09 | 2018
Edition 76

“Know your enemy”

Interview with Marc Hofmann, CISO SWIFT, on the fight against cyber risks

Digital crown jewels of the financial center and cyber defense

After the harmonization is before the harmonization

it

The Swiss professional journal for payments

IMPRESSUM

PUBLISHER
SIX INTERBANK CLEARING LTD
Pfingstweidstrasse 110
CH-8005 Zurich
T +41 58 399 4747

ORDERS/FEEDBACK
clearit@six-group.com

EDITION
Edition 76 – September 2018
Published regularly, also online at www.clearit.ch
Circulation German (1,300 copies), French (400 copies) and English (available in electronic format only on www.clearit.ch).

TRANSLATION
English: Word+Image AG
French: Denis Fournier

LAYOUT
Felber, Kristofori Group, Advertising agency

PRINTER
sprüngli druck ag

Additional information about the Swiss payment traffic systems can be found on the Internet at www.six-interbank-clearing.com

FRONT PAGE
Marc Hofmann, Chief Information Security Officer at SWIFT

Marco Menotti

Dear reader,

The term 'ecosystem' from biology refers to a symbiotic community of plants and animals in a habitat. A tree along with its fungi and other living creatures forms an ecosystem. Together with the surrounding meadow, which is an ecosystem in itself, a larger one is formed, and together with the entire forest, an even larger ecosystem emerges.

The situation is similar in business ecosystems. The Swiss mobile payment network TWINT, for example, can be considered an ecosystem for payments (see clearit 72, September 2017). If you consider that instant payments are growing ever more important, it is obvious that this mobile P2P solution is to be placed in the context of interbank payment traffic, where payment initiation and payment crediting have been handled in real time for decades. In this way, an ecosystem can seamlessly transition into another one – such as is the case with the tree and the surrounding meadow.
Under my leadership, SIX is in the process of establishing, and especially expanding, payment traffic as a new ecosystem in order to meet the current and future needs of our owners, the banks. Crucial in this process is that we understand the current ecosystems so that we can interact between the various ecosystems and then reap the potential of synergies – particularly in view of the technological or regulatory dynamic, which is increasingly influencing payment traffic work routines among the banks.

We are now creating and using a large ecosystem for products and services, which includes TWINT, eBill, LSV, QR-bill, cards, ATMs and SIC/euroSIC, among other things. The result shall be cost advantages, network effects and targeted innovations from SIX for the banks. In a reduced form, SIX Interbank Clearing Ltd – with its IT Management and Operations Center – will continue to operate the Swiss RTGS platform and thus ensure that the Swiss National Bank can have a direct influence on shaping the systemically important SIC. All non-core areas of SIC will be grouped in the new functional organization of the business unit, but will continue to provide all their current services to SIX Interbank Clearing. Issuing, Processing and ATM operations from SIX Payment Services will also be part of the new business unit, including extensions of the current business fields, e.g. through new offers for an integrated cash supply ('Ecosystem Cash').

And, last but not least, the 'Swiss Corporate API' (see clearit 75, June 2018) will be housed with us and, as the 'Ecosystem Connectivity', will positively influence all the other ecosystems mentioned and open up new business fields extending beyond payments, leaving room for innovative services as we expand and round off our business model. Tree, meadow and forest in and of themselves are insufficient to meet our strategic requirements. We are focusing on the enlargement of the ecosystems. With this in mind, our aspiration for the restructuring is: "Today we are payments – tomorrow we are banking services" – starting 1 October 2018 in the SIX Business Unit Banking Services.

Marco Menotti
Head Business Unit Banking Services, SIX

Marc Hofmann,
Chief Information Security Officer at SWIFT

Cyber security – It's a race for time

Know your enemy. Develop detection and defense strategies, create threat assessments, increase awareness of cyber risks and promote an exchange of experience within the community. These are a few of the aspects that Marc Hofmann, Chief Information Security Officer at SWIFT talks about in the following interview.

"Virtually everybody is exposed to cyber risk in some form," stated IMF experts in a paper last year. That sounds as banal as a police reminder about the risk of accidents. Mr. Hofmann, how do you feel about this?

Contrary to the cyber risks, I do not believe that the risk of road traffic accidents has increased tremendously in recent decades. Criminal hackers today are essentially better organized than they were a few years ago and have a wide range of resources. They act like a globally active company. This has massively changed the threat situation. Another aspect is that there's greater exposure to cyberattack: digitalization, the opening of our networks to the Internet – that particularly pertains to the customer-bank interface. Consider the keyword, open banking, or the Internet of Things, or the regulation stipulated by PSD2, which opens the customer interface for third parties with the help of APIs.

