Association suisse de la sécurité de l'information
Clusis
Rapport annuel d'activité et de gestion à l'assemblée générale 24 avril 2012

L'association suisse de la sécurité de l'information, Clusis

L'association suisse de la sécurité de l'information est un lieu d'échange à l'intention des personnes qui ont déjà suivi une des nombreuses formations actuelles proposées à l'EPFL, dans les HES ou dans les Universités ainsi qu'à celles qui bénéficient d'une expérience acquise dans les organisations.

Les activités du Clusis par des conférences, des ateliers et des témoignages aide à la consolidation des concepts théoriques et méthodologiques et facilitent la mise en oeuvre dans les organisations. L'expérience transmise par la présentation de cas réels, enrichis par des exposés de l'état de l'art est encore augmentée par l'échange avec les participants qui ont eux aussi une grande expérience.

Par ses activités, ses membres et leurs compétences réunies, le Clusis se positionne comme organisme de référence en matière de sécurité de l'information, de cybersécurité et de toute activité dans ce domaine.

Le Clusis, association suisse de la sécurité de l'information consolide sa position privilégiée d'échanges d'expériences et de compétences au bénéfice des membres de l'association.

Tout au long de l'exercice, le comité a développé ses activités dans le but de réaliser un programme en réponse à vos attentes et en prévision de vos besoins futurs.

L'association suisse de la sécurité de l'information

En 2012 à ce jour, 114 personnes dont 1 étudiant et 140 organisations font partie du Clusis.
Au total 254 personnes ou organisations (219 en 2011) soit une augmentation de 15.9 %.

Les conférences passées:

La Protection des données dans les nuages!
Cloud computing: sécurité et confidentialité en péril? 12 avril 2011, Lausanne

La conférence, après l'assemblée générale, met en regard les missions et leurs applications du Préposé fédéral Pierre-Yves Baumann et des Préposées genevoises Isabelle Dubois et Anne-Catherine Salberg à la protection des données et à la transparence et les perspectives du Cloud computing présentées par Olivier Leclère, collaborateur scientifique, HEG Ge.
Responsable de projets de sécurité à l'Etat de Genève, Enrico Viganò insiste sur les freins à l'utilisation des services Cloud et le besoin de contrat et de conditions d'utilisation.
Le responsable du Département Services, hôpital fribourgeois (HFR) Marc Devaud, présente la mise en pratique des droits d'accès sur un système d'information médicales à l'HFR.
93 participants.

Cybersécurité en Suisse. Rôle de l'Etat et les attentes des PME. 27 mai à Genève
en collaboration avec le GRI

Des conférences de haute tenue
Cyber menaces des entreprises et rôle de l'Etat, Nicolas Arpagian, auteur, rédacteur en chef du magazine «Prospective Stratégique» et directeur scientifique du cycle «Sécurité Numérique».
- Quels sont les risques pour les entreprises?
- Les états peuvent-ils jouer un rôle dans ce nouveau territoire?

Mise en place d'une stratégie nationale de Cyber Défense, Gérald Vernez, Directeur suppléant du projet Cyber Défense au Département fédéral de la défense, de la protection de la population et des sports (DDPS).
- A quelles menaces sommes-nous confrontés? S''agit-il vraiment que d''informatique?
- Qui est touché / concerné par cette menace? Y a-t-il une séparation à faire entre les mondes civil et militaire?
- Qui doit faire partir de la solution? Est-ce uniquement une question nationale?
- Comment tout cela va-t-il évoluer? Les solutions d'aujourd'hui seront-elles encore valables demain?

Des ateliers pour apprendre à faire:
Les ressources humaines comme levier pour la sécurité de l'information. Claudia Saviaux Druliolle et Sebastian Lopienski.
Chacun est responsable de la sécurité des données au sein de l'entreprise. Comment mettre en œuvre ce concept très souvent entendu, pas souvent vérifié?

