



The Risk Watch

Towards Effective Risk Management in Africa Re

APRIL - JUNE 2011

EDITION X

Inside This Issue

Page 1
From the Editor
/ Mot du
Rédacteur-en-chef

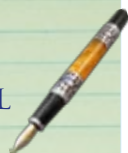
Page 2
Business Continuity
Management (BCM): The
Importance for Africa Re
/ La Gestion Du Plan De
Continuité: Quel Intérêt
Pour Africa Re

Page 6
Interview of Mr. Alain
Ravoaja The Outgoing
Director of Central
Operations Africa Re /
Interview de M. Alain
Ravoaja, Ancien Directeur
Des Opérations Centrales
d'Africa Re

Page 10
The Future of Security:
Evolve or Die
/ L'avenir de la sécurité:
Evoluer ou mourir

EDITORIAL TEAM:

• S. M. Kaba • I. O. Uduma
• A. Adewusi • M. Bakayoko



From The Editor

Dear Colleagues,

The Corporation recorded an excellent performance for the financial year ended 31 December 2010. The underlying underwriting result is driven essentially by consistent leadership inspired by the Executive Management and the cautious underwriting approach adopted by our technical team which focused more on achieving reasonable profit rather than mere premium growth. Consequently, remedial measures were put in place to address identified underwriting challenges in some key production locations which have now become profit making.

We should continue implementing this cautious underwriting by ensuring that our underwriting staff have the necessary commitment with regard to risk management through compliance with the Corporation's underwriting guidelines and other best practices.

The uncertainty experienced in various regions covered by the Corporation represents a new challenge, which requires strategies to raise organizational flexibility in order to meet international trends and standards. The Corporation's Business Continuity Management (BCM) aims to overcome the operational difficulties resulting from any major adverse incident.

The 10th edition of your newsletter presents two articles: "Business Continuity Management (BCM): The importance for Africa Re" and "The Future of Security: Evolve or Die".

The Chief Risk Officer, who is the author of the first article, provides the factors and steps necessary to prepare for a disaster so that the organization can take all the appropriate actions to ensure continued viability. He also provides a step by step guide to business continuity plans and presents the current BCM Project of the Corporation to the readers.

In the second article "The Future of Security: Evolve or Die", the Senior Internal Auditor sheds light on the rapid IT development and its related security concerns. As personality of the edition, the underwriting guru and former Director of Central Operations & Inspection, Mr. Alain Ravoaja shares his rich experience with us by responding to our questions in this newsletter. We wish him a happy retirement!

Have a rewarding reading and feel free to make comments on the newsletter and the articles.

Editor-in-Chief and Chief Risk Officer

Sere Mady Kaba



Mot du Rédacteur-en-chef

Chers collègues,

La Société a enregistré d'excellents résultats en 2010. Ces résultats, nous les devons en grande partie aux choix cohérents de la Direction générale et à la prudence dont notre équipe technique a fait preuve en matière de souscription, privilégiant la rentabilité des affaires et non la simple croissance du volume de primes. En effet, des mesures ont été prises au cours de l'exercice pour résoudre les problèmes techniques décelés dans certains centres de production devenus rentables aujourd'hui.

Cette prudence dans la souscription doit demeurer. Pour ce faire, l'équipe de technique doit continuer de se conformer aux Directives de la Société en matière de souscription et à d'autres bonnes pratiques en la matière.

Les événements récents dans diverses régions du continent où la Société opère constituent un motif de préoccupation. Ils exigent de la Société qu'elle adopte des stratégies visant à améliorer sa souplesse organisationnelle pour s'adapter aux tendances de l'heure et aux normes de la profession. En effet, le plan de continuité de la Société doit lui permettre de venir à bout des difficultés opérationnelles qui naîtraient de tel ou tel événement défavorable majeur.

La 10^{ème} édition de votre bulletin d'information comprend deux articles intitulés «La gestion du plan de continuité: quel intérêt pour Africa Re ?» et «L'avenir de la sécurité : Evoluer ou mourir».

Dans le premier article, le Responsable principal des risques évoque les facteurs et les mesures nécessaires pour se prémunir contre toute catastrophe. L'auteur décrit les différentes étapes de l'élaboration d'un plan de continuité et présente le projet de plan de continuité de la Société.

Dans le second article, l'Auditeur interne principal nous éclaire sur le rapide développement des technologies de l'information et les problèmes de sécurité qui s'en accompagnent.

Enfin, en sa triple qualité d'ancien membre du Comité éditorial, d'icône de la souscription et d'ancien directeur des Opérations centrales et de l'Inspection, M. Alain Ravoaja partage sa riche expérience avec le lecteur dans un entretien avec votre bulletin d'information. Nous lui souhaitons une paisible retraite.

Bonne lecture et n'hésitez pas à nous faire part de vos commentaires et observations sur votre bulletin d'information et son contenu.

Le Rédacteur-en-chef et Responsable principal des risques

Sere Mady Kaba



Business Continuity Management (BCM): The Importance for Africa Re

I. Background

In an increasingly uncertain world, Business Continuity and Disaster Recovery are fundamentally essential to the operational framework of any organisation. This article summarizes the necessary strategies to raise organisational flexibility to meet international trends and standards. It also recapitulates the contents of Africa Re's BCM project.

2. What Is Business Continuity And Why Is It Important?

Business continuity is the planning process that aims to ensure that whatever the cause of any direct or indirect incident such as failure in the supply/production chain, an act of terrorism or fire at business premises, effect on business should be minimal. It helps organisations anticipate, prepare for, mitigate, respond and recover from disruptions as quickly as possible with minimal effect on the business.

Actually, it is about thinking ahead and planning for a crisis. Therefore, in the event of an adverse incident, it is essential that the business is resilient enough to survive and critical functions are maintained.

Business continuity plan is a set of instructions of what to do and what not to do to ensure minimum disruption to a business in case of a major adverse incident or a disaster. The plan is established to mitigate the risk of damage to reputation, loss of customers and subsequent loss of business, loss/harm to staff and loss of property. It also ensures that staff members know their roles and responsibilities in the event of the an unexpected incident to ensure a rapid and well managed response to the disaster.

Several businesses suffer major disruptions every year. Any business could be affected and without a recovery plan, the chance of survival is actually reduced. A Business Continuity Plan ensures that business returns to normal as quickly as possible when faced with an emergency . It also provides a framework for building resilience and the capability for an effective response that safeguards the interest of key stakeholders, the reputation of the brand and value creating activities of the business.

Without a Business Continuity Plan the business could suffer from:

- Loss of business
- Damage to reputation and consequently loss of customers
- Loss of staff

La Gestion Du Plan De Continuité: Quel Intérêt Pour Africa Re

I. GENERALITES

Dans un monde de plus en plus incertain, le plan de continuité et le plan de reprise après catastrophe sont des éléments essentiels du cadre opérationnel de toute entreprise. Le présent article résume les mesures à prendre pour permettre à l'entreprise de s'adapter aux tendances et normes internationales. Il revient également sur le plan de continuité d'Africa Re dont il présente les grandes lignes.