> "The SWIFT community has a steadily increasing common interest in its own security."

Two years ago, as a reaction to cyber bank robbery at the Bangladesh's central bank, SWIFT announced a series of security measures and introduced them under the name, Customer Security Programme (CSP). An article about this appeared in clearit 12/2017. By the end of last year, all SWIFT customers had to prove that they have complied with the mandatory security controls. Apparently, 89% did so. What happens to those who do not cooperate?

I am pleased to say that meanwhile more than 90% of our 12,000 customers completed the self-attestation. And this number is growing as we speak. That's good news. Taking a closer look at the numbers shows that this figure covers more than 99% of all SWIFT FIN messages. We are striving for 100% by the end of 2018 and will help the remaining customers to carry out the CSP attestation. And there we are welcomed with open arms, because the SWIFT community has a steadily increasing common interest in its own security. Together with our stakeholders, we're doing everything we can to achieve this goal. This also includes reporting those who do not adhere to the requirements to the relevant supervisory authorities.

Apropos community: One would expect that a regular exchange of information and experience takes place between the individual members. According to our information, that doesn't always seem to be the case. Only very few banks are interested in the security attestation status of counterparties. What's the reason for this?
That does not correspond with my experience. Actually, I see just the opposite: a much stronger and growing interest in the security of counterparties. And that applies not only to counterparties, that goes for all relationships with third parties – in contrast to previously when one was primarily limited to one's own security. I have noticed in many banks that rules and processes have been set up to ensure security among partners, and requests for attestation information are also growing worldwide. Because we are in a learning process, it goes without saying that there's still plenty of room for improvement.

> "As long as hackers hope to be able to earn money, their activities won't stop."

How much fraud is being effectively prevented due to the CSP activities?
We have actually made tangible and measurable progress in the fight against fraud. I can, however, not provide you with figures or even individual cases. We have observed that our measures to prevent payment fraud have proven effective in numerous cases. An additional important aspect is that our customers show a significantly higher level of awareness of their own security and – as I indicated before – also that of their counterparties who also are raising their capability to recognize threats. We're getting better every day. But from what I'm able to gather, the number of fraud attempts is not really decreasing. In fact, the opposite is true. As long as hackers hope to be able to earn money, they won't stop.

Is there any indication that hackers have meanwhile shifted their criminal activities to other channels and areas as a result of the CSP?
We know that criminal hackers make increasingly greater efforts to bypass security measures. Thus, regardless of what financial institutions have introduced, criminals attempt to find a way to get around them. Using deception technology, we simulate false servers and accounts, amongst other things, to trap them. They are meanwhile reacting to this and that will also be the case with other measures, and the CSP is no exception. What does that mean for us? It means that we cannot rest, must continually question whether our measures are appropriate and we must logically continue upping the ante.

We detect many fraud attempts very early on with our integrity check tool, which shows whether a message has been transmitted in a falsified manner.

Apropos tool: With the new Payment Controls service, SWIFT has launched a new tool for fraud protection – real-time screening of outgoing payments. Why not also for incoming payment instructions?
First of all, it's the obligation of each individual company to check outbound messages to make sure they are not fraudulent. And that's the reason why we started there. The future expansion to the recipient side is thereby not ruled out.

That's one of the next steps in the race against the criminals…
Possibly, yes. The thing is though; you need to be able to ultimately bring the entire community along with you. Few things function with simply the flick of a switch, and suddenly the effect works for the entire community. Rather, a joint effort is required for most things. And that means: Together with our customers we must consider where our priorities lie and where we can achieve the best effect with a view to both the current and anticipated threat situation.

The cyber threat is the reverse side of digitalization. Politics, business and society seem to have recognized the seriousness of the situation. To name just

a few examples: EU countries have come together to create rapid cyber attack troops, the Swiss Federal Council has been given a 'Mr./Ms. Cyber Security', and in Germany, the world's largest research center for IT security shall be built (Cispa) with a masters study program in cyber security. How is SWIFT integrating itself in the race to create security with global initiatives?

First of all, I find the promotion of cooperation in the battle against crime to be an extremely important issue – and I mean not just banks or our customers, but also law enforcement authorities. I believe that cooperation, or at least the exchange of information about the modus operandi of cybercriminals with government organizations as well as universities will be one of the crucial capabilities for us to be able to effectively defend ourselves. Therefore, we've already undertaken numerous steps in this regard and are planning more. For example, we're working with organizations such as the International Monetary Fund and the World Bank. We're also part of the FS-ISAC, an organization for the financial sector which provides information about cyber threats to its 7,000 members around the world. The annual meeting recently took place in Miami, where the chief information security officers of the banks conferred and did some straight talking.

