Jeimy J. Cano M., Ph.D, CFE, is a research member of the Information Technology, Telecommunications, Electronic Commerce Studies Group (GECTI) of the Law School and a distinguished professor at Universidad de los Andes, Colombia. Cano can be reached at *jjcano@yahoo.com*.

The Information Security Function

Current and Emerging Pressures From Information Insecurity

International trends reflect a paradigmatic change in current business models caused by the markets' asymmetry and dynamics where instability is the constant and change is the norm. In this sense, new strategic business statements that change an organization's way of thinking and cause breakdowns in the supposed fundamentals of their operation are being seen (**figure 1**).[1, 2]

Figure 1—Changes to Business Models

Current Statements	New Statements
Development and completion of sustainable competitive strategies	Development, completion and withdrawal of transient competitive strategies
Product design based on needs	People-centered design
Development of an IT culture at the organizational level	Development of a digital business culture
Development of strategies for target groups	Development of a possibility and content ecosystem
Reach a privileged position in their business sector as compared to others	Take the greatest amount of territory surpassing others

Adapted from: Gunther McGrath, R.; *The End of Competitive Advantage: How to Keep Your Strategy Moving as Fast as Your Business*, Harvard Business Review Press, 2013. Leinwand, P.; C. Mainardi; "What Drives a Company's Success? Highlights of Survey Findings," Booz & Company, 2013, *www.strategyand.pwc.com/global/home/what-we-think/reports-white-papers/article-display/what-drives-a-companys-success*

Reviewing the current and new statements, it is apparent that the current statements are associated with consolidating formally designed strategies that may not evolve with time and within their environment and are still in place, even when their context reflects significant and unexpected changes that are outside their capability of anticipation.

The new statements are sensitive to fluctuations in the environment and follow a trend based on peoples' expectations and motivations. This entails an information management capability for developing and capturing new and seasonal sources of value, which are used to take control of emerging territories and to surpass competitors—not necessarily in their field of specialty, but where there are possibilities that make the difference.[3]

This business reality represents a challenge in creativity, velocity, flexibility and significant collaboration for companies. Specialized professional teams no longer hold the answers for making predictions on emerging trends, but instead have the corporate capability to create community schemes, with clients and other people, to build and develop capabilities that change the client experience, driven by the significance and value of the contents and new possibilities.

This being the case, companies that wish to remain in the turbulent waters of unexpected changes and emerging challenges must have a different way of providing value when faced with customers' expectations, developing exclusive operating capabilities (things they know how to do very well that their clients recognize and others cannot imitate), and maintaining the exercise of coherence and harmony between both in order to compete using different approximations in several categories and markets.[4]

If this is correct, the key information concept for the company is in opposition with the current information protection doctrine in which management of the asset is understood as a resident in known sites, processed in identified computers, and accessed by authorized and trustworthy personnel.

This new business reality entails a greater level of information exposure, collaboration, submission, exchange and flow, which requires rethinking the current control and security schemes based on rules and procedures adjusted

Disponible también en español
www.isaca.org/currentissue

to a calm and predictable environment. This should be done by those who recognize the information management dynamic—the clients' needs and expectations generally associated with mobility, access and capability to share.

CHANGE OF FOCUS: FROM RESTRICTION TO FACILITATION

In this new business context and with the avalanche of new technology possibilities, information security must evolve to adjust to the challenges it faces from business dynamics and the need to create new competitive advantages, leaving the known comfort zone of traditional controls and renewing the understanding of information protection in an open, mobile and eminent social reality with third parties.

In this sense, the transformation being seen in the management and administration of information security entails understanding its current model and moving toward evolution according to the challenges imposed by society (**figure 2**).[5]

Figure 2—Current and Evolutionary Information Security Model

Current Information Security Model	Evolutionary Information Security Model
Based on risk mitigation (risk reduction)	Based on risk management (acceptance risk threshold)
Aimed at critical information assets	Aimed at reliable functioning of critical processes
Founded on assurance of the defined technology perimeter	Founded on the change of behavior of people toward information
Based on control and security guides and procedures	Based on use agreements and rules founded on the impacts
Supported by sanctions and preventive actions	Supported by prediction and active monitoring actions

Source: Jeimy J. Cano. Reprinted with permission.

The risk mitigation focus is a strategy that, even though it responds to a corporate demand that unconsciously thinks the risk will disappear, is susceptible to a permanent loss of trust when the warned threat materializes for reasons that often cannot be explained.

At this time, senior management is likely to ask: "Did you not establish a set of activities to mitigate the risk?" Generally, the response to this question is, "We did not take these other scenarios into account."

Mobilizing efforts toward risk management is to accept a threshold of known risk that is openly declared and accepted by the first level of the company. That is, the boundaries of risk in critical business processes, strategies applied to keep risk within the defined threshold, and applicable activities and monitoring of risk exposure level are known.

Accepting the risk threshold also involves understanding that it could materialize. Therefore, the actions in place to prevent risk are what will make the difference between constant understanding and active monitoring.

