The cyberthreat facing the financial services industry

Received (in revised form): 12th June, 2018

Pat Antonacci

is programme director for SWIFT's Customer Security Programme (CSP), a global initiative to reinforce the security of international banking, with responsibility for the implementation and future direction of the programme. Previously, he led the Customer and Third Party Engagement stream of the Customer Security Programme. He is also head of the services organisation for SWIFT's Americas and UK region, including the management of consulting, training, support and operational services. He joined the Americas executive team in 2012 leading consulting, training and technical pre-sales, following earlier roles in consulting services from 2007–12. Before joining SWIFT, Antonacci was consulting for JP Morgan Chase, where he provided business analytics and programme management for the private bank. He has previous experience at State Street, Deutsche Bank and Bankers' Trust, where he held executive positions in custody operations and programme management. He is an accomplished financial services professional with more than 20 years' global experience in developing and implementing new technologies, managing technical and business re-engineering projects, implementing SWIFT functionality and managing business operations.

SWIFT, 7 Times Square, 45th floor, New York, NY 10036, USA
Tel: +1 212 455 1800; E-mail: Pat.ANTONACCI@swift.com

Abstract The financial industry is a clear target for cybercriminals. In early 2016 a cyberattack on a bank in Bangladesh resulted in the attempted theft of US$1bn, an event that proved to be a watershed moment for our industry. It rapidly became clear that this was not an isolated incident, but part of a wider and highly adaptive campaign targeting banks around the world. This paper considers the Customer Security Programme (CSP), the dedicated initiative that SWIFT established to help the industry better protect itself against further attacks, and to reinforce and safeguard the security of the wider payments ecosystem. As a global cooperative, the approach the programme has been able to take is far-reaching and all-encompassing; it is aimed at every customer, from the smallest to the largest, and from weakest to strongest. By design, it seeks to overcome barriers and reach all geographies. SWIFT's global reach, its cooperative structure and its unique governance have enabled us to both prepare our response and ensure its aptness. It has afforded us the privilege of being able to learn from, and to reach out to and assist the community — transferring skills and experience from one customer to another, and from one geography to another — all the while preserving confidentiality.

KEYWORDS: Customer Security Programme (CSP), SWIFT ISAC, cyber security

INTRODUCTION

The financial sector is arguably among the most advanced economic sectors when it comes to the use of IT and, logically, has invested hugely in IT security systems. But it is also one of the most interconnected worlds — and a clear target for cybercriminals.

The World Economic Forum (WEF) has cited cyberattacks as a top global risk and its analysis shows that, across the globe, the good guys are not winning the fight by any stretch of the imagination — cyberattacks were in the WEF's top ten risks in 2016 and top five in 2017; in 2018 they feature in the top three risks to the global economy.

Looking back a few years, the cyber security company Mandiant categorised the attacks carried out by actors targeting financial services as 'smash and grab'. The attackers did not hide their actions; their attacks were loud, and recovery was straightforward. The attacks were largely opportunistic, the tools rudimentary and the skill of the attackers — in all but a few cases — was limited.

Today, the line between the level of sophistication of certain financial attackers and advanced state-sponsored attackers is not just blurred — it no longer exists. According to IBM, through Internet-shattering distributed-denial-of-service (DDoS) attacks, troves of records leaked through data breaches, and a renewed focus by organised cybercrime on business targets, 2016 was a defining year for security. Indeed, in 2016 over 4bn records were leaked, more than the combined total from the two previous years, redefining the meaning of the term 'mega breach'. In one case, a single source leaked more than 1.5bn records.[1]

Even more notably in 2016, financial attackers moved to customise their attacks. While state-sponsored attackers will continue to set the bar for capabilities and sophistication, financial attackers can no longer be categorised as smash and grab. An attacker that is harder to detect, investigate and remediate is inherently more likely to remain in an environment to accomplish their mission, which means the theft of greater volumes of financial information.

