Ed Gelbstein, Ph.D., has worked in IT for more than 40 years and is the former director of the United Nations (UN) International Computing Centre, a service organization providing IT services around the globe to most of the organizations in the UN System. Since leaving the UN, Gelbstein has been an advisor on IT matters to the UN Board of Auditors and the French National Audit Office *(Cour des Comptes)* and is also a faculty member of Webster University, Geneva, Switzerland. He is a regular speaker at international conferences covering audit, risk, governance and information security and is the author of several publications. Gelbstein lives in France and may be contacted at *ed.gelbstein@gmail.com.*

Strengthening Information Security Governance

The IT Governance Institute (ITGI) and ISACA were among the first to issue guidelines for the governance of information security, and their various publications[1, 2] have been complemented by other governance frameworks, including the yet-to-be issued international standard ISO 27014[3] and the latest revision of the Information Security Forum (ISF) *Standard of Good Practice*.[4] Other frameworks have been proposed by industry advisory services such as Gartner Group.[5]

All of these are welcome support for a domain that has become increasingly visible and sensitive. In the last couple of years, it has become evident that no organization can avoid being influenced by the tsunami of innovative technology, with ever shorter life cycles.

When Bill Gates and Paul Allen, the founders of Microsoft, dreamt of having a computer on every desk and in every home, they were right, but it took some 30 years to get there. When Apple introduced the iPad tablet, the demand had no precedent in the IT industry, as it became, almost overnight, a must-have gadget. IT departments and security managers were caught unprepared and resorted to a "you cannot have one—it is policy" statement that did not win them many friends in the executive suite. Besides, no organization is invulnerable to attacks on its information.

Suspected culprits include a wide range of actors, ranging from the individual hacker to organized groups (such as Anonymous), and other unidentified but highly competent groups suspected of having a measure of state support, assorted spies (industrial and other), organized crime, and insiders.

Significant security breaches recently included Wikileaks, fraud at UBS London and the insertion of the Stuxnet malware in the uranium enrichment facilities in Iran. These, of course, are only the tip of the proverbial iceberg. Cyberattacks of one form or another are a daily occurrence, and many are simply not reported in the media, as their severity is not sufficient to make headlines.

However, as installers of burglar alarms know very well, unless their insurance company insists they do so, most people will have an alarm installed after being burgled. Does information security governance fall in the same category?

STATE OF ISG: NOT A PRIORITY, POLITELY IGNORED AND LIMITED RESOURCES

The purpose of information security governance (ISG) is stated clearly enough in various frameworks and can be summarized as evaluating, directing and monitoring information security to:

- Ensure business needs are met
- Strengthen information assurance
- Ensure information risks have identified owners
- Reduce the risk of noncompliance
- Reduce the risk of litigation
- Achieve sustainable confidentiality, integrity and availability (CIA)

Information technologies, including security components, have many common elements shared among organizations almost regardless of the nature of their activity. This is true for servers, storage and networks, applications such as enterprise resource planning (ERP) and customer relationship management (CRM), and services such as e-mail and remote access.

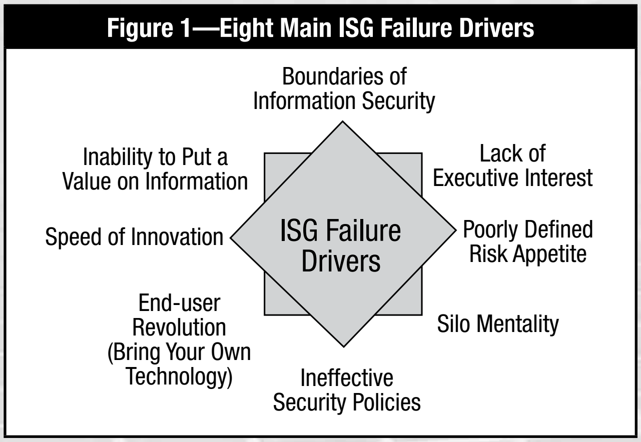
However, organizational culture and the degree to which information risk is accepted mean that their individual security needs vary greatly. At one extreme are the critical information infrastructures on which society depends (e.g., utilities, emergency services, national security) and at the other extreme there are those among which, if they had a significant incident, the impact would not propagate beyond their walls—i.e., nobody would notice and, at worst, their reputation may be dented for a short time.

