible impact while the same service interruption extended over three days may prove catastrophic to the business.

As BIAs are based on available and credible data evaluated by individuals familiar with specific business processes, they allow the impact to be assessed in a plausible manner. Even if the numbers are not accurate, they can be accepted as “reliable enough.”

The outcome of BIAs should be a set of well-designed, tested and updated plans (incident response, disaster recovery, business continuity and crisis management). The effectiveness of such plans can determine the difference between survival and business failure.

Enterprise risk management (ERM), of which IT risk is a component, arose from different concerns relating to a risk-based approach to management that integrates aspects of internal control and strategic planning and includes, among other things, regulatory compliance. Like understanding impacts, ERM should be owned by business managers. Figure 1 illustrates the main differences between BIA and ERM.

Two disciplines—information risk management and information security—have migrated from their specialized niches into the wider field of enterprise management.

Risk assessments and the calculation of ROI for information security are linked topics. The discussion that follows examines how and why. Information security practitioners are expected to master both disciplines and this article attempts to describe the many trappings these topics contain.

INFORMATION RISK MANAGEMENT

Information risk management (IRM) came to the attention of business managers through the following factors:
• The convergence of increasing dependency on information technology in enterprise operations
• The mission-critical nature of many information systems and services
• The reliance on an open global network (the Internet) and its side effects (notably cybercrime and malicious software of unknown origin)
Increasing concerns about the militarization of cyberspace and the potential for cyberwar and cyberterrorism

ISACA’s The Risk IT Framework and The Risk IT Practitioners Guide provide a comprehensive, well-thought-out and articulate set of processes. Chapter 4 of The Risk IT Practitioners Guide is devoted to communicating and describing risk. It recognizes that qualitative assessments are simple to carry out and that quantitative assessments require not-readily-available (if at all) data. Figure 2 presents the five strategies to deal with individual risk and the components of a risk assessment. This is simple and concise view regarding risk assessment. A more comprehensive view of this topic can be found in The Risk IT Framework.

Figure 2—Factors to Consider When Assessing Risk

<table>
<thead>
<tr>
<th>Threat</th>
<th>Capability</th>
<th>Probability</th>
<th>Asset Vulnerabilities</th>
<th>Business Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Force of Nature</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Human Accidental</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Human Deliberate</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

ASSET VULNERABILITIES

The rapid innovation in IT has added complexity to vulnerability management for several reasons.

The Growing Complexity of IT Products

Operating systems (OSs) are one example. When IBM introduced System 360 in 1967, it became the largest software project at the time, totaling an estimated one million lines of code. Delivered a year late, its cost was four times the initial budget and it was full of errors that took years to eradicate. In 1969, IBM acknowledged that each release of this software had about 1,000 errors and this number was reasonably stable.

Microsoft introduced Windows 7 in 2009 (and replaced it with Windows 8 in 2012). The original release of Windows 7 contained an estimated 50 million lines of code (50 times the size of System 360). Microsoft has not disclosed the number of errors of the original release version of Windows 7 and no reliable information on this could be found from other sources. However, hot fixes for Windows 7, many of which are labeled critical, are issued on a weekly basis.

Such complexity can be found in virtually every other product, including servers, routers, tablets and smartphones. This is also true for downloaded mobile applications (“apps”) and enterprise applications. It should be assumed that every piece of equipment and software has vulnerabilities (some known and others yet to be discovered) that can, and most likely will, be exploited with malicious intent.

To add to the problem, the current software ecosystem is small and some components are used all over the world (e.g., Windows, Android, Java). The errors in these systems are constantly being investigated and reported. The reports give

• A malicious insider with the capabilities, motivation and opportunity to interfere with information systems and data could remain undetected for a long time (if ever detected).

In the absence of supporting data to calculate and quantify the probability of a deliberate human attack on information assets, risk assessors can, at best, rely on their knowledge of the enterprise, its culture and people, and their experience. In the absence of reliable intelligence regarding such attacks, a qualitative assessment is more or less an informed guess. Whether or not this is good is subjective and different for each enterprise depending on its nature.