Currently, information security management insists on a preventive and sanctioned focus to motivate a change in behavior toward information handling. Though this approach has been highly successful in the past (with static, known and stored data), organizations are faced with a new reality with regard to high mobility, bold proposals (generally to share information) and third-party participation.

Information access is no longer the main reason for relations among people and organizations. Rather, it is the use of information that defines a new concept and statement for information security managers: "They must see themselves first as business leaders and then as managers with a specialty in security and risk management."[6]

As a result, information security managers who want to be successful in the current conditions of uncertainty, market asymmetry and mobility must:[7]

- Make business, not security, decisions
- Work with and through others to reach their objectives
- Be a bridge between areas and not a barrier for the business
- Be familiar with their industry and its challenges
- Change their language and communicate in business terms

RISK SCENARIO: FROM KNOWN CONTEXTS TO NEIGHBORHOODS AND EMERGING ACTORS

According to Gartner, there will be several possibilities and scenarios that organizations may have to deal with in 2020.[8] It will not be a calm time and new proposals and new roads will have to be explored to discover the information insecurity mutations in a world dominated by mobility, operations with third parties, social networks and IT tensions among nations.

Gartner mentions four scenarios to be analyzed:[9]

1. Regulated risk
2. Coalition rule
3. Neighborhood watch
4. Controlling parent

The regulated risk scenario warns of the increase in government regulations regarding information protection. Matters such as privacy, critical infrastructures, behaviors of people in social networks and the use of mobile devices will have standards that adjust the behaviors of individuals regarding proper information handling. Likewise, attacks on technology infrastructures may be considered acts of war, creating tensions that may result in international conflicts resolved by known and unknown information weapons.

The coalition rule suggests that attackers will remain focused on organizations, looking for new ways to attack or deceive, using advanced evasion techniques (AET)[10] or the known persistent and advanced threats generally focused on people. The attacks will be organized by groups, hacktivists or mercenaries who will seek to disrupt the companies' stability, cause damage to the businesses' operations and compromise their value creation model.

Neighborhood watch essentially suggests a time of anarchy dominated by people and their interactions, considering a context with little governmental intervention and regulation. Electronic militias will be formed to confront the actions of hacktivist groups causing self-organization of companies to create a society with information protection practices that operate in a coordinated manner. Trust will be a value that will be compromised, in general, by organizations and people.

The controlling parent will be represented by government entities that will seek to protect individuals, creating distractions and limiting opportunities to do business. It will be a time where the increase of attacks on individuals (based on darknets and botnets) will motivate the actions of governments to control this phenomenon, strengthening their position on the respect and dignity of people regarding their information. Active data monitoring and analysis will be the norm to maintain a close view of those carrying out social activities.

In light of these analyses, companies and people must take note and act as a result. To this extent, the information security business manager must shape emerging actors, prepare technology infrastructures, prepare plans that increase resistance to attacks on people and recognize new information flows to anticipate emerging threats and be prepared to learn new lessons on information insecurity.

COMMON ARCHETYPES FOR INFORMATION SECURITY RESPONSIBILITIES AND FUNCTIONS

Considering the changes to business models and the challenging scenarios, it is increasingly difficult to meet the

Figure 3—Archetypes of the Information Security Function

Emphasis	Operations	Government	Operations and Government	Operations, Government and Legal Aspects
Responsibilities	• Information security • Event analysis and monitoring • Response to incidents and forensic analysis • Threat and vulnerability management	• Established risk appetite level • Information security risk management • IT compliance • IT risk • Information protection • Information classification	Additional to those under operations and governance: • Security risk management with third parties • Access and identity management • Security architecture design	• Notification of privacy breaches • Information protection • Electronic discovery (electronic support for disputes) • Event analysis and monitoring • Response to incidents and forensic analysis • Information classification • Threat and vulnerability management

Source: Adapted and translated from CEB CIO Leadership Council, *Common Archetypes of Security Functions: Implementation Tool, www.irec.executiveboard.com*

challenge of anticipating emerging risk factors that affect the reliability of operations and to protect a company's value creation model. Therefore, it is essential to remain alert and attentive to the changes made to the organization's dynamic.

The analysts of the CEB CIO Leadership Council have designed a base study of four archetypes of patterns related to exercising the information security function (operations; government; operations and government; operations, government and legal aspects), which can orient organizations on where the current practice is (**figure 3**).[11]

Upon review of the archetype aimed at operations, it is clear that the emphasis is on technology controls, information security technologies, technologies' implementation and guarantee as a way to respond to information security management's expectations. This scenario is dominated by a specialized technical language with a high concentration of profiles for configuration and guarantee of security technology management, incident management, correlation of events and forensic analysis, which generally require a high level of technical training and continuous updates as a result of changes to them.

In the archetype based on the government, the dominant language is of information risk, protection of the company's value creation model, the search for strategies to protect the company's value, a guarantee of regulatory compliance in the context of corporate governance and an understanding of the known risk threshold declared by the company. This scenario requires profiles that understand the business's needs, information flow and strategic objectives to provide strategies that are light, simple and effective to reach reliable functioning of the organization.