This article reflects the findings of audits performed in the last few years in the not-for-profit sector and discussions with peers during information security conferences in Europe, the Middle East and Africa as well as other professional gatherings. While the sample may not be statistically significant, the outcome suggests that in trying to rank the perceived importance of ISG, the board members and executives do not include it in their "top 10" areas of concern.

The findings, gathered by the author over the last 10 years, are presented in the form of failure drivers—those factors that result in weak or no governance of information security, leaving practitioners to do whatever they think is best with limited resources and no forum to make their case.

The eight main failure drivers are summarized in **figure 1**.

Figure 1—Eight Main ISG Failure Drivers


Boundaries of Information Security
Lack of Executive Interest
Poorly Defined Risk Appetite
Silo Mentality
Ineffective Security Policies
End-user Revolution (Bring Your Own Technology)
Speed of Innovation
Inability to Put a Value on Information
ISG Failure Drivers

ISG FAILURE DRIVER 1: BOUNDARIES OF INFORMATION SECURITY

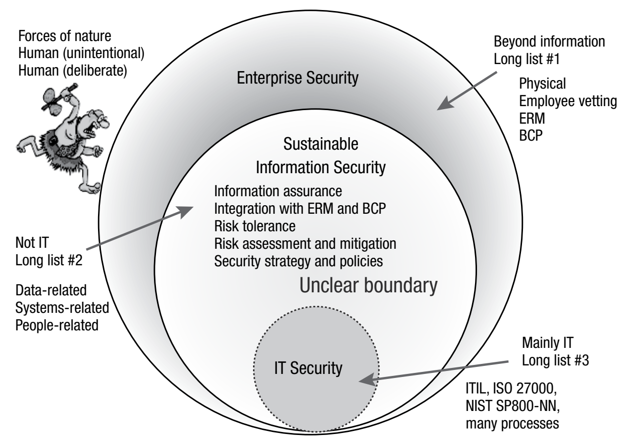
Too often, executives and senior managers believe that information security is the responsibility of the IT department and, if reliant on a service provider, then it is the outsourcer's responsibility to manage security on the organization's behalf.

This is only partly true, as illustrated in **figure 2**. Defining who can have access to a system and with what privileges for functions and data should be the responsibility of functional managers.

The same is true for the life cycle of identity and access management, arranging security briefings, and training of staff, etc. More important, it is up to business managers to engage in information risk assessment and management, business impact analyses, and business continuity plans that reflect the role of individual systems and electronic facilities.

Similarly, while the IT department can provide security-related policy outlines, these must be reviewed and approved by other parties, which may include human resources (HR), legal counsel, and, depending on the organization, staff representatives and other parties. Moreover, unless such policies are enforceable, they are wasted effort.

Figure 2—Information Security in Context



ISG FAILURE DRIVER 2: LACK OF EXECUTIVE AND SENIOR MANAGEMENT INTEREST

Working with, meeting and talking with many chief executive officers (CEOs), ministers, diplomats and senior managers in the public and private sectors have made one thing crystal clear: their time is at a premium, and this forces them to focus on matters of here-and-now importance. IT and information security generally do not come into this category unless things have gone spectacularly wrong, and then their reaction is "fix it."

In the somewhat unlikely event that they decide to attend an IT or an ISG discussion, they are likely to find it, and they openly admit it, to be a waste of their valuable time because the focus is not on the business, but on technology issues. If there is another meeting, they will likely delegate someone else who will not have delegated authorities.

Trying to get them to think in terms of "what if" is usually a lost cause. While they acknowledge that information systems are of considerable importance to their organization's activities, they will freely admit that they do not lose sleep over potential security breaches—at least not until a breach occurs.

When (not if) a breach occurs and has significant impact—as was the case when in 2007 Société Générale (in France) lost more than US $7 billion and in 2011 when UBS (in London) lost more than US $2 billion, both through unauthorized trades—the matter rapidly escalates into crisis management.

Once the short-term issue has been resolved, executive interest evaporates and the belief that "IT is dealing with security" is reestablished.

This situation has been familiar to IT security managers for many years; they yearn to be "at the top table," but are usually not invited. This may be partly because they communicate using jargon, rather than the language of the business, and also because they are perceived as an obstacle to innovative ideas and business initiatives. Many an information (technology) security manager is known in the organization as "Dr. No."

Executives who want the latest shining gadget (in 2011 these were tablets) and are told by IT that they cannot have one "because of security issues" are not likely to be supportive, and are likely to lose interest even further.

