English

CYBER SECURITY

Report 2020

Welcome

Dear Reader,

These are extraordinary times. None of us has ever experienced anything like the coronavirus pandemic. and it remains uncertain when normality will return. So far, 2020 brings few rays of hope, but at least one positive thing has emerged from the crisis: companies, administrations and educational institutions are experiencing an enormous surge in digitalization, considered unlikely in January of this year.

Using remote working, video conferencing tools and the cloud brings challenges, though, especially for financial institutions. The Swiss Financial Market Supervisory Authority (FINMA) speaks of a "sharp rise" in the number of phishing attacks during the pandemic, adding that "cybercriminals are creative and ruthless" and are "using the current crisis to refine their attacks".

So what must be done to prevent this? There is a simple answer to this question: we need more cohesion and cooperation in the financial sector. Cyber defence works best if the global network of banks, insurance companies, FinTechs, InsurTechs, RegTechs, as well as politicians and data scientists, are united in their approach.

The annual SIX Cyber Security Report is intended to grow the level of knowledge in the community. We have been able to attract a wide circle of authors and interview partners for this issue, with the business side represented by Alain Beuchat, one of Switzerland's most renowned security specialists, the political side by Florian Schütz, the Confederation's delegate for cyber security, and the scientific side by the Swiss Federal Institute of Technology in Zurich (ETH Zurich). Another new aspect of this year's report is that we are looking ahead in an effort to anticipate the threats and defences of tomorrow.

Finally, I would like to draw attention to our SIX Cyber Security Hub. In 2018, we founded this exchange platform for cyber security. Within a very short amount of time, it has established itself as a central location for cyber security in the financial sector. For this year's report, we conducted a survey with over 90 members on the topic, the findings of which we analysed and compiled.

I hope you find the report insightful, exciting and educational.

Jos Dijsselhof
CEO SIX

Table of Contents

Executive Summary

This report provides insights into the cyber security threats observed within the Swiss financial sector.

As in the previous year, the report investigates the cyber security situation from two different angles. Firstly, it compares how the financial sectors of selected countries are affected by cyber security threats. Second, it provides a view from within the Swiss financial sector on what it perceives to be the most important cyber security issues currently. Additionally, it features an emerging technology that may improve the security and resilience of the use of Internet connectivity by Swiss financial institutions in the future.

To start with, the Macro Analysis section of the report is primarily based on the evaluation of open source intelligence information. The Micro Analysis section is, to a large extent, based on information contributed by members of the SIX Cyber Security Hub. The final part is formed from a cooperation between ETH Zurich and SIX.

Comparing the cyberattacks experienced by the Swiss and other national financial sectors over the last year, they continue to be subject to frequent attacks. Overall, the number of attacks observed has remained at the same level as the year before for each country. A significant difference, compared to the previous year, is a clear rise in the number of cyberattacks around March, which is related to the COVID-19 pandemic outbreak. As in last year's report, by far the highest number of attacks on the financial sector were recorded in the USA, followed by the UK. Regarding the type of threats, the most prevalent threat observed was ransomware, followed by phishing attacks.

Focusing on the Swiss financial sector, the report first investigates the structure of security incidents as observed by contributing organizations, with a special focus on the impact of the COVID-19 pandemic. Phishing, followed by ransomware, were the highest perceived threats by these institutions. This correlates with e-mails being the top attack vector on financial institutions. We also observed a clear spike in attack activity correlated with the COVID-19 pandemic. The report then investigates the structure of CISO operations within the sector, providing insight into the available resources and their use within organizations. This shows a correlation between reported visibility and the number of observed incidents within an organization where higher visibility increases the number of incidents.

Shifting the focus away from cyberattacks, the report introduces a new network technology emerging from research efforts to address some of today's Internet shortcomings. This new technology addresses how data is transported in the Internet. Its properties make it interesting for use in a financial setting, where it restricts transmitted data from leaving Switzerland. As a result, a group of financial institutions, in collaboration with SIX, are currently evaluating this technology further to determine its potential to transport financial data, such as payment information.

This report is authored by SIX, together with research input from QuoIntelligence and data from Recorded Future.

Key Findings

- The overall number of attacks observed remains comparable to the level reported in last year's report.
- An increase in observed cyberattacks occurred during the onset of the COVID-19 pandemic in March.
- The most frequently observed attack methods are generally the same across all countries assessed.
- The ITU Global Cybsecurity Index of the countries does not correlate with the reported number of observed attacks.
- The Swiss financial sector continues to see a very low number of cyberattacks compared to other countries.
- Regardless of the size of organizations in Switzerland, the rapid changes caused by digitalization and the corresponding need to rapidly adapt IT architecture are viewed as the greatest challenges to maintaining cyber security.
- Swiss Chief Information Security Officers (CISOs) are concerned about being able to address these changes, highlighting the need for adequate funding for their operations and the challenges of retaining a skilled workforce needed to maintain high levels of cyber security.
- According to various Swiss financial institutions, the cyberattacks that they find themselves at risk of most are phishing, malware and ransomware.
- There is a correlation between the number of incidents observed and the maturity, and visibility, of CISO operations in the Swiss financial sector. CISOs who ranked visibility and maturity higher also observed more incidents.

Why This Report

This SIX Cyber Security Report provides an overview of the Swiss financial industry's current cyber security situation and the threats it is facing. In order to paint as comprehensive a picture as possible, surveys and evaluations were conducted and insights from prominent business, political, and research representatives were also included.

The number of reports, studies and analyses in cyber security has grown considerably in recent years. As such, it is increasingly difficult to fully comprehend the situation. The present report is primarily focused on Switzerland and, in particular, the Swiss financial industry. This includes all banks and insurance companies, as well as FinTechs, InsurTechs and RegTechs based in Switzerland.

Although the SIX Cyber Security Report looks at the Swiss financial industry in detail and analyses its specific threat situation, the report also covers a broad spectrum and compares the Swiss financial sector with other countries.

At SIX, we believe a strong cyber security community is the best response to the current threats. To strengthen this community, and because representatives of the financial industry can learn a lot from each other, we publish the SIX Cyber Security Report annually. The anonymous surveys conducted among more than 90 members of the SIX Cyber Security Hub provide an in-depth and thorough insight into the challenges facing the local cyber security community.

Insights from prominent business, political and research representatives

This report is primarily focused on Switzerland, in particular the Swiss financial industry

To strengthen the cyber security community

Contributors

The SIX Cyber Security Report offers a comprehensive and detailed picture of the current cyber security threats facing Switzerland, and draws on the expertise and opinions of a large number of experts. As a central body of the financial sector, SIX brought together the various participants and consolidated their thoughts.

The following organizations are involved in this year's SIX Cyber Security Report:

- SIX operates the system-critical infrastructure for payment traffic and for the Swiss Stock Exchange and has established a world-leading SOC.
- Recorded Future collects global Open Source Intelligence (OSINT) data, on which the macro and part of the micro analysis of this report is based.
- Over 90 members of the SIX Cyber Security Hub took part in a survey regarding the threat situation in Switzerland. The results are published anonymously in this report and form the data basis of the micro analysis. The members of the Hub include banks, insurance companies, FinTechs, InsurTechs and RegTechs.
- QuoIntelligence is responsible for a substantial part of the data collection and analysis.
- ETH assesses the significance of new technologies (here SCION) on the current security situation (Department of Information Technology and Electrical Engineering).

The SIX Cyber Security Hub is a non-commercial platform that ensures the constant exchange of information on the subject of cyber security. The community exchanges experiences, learnings and know-how as well as information on weak points and attacks.

How do you become part of the Cyber Security Hub? All Swiss banks and insurance companies regulated by FINMA are invited to participate. If you are interested, please contact securityhub@six-group.com.

Methodology

The micro and macro analyses are based on an evaluation of structured collected data, among other things, which was evaluated jointly by SIX and QuoIntelligence. The necessary data was defined, collected and analysed in order to understand the threats present in cyber security.

The macro analysis examines cyber threats in the financial sector of various G20 countries and Switzerland. The countries were selected on the basis of their geographical proximity to Switzerland, existing import/export relations, and whether their financial sector is similar to Switzerland's. The macro analysis shows the total number of incidents per country, and sentiment regarding cyberattacks was surveyed based on publicly expressed opinions via platforms such as Twitter. Special attention was also paid to the comparability of the countries. The data is based on OSINT information, collected by Recorded Future.

For the micro analysis of the Swiss financial sector, financial institutions were grouped based on their size into small, medium and large organizations. The raw data was obtained from a survey of over 90 members of the SIX Cyber Security Hub. They were anonymized, aggregated and, where appropriate, supplemented by OSINT data.

Applied Research: the question here is what influence new technologies could have on the threat landscape of the Swiss financial sector. For this report, the ETH SCION project was selected, which is already being used by SIX, Swisscom and other players in Switzerland. The abbreviation stands for Scalability, Control and Isolation on Next-Generation Networks – a kind of new, very secure Internet. In addition, there is a first global SCION network that enables comparisons to be made with other countries. The SCION technology aims to completely replace traditional Internet connections. This report discusses the benefits and security improvements that SCION will bring and those it will not.

Over 90 members of the SIX Cyber Security Hub

"Scalability, Control and Isolation on Next-Generation Networks"

Alain Beuchat,
CISO Lombard Odier

Florian Schütz,
Delegate of the Federation
for Cyber Security

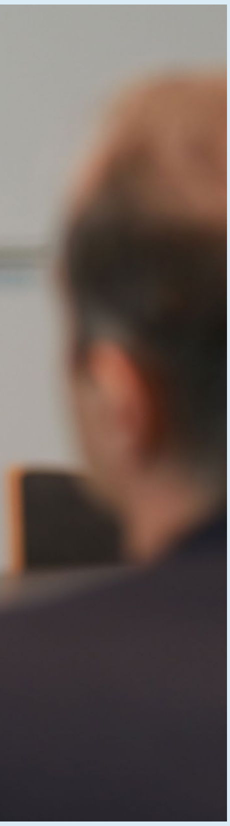
Interview questions with Mr. Schütz and Mr. Beuchat

SIX: Mr. Schütz, please could you describe your role and your mandate.

Mr. Schütz: I am the Swiss delegate for cyber security. On the one hand, this means I am responsible for coordinating all cyber activities within the Swiss government across all departments. In Switzerland, there are two main contributors to the cyber topic: the Department of Defence and the Department of Justice. The Department of Justice is mainly responsible for cybercrime. The Ddepartment of Defence is responsible for cyber defence, military defense, and intelligence. We also have the financial department, where I am based, which is primarily responsible for cyber security. On the other hand, I am also responsible for the coordination and implementation of the national strategy for the protection of Switzerland from cyber risk, the NCS. At NCS, I coordinate the steering committee, which consists of people from the economy, cantons, educational institutions and the government.

SIX: So, you are not only looking at the public sector, but also at the private sector. In other words, working on how to improve cyber security for the whole nation?

Mr. Schütz: Exactly. That is the mandate for the NCS. **Our first goal is to always ensure we can position Switzerland in a secure and digitalized world, where we can act as freely as possible.**



SIX: Have you seen an increase or decrease in the number of cyber incidents and a change in their overall sophistication over the last 12 months?

Mr. Beuchat: The financial sector has seen an increase in cyberattacks over the last 12 to 18 months. Criminals have been using ransomware to gain substantial benefits from cyberattacks. Attacks are becoming more targeted, as criminal organizations are systematically exploiting the new vulnerabilities that are disclosed by vendors and security firms. In the past, it could take months before criminal organizations started to exploit disclosed vulnerabilities. Nowadays, we observe the active exploitation of newly disclosed vulnerabilities within days. **The risk for organizations has been especially high in 2020, as a multitude of vulnerabilities affecting Internet-facing systems such as firewalls were disclosed.** This means that we must be very agile and in a position to protect ourselves as soon as possible. If we cannot fix the vulnerability because we lack the necessary patch, then we need to ensure that we have the capability to monitor potential attacks and, as a last resort, block the access to our systems to protect our environment.

SIX: Stop your systems?

Mr. Beuchat: Well, this would be the last resort. Fixing vulnerabilities means obtaining the related security patch, testing all business functionality, and applying the correction in all instances. This process can take days, and if we observe any attack during that time, we would have to potentially block the access to the vulnerable systems, as the risk would be too high.

“The financial sector has seen an increase in cyberattacks over the last 12 to 18 months.”

Mr. Beuchat

SIX: Was your senior executive, the Board of your organization, aware that there was a possibility that you would have to stop (the system)?

Mr. Beuchat: That is a good question. **We inform our senior management when there is a critical vulnerability affecting our systems.** We monitor the situation closely through our threat intelligence capability and by triggering alerts in case of an attack on our systems. **If the risk increases, we decide, together with the organizations impacted, whether we will block the access to the systems or not.**

Mr. Schütz: From our perspective, the number of attacks is indeed increasing. We looked back on the last 15 years when MELANI (Melde- und Analysestelle Informationssicherung) existed, and it has increased dramatically. **One of the main reasons for this is that the world is becoming increasingly digital and the criminals have moved online.** What we also see is that the attacks become more sophisticated where there’s a lot of potential gain, which is almost always the case when financial institutions are a target. At the same time, we also see an increase in the very simple attacks that you can easily protect yourself from. But because so many companies have digitalized so quickly and without a core understanding of the potential dangers, it makes them easy targets. So we see that diversification. Interestingly, we always look at attackers as players in a completely deregulated market: in the end, they want to maximize their profit, they don’t have any rules to follow, and they really are inventing their own business model. Ransomware used to encrypt your system as soon as it entered. Attackers have now started to move towards targeting the core, aiming at an organization’s more valuable systems. Now ransomware steals your data first, then it encrypts. If you don’t pay for the decryption, the attackers will publish your data. They are very carefully calculating the amount that they ask from you. So they invest a lot in more sophisticated operations and innovate their business model.

Mr. Beuchat: There was an article recently on how such business models work. Typically, there are attackers that are only focused on finding ways to hack into an organization; they are called “initial access broker”. They are not looking to exploit these accesses themselves, but will sell them to organizations such as ransomware operators, who will exploit them as Mr. Schütz alluded to.

Mr. Beuchat: And I think that’s one of the reasons why the pace of these attacks is so fast now. It is a matter for the initial access brokers to identify and exploit vulnerabilities and, as soon as they are successful, sell the access for example to a ransomware operator. The ransomware operator will then use the access to deploy the ransomware at its target.

SIX: It is an ecosystem.

Mr. Beuchat: Yes, **we always talk about ecosystems**, but we did not find them that often outside the financial sector in the past. For example, the “money mules” networks, which used to cash out the money stolen from fraudulent transactions, were part of an ecosystem. Nowadays, for example concerning ransomware attacks, I think we feel it much more often that we deal with very sophisticated threat actors. We have observed the transformation of ransomware attacks. A few years ago, they were focused on individuals with a small return, perhaps CHF 300 to 500. Now they are targeted attacks against organizations, so called “big game hunting”, with returns that could be in the millions.

