Supported by

Cyber Security in the Financial Industry

The SWIFT Institute and the KU Leuven will host a one day conference focusing on cyber security issues impacting the global financial industry.

Today's cyber threat is a very real and persistent one. Cyber-attacks are growing ever more sophisticated, and the landscape is becoming increasingly complex. As cyber criminals become better organised and funded, there are also state actors focussing both on snooping and disruption. Cyber security is the issue that keeps most CEOs awake at night, not least of which in the financial industry.

Cyber threats to the financial industry are not only external, but also internal. Amongst all reported cybercrimes, those committed by malicious insiders in financial services are amongst the most significant threats to networked systems and data. Financial institutions face the ongoing challenge of securing legacy systems that are linked together in an often less than ideal way. Online banking has become commonplace, whilst new digital currencies are regularly appearing (but little understood). In the post-Snowden world, cyber security has never been more crucial.

At a country and regional level cyber security is taking centre stage (e.g. the European Union's Cyber Security Strategy). In the world of cryptography, new developments are appearing aimed at protecting your data. What more can and should be done? What do you need to do to protect your financial institution?

In this one day event you will hear from and have the opportunity to engage with leading cyber academics and experts from the financial and technology industries as well as those involved in law enforcement.

We will end the day with a cocktail, and for those interested in playing, a role-play board game designed to increase awareness of cyber-security risks and the measures you can take to protect your company.

We look forward to seeing you in Belgium in November.

Peter Ware
Director, SWIFT Institute

Professor Bart Preneel
Department of Electrical Engineering-ESAT/COSIC (Computer Security and Industrial Cryptography) – KU Leuven

Date: 19 November 2014

Venue: Chateau du Lac, Avenue du Lac 87, B-1332 Genval (Brussels), Belgium

Register Now! https://b-com.mci-group.com/Registration/SWIFTINST.aspx

Agenda

08:30 – 09:00	**Welcome Coffee & Registration**
09:00 – 09:15	**Welcome Address** • **Gottfried Leibbrandt**, Chief Executive Officer, SWIFT and Advisory Council Member, SWIFT Institute
09:15 – 10:00	**Keynote Speech - *Mitigating the Insider Threat to the Financial Industry*** *Chris Hurran will discuss insider threats to the financial industry, looking at both malicious and non-malicious threats, and beyond. Whilst today's cyber threats are ever increasing, there is light at the end of the tunnel. Chris will share practices and methods by which these threats can be mitigated.* Chris Hurran is a Senior Associate Fellow at University College London. He was awarded the *Order of the British Empire* (OBE) as a result of his more than 45 years of public service in the British Royal Engineers, the Diplomatic Service, NISCC (National Infrastructure Security Coordination Centre) and CPNI (Centre for the Protection of National Infrastructure). In NISCC Chris led all aspects of contingency and crisis management planning. In CPNI he was responsible for the delivery of research based guidance and tools on personnel security issues. He has particular expertise in counterproductive workplace behaviour, organisational culture and the management of employee risk. • **Chris Hurran OBE**, Senior Associate Fellow, Institute for Security and Resilience Studies, University College London
10:00 – 11:00	**Malicious Insider** *Amongst all reported cybercrimes, those committed by malicious insiders in financial services (more than 50% of all cybercrimes) are amongst the most significant threats to networked systems and data. Much of the existing academic research and professional literature focuses on how to detect and prevent cybercrimes based on past crime patterns. A quantitative forecast on the cost impact of cybercrimes is still a challenging task. This session will feature a presentation of new research, sponsored by The SWIFT Institute, which aims to formulate a predictive cybercrime cost model that can be applied to malicious insider attacks within a financial institution.* **Presentation**: • **Vincent Lee**, Clayton School of Information Technology, Monash University **Panel**: • **Richard Benham**, Professor of Cyber Security Management and founder of The National MBA in Cyber Security ®, Coventry University • **Chris Hurran OBE**, Senior Associate Fellow, Institute for Security and Resilience Studies, University College London • **Vincent Lee**, Clayton School of Information Technology, Monash University • **Moderator**: **Mike Loginov**, Chief Strategist, EMEA Public Sector - Cyber Security & CTO Strategy Group, HP Enterprise Security
11:00 – 11:30	***Networking / Coffee Break***

