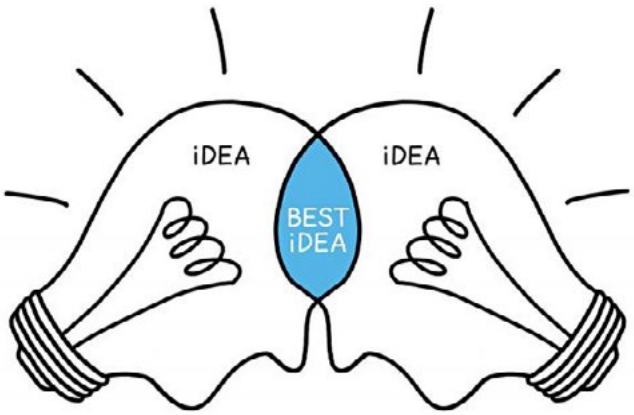
Premium Services Forum Europe

27–28 November 2017 | Hotel Okura | Amsterdam, Netherlands

WRAP–UP REPORT



Plenaries

READ MORE

Work session summaries

READ MORE

Shaping next year's event

READ MORE

Thank you!

READ MORE

Operations Collaboration Excellence

READ MORE

Links

PRESENTATIONS
(swift.com login required)

PHOTOS
(Smugmug)

OPENING VIDEO
(YouTube)

CLOSING VIDEO
(YouTube)

Operations — Collaboration — Excellence

Opening the Premium Services Forum 2017, Peter Benz, Head of EMEA Key Client Service Management, SWIFT welcomed the 147 participants from 65 institutions in attendance and ran through the programme for the event. In his opening remarks, he spoke about the importance of collaboration in the achievement of higher levels of operational excellence. Benz encouraged attendees to make the most of all of the data that is available nowadays in the financial industry, but to not lose sight of the big picture and the purposes that data is meant to serve. He also spoke about the importance of trust and of effective risk management.

Referencing the theme of the event, Operations – Collaboration – Excellence, he encouraged everybody to make the most of the time together to network and to exchange experiences and ideas. “My team of service managers and our Key Client Support Teams are ready to work with you on all of the challenges that you face within the SWIFT ecosystem. We hope you will enjoy your time at the Forum and that you will actively participate in the discussions,” he concluded.

Plenaries

How organised criminal gangs are trying to break into your company

Our guest speaker at PSF this year was Graham Cluley, an award-winning security blogger, researcher, podcaster, and public speaker. Cluley started by pointing out how much has changed since the days when 20 new viruses written every month and anti-virus updates were sent out on floppy disks every 3 months. Today, 400,000 samples of malware are released every 24 hours, 7 days a week, 365 days a year. That's one every 0.4 seconds.

Using examples, he showed some of the ways in which cyber criminals are trying to hack into companies. Starting with phishing email aimed at getting information, such as user credentials, Cluley warned the audience that "if you use the same password in multiple places, then once the hackers have the password for one thing, they have access to everything else." Phishing emails, Cluley explained, exploit human beings as the weak link.

"Many cyber criminals aren't geniuses. And they don't need to be. But as well as the individuals, there are organised criminal gangs, who are out to monetize, to gain access to intellectual property, Typically it's all about money and as the famous bank robber Willy Sutton, said "the banks are where the money is." So you, the banks, are the object of many attacks," said Cluley. "The ecosystem has really changed," he went on to say. "We now have organised criminal gangs. There's a whole industry out there, with networks of suppliers across the world, set up to potentially make huge amounts of money."

Other methods of attack covered were business email compromise and social engineering. Cluley set out how easy it is for someone to impersonate a figure of authority to get an employee to do something – such as transfer a large sum of money – in a way that does not comply with established processes and procedures. "Email is inherently insecure," he warned, encouraging attendees to pay careful attention to how they react to emails and explaining how easy it is for criminals to get employee details from LinkedIn and send an email that appears to come from a figure of authority such as the CEO.

Lastly, Cluley touched on the insider threat. "External hackers are a genuine threat but there is a comparable if not larger threat posed by your employees," he stated. Everyone who has access to company premises poses a potential threat – from employees, to cleaning staff and even security guards. Disgruntled employees can be inclined to harm the company by either committing criminal acts such as disclosing confidential data or by letting a criminal onto the premises. "You need to be very careful about insider threats," said Cluley. "You need to check that people are who they say they are. Challenge them. If you see something odd, let the security department know. There is so much that can be lost."

Cluley closed his speech on a positive note, praising the financial industry for its ability to set competition aside and collaborate to make things safer for everyone. "Events like this are an opportunity to build stronger, safer firms and help all of us benefit from a safer internet," he concluded.