La gestion du changement dans l'environnement IT, facteur d'insécurité. Thierry Wohnlich et Katja Rupp
L'environnement IT des entreprises subit des changements continuels: évolutions, modifications de l''environnement, obsolescence etc.
Ces changements sont des facteurs majeurs d'insécurité, à moins qu'ils ne soient opérés avec diligence. Est-ce toujours le cas? Nous traiterons ce sujet sous un angle pragmatique et nous dresserons les points critiques à maitriser pour garder le contrôle dans ce monde si évolutif.

Externalisation des développements, cloud computing et SaaS. Quelles mesures pour réduire les risques à la signature du contrat ?
Antonio Fontes
Les applications web sont actuellement la première cible dans la grande majorité des attaques informatiques recensées — 75% selon Gartner. L'objectif de ce workshop sera, d'une part, d'éveiller la sensibilité des participants aux différents scénarios de risque induits par l'externalisation des processus de développement ou d'hébergement (développement offshore, location SaaS, déploiement en environnements cloud computing, etc.). En second lieu, nous observerons les différents outils (tels que le Secure Contract Annex) mis à disposition par l'OWASP pour optimiser l'intégration de la sécurité déjà lors du l'établissement du contrat.

Résultats compilés sur la base des autoévaluations des participants
env 65 participants.

Data Loss Prevention, 13 septembre 2011, à l'IDHEAP, Chavannes-près-Renens.

Avez-vous identifié quelles sont vos informations les plus précieuses selon la classification propre à vos activités? Et savez-vous comment les sécuriser en conséquence? Le Clusis vous propose pour la rentrée une discussion animée par un panel de spécialistes de renom à qui vous pourrez soumettre vos questions.

DLP et DRM: Enjeux, défis et opportunités pour la protection et le contrôle de l'information
Jean-Henry Morin (HEC) - Professeur Associé, Institute of Services Science (ISS), HEC Genève, Univertisé de Genève
A l'ère de l'entreprise virtuelle étendue et du cloud computing, la protection et le contrôle de l'information (IPC) représente un enjeu de plus en plus critique pour les organisations. Dans ce contexte, les technologies DRM de protection persistantes offrent des perspectives complémentaires intéressantes mais présentent aussi des limites dans leurs approches traditionnelles. La question de la confiance y joue un rôle important méritant discussion et permettant d'envisager de nouvelles opportunités.

La valeur d'une démarche d'audit pour la protection des données critiques.
Jürgen Müller (PwC), Partner - Swiss Territorry Leader of Risk Assurance
Dans quelle mesure une démarche d'évaluation et de contrôle d'une situation courante, d'un projet en cours ou d'une situation de crise peut aider les organisations à protéger les données sensibles et critiques.

Pistes de réflexion pour une approche holistique à la protection des données critiques.
Fabien Mooser (PwC), CISA, CISM - Manager OneSecurity, Risk Assurance
Discussion et réflexion autour de l'intégration de la protection des données critiques dans les dimensions structurelles de la sécurité des systèmes d'information et évaluation de l'impact des contraintes environnementales sur cette intégration.

Aspects juridiques relatives au stockage et à la protection des données.
Carole Aubert (FHS), Avocate, DEA en droit, sécurité et criminalité des nouvelles technologies, avocate indépendante et responsable de la lutte anti-contrefaçon sur Internet à la Fédération de l'industrie horlogère suisse.
Le stockage des données recouvre de nombreux aspects juridiques: hébergement externe/interne et externalisation des risques, assurances, protection des

données, problèmes transfrontaliers, responsabilité en cas de perte des données, etc.

Démonstration **Symantec DLP**, Manuel Wolf, Symantec Corporation: une solution DLP doit non seulement protéger les informations essentielles de votre organisation, mais encore le faire de manière contextuelle. Il s'agit de trouver un bon équilibre entre la sécurité et la productivité. Présentation d'exemples concrets de gestion de l'information sécurisée.
80 participants.