ISG FAILURE DRIVER 3: POORLY DEFINED RISK APPETITE

ISACA's Risk IT framework states that IT risk encompasses more than the negative impact of operations and service delivery and includes the value-enabling risk associated with missing opportunities to use technology to enable or enhance business.[6] The framework's chapter 5, Essentials of Risk Governance, makes it clear that the terms "risk appetite" and "risk tolerance" are frequently used, but the potential for misunderstandings is high, as these terms should not be used interchangeably.

From the point of view of ISG, the Risk IT framework (**figure 3**) illustrates the benefits of adopting it to boards and executive management as better understanding of their responsibilities and roles with regard to IT risk management, the implications of risk in IT to strategy objectives, and how to better use IT to reduce risk in strategic moves.

A risk appetite that defines how much risk an organization is willing to accept before taking mitigating actions implies that resources need to be made available to implement such actions. A broad statement of risk appetite but no resources to address the necessary actions is of little help to the risk owner.

The governance challenge is finding a balance between the never-ending pursuit of cost reductions and the need for resources to mitigate risk in an environment in which uncertainty rules. Here, history and statistics are of little help. Cost reductions, by default, tend to increase the organization's risk appetite.

When the impact of an incident is greater than the risk appetite, blame is likely to be assigned to someone other than the person who authorized the cost reductions.

Figure 3—Audiences and Benefits

Role	Benefits of/Reasons for Adopting and Adapting the Risk IT Framework
Boards and executive management	Better understanding of their responsibilities and roles with regard to IT risk management, the implications of risk in IT to strategy objectives, and how to better use IT to reduce risk in strategic moves
Corporate risk managers (for ERM)	Assistance with managing IT risk, in line with generally accepted ERM principles
Operational risk managers	Linkage of their framework to Risk IT; identification of operational losses or development of key risk indicators (KRIs)
IT management	Better understanding of how to identify and manage IT risk and how to communicate IT risk to business decision makers
IT service managers	Enhancement of their view of operational IT-related risks, which should fit into an overall IT risk management framework
Business continuity managers	Alignment with ERM (since assessment of risk is a key aspect of their responsibility)
IT security managers	Positioning of security risk among other categories of IT risk
CFOs	Gaining a better view of IT-related risk and its financial implications for investment and portfolio management purposes
Enterprise governance officers	Assistance with their review and monitoring of governance responsibilities and other IT governance roles
Business managers	Understanding and management of IT risk—one of many business risks, all of which should be aligned
IT auditors	Better analysis of risk in support of audit plans and reports
Regulators	Support of their assessment of regulated enterprises' IT risk management approach
External auditors	Additional guidance on IT-related risk levels when establishing an opinion over the quality of internal control
Insurers	Support in establishing adequate IT insurance coverage and seeking agreement on risk levels
Rating agencies	In collaboration with insurers, a reference to objectively assess and rate how an enterprise is dealing with IT risk

Source: ISACA, *The Risk IT Framework*, USA, 2009

ISG FAILURE DRIVER 4: SILO MENTALITY

Maintaining information security in the broadest sense requires the commitment of many parties outside the IT function/service providers and the chief information security officer (CISO). The main players include:

- **System and data owners**—Key players by being accountable for (at a minimum) data classification, defining access rights on a need-to-know and least-privilege basis, ensuring appropriate segregation of duties, and providing input to business impact analysis
- **Applications development**—Accountable for providing assurances that applications do not contain embedded logical bombs, back doors or other facilities that can provide access to production data
- **HR**—Accountable for guiding the development and implementation of security policies that have a direct impact on staff and for the development of awareness and training programs that support and strengthen the information security culture and practices of the organization
- **The procurement function**—Accountable for ensuring that contracts with vendors and service providers include appropriate protection against vulnerabilities and security breaches
- **Legal counsel**—Accountable for guiding the organization through all legal and regulatory compliance needs, the rights of staff and other users, requirements for the seizure and chain of custody in the event of an investigation, and validating draft security policies
- **Internal Audit**—Accountable for providing independent and objective assurance to management
- **Others**—E.g., trade unions/staff associations, the budget office, depending on the nature of the organization

Every one of these functions is likely to be busy with its core activity, and information security governance may potentially be seen as a distraction. In extreme cases, someone may say "it is not in my job description" (i.e., silo mentality). The inescapable office politics are another factor that can weaken ISG further.

ISG FAILURE DRIVER 5: INEFFECTIVE SECURITY POLICIES

Information security policies are, all things considered, a set of do and do-not rules. In line with law in most countries, the directors of an organization are responsible for establishing policies to protect its assets on behalf of the stakeholders. In a perfect world, the development of a policy would make senior management aware of and involved in information security, and make it an appropriate priority.