Mr. Schütz: It’s interesting that the dynamics have changed. One thing that is more and more concerning from the government’s perspective is the growing cyber insurance market. If we look at the USA, for example, some cyber insurances have decided that it is cheaper to pay in case of ransomware and other cyberattacks than to cover the cost of reconstruction. This sends the message to the threat actors that their business model is working. When we look at these things, we wonder how we can really disrupt their business models. This is why we are not only focusing on what technology is in use. Combined with our intelligence service, the federal police and the cantonal police, we also try to identify how these organizations operate, where they operate, and how they exchange information. This is a truly global business. **We have analysed attacks in the financial sector, where the people supplying the technology were based in Nigeria and the people committing the attack were operating from the Netherlands**. That’s the global context we talk about when are trying to provide an overview of how this works. **Future projects and ideas are about trying to make this kind of information more accessible to organizations**, not just financial institutions, but also other sectors. There are pilot projects in that area, where we can actually give that information to organizations so that they can protect themselves effectively.

SIX: If you speak too openly about these procedures, Mr. Schütz, could this be a risk? The threat actors could profit from your information and create a counter-mechanism.

Mr. Schütz: There is always that risk. I see that risk primarily when we talk countermeasures on the technological side, and on how we do investigations. So, we do not disclose that. But, as this is a global market, **these organizations will move their business model to where things are safe, and that is why I always encourage organizations to talk about their cyber incidents**.

Mr. Beuchat: Yes, I believe that info sharing is key, because criminal organizations themselves share information amongst mselves. By sharing information about attacks, we give them fewer opportunities to attack other organizations.

SIX: Mr. Beuchat, what would you define as your top three challenges, and why?

Mr. Beuchat: We need to stay agile in order to be able to understand and cope with new types of attacks. Furthermore, the dependency on third-party providers such as managed security service providers and other vendors is a challenge. We need to ensure that they maintain an equivalent level of cyber security and data protection for their operations than the one that is prevalent in the financial sector.

SIX: So, what is the solution to bring managed security services back in-house?

Mr. Beuchat: I do not think it is possible. On one hand, in-house security services would be too costly for most small and middle-size organizations; and on the other hand, we would not find enough qualified staff anyway. I think it is a question of working together with managed security services providers.

Mr. Schütz: When I look at the government’s cyber operations, I see a similar challenge. We have a lot of operating models, and so we are dependent on outside providers and SAPs. Also, the cloud is a big topic. In my opinion, we must consider the cloud or we fail to be competitive. For me, the solution should start with data governance. What happens if a bank needs to be switched off due to a cyberattack – who has the authority to make that decision? How can it be decided? What are the dependencies between the banks? Let me give you an example of why this is relevant. In the first Gulf War in the 1990s, the Americans questioned if they could attack Saddam Hussein’s banks and what the effects would be on other global banks, because there are so many interdependencies. Dependency is an even bigger issue today. We are talking about managing dependencies with multiple types of data, and I think we need smart solutions here. That brings me to the second challenge. I see, especially in Switzerland, that we are educating some very skilled people. But there is little opportunity for them to take management positions domestically. I think we need to change the attitude on the Board level. We need people there who realize that our dependency on technology has become so big now that it is no longer an operational issue, but a strategic issue. And we need to have someone at the table who understands that. At the same time, existing leaders in the financial sector and beyond must start to understand the digital aspects of their business better. ■

p:slideV
ViewPr></p:
ViewPr></p:note
x="0" y="0"/ /p:
<p:scale><a:sx n
orient="horz"
y=72008l /p:viewPr
/p:normalViewPr p:slideViewPr>
p:origin x="

Macro Analysis

Comparison by Country

Methodology

For the purpose of this report, SIX, in cooperation with QuoIntelligence and Recorded Future, collected, analysed and assessed data on the cyberthreat landscape of selected countries. The data analysed for this report is sourced from open source intelligence information (OSINT). The majority of data was provided by Recorded Future, with additional data provided by QuoIntelligence. In some instances, we filtered the data set pro-vided to only include data points with sufficient information available. For example, not every data instance also includes a specific attack method. So when we analysed attack methods, we filtered them down to data points that include this information.

The selected countries analysed for the macro part of this report are Germany, France, Spain, the Netherlands, the UK, the USA, and Singapore. The purpose of the macro analysis is to identify key similarities and differences between the cyberthreat landscape pertaining to the Swiss and the other selected countries' financial sectors.

The financial sector is an attractive target for cyber actors, given the potential access to financial assets and highly sensitive client data. Due to these factors, the financial sector is targeted by many types of cyber actors, from hacktivists with little capabilities, to opportunistic attackers leveraging malware bought in underground forums, to highly sophisticated state-sponsored actors. At the same time, the attack surface of financial institutions continuously increases, due to a larger need for digitalization and demand for online services. These developments, which were observed in previous years, were further accelerated and exacerbated by the onset of the COVID-19 pandemic. Within weeks, organizations shifted to remote working and customers relied more than ever on online banking applications, creating new targets for malicious cyber actors.

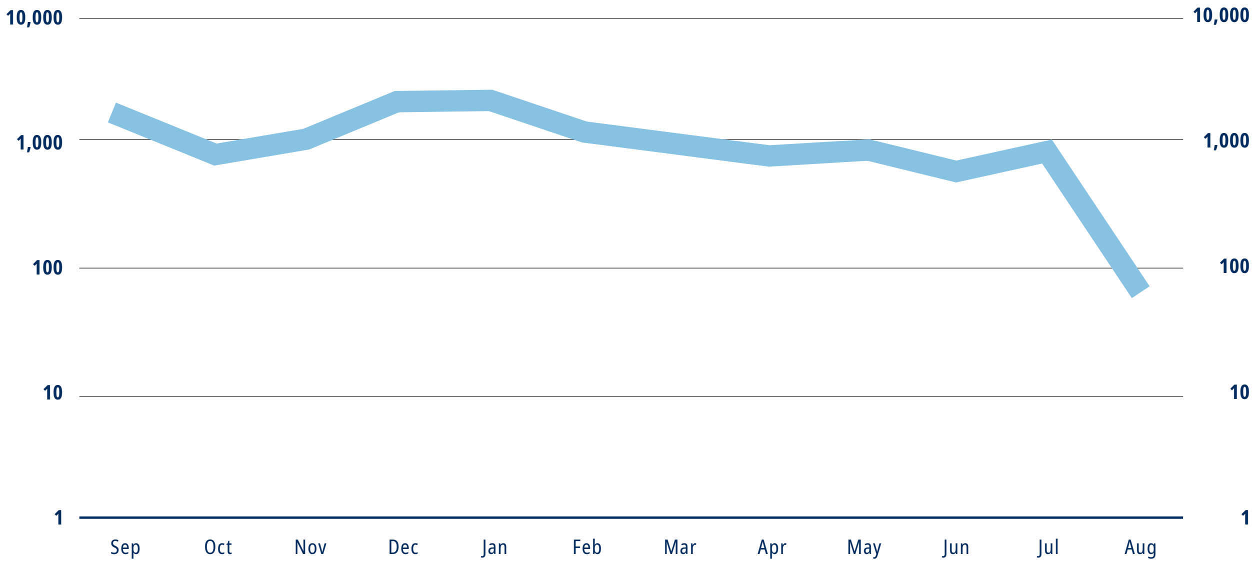


Figure 1 — Total Number of Cyberattacks Observed in Selected Countries (September 2019–August 2020)

As can be seen in Figure 1, the second-highest number of cyberattacks recorded across our selected countries occurred in March, coinciding with the first wave of COVID-19 restrictions in Europe. However, in general, the number of incidents remained fairly steady over the reporting period. The dip in August is caused by our cut-off date to receive data and does not necessarily imply a decrease in cases.

In this part of the report, we outline and highlight key similarities and differences between the cyberthreat landscape in Switzerland compared to our selected countries. This includes a brief overview of the regulatory maturity of each of the assessed selected countries, as well as key developments and cyber incidents observed over the previous year. We used the ITU's Global Cybersecurity Index (GCI) ranking[1] as a baseline for assessing each of our selected country's cyber security commitment and situation.

Member State	Score	Global Ranking	Regional Ranking
United Kingdom	0.931	1	1 (Europe)
USA	0.926	2	1 (Americas)
France	0.918	3	2 (Europe)
Singapore	0.898	6	1 (Asia Pacific)
Spain	0.896	7	5 (Europe)
The Netherlands	0.885	12	8 (Europe)
Germany	0.849	22	13 (Europe)
Switzerland	0.788	37	22 (Europe)

The structure of the following report is based on this ranking, with the highest-ranking country being analysed at the beginning and concluding with Switzerland as the lowest-ranking country.

[1] ITU, November 2019, Global Cybersecurity Index 2018

United Kingdom

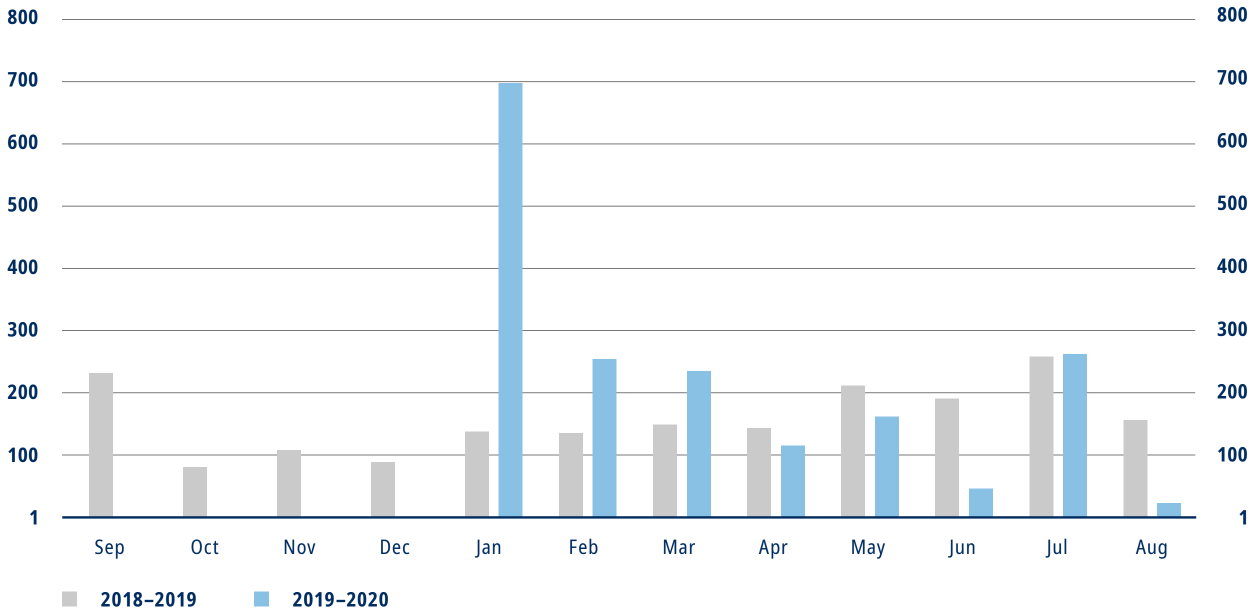


Figure 2 — Total Cyber Incidents Observed Targeting Financial Institutions in the UK (2018–2020)

London is a financial hub in Europe, with the largest European stock exchange, the largest bank in Europe (HSBC Holdings), and three United Kingdom (UK) banks out of Europe's top ten largest banks.[2] The financial sector of the UK is regulated by the Prudential Regulation Authority (PRA), and in terms of cyber security, the UK is ranked in first place internationally by ITU, due in large part to strong performance in the ITU's organizational and regulatory pillars. According to a recent survey by the UK government, the financial sector identified cyber security as a very high priority.[3] Additionally, the lowest ratio of cyber incidents to breaches was recorded in the UK, potentially indicating a high capability in mitigating attacks.[4] However, the highest-recorded total loss by one organization was recorded by a UK financial services firm, which amounted to EUR 94 million.

Based on our data set of observed incidents and filtered for data points with attack methods included, ransomware was the most popular attack method, used in over 70% of incidents (⟶ Figure 3). This was followed by phishing and SQL injections.

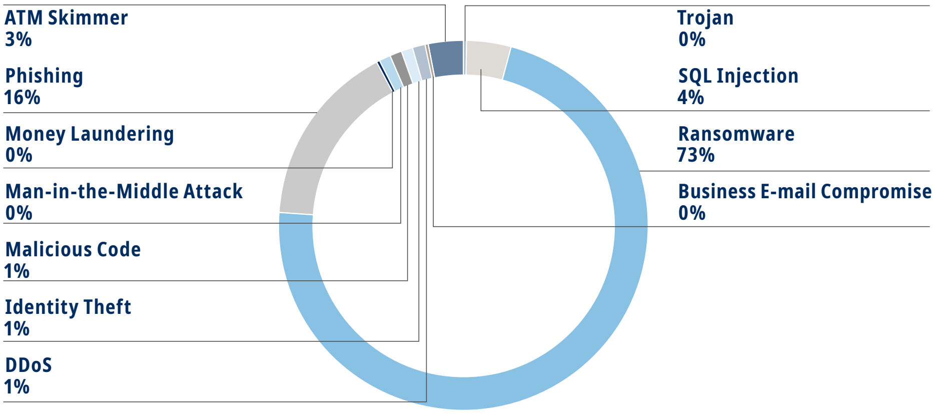


Figure 3 — Attack Methods Observed Targeting Financial Entities in the UK

[2] S&P Global, April 2020, Europe's 50 largest banks by assets, 2020

[3] Department for Digital, Culture, Media and Sport, March 2020, Cyber Security Breaches Survey 2020

[4] Hiscox, June 2020, Cyber Readiness Report 2020

USA

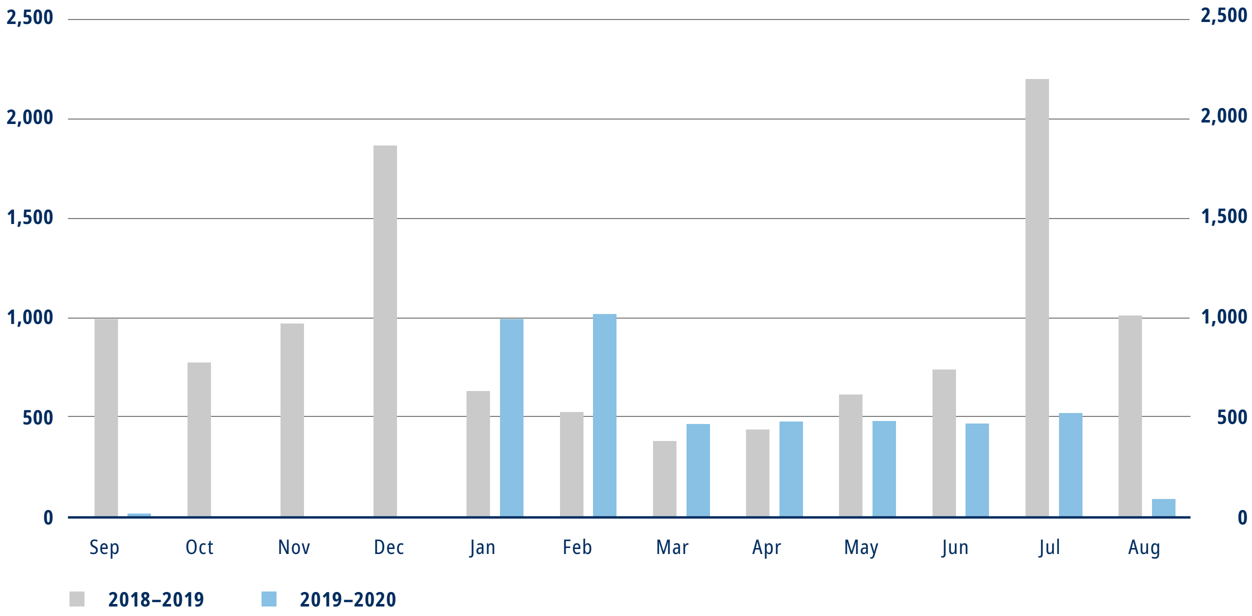


Figure 4 — Total Cyber Incidents Observed Targeting Financial Institutions in the USA (2018–2020)

The USA has by far the most recorded number of incidents out of all the selected countries in this report, which is partly due to the USA being a hugely attractive destination for cyber actors. However, the prevalence of cyber security organizations, which meticulously record and analyse cyber incidents across the region, as well as the high capability and maturity of cyber security mitigations and the overall importance of the US financial sector globally, likely contributed to this large amount of available information. While the USA is highly likely to be among the countries most targeted by cyber actors, the transparency and maturity in which cyber incidents are recorded also contributes to this high availability of data. The USA also ranks highly in terms of their cyber security, ranking second globally.