Gestion des identités numériques – Bas les masques ! 11 Octobre 2011 au CTI, Genève

L'anonymat qui a longtemps prévalu sur Internet, n'est-il pas en train d'être relégué définitivement au nombre des utopies ? A travers l'utilisation croissante des médias sociaux et de la multiplication des contenus générés par l'utilisateur, on s'expose et on s'exprime de plus en plus sur le web. Par contrecoup, la question de l'identité numérique et de la gestion des multiples représentations d'un individu qu'elle regroupe devient centrale. Dans l'univers Internet, notre identité se forge à partir des traces que nous y laissons, mais aussi à partir de ce que les autres disent et publient sur nous, ce qui rend identité et réputation numériques **difficilement contrôlables**.
Une identité numérique multiple, mais également active et dynamique, Jacqueline Reigner et Enrico Viganò
A l'image de l'ADN, l'identité numérique permet de stocker des informations spécifiques à l'internaute et de les transmettre au fil du temps avec la plus grande fidélité possible. Cependant, elle peut se modifier au cours du temps car l'identité numérique est active : elle est changeante, mobile, expressive, négociable, valorisable. L'identité numérique est aussi plurielle : un internaute possède plusieurs représentations de lui-même, pseudonymes ou avatars (l'identité est alors dans ce dernier cas entièrement virtuelle). Elles coexistent dans trois sphères : **personnelle, professionnelle et administrative**.
Ainsi la maîtrise de l'identité numérique nous concerne tous, **individus** comme **entreprises et administrations publiques**, ne serait-ce que pour des questions de notoriété et de valorisation de cette notoriété.
Exemple d'une administration :
Vers une Gouvernance des Identités Numériques et des Accès (GINA) : L'approche du Canton de Genève basée sur le modèle ORFAG, présentée par :
Roland Burgniard, responsable du service Sécurité du Centre des Technologies de l'Information de l'Etat de Genève, diplômé d'un MBA et d'un MAS spécialisé en management de la sécurité des systèmes d'information,
et **Damien Rigoudy**, ingénieur sécurité au sein du service Sécurité du Centre des Technologie de l'Information, responsable de l'évolution de l'infrastructure de sécurité de l'Etat de Genève.
Roland Burgniard a déjà conçu et mis en place avec son équipe une solution globale de gestion des identités et autorisations (GINA) qui répond aux besoins des divers métiers qui composent l'Etat de Genève et également de ceux des administrés dans le cas de l'Administration en Ligne (AeL)
Dans les Universités et Hautes Ecoles, comment ça se passe?
Les solutions retenues par SWITCH : AAI - Shibboleth, présenté par
Lukas Hämmerle, software engineer in the Middleware team of SWITCH, developing and operating the SWITCHaai infrastructure, graduated at ETH Zurich as M.Sc. in Electrical Engineering und Information Technology.
Since 2005 SWITCH has coordinated and operated a Shibboleth-based federated identity management infrastructure called SWITCHaai. It allows more

than 300'000 Swiss Higher Education users to access services inside and outside their organisations using one single digital identity.
62 participants.

Fraudes et malversations: Pas chez moi! Pas dans ma banque!
Analyse des traces d'activités. 15 novembre 2011, à l'HEPIA, Genève

Tous les systèmes d'informations génèrent de nombreuses traces d'activités. Comment les exploiter? Qu'avons-nous le droit d'enregistrer dans le respect de la sphère privée?

David Billard (Prof. Digital Forensics, HEG): Besoins en traçabilité numérique
Dans le cadre d'une investigation judiciaire, les traces numériques collectées deviennent des éléments de preuve auprès des juridictions. Mais qu'en est-il des traces numériques en dehors du cadre judiciaire, par exemple lorsqu'une organisation est confrontée à un employé indélicat, ou à une cyber-menace ?
Tous les systèmes d'information génèrent de nombreuses traces d'activités. Quelles informations pertinentes véhiculent-elles ? Peut-on ou doit-on légalement les conserver ? À quoi peuvent-elles servir ? Dans un contexte particulièrement mouvant et sensible, comment intégrer les technologies SIEM (permettant la capture et la gestion des traces d'activités) ?