THREATS

Until the 1990s, risk practitioners focused on the threats presented by forces of nature, such as hurricanes and earthquakes. As information technologies became ubiquitous, it became necessary to address incidents arising from accidental human activities (such as incorrectly configuring a device and undetected software errors). Deliberate actions ranging from avoiding a test to save time to fraud and sabotage also had to be added to the threat landscape. Ignoring these risk factors may not be a prudent course of action. Deliberate human threats can be the biggest challenge, particularly for critical infrastructures because:

• Such actions are unpredictable, not random. Thus, statistical analysis of past events cannot help.
• The individuals behind these threats are unknown, rarely identify themselves, and may be external or internal. Good intelligence is essential, but hard to find.
potential attackers a significant advantage because the scale of complexity of installing and testing all error fixes takes time and not all are implemented.

**Time to Market**
The recent wave of technical innovation is driven by the competitive nature of the IT industry. Its innovative culture encourages designers and vendors to bring their products to the attention of potential customers as early as possible. Some innovations are presented at trade exhibitions and are, at best, beta versions. Some are marketed early, possibly without full code reviews, testing and other quality assurance processes.

The hundreds of thousands of apps for smartphones and tablets that end users can download and install make the assessment of security of such devices extremely complex if not impossible.

End-user license agreements (EULAs) for packaged software limit the vendor's liabilities and describe warranty disclaimers when the software causes damage to the user's computer or data. These lengthy and complex agreements are hard to read and understand, are nonnegotiable, and must be agreed upon as a condition for installing the software.

Imperfections in technology, such as errors in design and manufacturing, appear gradually and some remain undiscovered (to become zero-day deliverables once discovered). Typically, the vendor offers a solution that could, and often does, introduce new errors.

**Vulnerabilities**
In addition to imperfect technologies used by imperfect people, the corporate use of information technologies relies on numerous processes (for a detailed description, refer to COBIT 5 and its companion publication COBIT 5 for Information Security). Vulnerabilities arise through:

- The extent to which these processes are implemented (Small organizations relying on internal resources are rarely able to implement all the processes listed in COBIT and those that are implemented may not be at a sufficiently high level of maturity to meet requirements.)
- The degree to which the processes follow the guidelines of established good practices such as the Information Technology Infrastructure Library (ITIL), the Data Management Body of Knowledge (DMBOK), the Software Engineering Body of Knowledge (SWEBOK) and the Project Management Body of Knowledge (PMBOK), as appropriate
- The level of compliance with these processes in practice, which is defined by the size and competencies of those who apply them. Time pressures, absences and lack of knowledge conspire to create shortcuts. Every exception should be treated as a vulnerability. This is defined by the organization's culture and the competencies, motivation and dedication of those applying the processes.

A sound assessment of vulnerabilities in technology, processes and staff is a prerequisite to effective risk assessment. Such vulnerabilities need to be related to their criticality to business processes and the impact these may cause when exploited by a specific threat.

**PROBABILITY**
A widely accepted definition of information risk states that it is "the potential that a specific threat will exploit the vulnerabilities of an asset." Many publications on risk present the formula as: Risk = Probability x Impact. However, the word probability is frequently replaced by likelihood. Beware! These two words do not mean the same thing. Probabilities have numerical values derived from statistical analysis. Statistics is a formal discipline using somewhat complex mathematics. This discipline is not well understood and statistics are often misused. This was recognized in the 19th century by the statement: "Lies, damned lies and statistics."

Statistics include two basic categories: *descriptive* and *inferential*. Descriptive statistics reflect past events and require sufficient data to meet specific requirements. Inferential statistics are predictive and use past data and mathematical formulae to support projections into the future.

Inferential statistics include those that can be calculated with some degree of accuracy. This is the case in games of chance.
such as dice and roulette. Casinos have relied on such statistics for a long time. "The gambling known as business looks with austere disfavor upon the business known as gambling." 

Inferential statistics and event intelligence are also used by insurance companies for the calculation of premiums for common events (e.g., driving a car, burglary, death). Insurance companies have the option of transferring the risk of a rare event to a reinsurance company or consortium. Some of the latter have lost vast amounts of money because statistics have limitations when it comes to events that are so rare that there is no reliable past data (e.g., explosion of a super-volcano). Venture capitalists and investors willing to gamble can become rich by betting early on the success of an innovator, e.g., the emergence of Google in 1998.

Information security likelihood is, at best, events that can occur with uncertain frequency and magnitude. Therefore they require an informed guess (and more often a gamble), subject to the evaluator's knowledge, experience and degree of paranoia (or optimism) when dealing with uncertainty.

Stating that likelihood of the manifestation of a threat may be low, medium or high and creating a risk matrix with little boxes colored green, yellow or red is a step forward—as long as all parties involved understand the subjective nature and agree on the assumptions and ratings made. Such matrices are often referred to as heat maps and can be misleading by themselves. Good practices require heat maps to be related to the organization's risk criteria to determine whether a given level of risk is acceptable (risk appetite).