According to a recent survey, 80% of financial institutions reported an increase in cyberattacks in 2020.[5] Cyberattacks reportedly increased further between February and April by reportedly almost 240%, correlating with the COVID-19 pandemic.[6] Based on our data set, we observed spikes in January and February 2020, and slightly higher numbers of incidents compared to 2019 in March and April (→ Figure 4). Ransomware attacks increased significantly during this time. Based on our data (→ Figure 5), which we filtered for clarity by excluding any non-statistically relevant attack methods and any incidents without relevant tags, an increase in ransomware, which dipped at the end of 2019, can be seen in February and March. Additionally, while numbers are generally low, distributed denial-of-service (DDoS) attacks increased in March.

[5] VMWare Carbon Black, May 2020, Modern Bank Heists 3.0

[6] VMWare Carbon Black, May 2020, Modern Bank Heists 3.0

Overall, similar attack methods targeting the financial sector in the USA compared to the other selected countries were observed, namely ransomware and supply chain attacks.

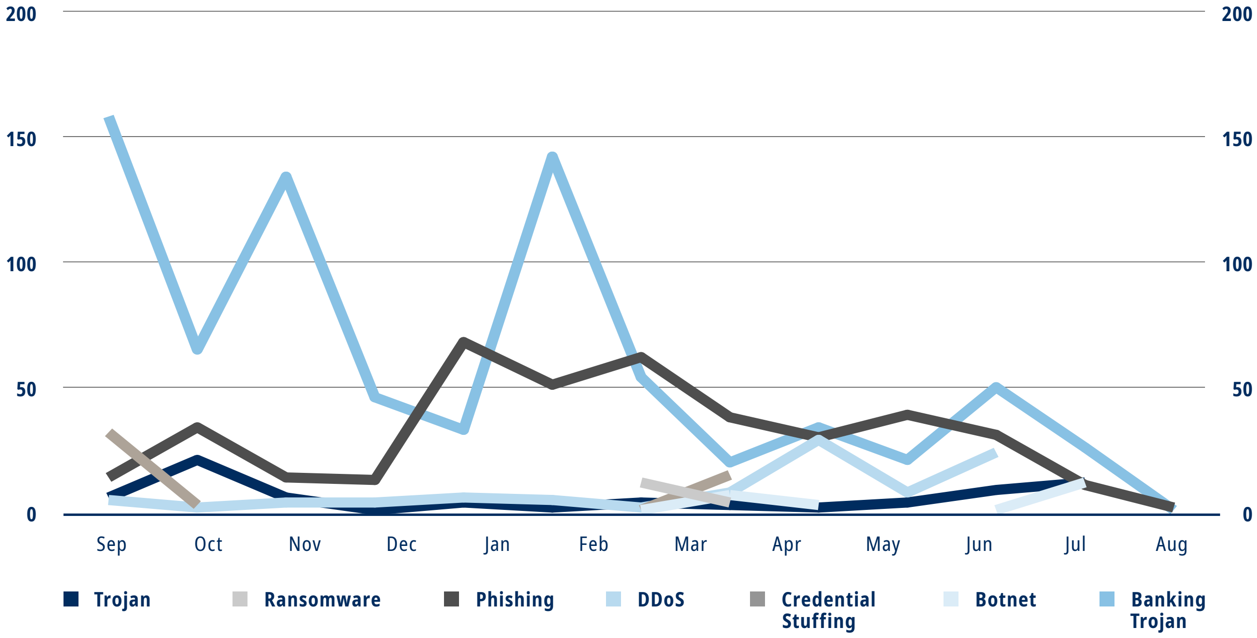


Figure 5 — Attack Methods Observed in Attacks Targeting Financial Institutions in the USA (2018–2020)

France

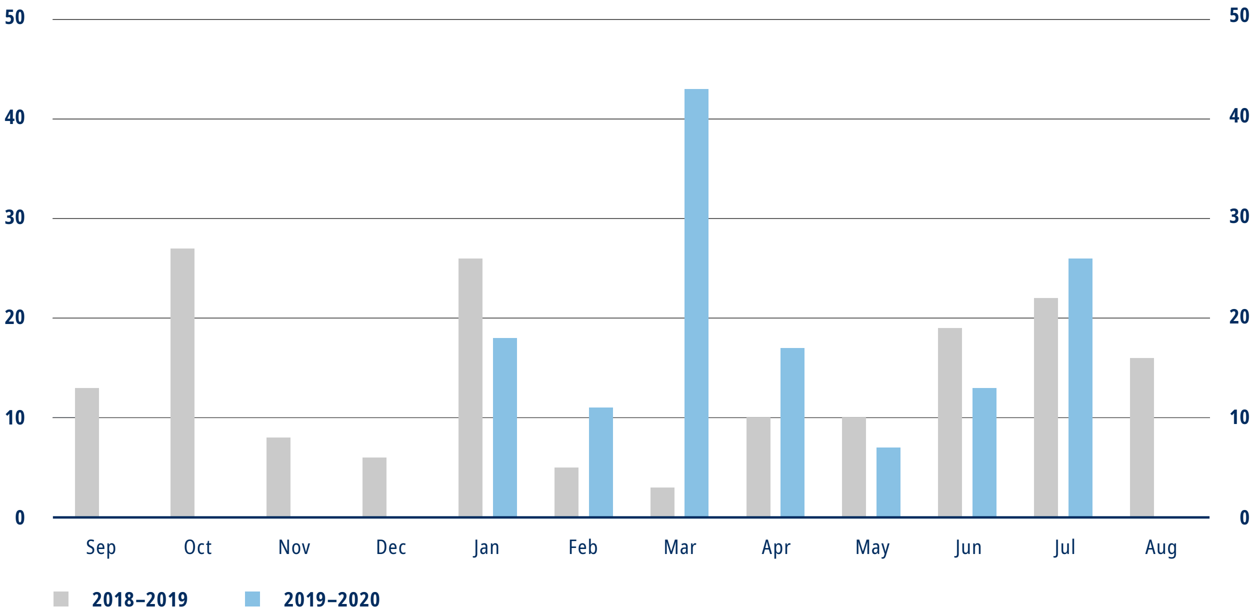


Figure 6 — Total Cyber Incidents Observed at Financial Institutions in France (2018–2020)

France is home to four of the eight Global Systemically Important Banks (G-SIBs), which are also among the ten largest banks in Europe.[7] These large, well-known and internationally operating banks – BNP Paribas, Crédit Agricole, Société Générale, and Groupe BPCE – put the French financial sector on the map for cyber actors. Possibly due to the knowledge of their exposition, France has clearly prioritized cyber security over recent years. According to the ITU, France achieved 100% in its legal and organizational pillars and ranked in third place globally in terms of cyber security.[8] France's national cyber security agency (Agence nationale de la sécurité des systèmes d'information, or ANSSI) recorded more than 370 cyber incidents in 2019, with nine being major incidents, as well as their involvement in 16 cyber defence operations.[9]

As can be seen in Figure 6, our data set includes fewer incidents, indicating the high visibility of ANSSI across the sector. Interestingly, a spike in cyberattacks was observed in March, April and again in July, coinciding with the onset of the COVID-19 pandemic. According to ANSSI, the main trends in France's cyberthreat landscape are ransomware attacks, espionage attempts and supply chain attacks, similar to threats observed in Switzerland.

[7] S&P Global, April 2020, Europe's 50 largest banks by assets, 2020

[8] ITU, November 2019, Global Cybersecurity Index 2018

[9] ANSSI, June 2020, ANSSI in action: Looking back on 2019

Based on our observations (→ Figure 7), and after our data set was filtered to exclude non-relevant entries, ransomware was most frequently observed in terms of attacks targeting French financial institutions. The spike in March, which can be seen in Figure 6, is largely due to an increase in ransomware. Phishing remained relatively steady throughout the year, while dipping in May with the onset of the third quarter. Interestingly, a wave of DDoS attacks occurred between March and May, coinciding with the onset of COVID-19 restrictions and the sudden increase in remote working. The strained bandwidths due to this increase as well as the remote working itself can make applying patches to vulnerable devices more complicated. This could lead to devices being left vulnerable and thus exploited for DDoS attacks.

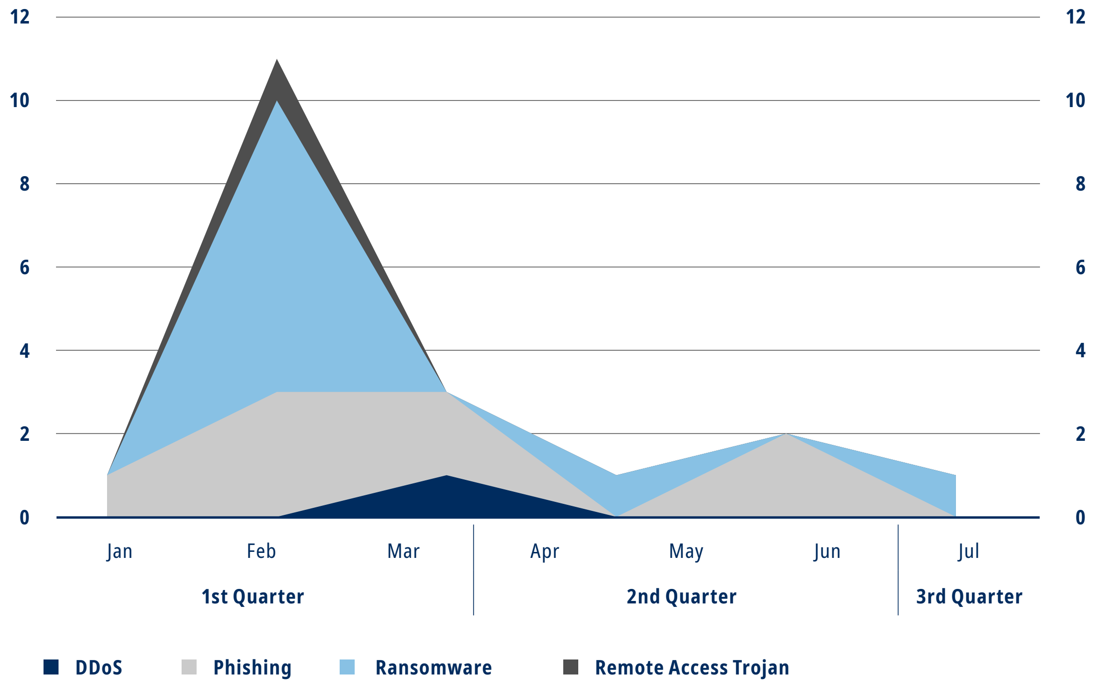


Figure 7 — Types of Cyberattacks Observed in France (2018–2020)

Singapore

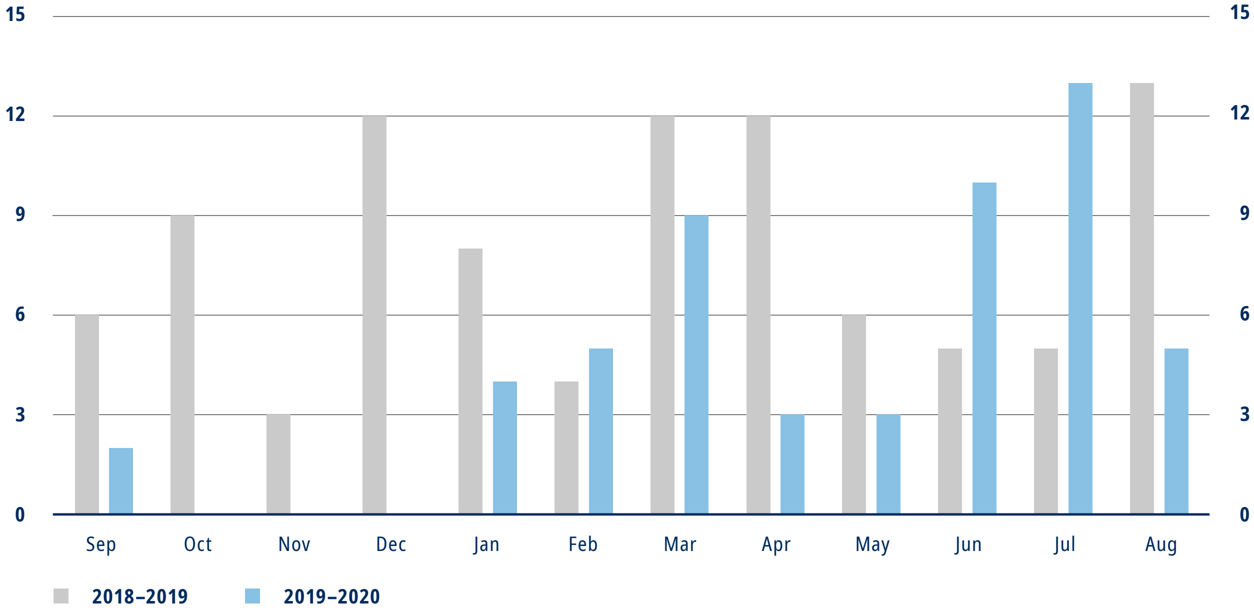


Figure 8 — Total Cyber Incidents Observed at Financial Institutions in Singapore (2018–2020)

Singapore is a major financial hub in Asia, where its geographical and geopolitical context significantly differs from the other selected countries in this report. This potentially impacts the nature and frequency of the cyberattacks targeting the country. In fact, according to a recent survey,[10] the most frequent type of cyberattacks observed by Singaporean Chief Information Security Officers (CISOs) over the previous 12 months was custom malware, with 75% of respondents from financial services saying it was the attack method most frequently used. Ransomware, which was generally among the most frequently observed methods in our selected countries, was only ranked in 10th place. Additionally, 80% of respondents suffered a breach following a cyberattack in the last year. In their annual report, Singapore's Cyber Security Agency (CSA) additionally identified website defacement, phishing, and malware infections as the highest concerns.[11]

Our data set for Singapore included the second-smallest number of incidents among our selected countries after Switzerland. This is surprising, given the numbers above, according to which 80% of CISO respondents suffered a breach. However, from the data available, fewer incidents were observed overall in 2020 compared to 2019. Only in June and July of 2020 were considerably more incidents observed compared to 2019 (→ Figure 8). The divergence between the low observation rate and a majority of CISOs reporting breaches could have several explanations. On the one hand, similar to the UK, a high number of incidents reported but a low number of breaches reported could indicate greater proficiency for mitigating cyberattacks. The ITU ranked Singapore sixth in their cyber security ranking, highlighting Singapore's high cyber security capabilities. On the other hand, this low reported number could indicate a lack of transparency or information sharing measures, in which cyberattacks are not publicly reported.