Such policies should be published documents that define an organization's philosophy, strategy, policies and practices with regard to confidentiality, integrity and availability of information and information systems. When well designed, they perform several functions:

- They define acceptable and responsible use of information systems and data.
- They define the delegated authorities to those managing information security.
- They provide a guide to the practice of information security by all concerned.
- They provide consistency and an electronic or paper trail to demonstrate due diligence.
- They are a prerequisite for compliance with international standards such as ISO 27001.

Having a set of security policy documents can be as easy or as hard as desired: Policy templates can be downloaded free of charge from several sources, purchased for a modest sum or crafted with great care given to every sentence and clause (the latter could take forever, as the temptation to indulge in the mindless pursuit of perfection is hard to avoid).

Regardless of the route through which the policies are developed, having the documents is not enough. To be effective, the policies must be understandable to everyone who needs to comply and must be effectively deployed (to avoid the "never got it" response). Most important, they should be enforceable.[7] None of these is easy to achieve. To make matters worse, in many organizations, it is not clear who owns the processes of policy creation, dissemination and monitoring for compliance.

In addition, recent audit experience has shown that many organizations are behind the times by not having policies that address the end-user revolution (see failure driver 6).

ISG FAILURE DRIVER 6: THE END-USER REVOLUTION

Corporate life was easier when organizations selected, installed and provided equipment and software to their workforces. In that scenario, there was a reasonable degree of control over what software was installed and what systems and services were accessed, and, generally, it was possible to monitor who was doing what in the digital environment.

The emergence of affordable computers for a home office and smaller and lighter portable devices created complications. The wide availability and steadily decreasing prices of devices marketed directly to individuals—notebooks, tablets, smartphones, pocket-sized high-capacity storage devices—has led to their enthusiastic adoption and, with it, pressure on organizations to let people bring their own technology (BYOT).

All of these have resulted in corporate security architectures being out of control and end users demanding access to corporate systems and data using their own devices, which may not be adequately protected and, thus, raising many questions, among them:

- Do the smartphone/tablet apps contain malware?
- Are the devices encrypted and, if so, who manages the keys?
- Is corporate information being stored somewhere that the organization is not aware of?
- Have devices been lost?

In addition to BYOT, Web 2.0 technologies introduced new challenges: They diffuse the boundary between professional and personal activities. First, the question of what the appropriate use of social networks, blogs and forums is when freedom of expression is the norm. Second is the matter of the cloud.

A recent audit, conducted by the author, identified that corporate data, including sensitive documents, were being uploaded to the cloud (in this specific case Google Docs and Gmail) because users were finding the remote access procedures of the organization cumbersome, and found a workaround. Word spread quickly on how easy and convenient it was, and contagion followed.

> "No organization is invulnerable."

Once such practices become established, they are difficult to eradicate.

ISG FAILURE DRIVER 7: THE SPEED OF INNOVATION

The rate of innovation (i.e., technology, services, facilities) and the passion with which digital natives (Generation Y) adopt them to become an integral part of their lifestyle can be thought of as the hare in Aesop's fable,[8] while the way organizations go about establishing policies and guidelines about their use is the tortoise.

Unfortunately, information security is a three-player race. The third player is any one of many actors that, out of curiosity, ego, emotion, malice, financial gain or political motivation, is intent on breaking an organization's protective measures. Such actors include, at a minimum and in an increasing order of threat:

- Young enthusiastic hackers and script kiddies, mostly a nuisance
- Rogue IT professionals with knowledge and experience, operating as cybermercenaries
- Activists and hacktivists with a cause, e.g., the Anonymous collective (who even have a Facebook page)
- Motivated insiders with knowledge and experience
- Industrial and other spies, targeting intellectual property and other confidential data
- Malicious software (malware) designers not associated with organized crime
- Malicious software (crimeware) designers working with organized crime
- Weapons-grade malicious software designers (sponsored by a state, the military or nonstate actors)

As stated at the beginning of this article, no organization is invulnerable. An optimist with experience would say that "nothing is ever so bad that it could not possibly get worse."

ISG FAILURE DRIVER 8: INABILITY TO PUT A VALUE ON INFORMATION

Critical information infrastructures are, in principle, better equipped to measure the impact of insecurity. Many collect data and use metrics, such as the cost of downtime of specific activities (a bank, for example, would have data for its trading desk). This cost would normally include the direct cost to the organization as well as that of legal liabilities to clients and reputational damage.