Risk matrices can be used to create a risk register, ranked by impact (which requires a robust BIA to provide such information) and where the appropriate risk strategy (e.g., ignore, accept, avoid, mitigate, transfer) is made explicit, together with accountability for its implementation if the chosen strategy is one of mitigation. It is at this point that a link to the estimation of the ROI of mitigation measures appears.

A contrarian note: A bureaucratic approach to risk assessment is sometimes practiced, for example:
- Bringing in consultants to run short workshops for managers on how to build risk matrices
- Asking managers to carry out a threat/vulnerability analysis that identifies what can disrupt the operations for which they are responsible, ideally as a one-page document. An impact assessment is not included beyond categories such as low, medium and high. It is rare to find references to "catastrophic."
- Another person (sometimes titled risk manager) collecting all these one-page documents and filing them in a thick folder. Little or no effort is made to identify dependencies or quantify and rank impacts.
- Filing the thick book and telling the auditors that "a comprehensive risk assessment has been completed"
- Doing nothing until an event occurs and then finding someone to blame. If or when a security event happens, it is probable that blame will be attached to someone, but not necessarily to the person who initiated and supported the bureaucratic approach.

In the absence of supporting data to calculate and quantify the probability of such an attack on information assets, risk assessors can, at best, rely on their knowledge of the enterprise, particularly its culture and people. A qualitative assessment is more or less an informed guess. It is, however, a major step forward from doing nothing.

**IMPACT**

The analysis of security events on the business is an essential component of risk management, as senior managers can estimate outcomes in financial terms and provide sensible answers to questions such as:
- How much could a security incident cost the business and other components of its supply chain?
- What would be the impact of a security incident on the organization's business operations, reputation and compliance requirements?

A BIA is a prerequisite for the development and invocation of disaster recovery, business continuity and crisis management plans. The critical success factors for a BIA include being:
- Owned by the business unit and/or functional managers
- Quantitative
- Regularly updated
- Validated by executives
- Reviewed and approved by the audit committee

Some organizations collect data on incidents and use them to estimate the incident’s impact. For example, the cost of downtime has been the subject of numerous publications over the years in addition to the cost of stolen intellectual property. There are, however, other domains in which such costs are difficult, if not impossible, to estimate accurately. A number being agreed upon by a group of senior managers represents progress, and thus, the number does not need to be accurate.
RETURN ON SECURITY INVESTMENT

As security incidents do have business consequences, organizations recognize that appropriate actions must be taken to deter, prevent and/or mitigate their impact and this requires resources—people, processes and technologies. How much should an organization spend on information security to protect its information assets? This is a derivative of an older question: How much should the organization spend on information technology to carry out its business?

Despite numerous publications and frameworks (including ISACA's Business Model for Information Security [BMIS]), this question continues to be debated, mainly due to the intangible and speculative nature of most investments in this area as well as an inability to deal with uncertainties.

It would be hard to argue against carrying out an ROI calculation for an IT security project such as the installation of barriers and door controls in a building. Such a project would have a substantial cost (and duration), be very visible, and require organizational and procedural changes.

ROI is best used for the comparative evaluation of alternative solutions to a business issue. Such a calculation must be comparable in terms of the cost factors included and in the assessment of the benefits for alternative proposals likely to have different functionalities, costs and timescales. An ROI for a single option is of little value as it is easy enough to come up with justification for expenditures.

The final decision may include factors other than ROI, for example, the experience of similar installations in other organizations, the vendor's support capabilities and warranties.

Expenditures on information security add a philosophical dimension:
• When are these really investments or just the cost of doing business?
• Would it be right to classify the cost of fire insurance for the business's offices as an investment?
• Is the purchase of antivirus software an optional item?

Discussions with many security professionals reveal that they regard these as operational expenses. However, they are increasingly being asked to provide a return on security investment (ROSI) to support their budget requirements.

There are many publications on this topic. Some have generated controversies, for example, several articles by Bruce Schneier, a well-known, respected and published security expert in the UK, who stated, "(ROSI)’s a good idea in theory, but it's mostly bunk in practice." Leaving aside the issue of investment vs. the cost of doing business, the contrarian views reflect the experience of many years of preparing business cases for executives focused primarily on financial numbers, rather than on what was “sensible” and/or “good for the business.” Either trusting or naive, these executives failed to realize (even when told) that the numbers were completely fictional and quite possibly wrong.