[10] VMWare Carbon Black, June 2020, Singapore Threat Report

[11] CSA Singapore, 26 June 2020, Cyber Threats Grew in 2019 Amid Rapidly Evolving Global Cyber Landscape

Spain

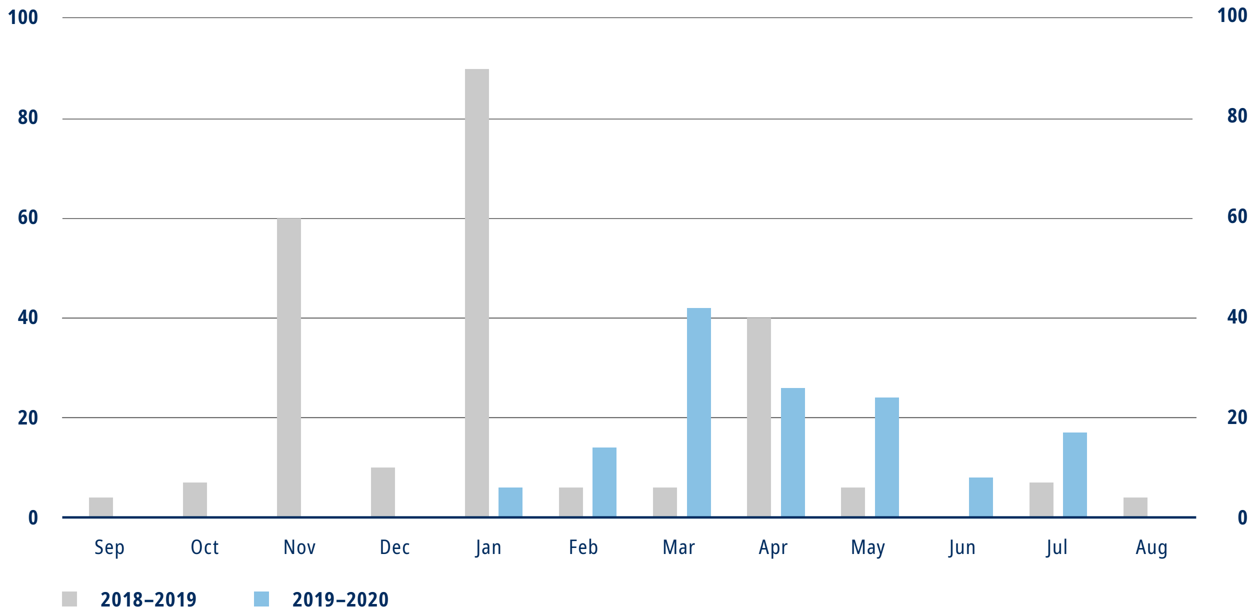


Figure 9 — Total Cyber Incidents Observed at Financial Institutions in Spain (2018–2020)

Spain's financial sector is smaller compared to France, Germany and the Netherlands, and only one Spanish bank, Santander, is among Europe's largest banks. However, Spain ranks highly in terms of cyber security, in seventh place in the ITU's index. Spain's government has clearly prioritized cyber security, and as a result, investment in cyber security has more than doubled in the year up to 2020.[12] Based on our data (→ Figure 9), cyber incidents observed spiked in March 2020, potentially coinciding the COVID-19 pandemic, and were generally higher over the course of the year compared to 2019, except for January 2019. In January 2019, several separate phishing and DDoS incidents were observed.

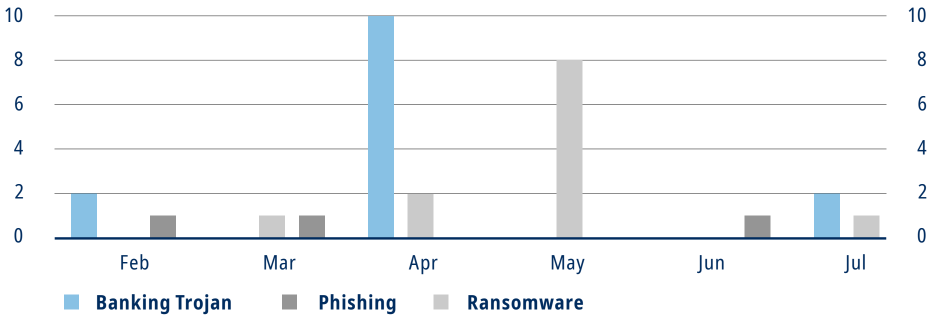


Figure 10 — Types of Cyberattacks Observed at Financial Institutions in Spain

Figure 10 outlines some interesting regional differences between Spain and other selected countries analysed in this report. After the data was filtered to exclude non-statistically relevant entries, we saw a spike in observed incidents in April, which correlated with the Brazilian banking trojan Grandoreiro targeting Spanish banks. Similar incidents were not observed in any of the other selected countries. However, similar to the other selected countries with the implementation of COVID-19 restrictions, phishing campaigns increased from April and peaked in May.

[12] Hiscox, June 2020, Cyber Readiness Report 2020

[13] ESET, April 2020, ESET investigates Grandoreiro, a trojan exploiting the coronavirus pandemic

The Netherlands

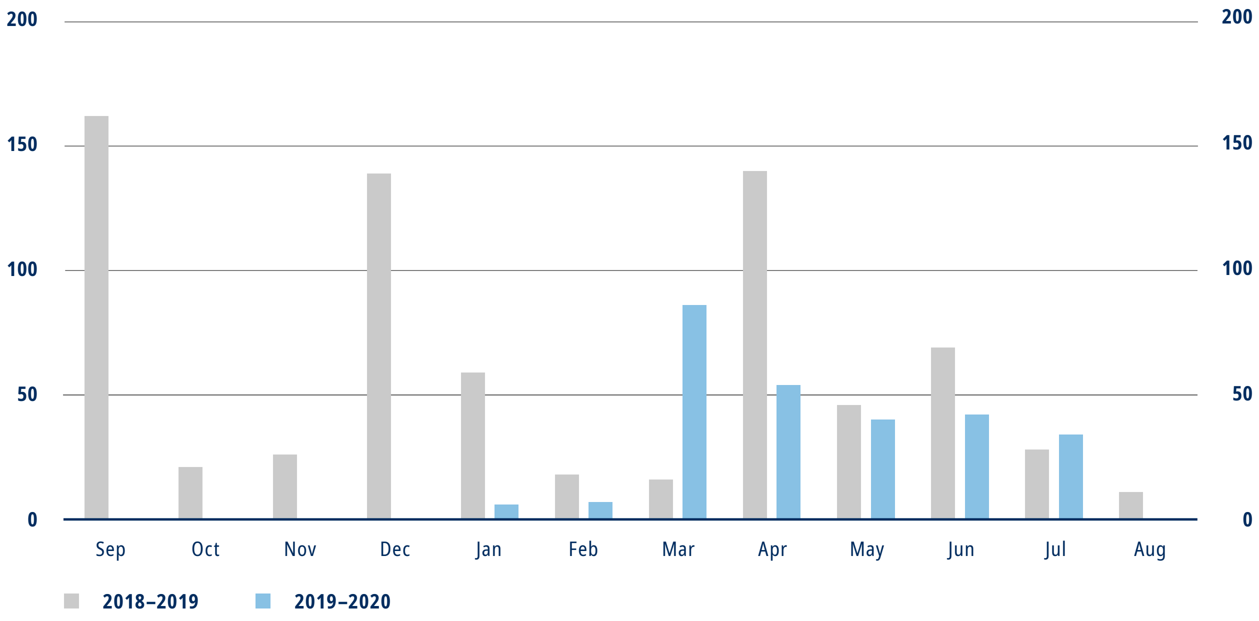


Figure 11 — Total Cyber Incidents Observed at Financial Institutions in the Netherlands (2018–2020)

The Dutch central bank stated in 2019 that cyber security threats are not consistently analysed, and data security measures are partly insufficient.[14] From our data (⟶ Figure 11), a clear spike in cyber incidents in March, April and May might be correlated with the onset of the COVID-19 pandemic. Overall, considerably more cyber incidents were observed in 2020 than in 2019. There was a lack of information on attack specifications observed in the Netherlands, making any analysis of attack patterns and trends difficult to perform. Overall, the Netherlands is ranked highly in their cyber security capabilities. They are ranked 12th globally by the ITU. The Dutch National Cyber Security Centre reported[15] in their Cyber Security Assessment that simple intrusion techniques, such as phishing, ransomware and misuse of supply chains, remained effective tools to breach financial institutions. Additionally, financial institutions were also targeted by DDoS attacks in 2020.

[14] National Cyber Security Centre, September 2019, Cyber Security Assessment Netherlands 2019

[15] National Cyber Security Centre, September 2019, Cyber Security Assessment Netherlands 2019

Germany

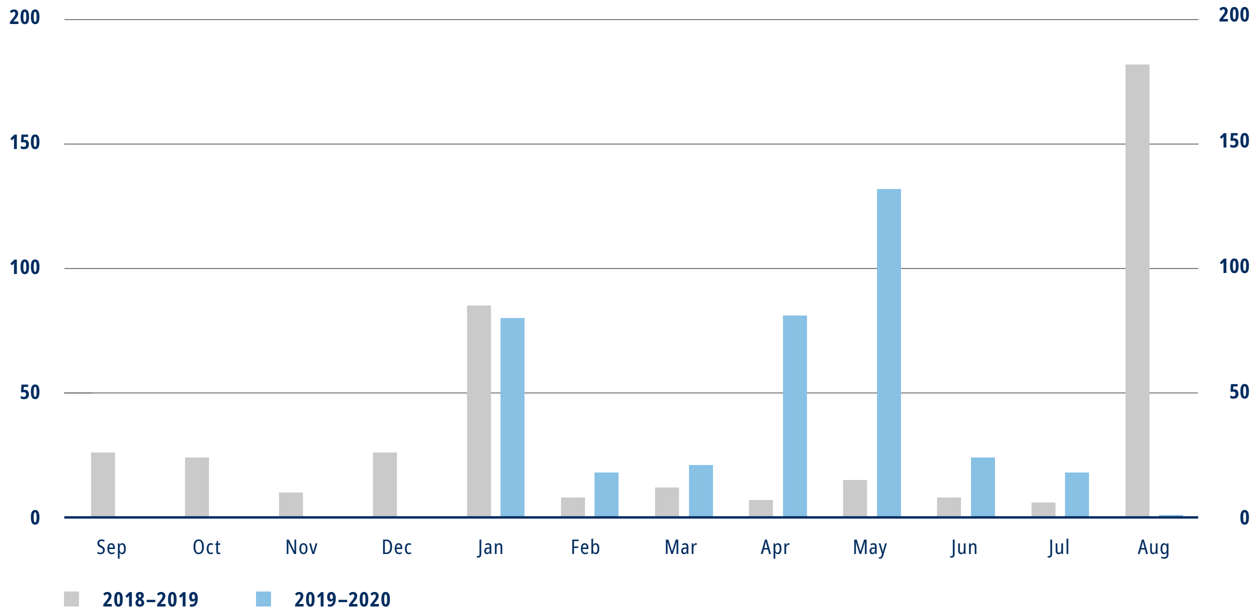


Figure 12 — Total Cyber Incidents Observed at Financial Institutions in Germany (2018–2020)

Germany is home to the EU's largest financial sector as well as to most European financial supervisory bodies, including the European Central Bank (ECB). This concentration of financial institutions in Germany makes it an attractive target for cyber actors.

Multiple cases of breaching of personal information of German politicians in January 2019[16] and a data leak at Mastercard in August 2019[17] caused spikes. Apart from that, the highest number of incidents was observed in April and May 2020 (⟶ Figure 12).

Based on observations by QuoIntelligence, the majority of cyberattacks recorded in Germany were targeted against the financial and industrial sectors (⟶ Figure 13). The attacks observed also increased considerably compared to the previous year.

[16] Süddeutsche Zeitung, January 2019, Seehofer verspricht volle Transparenz zu Daten-Hack

[17] Verbraucherzentrale, August 2019, Datenleck bei Mastercard: Was Kreditkartenbesitzer jetzt tun sollten

Germany's financial sector is highly regulated and has specific regulatory requirements for cyber security. However, compared to the other selected countries in this report, Germany is ranked relatively low by the ITU, in 22nd place. The attack vectors observed in cyberattacks at financial institutions are similar to observations in Switzerland, with the most commonly used attack vector being malicious e-mails, spread via (spear) phishing campaigns, followed by supply chain attacks (→ Figure 14).