While this cooperation is certainly important, is it also strategic?

Definitely. And for various reasons. The most obvious one is cooperation when it comes to intelligence information. In this regard, we share so-called indicators of compromise in near real-time with the SWIFT community, which is data about threats regarding malware or perpetrator groups so that community members can also quickly adapt their defense. These indicators are also fed by experiences gathered by others. I find it extremely important that we exchange such information and that we mutually warn one another about potential threat situations. And we have actually been able to successfully defend ourselves against several attacks, in answer to your earlier question about where we have been effective against cyber fraud.

A further strategic aspect is that we seek to sharpen awareness throughout the entire SWIFT community in this context. We provide examples of how attacks function and how criminal hackers do it; how they are sometimes very, very patient, that after penetrating a company's network, they spy on the environment and user activities, unnoticed, for months or even more than a year before attacking. We have evidence that criminals very cunningly strike on national holidays or weekends in order to take advantage of the behavior of local operators. We must share this information and enhance risk awareness for concrete situations so that companies then also make targeted investments where it makes the most sense. We should not go around with a watering can and futilely attempt to

equally protect ourselves from everything, but apply our efforts where they are most effective. True effectiveness is only possible when the community works together.

The SWIFT master plan for cyber security is structured according to four main criteria. The first of which is: Know your enemy. We may be familiar with the know-your-customer principle. But how does one recognize an enemy?
Creating threat assessments is a very important first step. The second aspect is the capability of the respective security operation center (SOC) to recognize intruders. That is a difficult issue because, after all, hackers inherently wish to remain unrecognized. However, technical support is available here, such as in the area of network behavior analysis. This makes it possible to detect unusual behavior in the network and to track it down.

This type of behavior analysis, like the above-mentioned deception technology, is a further possibility to raise awareness in technical terms in regard to the infrastructure. And then, it goes without saying, there is the business side. The priority here is how to detect a fraudulent payment, for example. I briefly mentioned our new Payment Controls service. Our daily validation report offers another possibility to protect processes involved in the daily reconciliation of transactions from fraud. If I have a message which arrives at an unusual time or is to be forwarded to a new creditor that is unknown to me, then it's quite clear that something may be wrong. And that is just what is meant by "know your enemy".

A new version of the CSP framework will be published this summer containing changes to many security controls. Why did the framework have be changed? Did the currently applicable one miss out on some essential aspects?
No, that's not the case. Regardless of how cleverly we defend ourselves against cyber attacks, criminals never sleep and are growing ever more sophisticated. That means that we also must continue to move forward. That goes for the CSP too.

We must continuously question and further develop the controls if we do not wish to lose the race. Because the risks and the threat situation are constantly changing, we were compelled to adapt the CSP accordingly. In this context, there will certainly be new mandatory security controls in the future, and perhaps some will also be dismantled. In any case, I expect that the framework will generally become stricter.

Is it then safe to assume that the framework will more or less undergo a release cycle?
That's how it is. We are constantly scrutinizing the controls. We will introduce such a cycle in tandem with the community.

Hackers fed fraudulent payments between the back-office system and SWIFT Alliance Access at the Bangladesh's central bank. The most effective control against such an attack is back-office data flow security. Why does the control point remain only 'just recommended' in the new framework instead of being mandatory?
We consider this to be an important issue. That's why it is also part of the control framework. We are sure that in the course of the further development of the framework there will be shifts from advisory to mandatory controls. We regularly review the importance and appropriateness of the respective controls and then consider whether an upgrade to 'mandatory control' is called for.

And this will come up in the next release...
That's how it is.

Due to its systemic importance for the stability of the global financial system, SWIFT has been supervised by the G-10 central banks for twenty years. How does SWIFT rate its own efforts in the area of cyber security?
Naturally, the issue of cyber security is not only extremely important for the community, but also for our own security status. That means that this issue has top priority for us. At the same time, we have substantially invested in our infrastructure and in our cyber strategy, and will continue doing so. We consistently proceed according to the international standards

“We have evidence that criminals very cunningly strike on national holidays or weekends.”

Marc Hofmann

(e.g. ISO) as well as best practice and determine where we can still go the extra mile. And beyond all that we can do here, we constantly keep the G-10 regularly up to date to facilitate them in their governance duties.