The combination of operations and government brings together two worlds with sometimes incompatible responsibilities. In operations, there is control of information security devices with control and operation standards defined by information security governance. This results in a collision between who plans and verifies and who acts and operates. This mix distracts the corporate security area, since it will be more concentrated on a clean and clear operation of the technology infrastructure (even more so if in the hands of third parties) and less attentive to the environment's instabilities, which may affect the business's operation and, therefore, destroy the company's value.

The archetype, which combines the previous view and adds the legal aspects, further reveals the need for the information security area to be attentive to legislative and regulatory changes in order to adjust its practice to the regulated environment in which the organization operates. It does not only include the previously presented limitations, but the challenge of incorporating the comprehension of a right, such as privacy, that clearly exceeds the understanding of the information security area, challenging it to combine the known information protection practice with a corporate objective, with government requirements and its sanction model for not meeting the customers' expectations regarding protection of their personal data.

This being the case, whatever the archetype is that prevails in an organization or the way the information security function is organized, the following elements must be taken into account:[12]

- Mutation of the threat environment
- Explosion of information and portable devices
- Electronic support to legal disputes
- Financial regulations and regulations of each industry
- Privacy protection in digital environments

CONCLUSION

Even though organizational pressure on the IT function to support the business's efficiency and effectiveness[13] will continually improve, the interest of senior management in the protection of key information will not decrease given the open environment inclined to sharing where it operates.

> One must unlearn the known and live with the discomfort of asking better questions.

It is necessary to understand not only the sector to which the company belongs, but also the ecosystem in which it operates in order to make progress in understanding the technological convergence of social media, mobile computing, cloud computing and information[14] and, thus, propose a light, simple and effective information security model that responds to the agility demanded by the business to conquer new territories and create new trends.

The scenario of information risk is the most challenging when exercising protection against the environment's threats. It demands the participation of the organization's areas

and their personnel, each time the new control and security perimeter is found in one of the individuals. This implies designing for and ensuring that the new "human firewalls" are trained to be resistant to attacks and reconfigure them based on the changing environment, increasing their sensibility to detect new attack vectors that affect the business's objectives.

Therefore, techniques aimed at monitoring and active response[15] are required to maintain an information security posture that pushes boundaries, learns from errors and studies new threat patterns to develop creative thinking, which generates new distinctions in the current control and security practices in the organization. That is, one must unlearn the known and live with the discomfort of asking better questions.

So, the information security function will have information insecurity as a teacher, the instabilities of markets as its operations laboratory and the textbook as a guide for the expectations of the organization's managers, in order to motivate an accelerated education process, to transform.

ENDNOTES

[1] Gunther McGrath, R.; The End of Competitive Advantage: How to Keep Your Strategy Moving as Fast as Your Business, Harvard Business Review Press, 2013

[2] Leinwand, P.; C. Mainardi; "What Drives a Company's Success? Highlights of Survey Findings," Booz & Company, 2013, www.strategyand.pwc.com/global/home/what-we-think/reports-white-papers/article-display/what-drives-a-companys-success

[3] Vollmer, C.; M. Egol; N. Sayani; R. Park; "Reimagine Your Enterprise: Make Human-centered Design the Heart of Your Digital Agenda," Booz & Company, 2014, www.strategyand.pwc.com/global/home/what-we-think/reports-white-papers/article-display/reimagine-your-enterprise

[4] Op cit, Gunther

[5] Security for Business Innovation Council, "Transforming Information Security: Future-proofing Process," 2013, www.emc.com/collateral/white-papers/h12622-rsa-future-proofing-processes.pdf

[6] Grimsley, H.; The Successful Security Leader: Strategies for Success, CreateSpace Independent Publishing Platform, 2012

[7] Ibid.

[8] Proctor, P.; R. Hunter; F. C. Bymes; A. Walls; C. Casper; E. Maiwald; T. Henry; Security and Risk Management Scenario Planning, 2020, Gartner Research, 2013

[9] Ibid.

[10] McAfee, "The Security Industry's Dirty Little Secret," Research Report, 2013, www.mcafee.com/us/resources/reports/rp-security-industry-dirty-little-secret.pdf

[11] CEB CIO Leadership Council, Common Archetypes of Security Functions: Implementation Tool, www.irec.executiveboard.com

[12] Harkins, M.; Managing Risk and Information Security: Protect to Enable, Apress, 2013

[13] Khan, N.; J. Sikes; "IT Under Pressure: McKinsey Global Survey Results," McKinsey & Company, 2014, www.mckinsey.com/Insights/Business_Technology/IT_under_pressure_McKinsey_Global_Survey_results?cid=other-eml-alt-mip-mck-oth-1403

[14] Howard, C.; D. C. Plummer; Y. Genovese; J. Mann; D. A. Willis; D. Mitchell Smith; "The Nexus of Forces: Social, Mobile, Cloud and Information," Gartner Report, 2012 https://www.gartner.com/doc/2049315

[15] MacDonald, N.; "Prevention Is Futile in 2020: Protect Information Via Pervasive Monitoring and Collective Intelligence," Gartner Research, 2013, https://www.gartner.com/docs/2500416/prevention-futile-protect-information-pervasive