Ben Musso, Executive Director, Head of Information Technology - Banque Reyl et **Sacha Mertenat,** Managing Director, Chief Risk Officer (CRO à partir de Basel III) - Banque Reyl.
Besoins en matière de contrôle des risques opérationnels.

Joël Winteregg, CEO-CTO NetGuardians SA: De la trace d'activité à la solution de Risk Mitigation.
Comment les traces d'activités permettent-elles de combattre les risques humains et responsabiliser ses collaborateurs. Quelles solutions sont à disposition et quels sont les pièges à éviter.

Lisa White, Directrice-adjointe, Deloitte SA, Traçabilité VS sphère privée
Du point de vue légal, quels sont les points critiques à respecter.

Journée stratégique
La cybersécurité dans 5 ans, 27 janvier 2012

Une réflexion sur l'avenir pour imaginer l'évolution de la sécurité de l'information et de la position du RSSI et prévoir ce que le responsable d'organisation / d'entreprise doit entreprendre dans les prochains 5 ans pour être prêt à surmonter les cyber-risques.
Un panel de conférenciers de talents développera une réflexion pour approcher la résilience des organisations d'une autre manière.

Jean-Marie Leclerc, ancien DSI Etat de Genève veille / observatoire technologique

Professeure Solange Ghernaouti-Hélie, HEC Université de Lausanne: Approche prospective de la cybersécurité et intelligence économique.

Gérald Vernez, Directeur suppl, du projet Cyber Défense, SG DDPS: Point de situation: la stratégie de la Confédération est déposée / acceptée par le Conseil Fédéral. Quid pour les 5 prochaines années.
« Quelles conditions cadres pour parvenir à l'état final dans 5 ans ? » (finances, sensibilisation, structures de direction de l'entreprise, personnel, etc.) car finalement les responsables de systèmes d'information devront apprendre à négocier différemment et plus intensément avec leurs partenaires de l'entreprise, de les convaincre.
« Sûreté de l'information dans l'entreprise et sécurité intégrale » ou comment faire comprendre aux uns et aux autres que dans 5 ans cette convergence devra impérativement être entrée dans les mœurs et qu'on ne pourra plus séparer les thèmes de sécurité.

Le Clusis reçoit le GREPSSI, groupe de réflexion de d'échange sur les problématiques liées à la sécuritédes systèmes d'information, **Jean-Yves Oberlé** et le CRIP ITO, club des responsables infrastructure et production, **Patrick Grogniet**, lancement en 2012.

Perspective: **Xavier Comtesse**, Avenir Suisse.

Atelier des praticiens: animé par **Johny Gasser**, Orange business services et Jean-Yves Oberlé SARAPIS Sécurité des SI
RSSI 2016 Soyons prêts
Se préparer aux défis et challenges actuels et à venir du RSSI.
Des éléments clés seront présentés et suivis d'un échange d'idées, de discussions et débats autour des moyens, méthodes et techniques pour réussir dans son entreprise.
Débat avec les sociétés de services en cybersécurité et Jean-Yves Oberlé et Charles-André Roh.

Ateliers Génération Y:
animé par **Giorgio Pauletto**, Observatoire technologique, Etat de Genève
Ils ont grandi avec la révolution digitale des années 90, alors que le web voyait le jour. Nous les cherchons partout, mais ils sont déjà parmi nous: ce sont nos enfants, nos voisins, nos amis et aussi... nos collaborateurs. Dites bonjour à la génération Y des natifs digitaux. Ils sont à l'aise dans le monde du Net et leur approche de celui-ci est différente, ils utilisent plus les SMSet les réseaux sociaux que l'email ou les outils classiques qu'on leur propose. Inutile d'interdire l'usage