2. QU'EST-CE QU'UN PLAN DE CONTINUITE ET POURQUOI EST-IL IMPORTANT?

Le plan de continuité est le système de planification qui permet de faire qu'un incident potentiel tel qu'une rupture de la chaîne d'approvisionnement ou de production, un acte de terrorisme ou un incendie dans les locaux d'une entreprise n'ait que des conséquences minimales sur les activités de l'entreprise, que les causes de l'incident soient directes ou indirectes. Il aide les entités à anticiper un incident potentiel, à y réagir ou à s'en remettre dans les meilleurs délais, avec les moindres dégâts possibles.

En fait, élaborer un plan de continuité, c'est gérer une crise de manière prospective. Il est essentiel en effet que l'entreprise puisse faire preuve de souplesse en cas de crise et soit en mesure de poursuivre ses activités principales.

Le plan de continuité est un ensemble d'instructions qui précisent ce qu'il faut faire et ce qu'il ne faut pas faire pour réduire au minimum l'impact d'un incident majeur ou d'une catastrophe sur les activités d'une entreprise. Le plan de continuité est conçu pour atténuer le risque de dommages à la réputation de l'entreprise, le risque de perte de clients, et le risque de perte subséquente d'affaires, le risque de perte d'employés ou de dommages corporels à ceux-ci et le risque de perte de biens. Le plan de continuité est aussi un moyen de sensibiliser les employés à leurs rôles et responsabilités respectifs en cas d'événement inattendu.

Plusieurs entreprises sont frappées par des événements perturbateurs chaque année. Aucune entreprise n'en est à l'abri, et, en l'absence d'un plan de continuité, les chances de survie sont réduites. Une entreprise qui dispose d'un plan de continuité devrait se relever d'une situation d'urgence aussi rapidement que possible. Le plan de continuité est également un outil de protection des intérêts des parties prenantes, de la marque et des activités créatrices de valeur de l'entreprise.

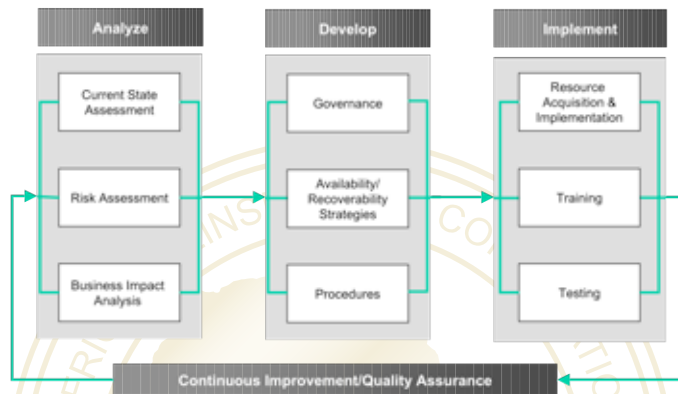


- Impact on expenses
- Loss of share value
- Failure of business

3. Business Continuity Methodology

The following graph illustrates the Deloitte BCM methodology. It is divided into distinct phases; each phase is made up of three separate modules. The fourth phase - Continuous Improvement and Quality Assurance - concludes the methodology.

Deloitte BCM Methodology



The key objectives and deliverables of the above phases and modules of the Deloitte BCM Methodology are summarized as follows:

Objectives

- To identify key risks; to promote a successful analysis of the threats the organisation will need to address.
- To deliver a business impact analysis (BIA) engagement; to establish the basis for understanding the BCM needs; to document recovery time objective (RTO) and recovery point objective (RPO) for major business functions / applications.
- To introduce key BCM governance; to explain the operational and functional roles and responsibilities of important stakeholders; to promote a successful BCM program.
- To determine the appropriate measures needed meeting stated objectives; to introduce a series of processes, infrastructure or personnel that must be put in place to address all resources required to run a business.
- To specify the activities, resources and personnel required to recover from a disruption; to demonstrate the sequence of recovery processes; to instruct all involved in their recovery roles.



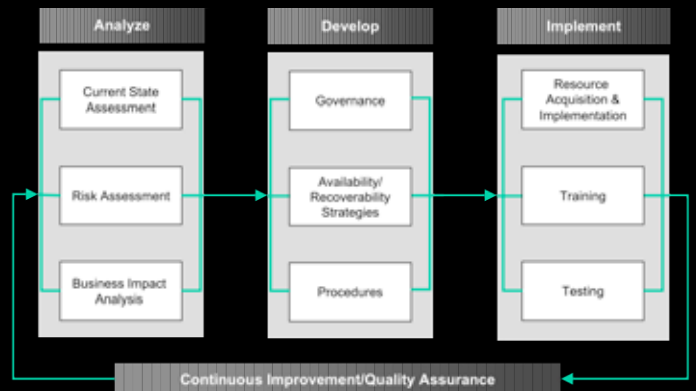
Sans un plan de continuité, l'entreprise est exposée à:

- Des pertes d'affaires;
- Des dommages à sa réputation entraînant des pertes de clients;
- Des pertes d'effectif;
- Des charges;
- La perte de la valeur de son action;
- Des interruptions d'activités.

3. METHODOLOGIE D'ELABORATION D'UN PLAN DE CONTINUITE

Le graphique ci-dessous présente la méthodologie d'élaboration d'un plan de continuité de Deloitte. Il comporte des phases distinctes. Chaque phase comprend 3 modules. La 4^{ème} phase - Amélioration permanente et assurance de qualité - est la dernière du modèle.

Méthodologie d'élaboration d'un plan de continuité de Deloitte



Les grands objectifs et résultats des différentes phases et modules du modèle de Deloitte se résument ainsi qu'il suit:

Objectifs

- Identifier les principaux risques; faciliter une bonne analyse des dangers auxquels l'organisation devra faire face;
- Faire une analyse d'impact sur l'entreprise; mettre en place le cadre d'analyse des besoins en matière de continuité des activités de l'entreprise; définir les objectifs en matière de temps de reprise et de point de reprise pour les principales fonctions/applications;
- Mettre en route les aspects essentiels de la gestion d'un plan de continuité; expliquer les rôles opérationnels et fonctionnels ainsi que les responsabilités des principales parties prenantes; promouvoir l'élaboration d'un bon programme de gestion du plan de continuité;



Deliverables

- Inherent risk register
- BIA management report
- Business process / function priority inventory
- IT application function priority inventory
- BCM strategic policy statement
- BCM organizational roles and responsibilities
- Strategic recommendations
- Analysis of alternatives
- Business continuity plan(s)

3. Africa Re's BCM Project

Experience shows that businesses are far more likely to survive a disaster if they have thought about it in advance and planned accordingly. Given the importance of such planning, it was decided to establish a BCM for the subsidiary (ARCSA) which is the top production centre for the Group.

Therefore, following an internal process at the subsidiary level, an independent consultant, Deloitte & Touche, was selected to conduct the project with the involvement of the Chief Risk Officer (CRO). The CRO is expected to use the experience gained in the subsidiary project to effectively roll out similar processes throughout the entire Corporation.

In each production centre the project should cover in each production centre the following four phases which constitute the BCM life cycle or BCM programme management.