> **"If there was something I could wish for, then it would be that all companies, without exception, would immediately turn to us if they suspect misuse so that we can help them."**

In your opinion, what are the remaining major hindrances to providing cyber security in the SWIFT community?

The reality is that whilst not the majority, many of our customers still shy away from exchanging information. Some view it as a competitive advantage to keep such information to themselves. That particularly applies to information about incidents. If there was something I could wish for, then it would be that all companies, without exception, would immediately turn to us if they suspect misuse so that we can help them. Or that we can share information through our channels to ward off damage to other companies, naturally only upon approval and in an anonymized form. In my experience, many companies are unfortunately not even in the position to be able to act along with us in a suspicious case. First, because they simply do not know who to turn to internally in matters involving legal and compliance in order to obtain approval for such an exchange of information. And even if this knowledge exists, it sometimes takes too long to obtain the approval, even days, either because those in charge are on holiday or are at least not available.

The second issue is that under some circumstances some companies cannot do more in technical terms. I have been able to observe several attacks in which criminals did extensive damage to the company's infrastructure (e.g. server, including mail server) in order to erase their tracks. Either they delete database entries or act in an extremely damaging way and encrypt or simply delete everything that gets in their way. In other words, it's not possible for customers to react quickly enough. In principle, criminal hackers set out to prevent or at least delay the reconciliation of incoming and outgoing payments. In the end, it's a race for time. Nothing matters more than time when it comes to the recovery of funds. Hackers know this too and therefore seek to erase their tracks and to slow down the reaction times of their victims.

Interview:
Gabriel Juri & Karin Pache
SIX Interbank Clearing

SWIFT CSP SECURITY CONTROLS FRAMEWORK

Secure Your Environment	1	Restrict Internet access
	2	Segregate critical systems from general IT environment
	3	Reduce attack surface and vulnerabilities
	4	Physically secure the environment
Know and Limit Access	5	Prevent compromise of credentials
	6	Manage identities and segregate privileges
Detect and Respond	7	Detect anomalous activity to system or transaction records
	8	Plan for incident response and information sharing

The future of payment security

Payment security has concerned people at least since the introduction of coins as a means of payment. In the age of advancing digitalization, the threats and security requirements are increasing exponentially. New strategies, tools and security features are indispensible in the battle against cybercrime.

The history of money going back nearly 3,000 years has been marked by a virtual 'race' between the 'good guys' and the 'bad guys': official versus counterfeit money. The result has been a steady improvement in the security features. For physical money, for example, this pertains to the material used, the colors, edge configuration or dimensions. Such features for bank notes often involve intaglio printing, security threads (silver threads), watermarks, holograms, microprinting, UV light and infrared fluorescence. Although the security features are constantly growing more sophisticated, in the long run, none of them are so secure that a counterfeiter cannot imitate or fool them.

The same thing can be said for the history of the Internet: cyber security versus cybercrime. Even the first digital computer connections were protected by technical measures and equipped with security features. Attacks by hackers succeeded nevertheless. New security features had to be developed. However, it is also applicable for the Internet: The opposition does not sleep – the race not only continues, but has strongly accelerated since it began.

In the present age of increasing and comprehensive digitalization, the scale of the threat through cybercrime is growing. Every company, every individual can be the target of cybercriminals. The threat consists of information theft, fraud and sabotage of business operations. It happens through various channels such as social media, e-mail, intranet, Internet, phone and letter. The threat stems from very different groups and individuals, from insiders and cybercriminals, hackers, organized crime syndicates, hacktivists and state-supported attackers.

IT security – technical and organizational measures combined

The dangers of an infection through malware can be reduced and IT security increased in company networks by taking technical measures. These measures include up-to-date virus protection, daily backups of all data, spam filters, firewalls and the encrypting of important data.

The weakest link in the chain in many cases is not the technology, but the user. This means that besides technical measures, organizational measures are needed to increase IT security.

Organizational measures are intended to ensure that the responsibilities are defined in regard to IT security in the company. Furthermore, employees must be trained, the risks must be regularly reviewed and a password policy must be defined in order to ensure security.

New security features

In the race against cybercriminals, there are numerous new security features that ensure the technological advantage and which shall additionally raise IT security in the future. Here are several examples:

Anomaly detection identifies suspicious patterns.

– **Two-factor authentication (2FA)** uses the combination of two different and mutually independent factors for the identification of a user. 2FA is considered to be very secure, but has the disadvantage that the respective token (hardware token, bank card or key) must be carried at all times. The **tokenless 2FA** was developed as an improvement and alternative. This new two-factor authentication is used by smartphones as a token. If the user wants to authenticate himself, then he uses his personal access code to the smartphone and a valid, dynamic, additional one-time password (OTP) that he receives through the corresponding app on his smartphone. The advantage of this method is that an additional token is not needed because the smartphone is something one always has at hand. The Google Authenticator and UBS Access App both function according to this principle.