de leurs sites favoris, ils sont de toute façon connectés par leur téléphone et leur ordinateur portable. Ils arrivent en masse comme les utilisateurs de nos organisations, de nos entreprises, de notre société. Mais sont-ils si différents que les stéréotypes des médias veulent bien nous le faire croire? Leurs approches sont-elles une opportunité ou un risque pour les entreprises?
Après une présentation de quelques tendances fondées sur des recherches dans le sujet, nous travaillerons ensemble sur les questions suivantes:
Comment bénéficier des capacités des nouvelles générations tout en préservant la confidentialité?
Quelles initiatives mettre en place pour répondre aux besoins sans pour autant mettre en péril l'information de mon organisation? Et... par quoi allons nous commencer?

Atelier marketing: **Nathalie Nyffeler**, Professeur HEIG-VD et **Sebastian Lopienski**, Chief, Deputy Computer Security Officer, CERN.
Comment vendre un projet impossible en entreprise. Une situation que les RSSI connaissent bien.
Conclusions et synthèse des résultats des ateliers
120 participants.

SCADA : Sécurité des infrastructures critiques et systèmes de contrôles, 13 mars 2012, CHUV, Lausanne

Selon l'Office fédéral de la protection de la population (OFPP) "La Suisse dépend largement du fonctionnement de ses infrastructures critiques. Ces dernières assurent la disponibilité de biens et prestations indispensables, tels l'énergie, les communications et les transports. Les défaillances d'infrastructures critiques ont en règle générale de lourdes conséquences pour la population et l'économie, et peuvent, par effet de dominos, s'étendre à d'autres infrastructures, elles aussi critiques", dans les secteurs : Finance, Santé publique, Industrie, Technologies de l'information et de la communication (TIC), Alimentation.
Après l'apparition de Stuxnet en 2010 et Duqu en 2011 (des malware conçus pour s'en prendre à des systèmes de contrôle utilisés dans l'industrie et les infrastructures critiques), beaucoup de personnes impliquées dans le développement, la maintenance et le fonctionnement de ces systèmes de contrôle et de commande à distance, savent qu'ils doivent prendre en compte le risque lié au cybercrime pour assurer le bon fonctionnement des installations et la continuité de la production et des prestations de service.
Le Global Risks Report 2012 du World Economic Forum, qui analyse les 50 principales menaces globales pour les 10 prochaines années et les classifie par rapport à l'impact et à la probabilité, place le cybercrime en tête des risques technologiques.
Pour développer cette problématique nous avons invité un expert renommé du Clusit, qui depuis des années participe à de nombreux groupes de travail nationaux et européens en la matière et un expert réputé de SCADA (Supervisory Control And Data Acquisition) et de la sécurité des systèmes de contrôle dans l'industrie et les infrastructures, le Computer Security Officer, Head of Computer Security, du CERN.
Jeremy Kenaghan, Responsable Sécurité des Systèmes d'Information, CHUV
Ouverture et bienvenue au CHUV
Fabio Guasconi, Graduated in Computer Sciences at Turin's University, @Mediaservice.net S.r.l.
Standards and regulations for critical infrastructures security
Global overview on international and national standards, on applicable laws and regulations regarding the security of the most relevant types of critical infrastructures. Hints for a specific and effective application of those elements are

provided in order to synergically promote the achievement of a security level adequate to face the continuous evolution of threats within the global scenario.
Stefan Lueders, Computer Security Officer, Head of Computer Security, European Organization for Nuclear Research
Why Control System Cyber Security sucks ?
Control system cyber-security is now around for more than a decade, but got appropriate (or even exaggerated?) attention only recently due to the Stuxnet worm attacking Siemens PLCs. Despite all the concerns from know-it-all IT security experts, securing today's commercial-off-the-shelf control system is far from being easy. Still too many control systems are designed without security in mind, lack basic security protections, or arenot even robust enough to withstand basic attacks. While embracing standard IT technologies, only few manufacturers also apply good security practises. And (too) few customers ask for it. On the customer side, a change of mind is necessary, too: control system cyber-security must become fundamentalingredient when running a plant. This presentation shall recap the current situation and outline why the presenter is still waiting for a change in paradigm: Control systems must not only embrace IT technology but also thoroughly apply standard IT security measures: timely patching, deployment of anti-virus software, integration of personal account and fine-grained access control, elevated robustness and resilience of control devices, and free information sharing between all stakeholders…
70 participants