Phase 1 - Business Impact Analysis (BIA) & Risk Assessment (RA): The objective of this phase is to identify and analyse the vulnerable areas of the business thus establishing the basis for understanding the BCM needs. A BIA, the cornerstone of a BCM program, identifies the risks of business interruption. It also evaluates the business impact of potential interruptions by measuring their financial, operational and regulatory impacts associated with a disruption of the business. It is an exposure assessment that will drive the definition of the business recovery strategy.

Phase 2 - Strategy Development: Determining BCM strategy based on prioritised critical functions/ services and the effect of known risks. It guides in determining the appropriate measures to recommend to meet stated objectives.

Phase 3 - Plan Development: Developing and implementing BCM response/plans to enable the company to continue to operate its critical functions in any worst scenario. It introduces



- Définir les mesures à prendre pour atteindre les objectifs arrêtés; mettre en place un ensemble de procédés et disposer des moyens matériels et humains nécessaires gérer un plan de continuité;
- Définir les activités ainsi que les moyens matériels et humains nécessaires pour que l'entreprise se relève d'un incident; faire apparaître les étapes du processus de reprise; préciser son rôle à chaque partie prenante au processus.

Résultats

- Registre des risques intrinsèques;
- Rapport de gestion de l'étude d'impact;
- Inventaire des fonctions prioritaires de l'entreprise;
- Inventaire des applications informatiques prioritaires;
- Déclaration de politique stratégique en matière de continuité des activités;
- Rôles et responsabilités en matière de plan de continuité;
- Recommandations stratégiques;
- Analyse des solutions de rechange; et
- Plan de continuité.

3. LE PROJET DE PLAN DE CONTINUITÉ D'AFRICA RE

L'expérience montre que les entreprises ont nettement plus de chances de survivre à une catastrophe lorsqu'elles y ont pensé à l'avance et ont pris les mesures nécessaires en conséquence. C'est fort de ce constat qu'Africa Re a décidé d'élaborer un plan de continuité pour sa filiale sud-africaine (ARCSA), principal centre de production du Groupe

C'est ainsi qu'un consultant indépendant, en l'occurrence Deloitte & Touche, a été retenu à l'issue d'une procédure de sélection interne pour réaliser le projet, avec la participation du responsable principal des risques du Groupe. Le responsable principal des risques devrait s'appuyer sur cette expérience pour élaborer des plans de continuité comparables dans tous les centres de production du Groupe.

Dans chaque centre de production, le projet devrait couvrir les 4 phases suivantes qui constituent le cycle de vie d'un programme de gestion d'un plan de continuité.

Phase 1 - Analyse d'impact & évaluation des risques: Cette phase consiste à identifier et à analyser les domaines de vulnérabilité de l'entreprise, et partant, de définir les besoins en matière de continuité des activités. Pierre angulaire du programme d'élaboration du plan de continuité, l'analyse



a series of processes, infrastructure and personnel that will be required to run the business.

Phase 4 - Maintenance: Exercising, maintaining and reviewing the BCM plans. It concerns the review and re-evaluation of the plans as well as simulation of the worst situation to test it.

The BCM Project for ARCSA has been concluded. The Management of ARCSA took delivery of the final reports - BCM Plans, BCM Strategy, Business Impact and Project Charter.

The documentation sets out detailed procedures and highlights a number of requirements to be put in place going forward. The Management of the Subsidiary had taken a number of proactive actions, some even before the finalization of the BCM documents.

A proposal for the annual review/maintenance support to ARCSA is currently under review for decision.

4. Conclusion

We would like to conclude by thanking the Executive Management for approving this anticipatory project for the Corporation. I also thank ARCSA Management and staff for the successful conclusion for their BCM. The project will soon take off in the other production centres. It will definitely boost the Corporation's risk management framework and processes.

By
Sere Mady Kaba
Chief Risk Officer



d'impact identifie les risques d'interruption des activités de l'entreprise et leur incidence en mesurant les conséquences financières, opérationnelles et réglementaires. C'est une évaluation des risques qui contribue à la définition de la stratégie de reprise des activités de l'entreprise.

Phase 2 - Formulation de la stratégie: L'objectif ici est de formuler une stratégie de continuité des activités de l'entreprise fondée sur les fonctions/services critiques et les conséquences des risques connus. Cette phase aide à déterminer les mesures à recommander pour atteindre les objectifs définis.

Phase 3 - Elaboration du plan: La 3^{ème} phase est celle de l'élaboration et de la mise en œuvre du plan de continuité ; elle vise à faire en sorte que les fonctions critiques de l'entreprise ne soient pas interrompues en cas de catastrophe.

Phase 4 - Maintenance: Il est question ici de tester le plan de continuité, d'en assurer la maintenance et de l'évaluer en simulant un scénario catastrophe.

Le projet d'élaboration du plan de continuité de l'ARCSA est achevé. Les rapports finaux, à savoir le plan de gestion de la continuité, la stratégie de gestion de la continuité, l'analyse d'impact et la charte du projet - ont été remis à la direction de la filiale.

Les documents définissent les procédures dans le détail et mettent en évidence un nombre de mesures à prendre désormais. La direction de la filiale a pris un nombre de mesures proactives dont certaines sont antérieures à la finalisation des travaux.

Un projet de document relatif à l'évaluation/appui à la maintenance du plan de continuité de l'ARCSA est actuellement en étude.

4. CONCLUSION

En conclusion, nous aimerions remercier la Direction générale pour avoir approuvé ce projet prospectif pour la Société. Notre gratitude va également à la direction et au personnel de l'ARCSA qui ont rondement mené le projet. Celui-ci démarrera sous peu dans les autres centres de production et améliorera incontestablement le cadre et la procédure de gestion des risques de la Société.

Par
Sere Mady Kaba
Responsable principal des risques



Interview of Mr. Alain Ravoaja, outgoing Director of Central Operations Africa Re



1. We recall that you were recruited in Africa Re in 1988. What made you to join the Corporation?

Madagascar adhered to the Agreement Establishing the African Reinsurance Corporation in 1988 and I was the first Malagasy to apply for a job in Africa Re. My recruitment in the Nairobi Regional Office, which was headed by my friend Mr. Appannah, was facilitated by the fact that at that time, there were few jurists with an insurance certificate with more than 15 years' experience. I had also had the opportunity to be in close contact with Africa Re senior staff, when I was the Deputy Managing Director of Ny Havana Insurance Company.

That said, I must admit that I was especially attracted to the prestige attached to a job in Africa Re, already known as one of the flagships of the achievements of the Organization of African Unity.

2. You left the Corporation in 1993 and came back four years later to start the Port Louis Office. What was your experience in Mauritius?

It was exciting and sometimes difficult. In any case, since the opening of the Mauritius Office in 1997, we have had unflinching support from well educated and versatile staff, as a driver also has to do the job of an archivist in a small office. I have not forgotten the assistance of our legal adviser and the active support of my wife and my son during the first months of operation of the Office. In fact the autonomy of the Office was achieved gradually and smoothly thanks to the capacity of our Mauritian colleagues to handle the various tasks entrusted to them, until the volume of work made specialization of the positions possible.