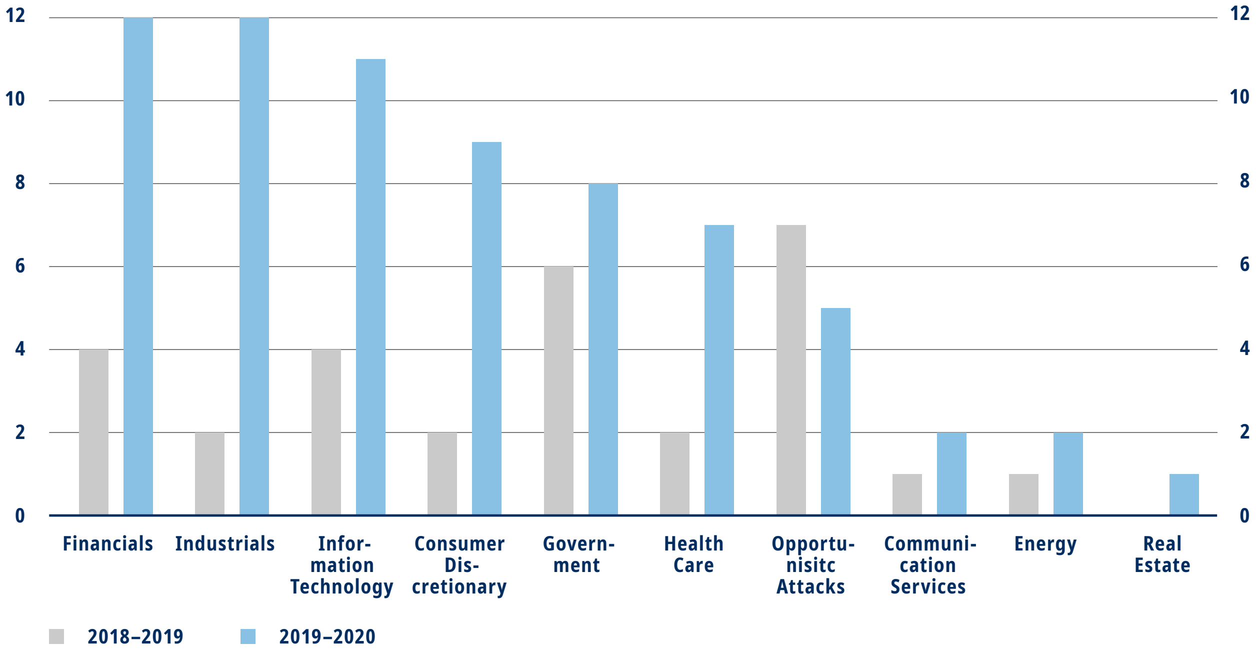


Figure 13 — Sectors Targeted by Cyberattacks in Germany (2018–2020)

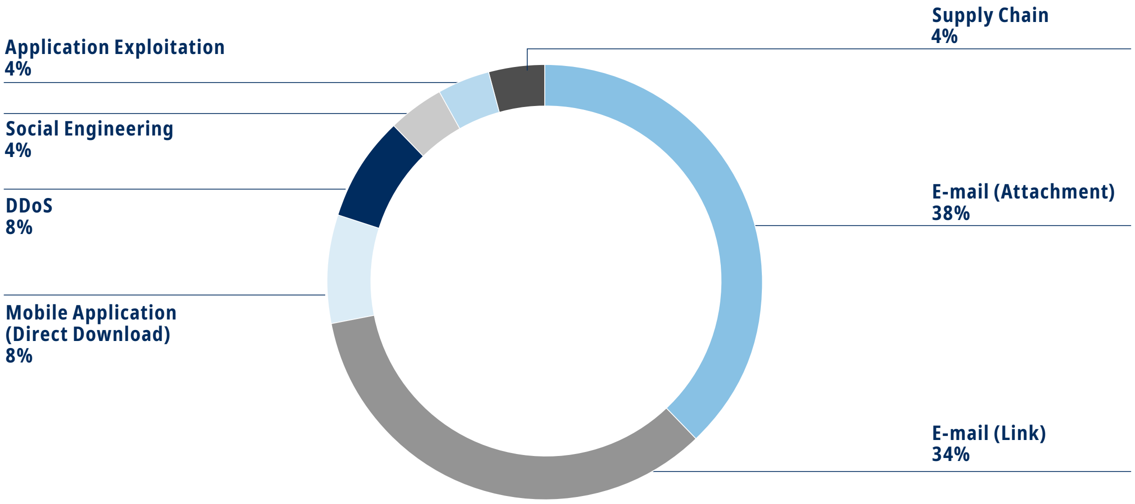


Figure 14 — Attack Vectors Observed in Cyberattacks Targeting Financial Institutions in Germany

Switzerland

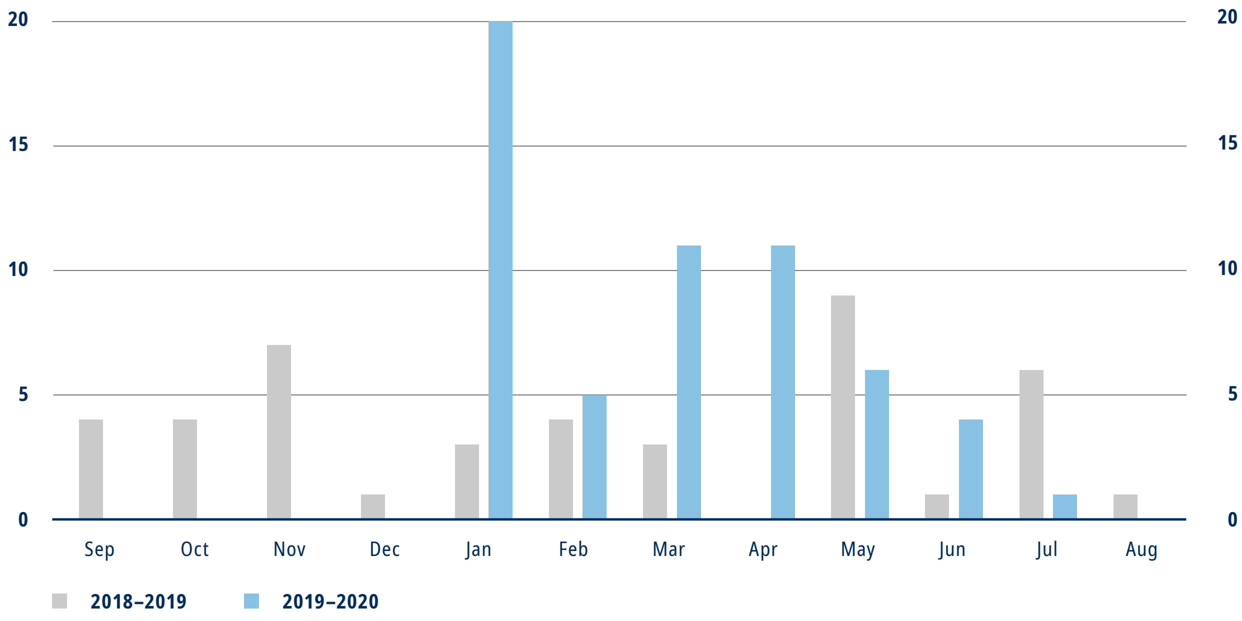


Figure 15 — Cyber Incidents Observed at Swiss Financial Organizations (2018–2020)

Over previous years, the number of cyberattacks at Swiss financial institutions has been consistently low[18] and much lower compared to any other selected country analysed in this report. In the Micro Section, we outline how this low observation rate does not necessarily indicate that Swiss financial institutions are targeted less than institutions in other countries. It is likely that some percentage of cases remain unreported due to a lack of robust information sharing infrastructure. Additionally, in the Micro Section we also hypothesize that there is a correlation between the visibility and maturity of a CISO operations and observed cyberattacks. However, Switzerland's financial sector is tightly regulated by FINMA and all institutions are required to have high cyber security standards in place.

In 2020, the number of cyberi ncidents increased compared to the previous year (→ Figure 15). The incidents observed were high, especially in January, March and April.

In the ITU Global Cybersecurity Index 2018, Switzerland is ranked in 37th place globally, which is lower than any other selected country analysed in this report. The Swiss federal government has seemingly acknowledged this shortcoming and is investing in improving the country's cyber security situation. In 2018, the national strategy for protecting Switzerland against cyber risks 2018–2022 (Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken, or NCS) was released,[19] and a central reporting and analysis center for information security – MELANI (Melde- und Analysestelle Informationssicherung) – was established.

Given these factors, and with Switzerland being one of the most attractive banking destinations while having a potential lack in cyber security capabilities, the low number of observed attacks is surprising.

[18] SIX Cyber Security Report 2019

[19] Der Bundesrat, A1, September 2018, SN002 – Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS)

Conclusion

The purpose of the macro analysis in this report was to understand the key similarities and differences between the cyber security threat landscape in Switzerland and the countries selected.

The first key similarity identified is that ransomware, phishing, and to some extent supply chain attacks, remain the largest cyber security threats to financial organizations, regardless of their size or location.

Secondly, an increase in cyberattacks observed occurred during the onset of the COVID-19 pandemic in March. This highlights that the attack surface grew due to the increased reliance on online services, as well as the willingness and capability of cyber actors to quickly adapt their methods to leverage any situation.

These similarities again highlight the need for a more global information sharing infrastructure. Given that most financial institutions are targeted by similar attack methods, financial institutions could benefit greatly from being able to access near real-time information on campaigns targeting other financial organizations. This would enable organizations to put specific mitigation measures in place,, as the likelihood of them being targeted by the same or similar campaigns is high.

A key difference between the selected countries analysed in this report is the difference in the number of incidents observed. While information on incidents in the USA is very extensive, much less is available for Switzerland and Singapore. Again, an international information sharing community could alleviate these problems as universally agreed definitions on what constitutes cyber incidents, how they should be reported and at which point, would provide more transparent data on incidents.

<p:normalViewPr>
Pr><p:slideViewP
cale><p:origin
pos="4898"/
n="33" d="
Pr><p:sc
Scale=
Pr><
cal
eft sz="16585" autoAdjust="0"/><p:restoredTop sz="9445
vPr snapToGrid="0" p:cViewPr varScale="1" scale><a:sx n
57"/></p:cViewPr guideLst><p:guide pos="2
nt="horz" pos="692"/ /p:guideLst /p:cSldView
33 d="100"/></p:scale><p:origin x="0" y="0"
d=2/a:sy n="3" p:scale><p:origin x="0" y="0"/
x n="1" d="1"/ a:sy n="1" d="1"/ /p:scale><p:ori
apTo="0" show uides="1"><p:cViewPr varScale=
7038" y="102" cViewPr><p:guideLst><p:guid
r></p:notesVie p:gridSpacing cx="72008" cy=
redTop sz=94 1 autoAdjust="0"/></p:normal
91 d="100"/ :scale p:origin x
guide orient
sy n="33"

Micro Section

Key Findings

The fast changes caused by digitalization and the corresponding need to rapidly adapt IT architectures are viewed as the greatest challenges to maintaining cyber security in the Swiss financial sector. We identified this in analysing the information collected, regardless of the size of organizations.

While this development has been ongoing for several years, the onset of the COVID-19 pandemic has considerably accelerated this process and exacerbated previous cyber security challenges.

The sudden shift to remote working required fast adaptation of new architecture and created more opportunities for cyberattacks.

Chief Information Security Officers (CISOs) are concerned about being able to address these changes, highlighting the need for adequate funding for their operations and the challenges of retaining a skilled workforce to be able to maintain high levels of cyber security.

According to various Swiss financial institutions, the cyberattacks that they find themselves at risk of most are phishing, malware and ransomware, followed by security architecture and risk management.

There was also a correlation between the number of incidents observed and the maturity, and visibility, of CISO operations. CISOs who ranked visibility and maturity higher also observed more incidents.

In order for CISOs to address their concerns over the rapidly changing cyberthreat landscape, it is essential that they receive adequate support from within their organization and from regulatory bodies. Firstly, sufficient funding is necessary to increase capabilities and visibility across the organizations, which is essential for risk mitigation. Additionally, funding is needed to retain a skilled workforce, which respondents highlighted as a concern. Secondly, cyber security must be prioritized by management to allow CISOs to fully operate throughout the organization. Additionally, CISOs are concerned by increasing digitalization, such as moving to the cloud, and related concerns over third-party risk management. Therefore, regulators and supervisory bodies need to ensure adequate security guidelines are available for third-party providers and those involved in supply chains to mitigate these risks.

The following report analyses the cyberthreat landscape pertaining to the Swiss financial sector over the previous 12 months. The findings in this report are partly based on confidential interviews with 53 cyber security executives of Swiss financial institutions conducted in July 2020, as well as on open and closed source analysis. Respondents were evenly divided across small, medium and large organizations. Therefore, the report provides insights into varied segments of the financial sector. In order to ensure confidentiality, all information was anonymized after collection and was only used in aggregate analysis.

Overall Findings

Respondents to our survey rated that threats, which fall within the category of Cyberattacks, were the top cyber security challenges to the Swiss financial sector in the previous year. This was followed by threats within the categories Security Architecture and Risk management (→ Figure 16).

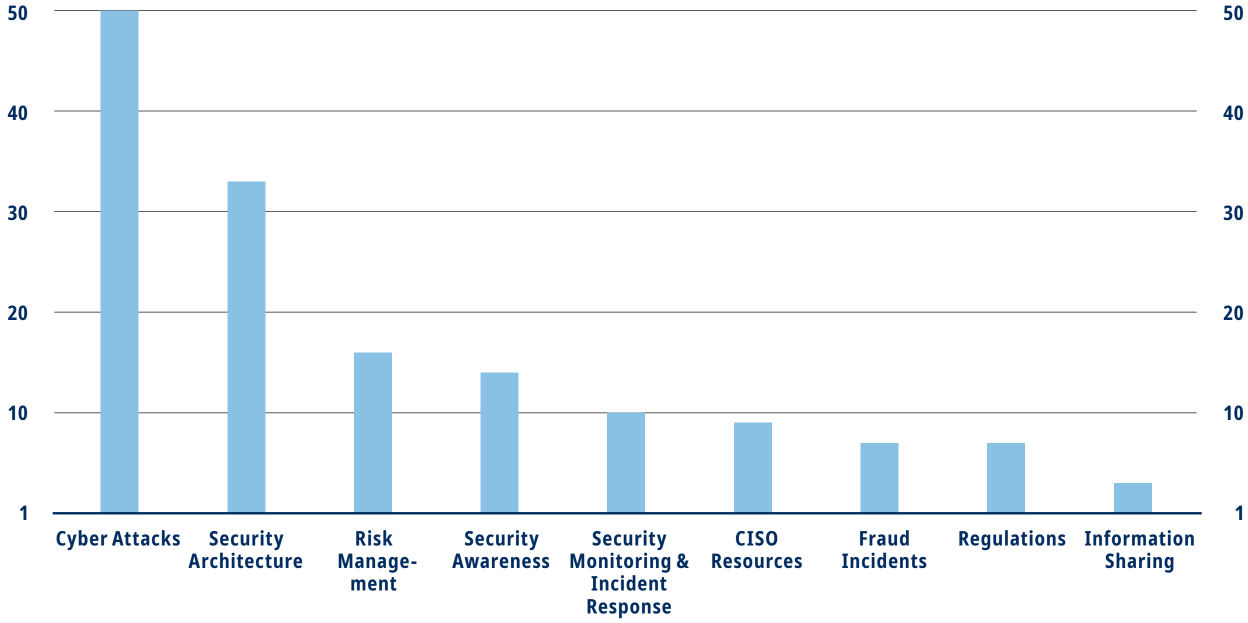


Figure 16 — Top Cyber Security Challenges Identified by Respondents

As can be seen in Figure 17, in terms of Cyberattacks, phishing, malware and ransomware were mentioned most often. In terms of Security Architecture, issues pertaining to the cloud and risk management of third-party suppliers ranked highest.

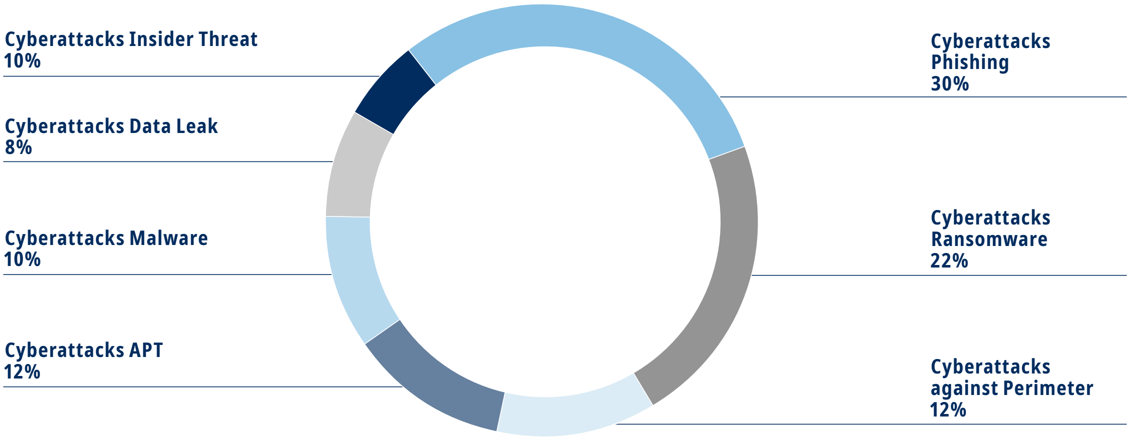


Figure 17 — Types of Cyberattacks Identified as Top Threats to the Swiss Financial Sector

These threats identified by respondents align with the methods of cyberattacks used against financial institutions last year. As can be seen in Figure 18, based on data by QuoIntelligence, e-mails with malicious attachments or links to spread malware were identified as a method of attack in more than half of incidents targeting financial institutions in which attack vectors were recorded. This was followed by attacks on supply chains. This trend is consistent with last year's findings, which listed phishing e-mails as the most frequent attack method.