So, while networked technology has introduced huge benefits to the global economy, trade and society — making hitherto unthinkable advances, facilitating trade and investment flows, and enabling banking to reach the previously unbanked — the risks the networked world brings cannot be ignored; security is key to ensuring that we reap the advantages of these advances.

At SWIFT, we take cyber security very seriously; it is core to the service we offer — a secure and reliable communications channel to facilitate financial message exchange between our 11,000+ customers across more than 200 countries and territories, in every corner of the world. Day-in, day-out, since our inception over 40 years ago, we have maintained an unrelenting focus on our security. Last year saw our FIN traffic hit an all-time high of 7.1bn messages, demonstrating the unique global utility that we are to the financial industry. We exceeded our 2017 operational availability performance targets, achieving 99.999 per cent availability, against the backdrop of growing volumes and ongoing technology renewal.[2]

Sustainability is at the core of what we do. As a neutral global cooperative, we are defined by our community. Our governance ensures the representation and engagement of all users, large or small. This close cooperation helps us understand users' needs and challenges, allowing us to adapt and innovate appropriately, and enables us to think and act long-term — to look beyond quick fixes to craft affordable, sustainable solutions. In the last decade we have reduced messaging prices, innovated and adopted new technologies, increased network resilience, added a third data site, raised financial reserves and developed new products and services.

SWIFT operates at the heart of the world's financial industry and takes this responsibility very seriously. As the common, trusted link between financial institutions all across the world, operational excellence and security are central to everything we do at SWIFT. Thousands of financial institutions trust us to deliver millions of financial messages safely and securely every day. Through our unremitting focus on security, resilience, reliability and integrity, we ensure that our systems and services live up to our high expectations and deliver on our promise to be 'the' secure global messaging provider for the financial industry.

In early 2016, a cyberattack on the Bangladesh Bank resulted in the attempted

theft of $1bn,[3] bringing these truths home like never before. While only a fraction of the funds were stolen, the event proved a watershed moment for our industry. It rapidly became clear that this incident was not going to prove a single occurrence, but part of a wider and highly adaptive campaign targeting banks around the world.

In each of the incidents we have subsequently seen, customers first suffered security breaches within their local environments. Having successfully targeted and compromised their environments, the attackers went on to exploit vulnerabilities in banks' funds transfer initiation environments, to steal credentials, create fraudulent messages and initiate the irrevocable funds transfer process, sending messages over our network. In a final step, the attackers also found ways to tamper with the statements and confirmations that banks sometimes use as secondary controls, thereby delaying the victims' ability to recognise the fraud.

The attacks on customer firms have neither targeted nor resulted in any breach of SWIFT itself and there is, of course, no question that each and every customer has to be responsible for its own security. However, it rapidly became apparent that even if the risk was not contagious, the attacks were at least replicable, and the threat global; not only were these attackers targeting the correspondent banking industry, they were prepared to invest time in their attacks. They exhibited a deep and sophisticated knowledge of specific operational controls within the targeted institutions and showed that they could rapidly scale and replicate the frauds in different geographies.

SWIFT'S RESPONSE

In a matter of weeks after the attack on the Bangladesh Bank, SWIFT had determined that a community-based approach would be the best way to solve the security issues facing the industry. The cooperative thus set out to establish a dedicated initiative designed to reinforce and safeguard the security of the wider ecosystem — a system that stretches right around the world. Addressing customers of all shapes and sizes in geographies near and remote, sophisticated and developing, the SWIFT Customer Security Programme debuted formally in May the same year.

Requiring an unprecedented effort — from SWIFT's board, management and staff, as well as from regulators and the entire SWIFT customer base — the CSP is uniquely global in scope and unparalleled in reach. It is designed to assist customers in protecting and securing their local environments; in preventing and detecting fraud in their commercial relationships; and in sharing and utilising fraud-related information to defend against future cyberthreats.