That said, we knew beforehand that we will be operating in rather competitive markets but we were however surprised

INTERVIEW DE M. ALAIN RAVOAJA, ANCIEN DIRECTEUR DES OPERATIONS CENTRALES D'AFRICA RE



1. Vous avez été recruté à Africa Re en 1988. Pourquoi avez-vous accepté de faire partie des effectifs de la Société?

L'année 1988 étant celle de l'adhésion de Madagascar à l'accord portant création de la Société Africaine de Réassurance, je fus le premier Malgache à déposer une demande d'emploi auprès d'Africa Re. Le recrutement au Bureau Régional de Nairobi dont mon ami Appannah était le Directeur fut facilité par le fait que les juristes titulaires d'un diplôme d'Assurance et ayant une expérience de plus de 15 ans n'étaient pas légion à l'époque et que j'avais déjà eu l'occasion de côtoyer des grands cadres d'Africa Re lorsque j'étais Directeur Général Adjoint de la Société d'Assurances Ny Havana.

Cela étant, je me dois d'avouer que je fus surtout attiré par le prestige attaché à un emploi chez Africa Re, déjà connu comme l'un des fleurons des réalisations de l'Organisation de l'Unité Africaine.

2. Vous avez quitté la Société en 1993 pour revenir 4 ans plus tard et ouvrir le bureau de Maurice. Parlez-nous de votre expérience dans ce pays.

Passionnante et quelquefois éprouvante: en tout cas, depuis l'ouverture du Bureau local de Port-Louis, en août 1997, nous avons pu compter sur le soutien sans faille d'un personnel bien éduqué, et passe-partout en ce sens que dans un petit bureau, un chauffeur doit par exemple aussi faire le travail d'un archiviste. Je n'oublie pas l'assistance de notre Avocat-Conseil et le soutien agissant de mon épouse et de mon fils durant les premiers mois d'opérations du Bureau. En fait, l'autonomie du Bureau a pu se réaliser progressivement et sans à-coup grâce à la facilité d'adaptation de nos collègues mauriciens à la diversité des tâches confiées à chacun d'eux en attendant le moment où le volume de travail a permis la spécialisation des postes.



by the very low premium rates in some of the markets, despite a high claims experience. That is why we decided at one point to suspend the underwriting of Facultatives in one of the markets.

3. What was it like to work in the multi cultural and multi religious environment of Africa Re?

We were not very surprised by the multi-cultural and multi religious environment of Mauritius due to the diverse origins of the Malagasy people. Rather, we admire the fact that beside the language of their countries of origin, Mauritians speak French, English and Creole - a French-based lingua franca that is a mixture of the other languages spoken in the country. Diversity of origins and multilingualism have contributed to the success of the country, not forgetting the hospitality of Mauritians. We can affirm that we were virtually adopted by the staff and clients of this country.

4. How would you compare your responsibilities as Regional Director and Director of Central Operations in the Headquarters?

The nature of the responsibilities is different and errors are likely to be detrimental or disastrous to the Corporation in both positions.

The Regional Director has to permanently preserve the image of the Corporation with a high sense of human relations coupled with impeccable technical know-how in insurance and reinsurance. In addition, he has the duty to successfully develop the production centre with regard to the premium income and results.

The Director of Central Operations has to successfully conduct the annual retrocession programme of the Corporation at the technical level and with regard to the cost, to enable the network to work effectively and serenely. Furthermore, he monitors the network throughout the year and is at their disposal, ready to meet their requests in the shortest possible time. He also has to seriously prepare the meetings with the rating agencies and manage the stress this engenders. He equally has to reflect on the means of improving the working tools and technical knowledge of the Underwriters. Lastly, in his capacity as Management staff, he has the duty to advise Executive Management on various issues sometimes of utmost importance.



Cela étant, sachant avant de venir que nous aurions à opérer dans des marchés plutôt compétitifs, nous avons tout de même été surpris par les taux de primes très bas pratiqués sur certains de ces marchés en dépit d'une sinistralité élevée, ce qui fait que nous avons du prendre la décision à un moment donné de suspendre la souscription en Facultatives dans l'un d'eux.

3. Comment avez-vous vécu votre séjour dans le contexte multiculturel et multi-religieux qu'est Africa Re?

En raison de la diversité d'origines de la population malgache, nous n'avons pas été trop surpris par l'environnement multiculturel et religieux de Maurice. Par contre, nous admirons le fait qu'en plus de la langue de leurs pays d'origine, les Mauriciens parlent le Français, l'Anglais et le Créole qui est une langue de synthèse des autres langues parlées dans le pays avec le Français comme base. La diversité d'origines et le multilinguisme ont favorisé la réussite du pays, sans oublier le sens de l'hospitalité des ilois. Pour notre part, nous affirmons que nous avons été pratiquement adoptés par le personnel et la clientèle de ce pays.

4. Quelles similitudes et différences y a-t-il entre les postes de directeur régional et de directeur des opérations centrales au siège de la Société?

La nature des responsabilités est différente, les erreurs étant susceptibles d'avoir des conséquences préjudiciables sinon désastreuses pour la Société dans un cas comme dans l'autre.

Le Directeur régional se doit de préserver en permanence l'image de la Société avec un sens aigu des relations humaines en plus de connaissances techniques irréprochables dans les domaines de l'Assurance et de la Réassurance. Il a par ailleurs une obligation de réussite en ce qui concerne le développement du Centre de Production en termes de chiffre d'affaires et de résultats.

Le Directeur des opérations centrales, quant à lui, se doit de réussir le programme annuel de rétrocession de la Société tant sur le plan technique que celui du coût, afin de permettre au réseau de travailler efficacement et sereinement. En outre, tout au long de l'année, il surveille le réseau et est à son écoute, prêt à satisfaire ses demandes dans les plus brefs délais. Il doit aussi se préparer sérieusement aux réunions avec les agences de notation, avec le stress que cela engendre. Il doit également réfléchir aux moyens d'améliorer les outils de travail et les connaissances techniques des souscripteurs. Enfin, en sa qualité de membre de la Direction, il a l'obligation de conseiller la Direction générale sur divers sujets quelquefois de grande importance.



5. Where do you think Africa Re is in terms of Risk Management and what do you think should be done to improve its ERM and corporate governance culture?

We think that Africa Re has become a model in Africa and should not rest on its laurels. It is necessary now to prepare the decentralization of Enterprise Risk Management, including the use of Remetrica software to make it effective in each production centre at 2015 at the latest.

6. What, in your view, is the greatest risk facing the Organization in such areas as: technical operations, external environment and human resources? What solutions can you recommend?

In my humble opinion Management and staff of Africa Re should confront three types of risks:

- lack of the sense of belonging related to the recruitment of younger staff: the idea is not only material well-being and a carrier plan but also, and maybe especially, the atmosphere. Africa Re should not become a Reinsurance school where people come and leave after 4 to 5 years.
- Management should ensure that staff are not overwhelmed by routine work as routine kills the spirit of innovation. Maybe, a Department of Studies and Training should be set up.
- The third risk, connected to the first two, has to do with managing overheads: as ratios are tools and not an end in itself, the risk is to tend to be extremely generous or, on the contrary, tight-fisted.

7. From a risk point of view, what was the most challenging event/period in each of your three postings in Africa Re: Lagos, Mauritius & Nairobi?