First, the easier component to evaluate is cost. Those who have experience in IT (and other) projects are aware that cost and timescale estimates are always optimistic. Besides, other than the initial cost of the product or service, there are many cost components that may be easily forgotten when preparing a business case, an ROI or ROSI analysis, for example:
• The cost of preparation of a request for proposals and their subsequent evaluation (sometimes assisted by consultants)
• The internal costs of the procurement process, including legal reviews
• The delivery, installation and configuration of the procured items
• The training of those who need to operate, maintain and support the procured items
• The projected life of the item (to reflect rapid obsolescence and the short life expectancy of many vendors)
• A long list of recurring items such as license renewals, maintenance, installation and testing of updates

An experienced practitioner should be able to create a comprehensive list and put numbers to it with, optimistically, a margin of ±30 percent (rarely an underestimate).

Assessing the benefits (the actual return) relies entirely on creativity as these are in the future and are either guesses or truly unpredictable. Uncertainty ensures that there will be several unintended consequences. They also rely on the validity of many assumptions such as:
• The quality of the delivered and installed item and the vendor's descriptions of its functionality are complete and true and the product does not contain errors or faults
• The item has been appropriately configured; in practice more of an aspiration than a demonstrable fact
• The item is appropriate to mitigate one or more of the identified risk factors and the analysis of impact on the business provides quantitative financial assessments of the business’s exposure
• The benefits have an identified business owner who is accountable for their delivery
• The timescales exist for achieving such benefits
Executives should be aware that when requesting a ROSI to justify an investment, the numbers may not be accurate and are possibly erroneous.

CONCLUSION
This article presents a contrarian view of two disciplines that have acquired much visibility and caused information security practitioners to spend considerable time searching for answers to questions from executives who need to decide on expenditures intended to mitigate information risk. While the questions are legitimate and should be asked, some of the most popular risk management methods are no better than astrology (with apologies to those who read their horoscope).

Practitioners are, therefore, faced with a significant challenge: the inability to provide robust numbers to demonstrate that risk is correctly assessed and that the measures taken to strengthen security are appropriate and add value to the organization. Two actions that help meet this challenge follow:
• A sound assessment of vulnerabilities in technology, process and people is a prerequisite to effective risk assessment. Such vulnerabilities need to be related to their criticality to business processes and the impact these may cause when exploited by a specific threat.
• An up-to-date and validated analysis is a prerequisite for the development of incident response, disaster recovery, business continuity and crisis management plans. These should be regularly tested, for example, when there are changes in the environment, their results analyzed for lessons learned, and the plans modified accordingly. When this is not the case, the organization may not be able to survive a disruptive incident.

The article also discusses elements that, although not quantifiable, should be explicit in discussions with senior management:
• In the absence of supporting data to calculate and quantify the probability of a deliberate human attack on information assets, risk assessors can, at best, rely on their knowledge of the enterprise, particularly its culture and people. A qualitative assessment provides a more or less informed guess.
• Errors in design and manufacturing appear gradually and some remain undiscovered (to become zero-day deliverables when discovered). Typically, the vendor offers a solution that could, in turn, introduce new errors.

• The use of probability theories and other statistical techniques to quantify information security is, at present, not a viable approach due to the absence of sufficient data. Therefore, the use of likelihood is likely to continue. However, it should not be forgotten that this is little more than a guess.
• When it comes to evaluating ROSI, given that there is room for considerable creativity in conducting such analyses, an experienced practitioner could well ask: Does the enterprise have any particular number in mind?
• Forecasting is not an exact science.

ENDNOTES
1 With the release of COBIT 5 in 2012, key elements of Risk IT have been incorporated in COBIT. COBIT for Risk is expected to be released in September 2013.
3 Ensmenger, Nathan; The Computer Boys Take Over (History of Computing), The MIT Press, 2010
4 NATO Science Committee, Software Engineering Techniques, in a report of a conference, April 1970, p. 15
5 Cowart, Robert; Brian Knittel, Microsoft Windows 7 In Depth, Que Publishing, 2009
6 Twain, Mark; “Chapters From My Autobiography,” 1906, in which Twain attributes the phrase to Benjamin Disraeli (UK Prime Minister)
7 Bierce, Ambrose; The Devil’s Dictionary, 1906
8 This is the essence of the book The Black Swan by Nassim Taleb.