Loss of data integrity is harder to measure, except when fraud through unauthorized modification of data is detected. The losses of Barings Bank (1999),[9] Société Générale (2007)[10] and UBS (2011)[11] are amongst the best-known frauds committed by the unauthorized modification of data by an insider.

The cost of information disclosures (leakage) varies dramatically between industries. For example, in 2009, DuPont alleged in court that a Korean company, Kolon Industries, had stolen trade secrets on DuPont's Kevlar product. In September 2011, a District of Virginia court awarded DuPont damages worth nearly US $920 million.[12]

DuPont had a less-satisfactory experience in 2007, when an employee downloaded tens of thousands of documents from DuPont's electronic data library. A raid of the employee's home uncovered more confidential documents on other computers and bags of shredded technical documents. The employee was sentenced to 18 months in prison and ordered to pay close to US $50,000 in restitution. The company assessed the value of the stolen information at US $400 million.[13]

At the other extreme, there are (in the author's opinion) many organizations that have not thought about how valuable their information might be. Auditors are told:

- "We favor transparency and disclosure and have nothing to hide," after which a few questions often elicit a "didn't think of that" answer.
- "Fraud is not an issue here; our staff is dedicated and we trust them implicitly," as if the fraud had not occurred.

CONCLUSIONS

When information security governance is weak or absent, information security is guided by the best efforts of a few individuals and limited in nature. In this scenario, the organization is poorly prepared to protect itself from any kind of cyberattack.

The main symptoms of poor preparedness include:

1. Functional management, executives and board members who are not knowledgeable or interested
2. Unclear systems and data ownership, and lack of accountability for security management
3. A belief that information security is purely an IT issue
4. An information security policy portfolio that is incomplete, incomprehensible, not tracked and not updated
5. Incomplete or nonexistent information risk assessment, no risk register, and no mitigation plans
6. Inadequate resources devoted to information security (e.g., people, tools, funding)
7. A lack of proper guidance for staff on responsible digital behavior
8. Anarchic deployment and use of end-user-owned devices
9. Information security policies and practices seen as an obstacle
10. No security metrics in business terms

The following method can be used to score an organization's preparedness: Give the organization one point for each of the symptoms noted that applies to it. A score of:

- 8 to 10 means the organization has a serious information security problem. Do the executives know?
- 5 to 7 means that the organization needs to do better if it requires good CIA. To which symptom should priority be given?
- 1 to 4 means the organization has a good state of affairs. Is anyone working to reduce the score?
- 0 means congratulations are in order; the organization is well prepared. Do the auditors agree with the assessment?

ENDNOTES

[1] IT Governance Institute (ITGI), *Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition*, USA, 2006

[2] ITGI, *Information Security Governance: Guidance for Information Security Managers*, USA, 2008

[3] International Organization for Standardization (ISO), ISO 27014 *Information Technology—Security Techniques—Governance of Information Security*, publication planned for release in 2012

[4] The Information Security Forum (ISF), *Standard of Good Practice*, 2011

[5] Gartner Group Research, *The Gartner Information Security Governance Model*, 2010

[6] ISACA, *The Risk IT Framework*, USA, 2009

[7] Creech, Jason; Matthew Alderman; "IT Policy Compliance for Dummies," J. Wiley and Sons, 2010, *www.qualys.com*

[8] Aesop; "The Hare and the Tortoise," Aesop's fables, available from several publishers

[9] *BBC News* staff reporters, "How Leeson broke the Bank," *BBC News*, 22 June 1999, *http://news.bbc.co.uk/2/hi/business/375259.stm*

[10] Fraser, Christian; "Societe Generale Trader Kerviel Jailed for Three Years," *BBC News*, 5 October 2010, *www.bbc.co.uk/news/business-11474077*

[11] *Financial News* staff reporters, "Meet Kweku Adoboli," *Financial News*, 15 September 2011, *www.efinancialnews.com/story/2011-09-15/kweku-adoboli*

[12] *Business Week*, "Kolon Loses 920-million Verdict to Dupont in Trial Over Kevlar," Bloomberg, 15 September 2011, *www.businessweek.com/news/2011-09-15/kolon-loses-920-million-verdict-to-dupont-in-trial-over-kevlar.html*

[13] The Kaspersky Labs Security news service, "Infamous Insiders: Eye-popping Heists by Insiders," 2011, *http://threatpost.com*