In Nairobi, the challenge was to quickly master the English language, though I needed to be immediately operational.

In Mauritius, it was the series of major losses that occurred in 1999. Besides cyclones, there were virtually unimaginable losses. For example, you are at home watching live on television a major fire loss in a hotel reinsured by Africa Re, when suddenly you notice that the fire has spread to another reinsured tourist complex more than 100 metres away, as the sparks were been blown there by wind!

In Lagos, it was the end of the year of transition to annual entry of technical reserves. This necessitated sensitizing staff of production centres, already overwhelmed with other end-of-year tasks, to carry out new vital responsibilities of collating and inputting data on claims payable, leading to considerable delay in the preparation of financial statements.



5. Quelle est, à votre avis, la situation d’Africa Re en matière de gestion des risques et quelles sont les mesures qui devraient être prises pour améliorer la GIR et la gouvernance d’entreprise au sein de la Société?

Nous pensons qu’Africa Re est devenu un modèle sur le continent africain et ne doit pas s’endormir sur ses lauriers. Il faudrait maintenant préparer la décentralisation de la gestion intégrée des risques, y compris l’exploitation du logiciel Remetrica, pour la rendre effective au plus tard en 2015 dans chaque centre de Production.

6. Quels sont, selon vous, les risques majeurs auxquels la Société est exposée en ce qui concerne les opérations techniques, l’environnement externe et les ressources humaines? Quelles solutions recommanderiez-vous?

A notre humble avis, la Direction et le personnel d’Africa Re doivent faire face à trois types de risques:

- Un sentiment d’appartenance insuffisant lié à l’objectif de rajeunissement du personnel: il ne s’agit pas seulement de bien-être matériel et de plan de carrière, il s’agit aussi et peut-être surtout d’ambiance. Il ne faut pas qu’Africa Re devienne une école de Réassurance que l’on quitte après 4-5 ans.
- La Direction doit veiller à ce que le personnel ne soit pas débordé par les tâches routinières car la routine tue l’esprit d’innovation. Il faudrait d’ailleurs peut-être créer un département des Etudes et de la Formation.
- Le troisième risque, lié aux deux premiers, a trait au souci de maîtriser les frais généraux : les ratios étant des outils et non des fins en soi, le risque est de systématiquement verser dans l’excès de largesse ou au contraire d’économie de dépenses.

7. Du point de vue du risque, quel est l’événement/le moment le plus exaltant qui a marqué votre séjour dans les trois localités où vous avez vécu pendant vos années de service à Africa Re: Lagos, Maurice & Nairobi?

A Nairobi, le défi à relever fut d’arriver à maîtriser rapidement l’anglais alors qu’il fallait être immédiatement opérationnel.

A Maurice, ce fut la série de gros sinistres survenus en 1999. En dehors des cyclones, il y eut des sinistres pratiquement impossibles à imaginer: par exemple, vous êtes assis chez vous devant la télé en train de vivre en direct un sinistre majeur Incendie d’un ensemble hôtelier réassuré par Africa Re lorsque soudain, vous constatez de visu que le feu s’est étendu à un autre complexe touristique réassuré situé à plus de 100 mètres



8. Looking back over the years do you feel satisfied with Africa Re's standing today? What changes, in your view, need to be made to ensure that Africa Re continues to be a success story?

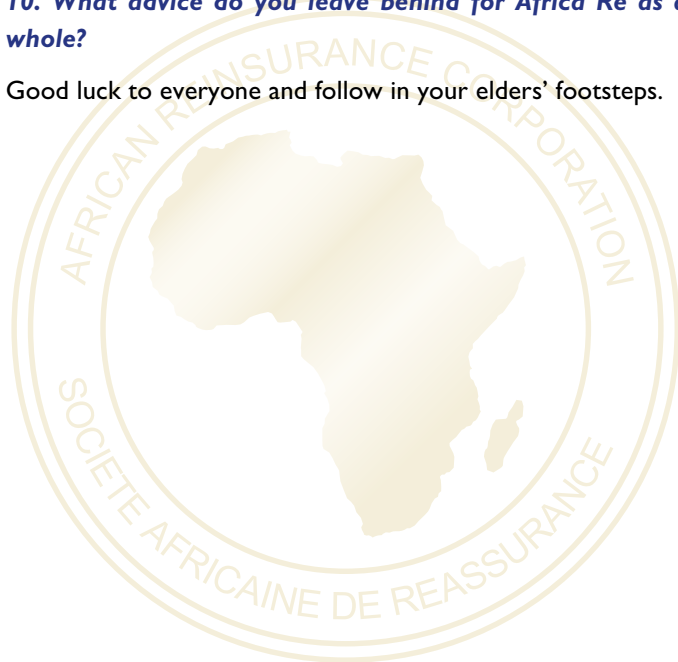
Africa Re has come a long way. With regard to changes, the corporate culture and team spirit have to be maintained, though this is not a change per se.

9. What do you miss most since you left Africa Re in July 2010?

The friendship of my colleagues, not only my direct collaborators but also a good number of colleagues from other departments and production centres with whom we established personal relations based on mutual respect.

10. What advice do you leave behind for Africa Re as a whole?

Good luck to everyone and follow in your elders' footsteps.



du premier, le vent ayant emporté des flammèches dans l'enceinte de ce dernier!

A Lagos, ce fut la fin de l'année du passage à la comptabilisation annuelle des provisions techniques, nécessitant la sensibilisation du personnel des Centres de production, déjà débordé par d'autres travaux de fin d'année, aux tâches vitales nouvelles de collecte et de saisie des données sur les sinistres à payer, entraînant un retard important dans le processus de confection des états financiers.

8. Si l'on tient compte du chemin parcouru, êtes-vous fier de la situation actuelle d'Africa Re? Qu'est-ce qui, à votre avis, doit changer pour qu'Africa Re continue d'engranger des succès ?

Africa Re a fait du chemin depuis... Pour ce qui est des changements, il faut surtout entretenir la culture d'entreprise, l'esprit d'équipe, mais ceci n'est pas en fait un changement.

9. Qu'est-ce qui vous manque le plus depuis que vous êtes parti d'Africa Re?

L'amitié des Collègues, non seulement de mes collaborateurs directs, mais aussi de bon nombre des collègues d'autres départements et des centres de production avec lesquels nous avons noué des relations personnelles basées sur l'estime réciproque.

10. Quel serait votre conseil pour la Société en général?

Bon courage à tous et marchez sur les pas de vos aînés.



1.0 The Future of Security: Evolve or Die

Business models have changed, the value of data has skyrocketed, and organizations are much more dependent on their IT systems. Concurrently, the pace of IT development has accelerated and cyber threats have multiplied. Unfortunately, many ICT functions have failed to match that pace and meet those threats.

Mobile devices, social media, cloud computing, and other developments have enabled new ways of working while disrupting the IT environment. Large volumes of unstructured data and collaborative computing platforms have made IT infrastructures rapidly changing works in progress. These changes have occurred at breakneck speed, dictated by the needs of the business, the development of IT and the speed of adoption by users.