Management de la continuité d'activité : Le Jour après.
22 mars 2012, Banque Gonet, Genève

Prendre des risques est le fait des entrepreneurs. C'est leur métier!
Gérer les risques opérationnels et préparer à temps un cadre de résilience permettra aux plus avertis de résister à la prochaine catastrophe informationnelle. Le management de la continuité des activités MCA est une approche privilégiée par les institutions normatives de référence et les entrepreneurs responsables. Le MCA prépare la continuité des activités essentielles en cas de sinistre majeur. Le témoignage d'une entreprise industrielle phare et la présentation des approches méthodologiques animeront la réflexion sur ce sujet primordial.

Afin de partager nos expériences et dans la perspective de la constitution d'un groupement d'intérêt romand, que nous désirons profiler comme véritable centre de ressources et d'échanges, le Clusis a le plaisir de vous convier à un petit déjeuner qui entend aborder, dans la convivialité et le dialogue, l'ensemble des aspects, tant théoriques que concrets, liés aux meilleures pratiques.
Nous traiterons ensemble, un florilège de thématiques de la continuité, depuis ses fondations organisationnelles jusqu'aux architectures utilisées pour assurer la continuité des systèmes d'informations.

« Memento mori », Souviens-toi que tu es mortel - Alfredo Sanchez, MIS Director chez KBA-NotaSys, Lausanne
Plan de continuité des activités et Disaster recovery – démarche et mode d'emploi - Henri Haenni, Associé & Senior Consultant, ardantic SA, Lausanne
Architectures de continuité d'activité - Jeff Primus, Associé & Senior Consultant, ardantic SA, Lausanne
Conclusion et lancement du groupement romand en Management de la Continuité d'Activité
41 participants.

Information informelle : comment en tirer parti? Hélène Madinier, Professeur HES, 24 avril 2012, SIG Genève.

Par définition, l'information informelle n'a pas de forme, pas de support, c'est volatile: c'est ce qui est échangé, verbalement, par téléphone…Or dans un contexte de veille, c'est souvent une information stratégique… si on sait en tirer partie. Et dans un contexte de gestion des connaissances, c'est justement ce qui constitue le savoir tacite, implicite, qui correspond à ce qui s'échange autour de la machine à café… et qui est particulièrement utile à partager pour une organisation. On verra autour de plusieurs retours d'expérience –notamment l'utilisation d'un RSE ou réseau social d'entreprise- comment « traquer », comment formaliser simplement cette information informelle pour en faire un avantage compétitif et une organisation apprenante.
Anthony Poncier, Lecko, expert en organisation et nouvelles technologies à Paris: Comment favoriser l'intelligence collective avec les réseaux sociaux d'entreprise.
Atelier par **Patrick Quinlan,** Cargill, **Hélène Madinier**, HES, **Anthony Poncier,** Lecko : La variété des outils capables de stimuler l'échanges et le partage des connaissances afin de délivrer une vraie création de valeur grâce à l'intelligence collective laisse encore nos organisaitons perplexes. Entre la peur de partager son know-how et la crainte de perdre son pouvoir et sa position, comment l'entreprise favorise-t-elle la création de valeur collective? Un atelier de travail pour lever quelques pistes et avancer d'un pas dans l'intégration des connaissances partagées par tous les acteurs.