– The **distributed electronic signature (DES)** will be indispensible in the future. With this type of signature, payment instructions are electronically transferred from the accounting or treasury department to the bank, but not yet booked. The authorized signatories can check whether the payment instructions ready for release are correct and which signatures have already been provided or which are still missing. The authorized signatories can then electronically sign the instructions to be signed. Only when all required signatures are present does the bank execute the instructions. Security can be enhanced even further if the payment instructions are additionally transmitted through a channel that is separate from the signatures. For example, the payment instruction can be transmitted to the bank via EBICS and the signatures needed for the release can be provided via e-banking. A cybercriminal would then have to overcome two very secure channels in order to be successful.

– **SwissID – the digital identity**. People today prove their identity with a passport, an ID card or driver's

MELANI

The website for MELANI (Melde- und Analysestelle Informationssicherung) at www.melani.admin.ch, is operated by the Swiss Confederation and is aimed at private computer and Internet users, as well as small and midsized enterprises (SMEs) in Switzerland. It contains information about current threats and frequent cases, along with documentation, a newsletter and reporting form, among other things.

license. Providing proof in this way for transactions over the Internet is very cumbersome. That is why an electronic proof of identity is needed which, for example, enables online portals to unambiguously identify and authenticate a person. SwissID in Switzerland is an efficient and broadly based solution for digital identity. The free service is provided by SwissSign, a joint venture of government-related operations, financial companies, insurance companies and health insurance companies. With SwissID, users can simply and securely log in to Swiss online services, prove their identity, purchase products, make payments and provide their signature online.

– **An anomaly detection system (ADS)** helps to recognize anomalous data and to thereby identify unusual purchases and unusual payment recipients as potentially fraudulent transactions. Automated anomaly recognition from banks for payment instructions is a complex task which involves areas such as machine learning, statistics and data mining.

Greater security through personal settings for payments and cards

By adjusting the personal settings for payments and cards, the security of payment instructions can be additionally increased. Customers should be able to themselves set whether they should be notified by smartphone about account movements above a certain amount. It will also be increasingly possible in e-banking systems to block payments and cards for countries to which money will never be transferred (geo-blocking). Furthermore, customers will be able to set up period-related limits for payments. If the limit is exceeded, then no further payments can be entered in the defined period. For multiple accounts, it will be possible to fully deactivate individual accounts for online payments. These accounts are then blocked for credit transfers and account transfers. Another feature, which will become widespread in the future, are payments to new creditors that must first be confirmed; in other words, a recipient to whom money has never been transferred must be additionally confirmed once for security purposes. Banks will certainly offer will offer a combination of some of these options to their customers. In this way, it will be possible for a customer to define that a confirmation for new creditors is only necessary as of a certain amount.

eBill – pay bills securely

With eBill invoicing partners can electronically transmit their bills directly from their billing software, securely and without media disruptions as an eBill to their customers' e-banking system. The payer need no longer type in payment information or scan payment slips. This also means there are no longer any entry errors, instead a consistent, reliable, secure and transparent paying of bills. Invoicing partners can thereby avoid damaging their reputation, which is not at all uncommon with e-mail bills due to spamming and phishing. Since eBill is free of media disruptions and therefore superior to e-mail bills, it will surely succeed as Switzerland's digital, secure bill in the long term.

Peter Ruoss
UBS Switzerland AG

ENROUTE TO E-ID

The Swiss Federal Council approved a draft law pertaining to electronic proof of identity (E-ID) on 1 June 2018. The user of such an E-ID should be able to prove that they are a certain person with a single login for online services provided by companies and authorities (e.g. online shopping, electronic patient dossier, ordering an extract from the police registry, municipal notifications, completing a tax declaration, etc.).

SwissSign Group AG, a joint venture from government-related companies (SBB, Swiss Post, Swisscom); financial companies (SIX, UBS, Raiffeisen, Credit Suisse, Zurich Cantonal Bank, Entris); insurance companies (Axa, Baloise, Helvetia, Mobiliar, Swiss Life, Vaudoise, Zurich) and health insurance companies (CSS, SWICA) is standing in the starting blocks. With SwissID, it offers a free and simple option for digital identification that meets all legal data protections requirements and which protects the private sphere of their customers.