In contrast, IT security evolves slowly. Many ICT functions still struggle to implement basic security practices, such as strong passwords, system information, event management tools, effective user training and awareness. And much of security remains compliance driven when compliance is but one element of an effective program.

1.1 Social media: Don't "friend" your enemies

Social media sites and blogs open new avenues of attack. An internetnews.com article cited attackers focusing on social media users and "attempting to trick [users] into downloading malware or divulging sensitive information." That same article noted that operating systems and browsers are irrelevant given that the user, not the technology, is being targeted.

Attackers have used social media to identify, profile, and compile personal identification data on potential targets. Data aggregation from multiple sites can lead to compromised passwords, data leakage, and security incidents.

Some organizations go to great lengths to limit their exposure to social media. Others take a mixed approach, for example permitting marketers to use social media to monitor public opinion and HR professionals to check backgrounds of potential hires. And some companies have no well-defined approach. The better approach is to consider the costs, benefits, risks, and rewards to the organization and its stakeholders, and the best ways of balancing them.

Steps to consider

- Get smart. Understand the features and dangers of social media sites and collaboration tools and foster awareness of their limitations and risks.



1.0 L'avenir de la sécurité: Evoluer ou mourir

Les méthodes de gestion ont évolué, l'information a gagné en utilité à un rythme fulgurant et les organisations sont nettement plus tributaires des systèmes informatiques. Dans le même temps, le rythme de développement des technologies de l'information s'est accéléré, et les cyberdangers se sont multipliés. Malheureusement, sous plus d'un rapport, les services informatiques n'ont su ni s'adapter à ces évolutions, ni faire face à ces menaces.

Les appareils mobiles, les réseaux sociaux, l'informatique en nuages et d'autres évolutions ont engendré de nouvelles méthodes de travail et modifié l'environnement des TI. Des volumes considérables de données non structurées et des plateformes collaboratives ont fait des infrastructures informatiques des ouvrages en rapide mutation. Ces évolutions se sont opérées à une vitesse mirobolante, dictées qu'elles étaient par les besoins des entreprises, le développement des technologies des TI et la cadence de leur adoption par l'utilisateur.

Inversement, la sécurité informatique évolue lentement. En effet, nombre de structures informatiques s'efforcent encore d'appliquer des pratiques aussi élémentaires que des mots de passe fiables, des outils d'information ou de gestion d'événements ou une formation et une sensibilisation efficaces des utilisateurs. De plus, la sécurité reste orientée essentiellement vers la conformité, alors que celle-ci n'est qu'un aspect d'un bon programme de sécurité.

1.1 Les réseaux sociaux: Ne fréquentez pas vos ennemis

Les réseaux sociaux et les blogs peuvent offrir de nouvelles possibilités d'attaque. Un article d'Internetnews.com a fait état d'attaques ciblant les utilisateurs des réseaux sociaux et visant à « inciter [les utilisateurs] à télécharger du malicieux ou à divulguer des informations sensibles ». Le même article faisait observer que les systèmes d'exploitation et les navigateurs sont sans intérêt dans le cas d'espèce étant donné que c'est l'utilisateur qui est visé, et non l'ordinateur.

Des cybercriminels se sont servis des réseaux sociaux pour identifier des cibles potentielles, définir leur profil et rassembler des informations personnelles sur les intéressés. L'accumulation de données en provenance de sites multiples peut entraîner des compromissions de mot de passe, le couplage d'informations et des incidents sécuritaires.

Certaines organisations font des efforts appréciables pour limiter leur exposition aux réseaux sociaux. D'autres adoptent une approche mixte, permettant par exemple aux commercialisateurs de se servir des réseaux sociaux pour suivre l'opinion publique et aux professionnels des ressources humaines de vérifier les antécédents de recrues potentielles. D'autres organisations encore n'adoptent aucune approche précise. La meilleure démarche serait de tenir compte des coûts, des avantages et des risques pour l'organisation et ses



- Create boundaries. Policies governing the use of social media and collaboration tools, data loss prevention and user education are essential.
- Educate your workforce. Training can promote proper use of social media and collaboration tools and limit inappropriate data sharing.

1.2 Mobile devices: Multiplying avenues of attack

Mobile devices have become pervasive and diverse as to type, capabilities, and risks. For this purpose, mobile devices include the full range of smartphones, laptops, notebooks, and tablets.

Mobile devices present relatively easy, low-risk points of entry to attackers, who can remotely monitor them for passwords, account numbers, and personal identification data. These devices also open avenues of attack through social media sites and communication media. (Executives demanding exemptions from security policies for their devices do not help matters.) Also, organization's security standards can be difficult to apply to applications being issued.

While many of today's smartphones can be configured to lock down browser access, limit downloading of third-party applications, and improve control over other functions, the policies must balance protection and productivity.

In general, although they are available, anti-virus and other protections tend to be underused on mobile devices. In addition, many users exercise a lower level of care with cell phones and PDAs, due to relaxed habits developed in using the devices in both their personal and professional lives. Yet mobile devices effectively become part of the corporate network and should therefore be viewed as such and their risks addressed.

Steps to consider

- Leave it home. Restrict users' primary mobile devices to domestic use, and issue temporary devices with minimal data for office and overseas travel.
- Lock it down. Configure mobile devices to minimize the chances of their being scanned, sniffed, or tampered with; many can be encrypted selectively, for example for travel to high risk geographies - or just a trip to the local internet hotspot.

1.3 Cloud computing: Cloudy with a chance of infiltration

Adoption of cloud computing will continue, and, hopefully, approaches to address its risks will evolve. The risks vary with the type of cloud (public, private, or hybrid), its architecture, and whether it is a software, platform, or total infrastructure



parties prenantes et des moyens de les concilier.

Mesures à envisager

- Etre futé - Comprendre les caractéristiques et les dangers des réseaux sociaux et des postes de travail coopératifs et promouvoir la sensibilisation à leurs limites et risques;
- Créer des frontières - Des politiques d'utilisation des réseaux sociaux et des postes de travail coopératifs et de prévention des pertes de données et de sensibilisation des utilisateurs sont essentielles;
- Sensibiliser le personnel - La sensibilisation peut contribuer à une bonne utilisation des réseaux sociaux et des postes de travail coopératifs et limiter le partage indu de données.

1.2 Les appareils portables: multiplier les possibilités d'attaque

Les appareils portables se sont généralisés et diversifiés du point de vue de leur nature, de leurs capacités et des risques qu'ils comportent. Ils vont du smartphone à la tablette en passant par l'ordinateur portable et l'ordinateur bloc-notes.

Les appareils portables constituent des points d'accès relativement faciles et à faible risque pour les cybercriminels qui peuvent en contrôler à distance le mot de passe, le numéro de compte et les données personnelles. Ils se prêtent à des attaques par le truchement des réseaux sociaux et autres moyens de communication. (Les responsables d'entreprise qui demandent à être exemptés des politiques sécuritaires ne facilitent pas les choses.) De plus, il peut être difficile d'appliquer les normes de sécurité des entreprises à des applications en cours d'utilisation.

Si nombre de smartphones modernes peuvent être configurés de manière à en bloquer l'accès aux navigateurs, à limiter le téléchargement d'applications de tiers et à renforcer le contrôle sur d'autres fonctions, les politiques de sécurité doivent concilier protection et productivité.