The Human Factor: Managing the insider threat

Picking up where Graham Cluley had left off, the insider threat was the topic debated in the plenary session first thing on Tuesday morning. After introductory remarks by Diana Makienko of SWIFT, Andrew Muir, Head of Standards Development, SWIFT hosted a panel discussion with Elsine van Os, Founder and CEO of Signpost Six, Clinical Psychologist and Intelligence & Security Expert, Mark Camillo, Head of Professional Liability and Cyber, AIG, Nuri Fattah, Principal Security Consultant, FireEye and Werner Hellinckx, Head of Human Security, SWIFT.

Van Os said that whilst the insider threat has been out there for decades, what is different today is that employees have access to vast amounts of data that can be shared very easily with the outside world. This means a malicious insider can easily transfer millions of files and share information with the outside world through public fora such as Wikileaks. She said that most malicious insiders tend to be disgruntled employees with latent personality traits such as narcissism and stated that the average malicious insider is male and 37 years old.

Hellinckx pointed out that whilst malicious insiders are indeed part of the insider threat, another problem is the amount of information that can get out unintentionally. The use of USB sticks, taken home or left around was cited as one example, as well as mistaken email addresses. "Most information leakage is through USB sticks and mistaken email addresses – things done by mistake and unintentionally," he said. "Awareness training is always a good thing, but people need to realise that the measures we put in place are there for a reason."

Hellinckx went on to say that on the intentional side, companies need to be wary of contractors, employees on fixed term contracts, and youngsters who feel entitled and believe that everything they do for the company is their own personal property and they have the right to take it all out with them. So it is prudent to have stringent leavers' processes in place, for both employees and contractors. He also stressed that people are also a company's best protection. "You can put as many measures as you want in place but only a person can tell something that just doesn't smell right," he stated.

Fattah was of the view that awareness training is all good and well but that individuals actually need to be a victim of cybercrime to become fully aware of the potential consequences of not paying adequate attention to the risks. He also stressed that whilst technology serves a very worthy purpose, combatting cyber threats efficiently can only be done through a combination of people, process and technology. When it comes to running simulations, Fattah said that you have to put yourself in the mindset of the attacker and act like an attacker so that the simulations that you run are as realistic as possible.

Camillo pointed out that the insurance industry has a lot of good information but that cyber insurance is still not seen as a partnership. "There's a lot of good data around – claims information, benchmarking data – it would be good to manage the risk rather than making it a transactional check box," he said.

The panel drew to a close with all panellists agreeing that companies should treat employees as their strongest asset in security and encourage them to know their colleagues, understand data, manage expectations, report anything that doesn't seem right and take responsibility for themselves as a part of a bigger whole.

"I really liked the plenary session on The Human Factor. The discussion that the panel had was very interesting and informative.

Work session summaries

Instant Payments – preparing your operations

The European banking community is getting ready for the Instant Payments challenge. More and more initiatives and projects are in implementation phase across EMEA and worldwide.

Isabelle Olivier, Head of Securities Initiatives and Payments Market infrastructures opened the work session with an introduction on the drivers behind the European Instant Payments initiatives. We explored the main issues faced by financial institutions in adopting Instant Payments and how SWIFT can help address some of these, such as multi-CSM connectivity services, consulting services, integration within banks systems.

Following on from Isabelle Olivier's introduction, Dirk Van Achter from Product Management introduced the SWIFTNet Instant portfolio, SWIFT's future-proof footprint evolution that will allow customers on the European market to connect to multiple instant payments services through a single connection.
The notion of not having SNL in the new SWIFTNet Instant Infrastructure as well as the idea that the new future proof AGI instance can eventually take over the role of the current SAG and SNL systems for FIN, FileAct and Interact traffic was clearly surprising information for most of the audience.

Questions from participants ranged from reusability of existing SWIFT Infrastructure at customer premises, to the ability to link current SNL/SAG and new AGI (Alliance Gateway instance) systems, and connectivity options for customers with global infrastructure in overcoming issues caused by network latency.

During the session, the audience were asked a number of poll questions, their answers to which demonstrated that they are all aware of, and preparing for Instant Payments coming to Europe. The results of this polling also confirmed that IP is high on the agenda of banks, with most of them planning to be live by November 2018 and confirming that the implementation of Instant Payments brings with it significant operational, technical and compliance challenges.
The SWIFTNet Instant portfolio will be available by November 2018. For further information, customers can reach out to SWIFT's Instant Payments team directly via Instant-Payments@swift.com

> **"The highlight for me has been the Instant Payments work session. I learnt a lot there and when I go back, I'll be finding out what we are doing as an organisation.**

Planning ahead – mandatory changes coming your way

With the many mandatory changes coming in the next few years, this session covered some of the key changes, including the new Weekend Change implementation approach, the MV–SIPN Footprint Evolution, and insights into the FileAct 7.2 enhancements. Firstly looking at the new weekend change implementation approach, participants were reminded of the key principles of the weekend changes. The audience also heard that SWIFT is looking into enhancements to their interface product specifications in order to handle the new maintenance disruptions. SWIFT will shortly be updating all documentation to reflect these changes.