Digital crown jewels of the Swiss financial center and cyber defense

The Swiss Value Chain forms the backbone of the Swiss financial center. The smooth and efficient functioning of its networked infrastructures – stock exchange, securities and payments processing – is equally a central prerequisite for the attractiveness of the financial center as is its resistance against cyber attacks. Because the question is not whether, but when such cyber attacks will happen.

The follow-up question is whether SIX, the operator of the completely standardized, automated and digitalized financial market infrastructure is armed against cyber attacks. Towards this end, technical measures alone – within the scope of business continuity planning (BCP) – are insufficient.

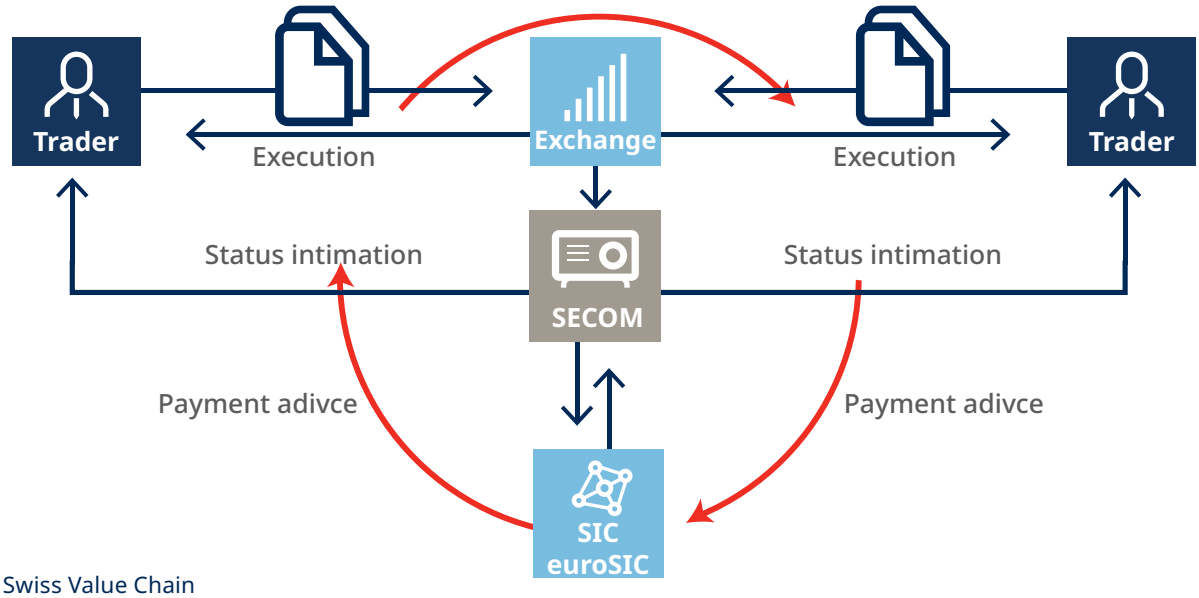
Proactive defense line

SIX is obligated to continuously optimize its existing security processes (e.g. BCP, internal control systems). Moreover, it identifies and evaluates new technological risks and, in line with best practices and global security standards in the financial industry, undertakes the necessary measures to protect itself and its customers in a constantly changing environment. Everyone is talking about how organized crime has shifted to the online world and causes immense damage to companies through increasingly sophisticated cyber attacks, but awareness of the threat is not yet really ubiquitous. This would require an active risk culture, which does not come into being on its own. SIX has proactively encouraged this culture in companies for some time now. An appropriate level of risk awareness by each individual is indispensable in this regard, when one considers that even a suspicious e-mail can become a relevant threat.

Switzerland's first cognitive security operations center

SIX has therefore equipped itself in terms of organization: The first security operations center (SOC) in Switzerland began operation in January 2018, which is

SOC processes



Swiss Value Chain

based on cognitive computing – a self-learning technology. The security analysts work together with operation monitoring on site in Zurich in an around-the-clock shift operation. This massively expands the possibilities to sustainably raise the security level in order to identify cyber threats, and thereby to protect SIX and its financial market infrastructure. Currently, among the billion log messages, there are 30 potential threats or security gaps per day which must be reviewed and handled.

Cyber security as a business field

SIX now supports its customers in the fight against cybercrime. It relieves other companies of the costly development and around-the-clock operation of an SOC and provides the required analysts specialized in cyber security. Especially smaller and mid-sized banks and insurance companies thereby have access to a maximum strength security solution which only large companies can otherwise develop for themselves. In the process, the data remains constantly with the customer – and always in Switzerland – only the incidents are forwarded for analysis. In addition, SIX intends to launch training and further education programs and promote and simplify the sharing of knowledge about the threat situation among all stakeholders.