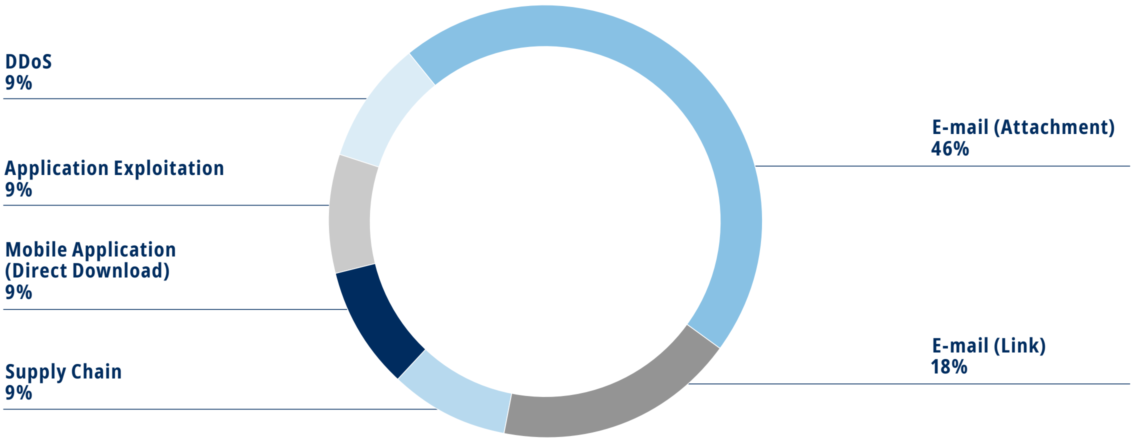


Figure 18 — Attack Vectors Observed in Campaigns Targeting Financial Institutions

When asked about threats to their own organization, more than half (around 53%) are "highly concerned" over malware outbreaks, which corresponds with the top threats facing the Swiss financial sector overall. This is followed closely by vulnerability exploitation (49%). While concerns over a skilled workforce ranked highly under the overall threats, when questioned about their own organization, the lack of security expertise and retention was only of "high concern" to 3% of respondents.

Understanding the Low Level of Cyber Incidents Observed at Swiss Financial Institutions

In the previous year, SIX observed that a majority of cyberattacks against financial institutions were targeted against large retail banks. Given the relatively small number of large retail banks in Switzerland, compared to other European countries, this factor could explain low levels of cyberattacks observed against Swiss financial institutions. In addition, cyber security regulation in Switzerland is very mature and financial institutions are required to have a high level of security in place. While this would not necessarily deter attacks, it will likely mitigate their damage.

However, another aspect that could contribute to this low level of cyberattacks observed is the limited visibility of CISOs across their organizations, as identified by the survey.

Incidents Observed

Over 80% of respondents only observed less than 50 security incidents in the previous year, correlating with the overall low observation rate of publicly available information on cyberattacks against Swiss financial institutions. Phishing attacks constituted most of these reported incidents.

While respondents believe that national financial regulators and high user awareness contributed to this low observation rate, other factors also potentially contributed. Namely, we identified that the number of incidents observed increased for CISOs who reported high visibility across their organizations. Conversely, almost 40% of respondents who reported less than 50 incidents also reported that they had inadequate visibility across their organizations. **This indicates that the low number of attacks observed might be caused by limited visibility.**

In the survey, we asked respondents to rate the visibility of the CISO across the organization from one (Limited Visibility), to three (Partial Visibility), to five (High Visibility). As can be seen in Figure 19, out of respondents who observed less than 50 incidents, more than 40% had Good Visibility across their organization. However, almost 30% had Partial Visibility, and 9% had Little Visibility. Around 20% had High Visibility.

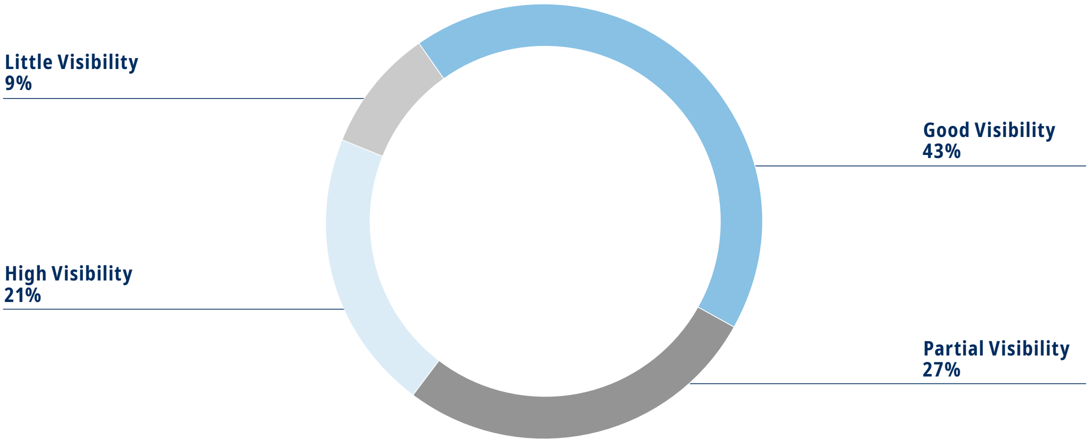


Figure 19 — CISO Visibility by Incidents Reported: 0 to 50 Incidents Observed

The higher the number of incidents observed, the more respondents said they had Good Visibility. Figure 20 shows that when between 51 and 200 incidents were observed, 80% of respondents had Good Visibility and 20% even had High Visibility.

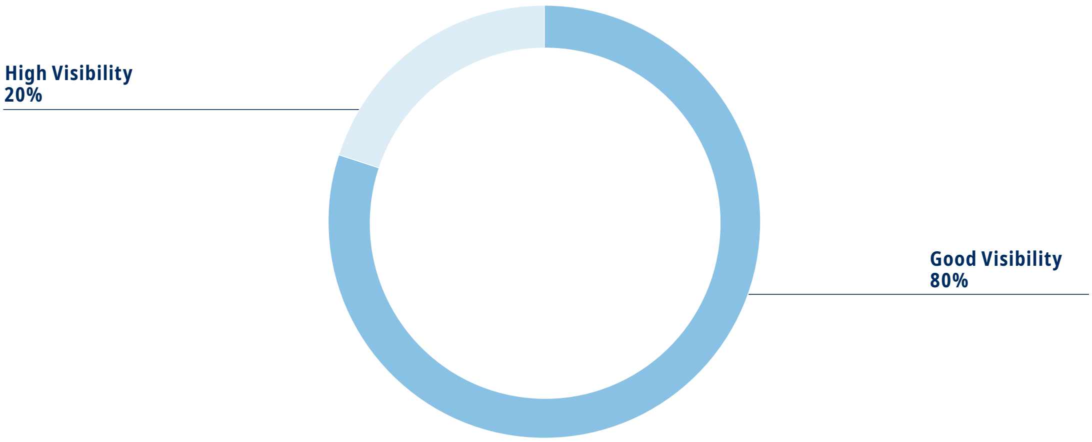


Figure 20 — CISO Visibility by Incidents Reported: 51 to 200 Incidents Observed

Finally, 100% of respondents who observed more than 200 incidents had Good Visibility.

Similar conclusions can be drawn when analysing the number of incidents reported and the maturity level of CISO operations. CISOs who ranked their operations' maturity as emerging or low recorded fewer incidents compared to CISOs, who ranked their maturity as medium. As can be seen in Figure 21, all respondents who ranked their maturity as Emerging observed less than 50 incidents. Respondents who viewed their maturity as Low viewed up to 200 incidents. All respondents who observed more than 200 incidents ranked their maturity as Medium. Interestingly, none of the respondents who rank their maturity as High viewed more than 200 incidents; however, around 20% viewed less than 50 and between 50 and 200 incidents respectively.

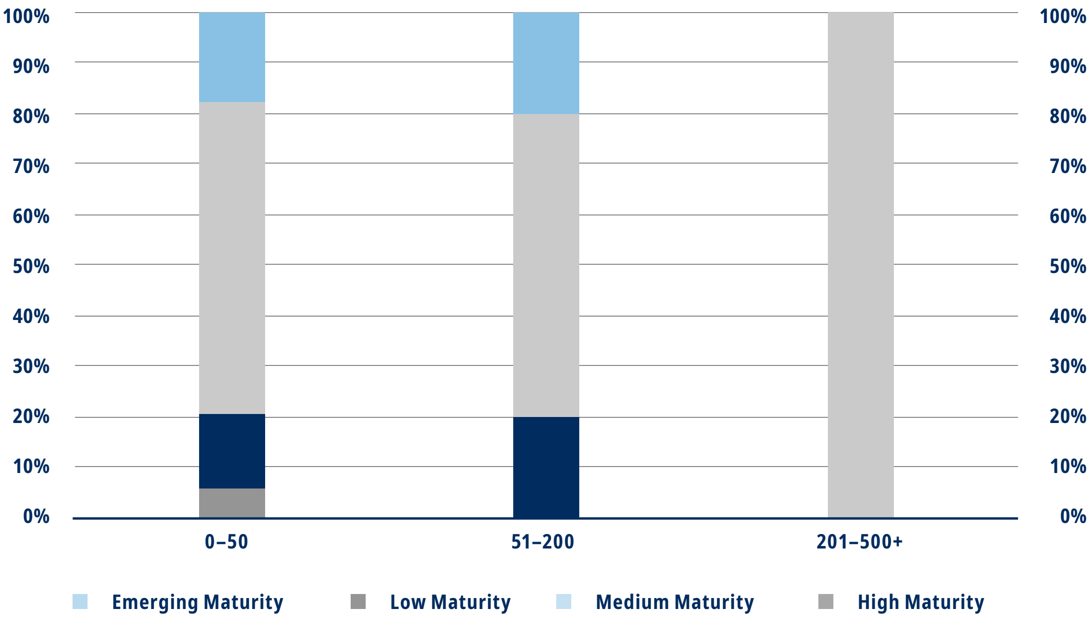


Figure 21 — Maturity Level by Incidents Reported

Respondents ranked the majority of the attacks observed as being of minor severity, such as phishing attempts, the use of fraudulent websites that abuse the financial institution‘s name or attempts to fraudulently impersonate executives. Out of the observed attacks, respondents said **only 15% of attacks were attributed to specific threat actors. This could, on one hand, indicate that most attacks were launched by opportunistic cyber actors. On the other hand, attributing attacks to specific actors requires time and capabilities and is seldom a straightforward and decisive action. Therefore, the low attribution rate could also be based on the difficulty of attribution.**

According to respondents, 32% of all attacks observed were targeting the financial institutions specifically, 23% targeting customers, around 15% targeting third-party providers, and around 20% targeting customers, the financial institutions and third-party suppliers indiscriminately. Overall, the majority of respondents said this pattern of targeting remained similar to last year. However, around 30% of respondents also saw an increase in customers targeted and indiscriminate targeting.

COVID-19: Accelerating Changes and Magnifying Existing Challenges

The COVID-19 pandemic has impacted all organizations globally, and immediately resulted in new opportunities for attacks and cyber security implications. When asked about new cyber security concerns, 75% of respondents identified an increase in remote working due to COVID-19 as a concern (→ Figure 22).

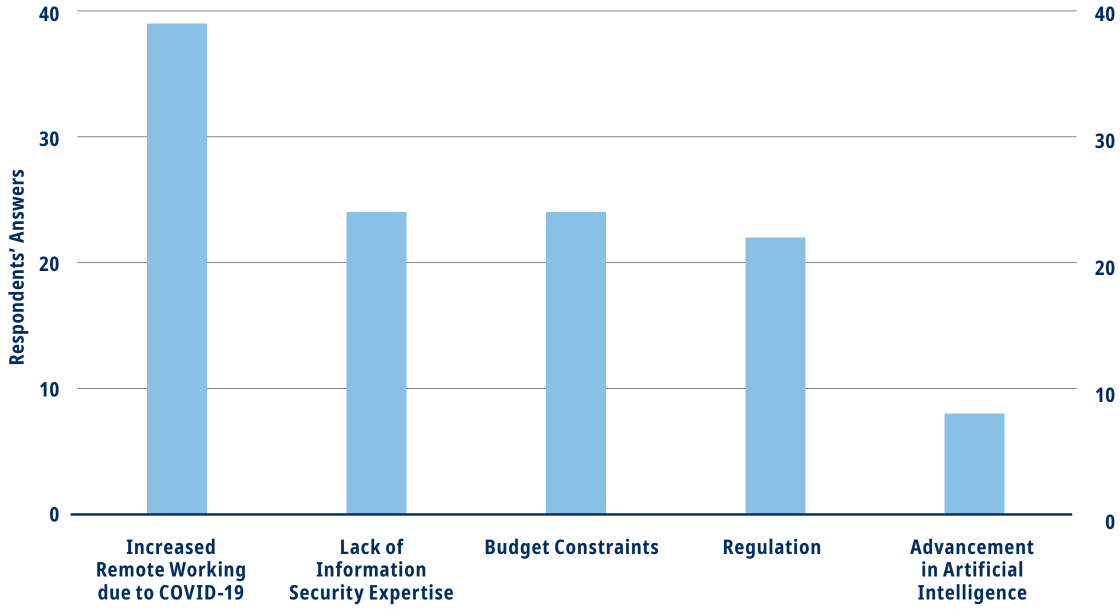


Figure 22 —New Concerns Identified Compared to Previous Year

This correlated with our analysis of cybe rincidents observed in Swiss financial institutions last year, which spiked in March and April (→ Figure 23 below, as well as the Macro Analysis section of this report for additional information).