In defining the CSP we had first to identify the key risk areas. We defined these as: the risks organisations present to themselves; the risks they present to each other; and the risks that the community, as a whole, can help to mitigate. We then structured the programme to address these three areas: helping customers protect themselves by enhancing SWIFT-related tools and security guidelines and by creating prevention and detection services; helping customers protect against the risks they present to each other by encouraging the adoption of market practice and the use of existing risk management tools, and by providing a controls framework; and, finally, helping the community as a whole by improving information sharing throughout the global community and by enhancing the support provided by third parties. To avoid the risk of developing a programme, products and solutions that did not meet customer needs, we worked closely with the entire community in designing and developing the programme, and in testing and refining the products and services.

Two particularly ambitious and innovative elements of the programme stand out: our

Information Sharing Initiative and our Customer Security Controls Framework.

Since mid-2016, SWIFT has been busy building out a unique information sharing initiative — the most global of its kind. We have established a dedicated Customer Security Intelligence (CSI) team and introduced a 'SWIFT ISAC' information sharing portal to share technical intelligence with the community. Focused on customer security forensics and analysis, the CSI team undertakes investigations on potential threats and security incidents at customer firms. Every time the team identifies an emerging attack pattern or technique, it publishes detailed security bulletins, informing customers of related indicators. This information has already made a tangible difference in the fight against fraud right across the world. By feeding back this intelligence in anonymised form to the wider community, sharing it with anti-virus vendors and other information security specialists, SWIFT has successfully helped customers on multiple continents both to prevent and to detect attempted frauds. The work also informs our security guidance and security updates and, as we release updates to our software, it helps us to build in critical additional measures to provide greater protection and security to counter the threats. This is all provided at no additional cost to our customers.

At its core, the Customer Security Controls Framework is a core set of controls that aim at enhancing customers' security baselines. Developing the controls was a challenge for SWIFT as they had to work for SWIFT's broad customer base, be in line with existing information security industry standards NIST, PCI-DSS and ISO 27002, and be product-agnostic.

While the framework is, in essence, a global security baseline for the industry, what is even more unique is the attestation process and structure that SWIFT has put in place to complement it. SWIFT customers of all shapes and sizes, and from all geographies, have to evaluate their current cyber defences against the best practices and attest their compliance against the controls. Furthermore, the attestation structure we have put in place enables (and encourages) customers to share their attestation information with their counterparts. In doing this, SWIFT's aim is to increase the level of cyber security transparency and awareness between users. The detailed controls were published in mid-2017 and customers had until 31st December that same year to attest their compliance against them. Although a challenging deadline, the community's response to complying with this first stage was extremely positive; by the deadline, 89 per cent of customers representing 99 per cent of SWIFT traffic had attested.[4]

IMPLEMENTATION AND ROLLOUT

In developing and rolling out the programme, we regularly communicated and consulted with regulators and have been — and remain — heavily engaged with our customers all around the world.

We have run webinars and workshops, roadshows and roundtables, training sessions and bootcamps in our bid to raise awareness, build competence and transfer skills. To ensure the programme and its tools are properly understood and adopted, and to help embed a sustainable cyber security posture across the community, particularly where skills have been most needed, all of this has been conducted in and translated into multiple languages.

The level of direct engagement we have made has been unique; for instance, we ran more than 200 dedicated workshops on our new customer security controls all around the world — workshops that attracted more than 14,500 attendees. And in many cases, we have seen evidence of local initiatives building and following our own, with individual communities choosing to work together to disseminate knowledge and

share experience, or with local regulators putting greater focus on cyber security and even mandating adoption of our guidance. The programme is transformational because it is the first time that the cyber security problem has been addressed systemically and globally through a community-wide approach that is agnostic to customers' size, location, or revenue potential. The impact and substantial benefits of this programme are game-changing for the financial community, due not only to its unprecedented nature, but also the speed with which it has been implemented and the alacrity with which it has been adopted. While the programme is already delivering tangible and truly transformational results, not only in raising awareness, increasing preparedness, building competence and helping to detect and prevent attempted frauds, we will continue to build on its successes in the months and years ahead as we forge ahead in our efforts to help the industry face this unprecedented threat.