Thomas Koch
Head Corporate Security, SIX

ORGANIZATIONAL NETWORK

SIX is an active member in the Swiss security communities and shares threat notifications and information with other financial market participants, and receives notifications in return, which serve to ward off cyber threats.

Furthermore, this year SIX launched the SIX Cyber Hub, a sector-specific, interdisciplinary and multilateral initiative. It is at the disposal of all participants in the Swiss financial center. The SIX Cyber Hub is intended to strengthen the resilience, cooperation, information exchange and 'digital trust' in the cyber resistance capability of the Swiss financial center.

FACTS & FIGURES

- 1,765 cyber break-ins were registered around the world in 2017
- 2.6 billion data entries were thereby stolen
- A cyber break-in costs a company USD 3.62 million on average
- 94 Swiss companies fell prey to cyber attacks in 2017

EU data protection also for the Swiss financial center

The revised EU General Data Protection Regulation has been in effect since 25 May 2018. What does it contain? And whom does it impact? And what consequences does it have for the Swiss financial center and its payment traffic?

The EU General Data Protection Regulation (GDPR) was issued to harmonize the data protection laws of European countries, to strengthen data protection for EU citizens and to guarantee the appropriate transparency. This means that the data protection procedures of companies and organizations in the EU member states will all have to be redesigned.

Who is impacted by the regulation?
All companies that process personal data from natural persons residing in the EU (customers, employees, etc.), must implement the regulations, regardless of where they are located. The requirement therefore also applies to companies located in Switzerland if they have business relationships with people living in the EU, or if they offer services to such people, but it does

Details about the GDPR are available at: www.EUGDPR.org

not apply to people living in Switzerland who have business relationships within Switzerland.

Heavy fines
Failure to adhere to the GDPR can result in fines ranging up to 4% of the annual business turnover or EUR 20 million (depending on which amount is higher).

Consequences for payment traffic
The GDPR must also always be implemented in payment traffic if personal data is processed. On the one hand, the GDPR rights must be guaranteed for natural persons. One the other hand, it must be ensured that the processes and systems meet the data protection requirements and are comprehensively documented. This pertains to the storing, processing and transmitting of personal data, both internally as well as with cloud-based applications, which typically involves e-banking activities, payment and stock exchange orders. In this sense, technical identifiers are already being applied throughout the banks' corresponding middle- and back-end processes, so that no conclusions can be made about a specific person.

Implicit approval not permitted
Service providers and employers who are only active in the Swiss financial center must comply with the EU guidelines for customers and employees who are resident in the EU. Implicit approvals are not permitted. The customer or employee must explicitly agree to the data storage; an X is also to be explicitly placed in the appropriate field. The service range or employment may not be made dependent upon approval in regard to expanded data storage.

The Swiss data protection law is currently being revised with an eye towards bringing it into line with the new GDPR, and will afterwards probably apply accordingly for all customers and employees of Swiss service providers and employees.

Manuela Giordano & Alain Hiltgen
UBS Business Solutions AG

HIGHLIGHTS OF THE REVISED REGULATION

Data protection by design and by default
A company that processes personal data must ensure that protection of the data is provided at all times by means of technical and organizational measures. A company must also ensure that, as a standard, only personal data that is necessary for the business process will be processed. This applies both to the volume of data collected and the processing thereof, as well as for the storage duration and access to the data.

The rights of natural persons
The regulation provides natural persons with transparency and corresponding power to act in regard to their personal data.

Right of access by the data subject
Every person has the right to learn whether, where and to what purpose a company processes their personal data. Moreover, every affected person must be given access to a copy of the processed data in an electronic form.

Right to data portability
With the GDPR, natural persons receive the right to receive the personal data from a company to which it has provided it within the scope of a business relationship.

Right to erasure
Every person has the right to request the erasure of their personal data and to stop the distribution thereof and, if necessary, the processing thereof by third parties.

Notification of a personal data breach
The GDPR stipulates that data protection infractions must be reported, which could lead to a potential risk to the rights and freedom of a natural person. The persons affected must also be informed. This notification is to take place within 72 hours.