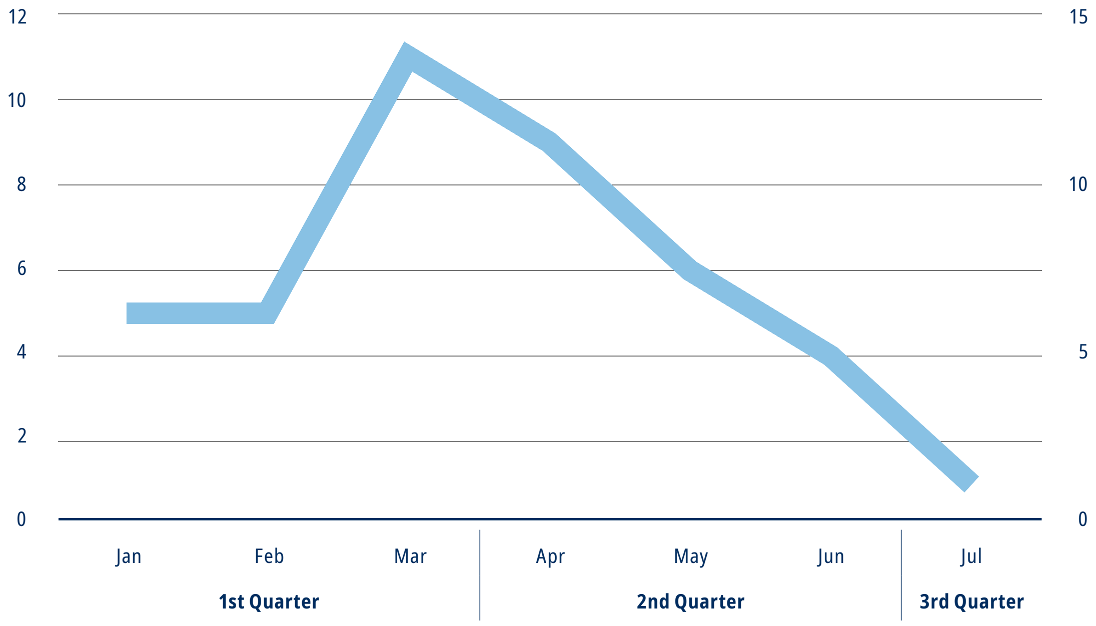


Figure 23 — Number of Cyberattacks Observed per Month

These concerns correlate with the overall cyberactivity observed since the onset of the pandemic. The sudden shift to remote working forced organizations to quickly adapt their security strategies to allow for uninterrupted continuation of business operations. This likely reduced the ability of security teams to conduct security monitoring. And enabling widespread remote working capabilities possibly led to a loosening of security policies.

Cyber actors have attempted to leverage these new vulnerabilities, as well as increasingly target employees and the general public, by taking advantage of people's fear.

DDoS:
The increase in remote working strained available bandwidth beyond usual expectations, making any DDoS attacks more likely to succeed. Almost half of respondents said that availability problems due to an increase in remote working has increased their cyber security concerns. In addition, remote software – such as VPN endpoints – is a critical component for the continuity of business operations for a teleworking labour force. The increased possibility of attack, due to the use of devices such as home routers or unsecured Wi-Fi network, is of concern to more than 40% of respondents. Additionally, remote working can complicate applying security patches across all endpoints, leaving devices vulnerable to exploitation. Other concerns raised were the use of unapproved employee workaround solutions and the potential for an increased risk of data exfiltration.

Spear phishing:
More than 60% of respondents said that COVID-19 increased the risk of users being victims of phishing attacks. Since the onset of the pandemic, threat actors, including Emotet[20], Hancitor[21], Trickbot[22], Netwalker[23] and Chinoxy[24], have used COVID-19-themed e-mails to spread malware. Given that Swiss CISOs already view phishing e-mails and malware as the largest threat to their organizations, the COVID-19 pandemic has further exacerbated this issue.

Identifying Future Challenges

In addition to COVID-19, when respondents were asked to identify any “new concerns”, almost half of CISOs identified the lack of information security expertise and budget constraints as new concerns. Almost 60% of respondents also highlight the need for additional funding. In terms of how attacks are evolving, most respondents identified that attacks and actors are becoming more advanced and sophisticated. **CISOs are concerned by the fast changes caused by digitalization and the corresponding need to rapidly adapt IT architectures. And they are also concerned about whether a skilled workforce and an adequate budget can be maintained to address these challenges**. While this development has been ongoing for several years, the onset of the COVID-19 pandemic has considerably accelerated this process and exacerbated previous cyber security challenges. While more than half of respondents state that their organizations are prepared to handle identified cyber security concerns, more than a third remain unsure if their organization is equipped to handle such threats. In addition, the majority of respondents work at financial institutions where organization-wide security testing only occurs yearly. Security testing is important in understanding the attack surface and potential security weaknesses, crucial in mitigating threats. A lack of testing could limit insight into an organization’s weaknesses and levels of preparedness for emerging threats.

[20] Bleeping Computer, B2, 18 March, Trickbot, Emotet Malware Use Coronavirus News to Evade Detection

[21] SANS, B2, 12 March, Hancitor distributed through coronavirus-themed malspam

[22] Bleeping Computer, B2, 18 March, Trickbot, Emotet Malware Use Coronavirus News to Evade Detection

[23] MalwareHunter-Team, C2, 19 March, @Malwrhunterteam

[24] Sebdraven, F6, 20 March, New version of chinoxy backdoor using COVID19 alerts document lure

The Structure of CISO Operations

The Swiss Financial Market Supervisory Authority (FINMA) assigns the financial institutions it supervises to five supervisory categories depending on their risk impact, with Category 1 being extremely large market participants presenting very high risks and Category 5 being small participants presenting low risk. As respondents to the survey were evenly divided across small, medium and large organizations, CISOs from all FINMA categories took part in the survey. Regardless of their organization's size, respondents rated their CISO operations capabilities as being average (56/100).

Across all respondents, the CISO operations consist largely of SOC, at more than 40%, followed by Incident Response teams at 30%. Threat Intelligence and Red Teams make up 16% and 10% respectively.

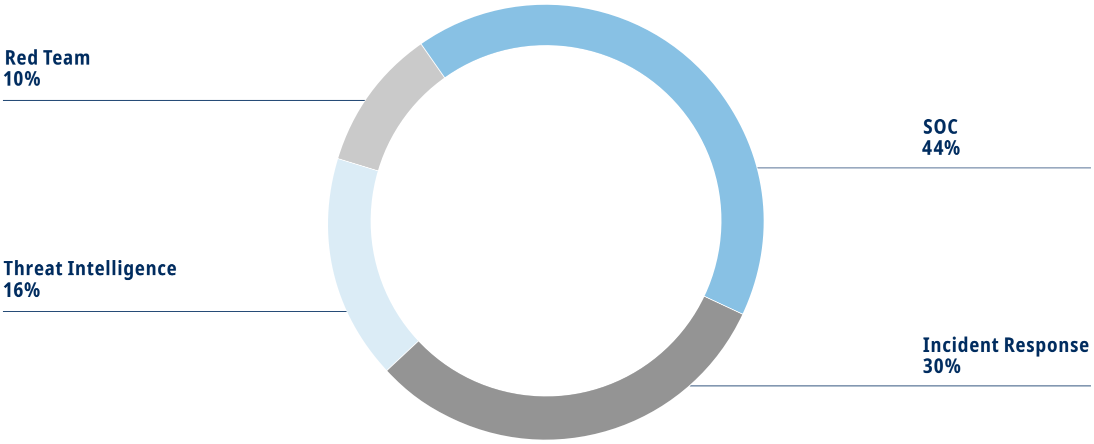


Figure 24 — Resources Split by Operation Functions (Average)

While SOC and Incident Response teams exist in all organizations, the fact that almost 90% of organizations also have Threat Intelligence teams is recognition of the important role of threat intelligence in CISO operations.

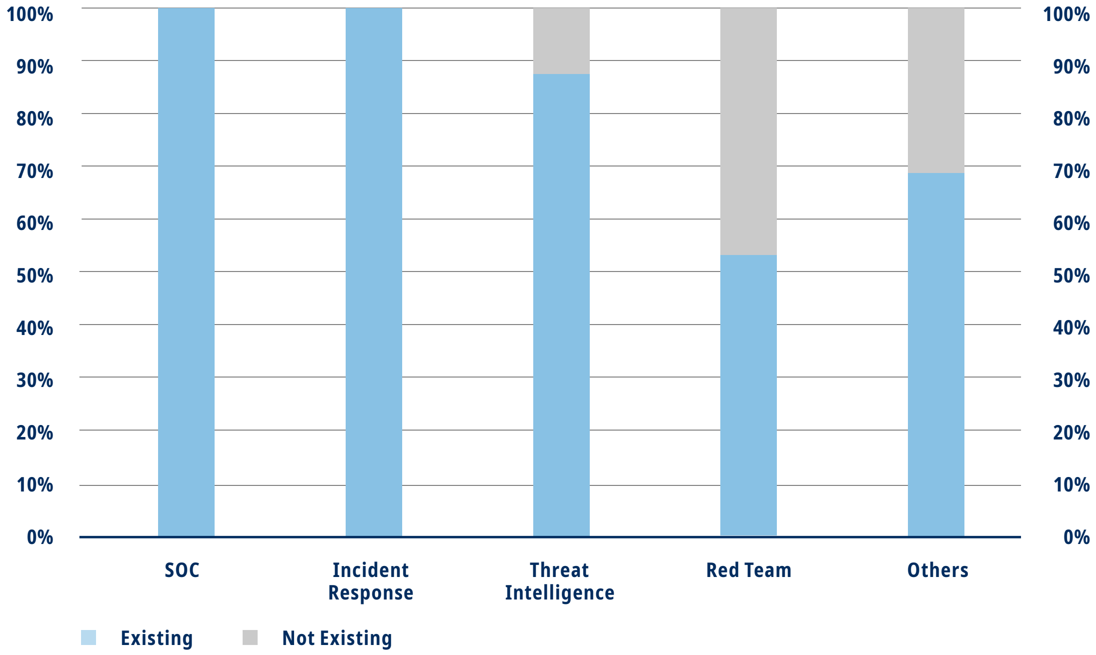


Figure 25 — Functions in CISO Operations

Regardless of the organization's size, the number of employees in CISO operations remained constant, indicating that all financial institutions take information security seriously, regardless of their size. As can be seen in Figure 26, the CISO headcount ranges between 26 and 75 on average.

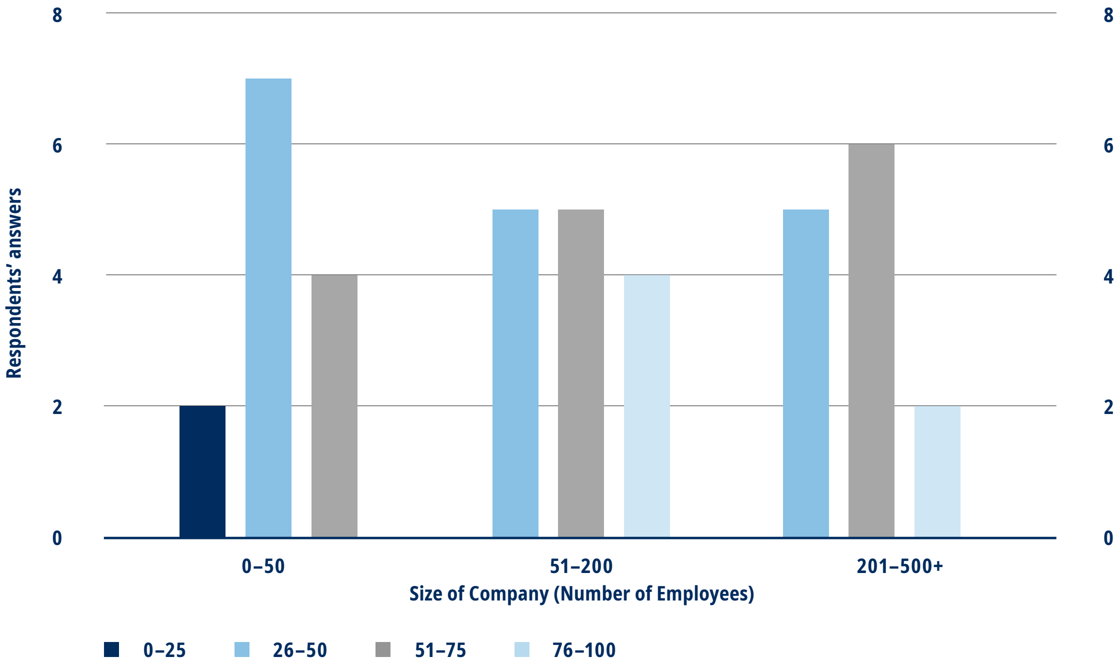


Figure 26 — CISO Headcount by Size of Organization

Across respondents, the majority viewed their budget as partially adequate (⟶ Figure 27).