Le Clusis soutien d'autres organismes et participe à leurs activités:

OWASP,Yverdon lors du Security Day

Moutier, Jurhacker Fest

Centre de compétence en Management de la continuité des activités

Un groupe de personnes impliquées professionnellement dans ce domaine s'est constitué avec comme objectif de produire un support de sensibilisation à l'intention des décideurs non informaticiens.

Leadership **Enrico Viganò**, Etat de Genève

Sous-Groupe "Utilisateur"

Le désir grandissant de partage d'expériences qui demeure jusqu'alors insatisfait au sein des structures d'accueil de groupes d'utilisateurs existants et dont la vocation est l'échange d'expérience entre des professionnels de la sécurité de l'information.

Caractéristiques :
Ce sous-groupe n'est aucunement un terrain de prospection. Il est en revanche un lieu de prospective.

Les membres qui se sentiraient importunés par des démarches commerciales le feront savoir afin que des mesures adaptées soient prises.
La confidentialité des informations échangées doit être respectée.
La participation active suppose que chacun assiste et s'implique dans les réunions et ateliers qui s'organiseront.
Ses membres s'engagent à respecter l'éthique du groupe et les principes de fonctionnement édictés dans la charte.
Leadership **Cédric Gaudard**, ELCA
En cours de constitution

Publication Arttesia

Une publication est en préparation avec l'appui logistique des éditions Arttesia.
Collection de 10 articles, de 20 pages chacun, declinés des conférences annuelles du Clusis, dont la valeur ajoutée réside sur l'approfondissement du contenu par le conférencier / auteur de l'article
Offert aux membres du Clusis et vendu auprès des libraires de Suisse Romande.
Y compris droits d'auteur.

Comité 2012-2013

Le comité 2012-2013:
Jacqueline Reigner, Présidente - Sémafor Conseil SA
Enrico Viganò, Vice-Président - Etat de Genève
Christophe Bouillard - Rolex
Christian Buchs - HEIG-VD
Stephan Conradin - consultant indépendant
Gaëtan Derache - HES Genève
Martin Dion - Banque Ming
Paolo Giudice - Cisca
Brian Henningsen - Banque Gonet
Bertrand Lathoud - Paypal
Kenza Majbar - Swissquote
Jean-Luc Pillet - Université de Genève
Matthieu Schaeffler - Etat de Genève
Igli Tashi - PWC
Sam Vuilleumier - Etat de Vaud

Activités du comité

La Présidence et les membres du comité ont pris une part active dans l'organisation des conférences et des centres de compétences tant par les moyens électroniques modernes, que par de nombreux téléphones entre deux activités professionnelles et par des réunions de travail autour d'un déjeuner rapide.
Le comité a de plus participé à des journées complètes de travail le 1er octobre 2011, le 14 janvier 2012 et le 14 avril 2012.
La Présidence a également organisé le travail administratif et financier avec les soutien de la fiduciaire Roubaty.

Rapport financier

En résumé, le bilan de l'association présente un total de CHF 171'199.-
Les fonds propres sont de CHF 152'853.55 et le résultat 2011 est un excédent de charges de CHF 14'290.78.

Les produits, essentiellement des cotisations, s'élèvent à CHF 80'356.83.-
Le montant consacré à l'organisation des manifestations est de CHF 22'744.20 pour un total des charges de fonctionnement de CHF 84'118.71 (voir le rapport de la fiduciaire Roubaty).

Au programme 2012-2013

12 juin 2012	Mobile security
4 septembre 2012	Sécurité dans le domaine de la santé
9 octobre 2012	Médiation informatique, déontologie
13 novembre 2012	Test de résilience des systèmes d'information
25 janvier 2013	Journée stratégique: La gestion de crise, à Lausanne
12 mars 2013	Investigation, recherches de preuves,
16 avril 2013	Assemblée générale 2013 --- analyse d'un événement exceptionnel
24 janvier 2014	Journée stratégique: Intelligence économique et veille stratégique

Le 24 avril 2012

Jacqueline Reigner, dr ès sciences
Présidente

Enrico Viganò
Vice-Président