11:30 – 12:30	**Crypto Developments** *Cryptography plays a central role in securing both retail and wholesale financial systems. Cryptographic methods allow for new technological developments that present exciting business opportunities, but in the next decade our cryptographic technologies face major challenges. First, the security of the public key algorithms in use today depends on the assumption that a small set of problems from algebraic number theory is hard; a breakthrough in mathematics or in the development of large scale quantum computers could undermine their security. Second, cryptographic implementations and in particular implementations of random number generators have proven to be less robust than initially believed. Finally, the Snowden revelations have shown that governments have deliberately undermined cryptographic standards, resulting in new threats. This session will offer a perspective by leading experts on the cryptographic challenges faced by the banking industry, in the format of three brief presentations followed by a panel session.* **Presenters & Panellists**: • **Daniel Bernstein**, Professor, Department of Mathematics and Computer Science, Technische Universiteit Eindhoven • **Richard Horne**, Partner, Cyber Security, PwC • **David King**, Vice President and Head of Key Management Services, MasterCard • **Moderator**: **Professor Bart Preneel**, Dept. Electrical Engineering-ESAT/COSIC (Computer Security and Industrial Cryptography), KU Leuven
12:30 – 13:30	***Lunch***
13:30 – 14:30	**Organic Security versus Security by Design** *Banks have legacy systems, quite often multiple legacy systems that are decades old. Evolving business streams, mergers and acquisitions result in many firms having a 'spaghetti of systems'. The cost and risk of replacing legacy systems often outweighs the benefits of replacing them with something new and improved. This presents challenges from a cyber-security perspective, as many banking platforms were designed at a time when cyber-security was not an issue. Protecting these systems requires a significant amount of cost and effort. How does this compare to firms who have designed their own new operating platforms? Does a new system offer better protection than a legacy system, or are the cyber risks simply different? What lessons can be learned from each model? With cyber-security an increasingly important focus area, are we approaching a time when legacy systems must be replaced?* **Panel**: • **Ebbe Skak Larsen**, Chief Security Architect, Danske Bank • **Jo Basselier**, Head of IT Security Management, Euroclear • **Alain Desausoi**, CSO, Head of Enterprise Security & Architecture, SWIFT • **Moderator**: **Dr. Starnes E. Walker**, Founding Director, Cyber Security Initiative and Professor, Electrical & Computer Engineering, University of Delaware

14:30 – 15:30	**New Financial Products and their Security Vulnerabilities** *Just as the cyber landscape is forever shifting, so too does the financial industry itself. New financial products provide new opportunities for banks and clients alike, but by definition of being new, they can also present new and unknown security vulnerabilities. Virtual currencies, including digital and crypto currencies, are a prime example. In the news daily they are gaining acceptance through listings on exchanges and as a method of payment by mainstream retailers. Central banks, however, are wary of their use highlighting possible issues surrounding anonymity and anti-money laundering rules. How do new financial products compare to existing products in terms of their safety and security? Do new products such as virtual currencies provide more and easier opportunities for cyber criminals, or are they safer than the traditional financial system? This session will begin with a brief presentation aiming to explain what virtual currencies are…and what they are not.* **Presentation**: • **Sarah Meiklejohn**, Faculty, University College London **Panel**: • **Sarah Meiklejohn**, Faculty, University College London • **Elizabeth Petrie**, Director Strategic Intelligence Analysis, Citi • **Marcus Treacher**, Global Head of Innovation, Payments & Cash Management, HSBC • **Moderator**: **Richard Brown**, Executive Architect, Banking and Financial Markets, IBM
15:30 – 16:00	***Networking / Coffee Break***
16:00 – 17:00	**Supply Chain post-Snowden** *As CEOs continue to look for cost reductions and efficiency improvements, working with third party vendors to supply key products and services is often the best way forward. Why do it internally if you can outsource it to someone who can do it better and cheaper? Trust and security, however, become ever more paramount when you have to rely on someone else, especially as you are still ultimately responsible to your customers. Most financial institutions work with multiple vendors, resulting in a complex supply chain. The bigger the supply chain, the greater the potential for cyber-attacks. What can and should you be doing to protect your institution and your network of suppliers?* **Panel**: • **Mike Loginov**, Chief Strategist, EMEA Public Sector - Cyber Security & CTO Strategy Group, HP Enterprise Security • **Jacques Hagelstein**, Deputy CSO, Enterprise Security & Architecture, SWIFT • **Elizabeth Petrie**, Director Strategic Intelligence Analysis, Citi • **Moderator**: **Bryan Glick**, Editor-in-Chief, Computer Weekly

17:00 – 17: 15	**Wrap-up & Closing** • **Professor Bart Preneel**, Dept. Electrical Engineering-ESAT/COSIC (Computer Security and Industrial Cryptography), KU Leuven
17:15 – 19:00	***Networking Cocktail & Cyber-security Board Game****

*** All registered delegates will be contacted prior to the conference with more details on the Cyber-security Board Game, asking interested participants to pre-register to play the game. Those attending the networking cocktail are welcome to watch those playing the game.**