En général, bien qu'ils soient disponibles, l'antivirus et d'autres protections sont généralement sous-utilisés pour les appareils portables. En outre, quantité d'utilisateurs prennent moins de précautions pour les téléphones mobiles et autres appareils portables en raison des habitudes relâchées qu'ils ont prises dans l'utilisation de ces appareils dans leur vie privée et professionnelle. Pourtant, les appareils portables deviennent effectivement une composante du paysage des entreprises et, par conséquent, devraient être considérés comme tels, et les risques y afférents pris en considération.

Mesures à envisager

- Laisser les appareils portables à la maison - Réserver les appareils portables à l'usage domestique et utiliser d'autres appareils avec des données minimales pour le bureau et les voyages à l'étranger ;
- Bloquer les appareils portables- Configurer les appareils



cloud. Regardless, cloud computing generally provides less direct control over applications, systems, and data security. However, cloud solutions can improve security, enabling some organizations to attain a level of security they may not otherwise be able to afford from a cost, resource, or process maturity perspective.

Given its stage of development and more open architecture, cloud computing can present serious risks. Data may reside anywhere in the cloud, in multiple locations, on shared devices, and in foreign nations. Most enterprises more fully understand business and legal conventions in their domestic (as opposed to foreign) locations; therefore, when cloud components reside in foreign locations, the complexities and risks increase and must be managed aggressively. Also, you may need to produce an audit trail or specific data for tax or legal purposes, and must have access and capabilities that permit such retrieval. Thus a number of issues must be addressed if cloud computing is to provide sufficient security.

Steps to consider

- Understand the configuration. Know where the cloud components and your data will be housed and who is responsible for which functions and risks.
- Apply your standards. To the extent possible, apply your standards to service providers, and remember that you can outsource functions but not risks.
- Trust but verify. Due diligence when selecting service providers is a must as is addressing each party's rights and responsibilities within the contract.

1.4 Software vulnerabilities: The soft underbelly of your IT environment

Software vendors regularly release patches, hot fixes, and public announcements of exploits for their software products. They have to, given the trade-off between meeting deadlines, incorporating features, and thoroughly testing products for bugs and security vulnerabilities. With a growing number of applications being released for multiple platforms (including some, such as mobile applications, with very short build-test cycles) the number of software vulnerabilities has never been greater.

Criminals and hackers stand ready to capitalize on these vulnerabilities. The online market for purchased exploits has matured to the point where websites have been established to sell exploits to the highest bidder. Purchasers of these exploits can take advantage of software vulnerabilities before they have been repaired.



portables de manière à minimiser les possibilités de se les faire scanner, piquer ou endommager ; nombre d'appareils portables peuvent être encryptés de manière sélective, par exemple lorsqu'on se rend à des endroits à haut risque;

1.3 L'informatique en nuages: nuageux mais avec un risque d'infiltration

L'informatique en nuages continuera de se généraliser et l'on espère que les techniques de gestion des risques continueront également d'évoluer. Les risques varient en fonction du type de nuage (public, privé, hybride), de la structure de celui-ci et selon qu'il s'agit d'un logiciel, d'une plateforme ou d'une infrastructure complète. Dans un cas comme dans un autre, l'informatique en nuages offre généralement un moindre contrôle direct sur les applications, les systèmes et la sécurité des données. Toutefois, l'informatique en nuages peut améliorer la sécurité et permettre à certaines organisations de parvenir à un niveau de sécurité auquel elles ne parviendraient pas autrement pour des raisons de coûts, de ressources et de maturité des procédures.

L'informatique en nuages peut présenter de graves risques en raison de son niveau de perfectionnement et de son architecture plus ouverte. Les données peuvent être stockées partout dans les nuages, à des endroits multiples, sur des appareils partagés et à l'étranger. La plupart des entreprises ont une meilleure compréhension du droit des entreprises et du cadre juridique de leur pays (par opposition à ceux d'autres pays). En conséquence, lorsque des composantes du nuage sont hébergées à l'étranger, les risques s'accroissent et doivent être gérés de manière dynamique. De plus, une liste de contrôle ou des données spécifiques pourraient être nécessaires à des fins fiscales ou pour répondre à d'autres exigences légales. Un nombre de questions doivent donc être résolues pour que l'informatique en nuages offre une sécurité suffisante.

Mesures à envisager

- Comprendre la configuration - Savoir où seront hébergées les composantes du nuage et vos données et qui est responsable de quelles fonctions et de quels risques.
- Appliquer vos normes - Autant que faire se peut, appliquer ses propres normes au fournisseur de services et se rappeler qu'on peut externaliser des fonctions et non des risques.
- Faire confiance mais se méfier – Autant le respect des procédures est nécessaire en matière de sélection des fournisseurs de services, autant il est impérieux de définir les droits et devoirs de chaque partie dans le contrat.

1.4 Vulnérabilités des logiciels: le ventre mou de votre environnement informatique

Les distributeurs de logiciel vantent régulièrement leurs produits dans divers types d'annonce. On peut les comprendre étant donné l'équilibre à faire entre les délais à respecter, les caractéristiques à incorporer et les tests à appliquer aux



Pirated software, which fosters malware distribution, has proliferated, particularly in countries with lax cyber laws. The overlap between work and home life, the growing use of independent contractors, and the sheer volume of pirated software make it easy for a virus, worm, or exploit to open a system to attack. Even legitimate software is at risk, given that freeware vendors, which rely on third party banners and advertisements for operating revenue, can be exploited.

No antivirus or firewall can guarantee protection. Collectively, attackers have almost unlimited time, skills, and resources to devote to creating and exploiting vulnerabilities. That gives them an advantage over IT security teams with limited resources and a broad range of priorities. Even the leading security companies cannot keep pace with new threats. Diligently implemented policies can improve security, although the impossibility of identifying all vulnerabilities underscores the need to anticipate incidents, take precautions, and assume that precautions could fail.

Whether you are creating software, implementing solutions, or developing in-house systems, you must employ vulnerability assessments, security design reviews, automated tools, and peer reviews. These measures should be applied in the context of cost-benefit analysis. The goal is not perfection, but consistent application of sound risk management practices.

Steps to consider

- Anticipate and defend. Anticipating failure enables you to develop damage control, system resiliency, rapid recovery, privacy protection, and notification and public relations plans.
- Define normal to identify abnormal. To monitor for unknown threats, it is possible to develop heuristics that can detect unusual code or activity.
- Exercise vigilance. Develop baseline metrics and maintain situational awareness of network activity, monitoring for unusual spikes or traffic destinations.

2.0 Conclusion

Evolutions take time - so start today

While it may be impossible to match the speed at which the environment is evolving, organization's management must urge and enable the ICT function to accelerate its own evolution. The speed and direction should be dictated by the value of assets, organization's dependence on them, resulting risks, and existing security capabilities. The process should begin with gauging the value of information and IT systems, assessing threats, and allocating resources accordingly.



produits pour en déterminer la résistance aux bogues et à d'autres vulnérabilités d'ordre sécuritaire. L'augmentation du nombre d'applications destinées à des plateformes multiples (dont certaines, à l'exemple des applications mobiles, ont un cycle de test incorporé très court) s'accompagne d'un accroissement correspondant des risques auxquels les logiciels sont exposés.