Designation of the data protection officer
Companies that process large volumes of personal data in their operative business field, must name a data protection controller with appropriate authority

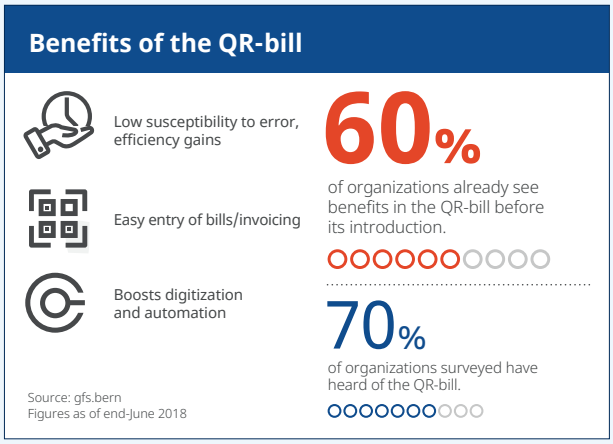
After the harmonization is before the harmonization

An important milestone has been reached: At the end of June 2018, more than 80% of Swiss companies had completed the ISO 20022 changeover in payment traffic. From this sustained dynamic it can be concluded that full-scale nationwide switchover will be achieved by the end of the year. This is also borne out by a representative survey conducted in the spring by gfs.bern. It indicated that 90% of those surveyed had already started a migration project and will have completed it by the end of the year. This paves the way to the QR-bill, which will be launched in mid-2020.

According to the survey by gfs.bern, the successful changeover is due to a large extent to the performance benefits of ISO 20022 and the work done by banks and software companies to provide information. In recent months they have actively supported their clients with information and advice. Around 70% of the organizations affected received guidance from an external partner, with 90% receiving information from their bank and saying they were fairly or even very satisfied with this support. Given these high figures, the assistance and information provided by banks and software providers can be seen as a key success factor in an infrastructure project of this scale.

Scoring with performance benefits

In the last few months ISO 20022 has established itself as an important basis for optimizing key financial processes. 60% of organizations see benefits in connection with the standardization of payment traffic. This figure increases to well over 70% the more frequently and regularly they make payments and the further along the changeover process they are. The most frequently cited benefits included less susceptibility to error thanks to the use of IBAN, the digitization of business processes, and more straightforward domestic and cross-border payments. This suggests that ISO 20022 is proving its worth in practice. What is striking about all the survey



findings is that organizations with growing everyday experience perceive the benefits more clearly than those that have just launched a project or handle smaller volumes of invoices.

Closing gaps in the changeover
Communicating positive survey findings and experience is thus a way of driving the changeover further forward. It is hugely important for all corporate users to have completed the switch to ISO 20022 by the end of 2018. It is crucial to meet this deadline because as of the beginning of July 2018 the existing DTA standard has no longer been supported, developed, or documented by SIX. Each bank is responsible for making sure its corporate clients have caught up in terms of migration by the deadline. If the changeover has not been made across the board, it will not be possible to implement the QR-bill, which is already recognized as a major component of the entire harmonization process.

High expectations for the QR-bill
A total of 70% of those surveyed by gfs.bern have heard of the QR-bill, with around 60% already seeing only or primarily benefits in the QR-bill, even before it is introduced. This positive attitude bolsters the Swiss financial center's intention of implementing the QR-bill with broad support and incorporating the previously received valuable market feedback into the next stage. Towards this end, a public consultation process is being held until the end of September, with the outcome communicated in fall 2018. This procedure will ensure that market participants have an opportunity to voice their views, and that the QR-bill will be broadly supported so that it can be successfully launched on 30 June 2020.

Gabriel Juri,
SIX Interbank Clearing

Consultation about the Implementation Guidelines for the QR-bill

The following eight points of the Swiss Implementation Guidelines for the QR-bill (Version 1.0 of 27 April 2017) shall be revised and adapted to meet current market requirements.
- Introduction of a perforation requirement for paper-based payments
- Introduction of a receipt slip
- Simplification of structured addresses
- No display of the biller's structure information
- Simplification of combination options for structured references
- For the time being, no use of the field 'ultimate creditor'.
- For the time being, no use of the field for alternative schemes.
- Introduction of an additional license-free typeface for non-Microsoft users

The consultation procedure is primarily aimed at banks and ERP software producers which develop their products and services on the basis of the Implementation Guidelines.

ISO 20022 implemented successfully

90%
of corporate users have launched a changeover project.

Source: gfs.bern
Figures as of end-June 2018

80%

of corporate users have completed the changeover and have migrated 80% of their transaction volume.

Source: SIX Interbank Clearing Ltd
Figures as of end-June 2018

DEEP DIVES:

More about cyber security
in the December 2017 edition

More about the Swiss Value Chain
in the September 2016 edition

More about the ISO migration & QR-bill
in the March 2018 edition