As well as guiding customers in improving the security around their operating environments, developing tools and services to help them detect and prevent fraud and creating a global cyberthreat intelligence sharing capability to guard against future cyberattacks, we have significantly contributed not only to a greater awareness of the importance of cyber security, but also to skills and competence building. This is vital, because if there is a widely acknowledge dearth of cyber security skills in large and sophisticated economies, it should come as no surprise that in some of the weaker and more susceptible geographies, the situation is considerably worse.

The educational, skills and knowledge transfer and competence building aspects of the programme have thus always been prioritised; in all this, our efforts have been directed where they have been most needed, irrespective of the revenue generated from or revenue potential of the geographies or customers concerned. (And we have a truly universal spread of customers, encompassing private and public sector banks, central banks, other financial institutions and corporates, stretching across every geography from Far East Asia to North America, and from Northern Europe to Southern Africa.) Where we have identified demand, we have run focused sessions for distinct groups of customers to deliver tailored guidance, specific to each group's particular needs; we then replicated these sessions in other applicable markets. To foster ongoing on-the-ground awareness, best practice sharing and ongoing engagement, we have also worked together with local associations, where necessary equipping these with the wherewithal to continue the discussions.

LASTING EFFECTS

Just 18 months into the programme we have made measurable, tangible progress in helping our customers gear up against the evolving threat. Attacks have been detected and thwarted thanks to increased awareness on the victims' parts, to the alertness of their counterparts, and to the tools we have developed.

The approach we have taken with the programme is far-reaching and all-encompassing. It is aimed at every customer, from the very smallest to the largest, and from the weakest to the strongest. By design, it seeks to overcome barriers and reach all geographies, and it does not differentiate between customers. It does, however, distinguish customer types one from another; we have, for instance, developed solutions tailored to some of our smallest customers — not because these present the most revenue potential, but because these might not have the economies of scale (or, sometimes, the sophistication) to build their own.

SWIFT's experience in investigating cyberattacks on customers has generated a wealth of knowledge and thus we have built a cadre of experts who are on hand to help our customers 24/7, with rapid response capabilities. Our global nature means we are

able to overcome not only the geographical challenges, but also the language barriers, through the use of multilingual experts and the production of educational and actionable information in a wide range of languages.

But perhaps where the programme may have its most catalytic effect is through the controls and attestation processes we have put in place. Already the overwhelming majority of our customer base has attested to their levels of compliance with our new customer security controls. Now, their counterparts are able to ask them for their attestation data — data that they can use to apply risk-based decision making concerning their business relationships, incorporating cyber risk considerations into their calibrations. Customers can calibrate their risk controls according to each particular counterpart they do business with, incorporating a greater or lesser degree of precautions, much as they might in the market or credit risk domains. This increased degree of transparency should motivate those at the stronger end of the security spectrum to continue reinforcing their posture, and those at the weaker end to improve theirs.

Our response in developing the CSP has required an unprecedented effort — from right across the organisation itself, our board, and from the entire community. The board has met first in extraordinary sessions, and subsequently in monthly sessions, to ensure the programme's success, while the subcommittees of the board have been closely engaged in the governance of specific elements of the programme, ensuring appropriate focus and prioritisation.

Above all, however, the programme has been designed for the community and has been shaped by it. From its very inception we have drawn on our community's expertise and experience, working in very close partnership with different user segments to define the detailed design of the programme, its roll-out and adoption. Drawing on the community's advice and input, we have set up expert, consultative and working groups; we have run workshops, established security officers' forums and initiated a close cyber dialogue right across the community.

THE EVOLVING THREAT

The cyberthreat is not transient or static, and the attackers' focus on the financial industry is neither accidental nor fleeting; the financial industry will always be a focus for cyber thieves.

Cisco have pointed to how the adversaries are taking malware to unprecedented levels of sophistication and impact, becoming more adept at evasion and weaponising cloud services and other technology used for legitimate purposes, often exploiting undefended gaps in security, many of which stem from the expanding Internet of Things (IoT).