Les cybercriminels et autres pirates informatiques n'attendent que la première occasion pour tirer avantages de ces faiblesses. Le marché électronique des exploits est tellement développé de nos jours que des sites web ont été créés pour vendre des exploits au mieux-disant. Les acquéreurs de ces exploits peuvent tirer avantage des faiblesses/vulnérabilités des logiciels avant qu'elles ne soient corrigées.

Les logiciels piratés, terreau de la distribution de maliciel, ont proliféré, en particulier dans les pays où la législation contre la cybercriminalité est souple. Le chevauchement entre la vie professionnelle et la vie privée, le recours croissant à des consultants indépendants et le volume même de logiciels piratés permettent à un virus, à un ver ou à un exploit d'ouvrir et d'attaquer aisément un ordinateur. Même des logiciels légitimes ne sont pas à l'abri étant donné que les distributeurs de logiciel sont tributaires de banderoles et autres supports publicitaires de tiers pour leur chiffre d'affaires.

Aucun antivirus ni aucun pare-feu ne peut assurer quelque protection. Les cybercriminels ont un temps, des connaissances et des ressources presque illimitées pour créer et exploiter des failles. Ils ont ainsi un avantage sur les équipes de sécurité informatique qui disposent de moyens limités et ont toute une gamme de priorités. Même les meilleures sociétés de sécurité informatique ne peuvent suivre le rythme auquel les menaces apparaissent. Des politiques de sécurité bien diligentées peuvent être utiles. Toutefois, étant donné qu'on ne peut identifier toutes les failles, il est nécessaire de prévoir les incidents, de prendre des précautions et de se dire que les précautions pourraient ne pas suffire.

Que ce soit pour inventer un logiciel, appliquer une solution ou concevoir une application interne, il est nécessaire d'évaluer les vulnérabilités, d'analyser la conception de la sécurité, d'utiliser des outils informatiques et de procéder à une évaluation par les pairs. Ces mesures doivent être prises dans le cadre de l'analyse des coûts. L'objectif recherché n'est pas la perfection, mais une application cohérente des bonnes pratiques de gestion des risques.

Mesures à envisager

- Prévoir et défendre - Prévoir les défauts permet de lutter contre les dégâts, de développer la résilience du système, de se relever rapidement d'une panne, de préserver la confidentialité des données et d'élaborer des plans de notification et de relations publiques.
- Définir le normal pour identifier l'anormal - Pour suivre les défauts inconnus, on peut développer une heuristique en mesure de détecter des codes ou des activités inhabituelles.



In the end, the solution lies in the following 3 step approach:

- Gather intelligence from variety of sources. ICT function must monitor the internal and external environment and enrich and correlate data from both types of sources in order to understand both environments. This calls for scanning, logging, and other monitoring capabilities.
- Transform that intelligence into actionable information. ICT function must analyze the data it gathers in order to perform threat trending and prediction, identify compromised devices, and assess business partners' security, spot information that has left or is leaving the organization — among other tasks.
- Operationalizing security so it can act on the information. ICT function must have the resources needed to protect the organization from threats, respond to incidents, and support business units and functions before, during, and after exposure to risks. ICT must enable business processes that depend on IT while protecting them.

By

Joseph GOMBE

Senior Internal Auditor



- Etre vigilant - Développer une métrologie de référence et une sensibilité situationnelle à l'activité du réseau et être attentif à toute augmentation brusque des destinations du trafic.

2.0 Conclusion

Il faut du temps pour évoluer - commencez donc maintenant

Bien qu'on ne puisse sans doute pas suivre le rythme des mutations de notre environnement, les dirigeants d'entreprise doivent inciter leurs services informatiques à accélérer leur évolution. Le rythme et l'orientation de cette évolution devraient être dictés par la valeur de l'actif, la dépendance de l'organisation vis-à-vis de ce dernier, les risques y afférents et les capacités sécuritaires existantes. Le processus devrait commencer par l'évaluation de la valeur de l'information, des systèmes informatiques et des menaces et par l'affectation des ressources qui en découle.

In fine, la solution passe par les 3 étapes ci-après:

- Collecter des informations auprès de diverses sources - Les services informatiques doivent suivre l'environnement interne et externe et enrichir et rapprocher les données obtenues des deux types de source pour comprendre les deux environnements. Cela suppose des capacités dans les domaines du scanning, de l'enregistrement chronologique des données et d'autres capacités de suivi.
- Transformer les informations collectées en informations utiles - Les services informatiques doivent analyser les informations collectées pour déterminer les tendances des menaces et les anticiper, identifier les outils compromis et évaluer la sécurité des partenaires d'affaires et identifier les informations qui sont sorties de l'organisation ou en sortent, etc.
- Rendre la sécurité opérationnelle pour qu'elle puisse agir sur l'information - Les services informatiques doivent disposer des ressources voulues pour protéger l'organisation contre les menaces, réagir aux incidents et appuyer les autres services avant, pendant et après l'exposition à un risque. Les services informatiques doivent mettre en place des procédures dépendantes de l'informatique et protéger ces procédures.

Par

Joseph GOMBE

Auditeur interne principal



African Reinsurance Corporation

Société Africaine de Réassurance

33 Boulevard Moulay Youssef
Casablanca
Morocco

Tel: (212-2) 22 43 77 00
Telex: 28079 M
Fax: (212-2) 22 43 77 29
E-Mail: casablanca@africa-re.com

7th ELKHALILY St,
Plot 1149 Massaken Sheraton,
Heliopolis
Cairo
Egypt

Tel: (202) 22 685 668
Fax: (202) 22 685 667
E-Mail: cairo@africa-re.com

Rue Viviane
A24 - Cocody Ambassade
20 BP 1623
Abidjan 20
Côte d'Ivoire

Tel: (225) 22404480/1
Telex: 22345 AFRE CI
Fax: (225) 22 40 44 82
E-Mail: abidjan@africa-re.com

AFRICA RE
Plot 1679 Karimu Kotun Street
Victoria Island
P.M.B. 12765
Lagos, Nigeria

Tel: (234-1) 266 3323, 262 6660-2
618820
Fax: (234-1) 2663282, 2626664
E-Mail: info@africa-re.com
Website: www.africa-re.com

Africa Re Centre
Hospital Road, Upper Hill
P.O. Box 62328 - 00200
Nairobi
Kenya

Tel: (254-20) 2730660-3
Telex: 23289 AFRICARE
Fax: (254-20) 2724896/2730608
E-Mail: nairobi@africa-re.com



11th Floor, One cybercity,
Ebene
Mauritius

Tel: (230) 454 70 74
Fax: (230) 454 70 67
Email: p.louis@africa-re.com

2nd Floor (West Wing)
Oakhurst Building
11-13, St. Andrew's Road
Parktown 2193
Houghton 2041
Johannesburg
South Africa

Tel: (27-11) 484 3764
4841970/1606
Fax: (27-11) 484 1001
E-Mail: africare@africa-re.co.za