For the MV–SIPN footprint evolution, the audience heard that after thorough research and vendor analysis, the Juniper SRX345 was selected for the new network connectivity footprint. This model matches the requirements to replace the current SSG5 VPN box. Among the key features of the SRX345 are increased security and improved cryptography, dynamic traffic re–routing and resilience supporting up to four leased lines per pack.

The audience heard that the MV–SIPN migration will start in May 2018 with an upgrade deadline of July 2020.

For the Release 7.2 FileAct enhancements some of the new features were shared, including support for larger files, resumption of file transfers, enhanced status of file transfers, enhanced transfer efficiency and dynamic control of concurrent file transfers.

Under attack! Are you prepared?

SWIFT's Customer Security Intelligence team delivered a brief introduction on the threat intelligence information that is shared through the SWIFT ISAC, followed by an explanation of what a typical cyber kill–chain looks like. Following this presentation, participants in this highly interactive session were put in the shoes of an institution which has just discovered it has been hacked. Each had to collaborate to make the right decision at the right time. This led to interesting discussions related to customers' infrastructure and cyber incident response readiness. The general feedback was that this session was fun, challenging and a great opportunity to share ideas.

Planning your ISO 20022 Adoption

The main objective of this session was to make the audience realise that ISO 20022 will not only impact the applications interface or the message format, but that adoption should also be considered as an opportunity in the larger context of the industry trend to move to ISO 20022, a change that SWIFT is very well equipped to help with.

This session was split into three parts looking at the status of the ISO20022 adoption and how the different market infrastructures drives this adoption, a workshop and discussion around operational readiness and internal infrastructure for banks, and the tools that support the ISO20022 adoption.

Generally it was felt that it was not easy to create a business case for ISO20022 adoption as the added value is not immediately seen. It was also felt that in some way, due to this, banks are deciding to not move to adopt ISO20022 unless either a Market Infrastructure or SWIFT mandates the change. This led to the question being asked as to whether SWIFT could take an authoritative role on the adoption of ISO20022.

> **“It’s always a great experience to exchange information and best practices with people doing the same job as you do.**

Collective Intelligence Cafés

The Collective Intelligence Cafés took place as one large session for all delegates with tables where different operational topics were discussed in parallel, and where participants chose which topics they would like to discuss. With each topic repeated three times, each participant was able to attend several discussions of their choice. The 12 tables were hosted by both SWIFT and customers, and this very interactive session allowed participants to share their experience on each of the chosen topics with other delegates and take away some ideas that may help them to do things differently or better.

Networking activities

Year Book 2017

Networking is a key component of our Premium Services Forums and one of your favourite aspects of the event. Every year, we strive to come up with a networking activity that will be both fun and valuable to you, that will help you expand your network and establish lasting business contacts.

Following the success of the PSF Yearbook over the last couple of events, we replicated the idea this year and designed another yearbook that contained a space for you to add the picture and contact details of each person that you met at the event. We hope that you came away with a book full of new contacts!

Off-site dinner

This year's off-site dinner took place at De Koninklijke Industrieele Groote Club in Amsterdam. The club, with its historical, monumental building, classic halls and modern atmosphere, was a great venue for our dinner. We hope that you enjoyed the evening and look forward to hosting another PSF dinner at another great venue in Amsterdam in 2018.

Shaping next year's event

In the closing plenary, hosted by Leo Punt, Head of Services and Support, EMEA, we asked you a few questions about the format that you would like to see for future PSFs. When asked whether you felt that the level of cyber security content was right, too little or too much, 67% of you responded that it is just right, whilst 19% asked for more and 14% asked for less. The next question asked whether you liked the changes that we made to the format of the Collective Intelligence Cafés this year. 76% of you responded that the format changes made the cafés better, whilst 15% said that they were neither better nor worse and 8% found that they were worse. The last question was also about the Collective Intelligence Cafés and asked you whether we should keep them next year with the same time allocation and format, or whether we should do more, or less. To this question, 67% of you answered that we should keep things as they are, 26% asked for more and 11% asked for less.

Thank you very much for your contribution and your feedback! This will help us to ensure that we keep evolving PSF in accordance with your requirements.

Thank you

Our thanks go to each and every one of you for your active participation in this year's Premium Services Forum. We would like to extend particular thanks to those customers who kindly agreed to help with the content and delivery of the Collective Intelligence Cafés – your contribution and all the work that you put into making these a success was most appreciated.

We hope that you all had an engaging, thought-provoking, productive, informative and highly collaborative Premium Services Forum. As always, should you have any questions about or suggestions for next year's event, please do not hesitate to contact your service manager. We look forward to working with you in 2018!