While the threat remains as large as ever, there are some positive signs of progress. The EU's agency for Network and Information Security (ENISA) recently stated that the collective cyber defence community is gaining evidence regarding monetisation methods and the dynamics within threat agent groups, and has scored some successes with several law enforcement agencies, governments and vendors shutting down illegal dark markets and arresting cybercriminals. Moreover, state-sponsored campaigns have been exposed and details of technologies deployed by nation states have been leaked. And mostly remarkable is the manifestation of the cyberthreat landscape within framework programmes that are about to be established in the financial sector: cyberthreats make up the basis for the development and implementation of red and blue teaming activities in the financial sector, both within EU Member States and across Europe.

But ENISA's view is that the cyber security community is still far from striking the balance between defenders and attackers. Although 2017 has reached records in

security investments, it has also brought new records in cyberattacks of all kinds, data breaches and information loss. From this perspective, one may argue that there is a market failure in cyber security; that is, the increased defence levels and expenses cannot successfully reduce levels of cyberthreat exposure.

The inevitable criminal focus on the financial industry means that the community needs to ensure it has effective cyber defences against well-funded, motivated and organised attackers. Threat intelligence and information sharing is a critical part of that.

In a joint expert report with cyber security specialists BAE Systems, we illustrated the sophistication of attackers' tactics and techniques and evidenced the positive impact of SWIFT's CSP. The report is based on evidence gathered through the detailed forensic work undertaken by SWIFT's CSI team, together with BAE Systems, and has been distributed to SWIFT customers around the world.

The joint report described how there has been a significant evolution in the cyberthreat facing the global financial industry over the last 18 months as adversaries have significantly advanced their knowledge. The adversaries have deployed increasingly sophisticated means of circumventing individual controls within users' local environments and have used ever more creative techniques to access users' critical assets. These include gaining administrator rights for operating systems, manipulating software in memory and tampering with legitimate functionality to bypass authentication.

The report also illustrated the chronology of a typical attack and explained how highly covert malware, designed to withstand traditional detection techniques, is being deployed in the attacks. This showed that in any single attack a mix of malicious files will often be used, whether to acquire credentials or to bypass authenticating requirements; to learn how internal operations or messages work; to create distractions and delay local security teams' responses; or to securely delete log files and other traces of attack.

As well as detailing the attack approaches, the report provides a useful summary of the safeguards customers need to put in place to protect against the threat, starting with basic perimeter and internal security measures, and evidences the impact and importance of SWIFT's CSP.

MILESTONES

In the immediate term, our next key milestone is presented in the further stage of our Customer Security Controls Framework. In what will mark a significant step-change, all SWIFT customers will need to reattest in the current year, confirming their full compliance with the 16 mandatory security controls. And even this will not be a one-off, as the exercise will be annual and the controls will continue to evolve over time. Our hope is that customers will soon view self-attestation as part of an ongoing change management cycle to drive real security improvements.

SWIFT's global reach, its cooperative structure and its unique governance have enabled us to both prepare our response and ensure its aptness. It has afforded us the privilege of being able to learn from and reach out to and assist the community: transferring skills and experience from one customer to another, and from one geography to another — all the while preserving confidentiality and anonymity.

References

1. IBM Security (March 2017), '2017 IBM X-Force Threat Index', available at https://www.ibm.com/security/data-breach/threat-intelligence (accessed 8th August, 2018).
2. Swift (January 2018), 'Exceeding 7 billion message mark, just one of the highlights of

a successful 2017 at SWIFT', available at https://www.swift.com/news-events/news/exceeding-7-billion-message-mark_just-one-of-the-highlights-of-a-successful-2017-at-swift (accessed 24th July, 2018).
3. Das, K. N. and Spicer, J. (July 2016), 'How the New York Fed fumbled over the Bangladesh cyber-heist', Reuters, available at https://www.reuters.com/investigates/special-report/cyber-heist-federal/ (accessed 24th July, 2018).
4. SWIFT (January 2018), 'Excellent community response to SWIFT's Customer Security Controls Framework', available at https://www.swift.com/news-events/news/excellent-community-response-to-swift_s-customer-security-controls-framework (accessed 24th July, 2018).