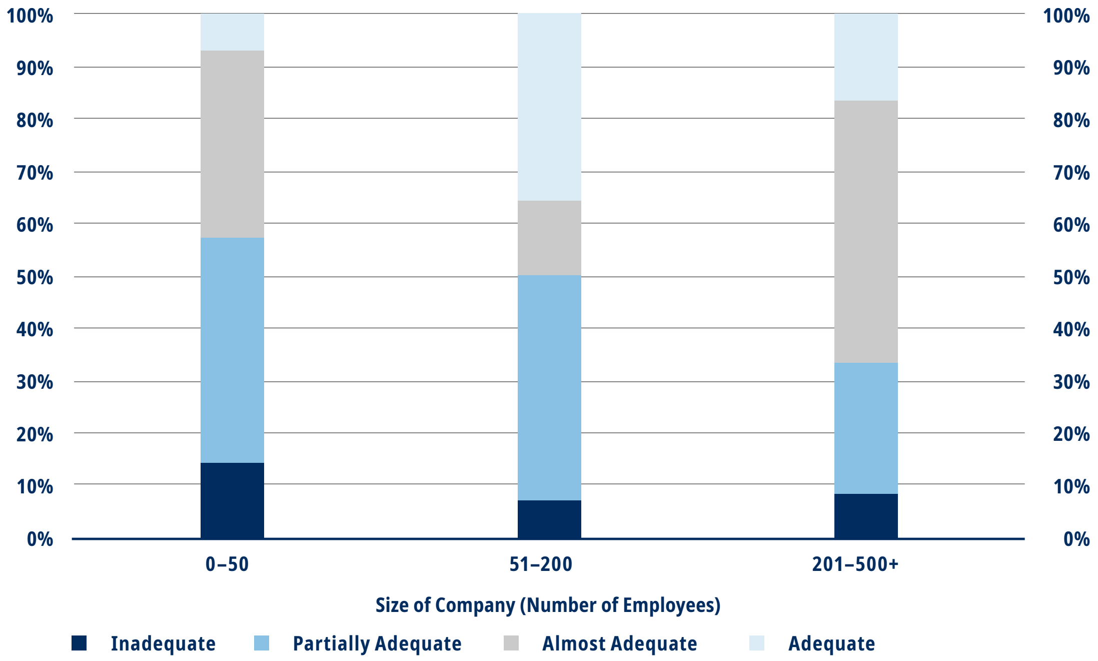


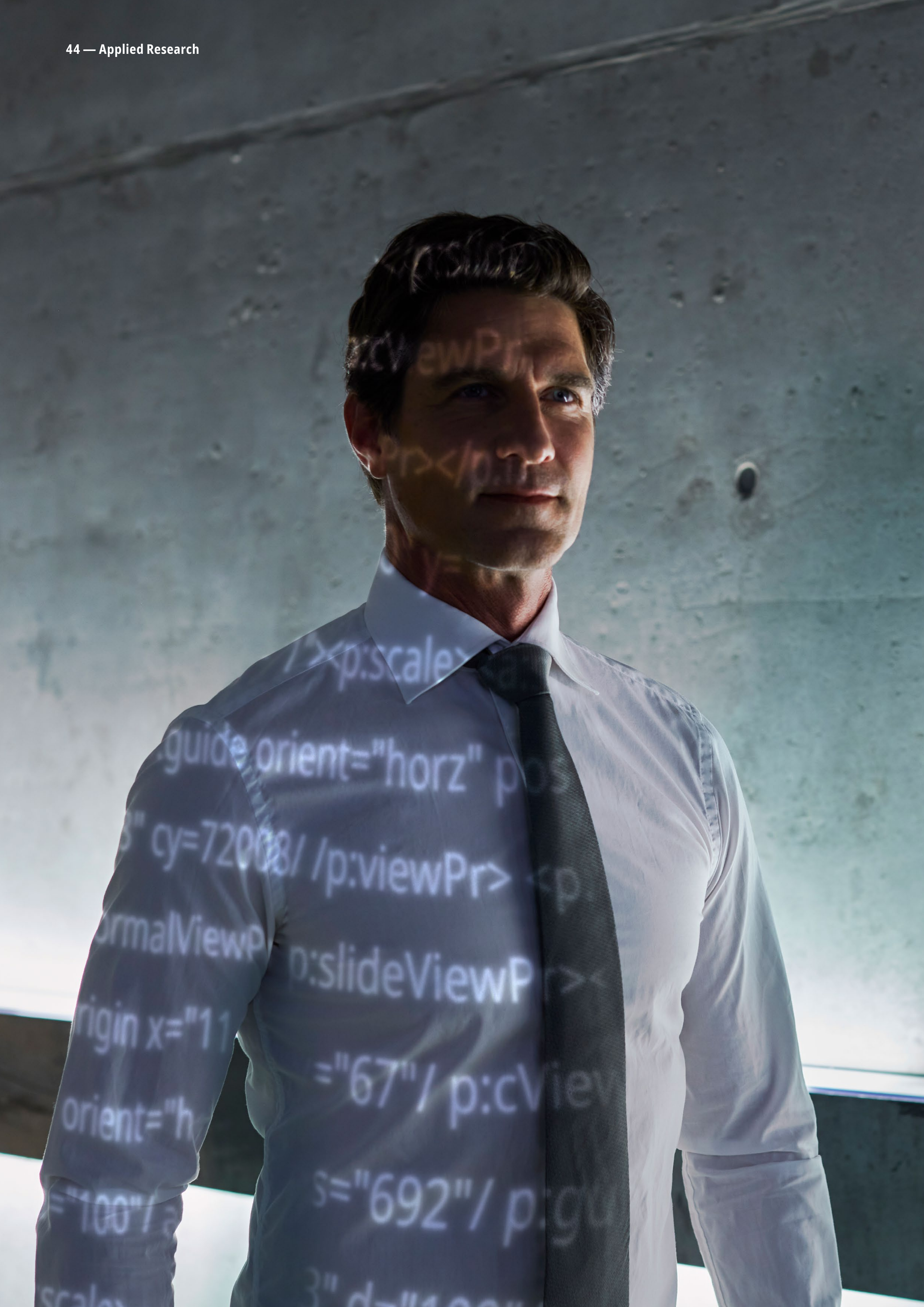
Figure 27 — Perception of Budget Adequacy by Size of Organization

While, overall, any size of CISO team felt prepared to handle cyber security threats, in smaller CISO teams (less than ten employees), more respondents said they were not prepared or unsure about it.

Conclusion

The survey we conducted as the basis for this report offered extremely interesting insights into the cyberthreat landscape pertaining to the Swiss financial sector. The greatest cyberthreats identified by respondents were cyberattacks, including phishing and ransomware, as well as threats against the cloud. This correlates with our analysis on incidents reported last year. In addition, the sudden shift to remote working caused by the COVID-19 pandemic has created additional attack surfaces and was therefore identified as a new concern by respondents. In fact, we observed an increase in cyberattacks in March and April, coinciding with the onset of the pandemic in Europe.

Lastly, the survey offered valuable insight into the correlations between the visibility and maturity of CISOs and the number of incidents observed. Respondents who rated their CISO visibility and maturity as higher also observed a higher nunber of cyber incidents.


p:cViewPr
Pr></p:
/><p:scale>
guide orient="horz" pos
3" cy=72008/ /p:viewPr> <p:
ormalViewP
p:slideViewPr><
rigin x="11
="67"/ p:cView
orient="h
s="692"/ p:gu
="100"/ a
scale

Applied Research – SCION

In this section, we present and discuss SCION (Scalability, Control, and Isolation On Next-Generation Networks), its potential impact, and the benefits it can bring for financial institutions. In this context, we move the focus away from cyberattacks and to the communication technology that is used by the financial sector every day. The focus of SCION is to change the basics of how data is controlled on the Internet. By doing so, every system or application built on top of it automatically benefits from the advancements that it introduces.

We will first give a brief overview of the current implementation and deployment status of SCION to highlight its relevance for the financial sector. Then, we will describe the origins of this technology, the aspects of the Internet it changes, and how such changes to the Internet can help to improve the cyber security situation.

Scalability, Control, and Isolation On Next-generation Networks

Move the focus away from cyberattacks and to the communication technology

SCION and the Swiss Financial Sector

The native SCION network spans two continents with various Internet service providers (ISPs) offering SCION connections to customers. Several Swiss banks, the Swiss Federal Department of Foreign Affairs and some blue-chip organizations use production-grade SCION.

The financial sector has faced many challenges in terms of distribution, flexibility and security when using the Internet for daily business activities. It is vulnerable to cyberattacks, including distributed denial-of-service (DDoS) or traffic-hijacking attacks. This has led the Swiss financial sector to use dedicated communication services such as Finance IPNet for critical services, such as the Swiss payment system. The establishment of a highly secure, flexible and functional communication system could create an alternative to Finance IPNet. This alternative would provide better control over the exchange of sensitive financial information among market participants while reducing implementation complexity and effort.

SIX is cooperating closely with the Swiss National Bank and other partners to implement a pilot of SCION-based alternatives to Finance IPNet. This potential alternative would come along with all the benefits of SCION, such as full control over the route the data packets travel (e.g. only inside Switzerland) and others which are described in the following subsections. Also, since August 2017, SCION has been used by a large Swiss bank, which has connected a branch office to its data center exclusively via the SCION network.

SCION is used at several Swiss banks, the Swiss Federal Department of Foreign Affairs, and some blue-chip companies.

Since August 2017, a branch of a large Swiss bank has used SCION exclusively.

History and Motivation for SCION

Originally developed as a small research network in the 1970s, the Internet has since grown into a system-critical infrastructure and is now used by billions of people every day. Still, the basic mechanisms have remained largely unchanged for decades. This long legacy means that these protocols and their deployment have been tested and optimized, but they also have a downside. At the time these protocols were developed, all actors in the Internet knew and trusted each other, and few people imagined the Internet to reach today's scale. Over the past two decades, it has become apparent that not all actors on the Internet can be trusted, as the number of attacks has increased dramatically. As a response, security mechanisms were added to the Internet ecosystem, but these only partially succeeded in defending against ever more sophisticated attacks.

This unsatisfactory situation has triggered research into clean-slate Internet architectures, and in 2009 Adrian Perrig, at the time professor at the Carnegie Mellon University and now professor at ETH Zurich, started working on a new architecture that was later named SCION. This architecture was designed with the clear objective of fundamentally solving the many security issues of today's Internet. Today, over 60 researchers around the world are actively working on development, implementation, verification and deployment of SCION.

Over the past two decades, it has become apparent that not all actors on the Internet can be trusted, as the number of attacks has increased dramatically.

Adrian Perrig started working on a new architecture in 2009.

SCION Technical Background

Fundamentally, the Internet is a network of smaller independent networks known as autonomous systems (ASes). Examples of ASes are ISPs, universities or large content providers. These ASes independently administer their own networks; they also interconnect with each other and exchange data traffic at these interconnection points to achieve global connectivity.

This fundamental structure of the Internet remains largely unchanged, with SCION improving the ability to deploy the new system, as ASes do not need to modify their internal infrastructure. It is, however, augmented by an additional concept called isolation domains (ISDs). They organize multiple ASes into independent groups with common trusted entities, such as countries.

The routing protocol (the process in which paths are discovered on the Internet) makes use of this additional structure, which improves both scalability and security compared to today's Internet. On the one hand, ISDs enable a separation of the routing protocol into an intra-ISD and an inter-ISD process, which reduces the overall complexity. On the other hand, by isolating the routing process within an ISD, the effect of misconfigurations and routing attacks is limited. Furthermore, all routing messages are authenticated based on a secure but flexible public key infrastructure (PKI) in which each ISD can independently define its own Roots of Trust. This provides network sovereignty by allowing network entities to select which ISD Roots of Trust they want to rely upon for verification. This also rules out global de-facto kill switches, which do exist in several of today's security mechanisms. As a result, the SCION architecture provides strong resilience and security as an intrinsic result of its design.

In addition to the routing protocol and other background processes, SCION also modifies the way data is sent and forwarded. In today's IP-based Internet, users have little control over the paths taken by their traffic; a packet only contains the source and destination address, all other decisions are made in the network and are hidden from the user. In SCION, users choose the path(s) their packets can take. The chosen paths are then explicitly added to the packets, which simplifies the forwarding process at the intermediate routers compared to the traditional Internet. Thanks to embedded cryptographic mechanisms in SCION, ASes still retain control over which paths can be chosen by users.

The Internet is a network of smaller independent networks known as autonomous systems (ASes) which interconnect with each other and exchange data traffic.

SCION introduces a new concept, the so-called isolation domains (ISDs), which combines several ASes into independent groups with common trust anchors.

All routing messages are authenticated based on a secure but flexible public key infrastructure (PKI).

In SCION, users choose the path(s) their packets can take.

Extensions to basic SCION that enable source authentication and bandwidth reservation, among others, are available. These features enable defences against most DDoS scenarios. For example, connections with a reserved bandwidth cannot be impacted by non-reserved volumetric DDoS attacks. As those features could be available on a standard SCION Internet link, dedicated lines (e.g. MPLS) would not be required any longer in most cases, bringing down costs, improving flexibility and reducing redundancy of Internet uplinks.

All these mechanisms are hidden from the user and normally controlled by software applications and the operating system. Generally, only software developers and system administrators will need to know about and configure the mechanisms provided by SCION. In simple terms, SCION can replace the current Internet's IP and routing protocol suite. Still, these new mechanisms have a profound impact on the levels of security offered to users and their quality of experience. This can be illustrated through two examples.

Consider an organization that has a regulatory obligation to ensure that certain data, cannot leave Switzerland. Today, this organization cannot use the public Internet to transfer this data as it cannot control the paths taken by its packets. **In contrast, with SCION, the organization can simply configure its system to only allow paths within the Swiss ISD, thus ensuring that all data remains in the country.**

As a second example, imagine a situation where a European organization is collecting financial information from South Korea. In today's Internet, traffic between Europe and East Asia is often forwarded via the USA, which can lead to a round-trip latency of around 300 milliseconds. **With SCION, the more direct eastbound connection can be used, which reduces the latency to less than 200 milliseconds, improving the round-trip delay by about one third.**

Conclusion

Several of the top-listed threats in this report, such as phishing, malware and ransomware, are application-level attacks where the immediate benefits of SCION are less evident. For other threats like DDoS or routing attacks, SCION provides major and more direct positive effects. Its impact is not limited to certain threat scenarios, and the main purpose of SCION is to extend the traffic-control aspects. The concepts of isolation domains and path selection provide the sender and the carriers with detailed control over how and where the data is flowing. Finally, various extensions that are available for SCION enable defences even against very sophisticated attacks.

Since 2009, SCION has matured from a purely academic project into a system with production-grade implementation that is deployed globally. It solves long-standing open problems, such as achieving communication guarantees in a public network, which were previously only available on closed, proprietary networks. What started as an intriguing idea over ten years ago has now become reality and is available to be used for production traffic to a wide range of organizations.

SIX
Cyber Security Hub

Geared towards the Swiss financial industry, the SIX Cyber Security Hub provides banks and insurance companies with reliable, relevant information on the current risks and potentially dangerous developments that exist in the world of cyber security.

Collaboration between the organizations involved in the Swiss financial sector helps improve protection against cyber risks, and it is this protection against cyberattacks that makes the Swiss financial industry so stable, and attractive.

The key elements of the Cyber Security Hub are:

- Sharing information and experiences
- Implementing and discussing coordinated measures in the event of attacks, and subsequent evaluation

A common platform developed and managed by an independent provider, such as the Cyber Security Hub, is absolutely necessary in achieving this. SIX is the main infrastructure provider for the Swiss financial sector and cyber security is one our key responsibilities.

To protect the system-critical infrastructure of the Swiss financial industry, SIX has set up a Security Operations Center (SOC). It works around the clock (24/7/365) and uses a unique sector-specific threat-analysis intelligence function. One of the key tasks of the SIX SOC is constantly updating use cases with optimized detection rules, specifically geared towards identifying and mitigating the risks facing the Swiss financial industry, based on the latest information about the current threat situation.

All this knowledge flows into the Cyber Security Hub so that all members can benefit from the experiences of the community.

Who Is the Offering Aimed at?

It is particularly beneficial to small and medium-sized banks and insurance companies. They often do not have sufficient resources for such activities while also handling other security issues. The SIX SOC obtains information from a range of national and international sources, selecting and evaluating the relevant information and finally compiling it in a digestible format for all participants in the Swiss financial sector.

Due to the constantly evolving and changing patterns of cyberattacks, SIX has established a research team dedicated solely to gathering, analysing and delivering this information.

What Does the Cyber Security Hub Offer?

Access to relevant and detailed information on cyber security prepared specifically for the target groups – banks and insurance companies. The focus is on three areas:

- **Strategic**
  Threat Landscape Report for strategic briefing of decision-makers
- **Tactical**
  Extensive library of best practice use cases and playbooks from SIX and other members
- **Operative**
  Threat information (indicators of compromised activity) from SIX and other participants who can read the systems

The Benefits

"As **CEO/CIO**, I bolster the employees in my security team, encourage them to network with colleagues and improve the overall cyber resilience of my organization."

"As **CISO/CRO**, I receive compiled information for the C-level so that I'm always aware of current trends and developments. This enables me to prioritize countering risks and defensive actions correctly."

"As **Head SOC**, I receive information that is relevant for the banks and insurance companies. This enables me to set the right short and medium-term focus points in the risk management process."

"As **Security Analyst**, I receive information about cyber risks, dangers and attacks that I can put to use in real-time for defensive actions. I don't have to worry about the quality and currency of the various sources."

The entire content of this publication is protected by copyright. Whether in full or in part, the copying, reproduction, modification, transmission (electronically or otherwise), reuse or other use for public or commercial purposes is expressly prohibited without prior written consent.
The information contained in this document neither constitutes an offer for the rendering of a service nor any advice or recommendations in the area of cyber security (or any other area). SIX Group AG or its direct and indirect subsidiaries (hereafter: SIX) accepts no liability for the completeness, accuracy, currentness and uninterrupted availability of this information, or for losses as a result of actions taken on the basis of information found in this or other publications of SIX.

SIX
Pfingstweidstrasse 110
Postfach
CH-8021 Zürich

T +41 58 399 2111
securityhub@six-group.com
www.six-group.com

#discoverSIX