

WHITE PAPER

The State of Cybersecurity in the Swiss Financial Sector

JULY 2023





Contents

1. Introduction	03
2. Increased Risk Due to Global Upheaval	04
3. Cyber Risks in the Swiss Financial Sector	06
4. Switzerland and Its Threat Space	09
5. Security-Conscious Card Issuers.....	15
6. Real-World Recommendations	16
7. Solutions from Mastercard	18



1. Introduction

«At Mastercard, we are committed to preparing our network for the future, building a one stop cyber-shop using the latest AI technology and invaluable insights. This single cyber service helps protect our customers against the threat – enabling them to build trust with theirs.»

Ajay Bhalla, President of Cyber and Intelligence Solutions at Mastercard

Cybersecurity has never been more important or more widely discussed than it is today. The digitalization of all industries – both in the private and public sectors – is progressing ever faster, makes these organizations more vulnerable to attack, and therefore requires strong protection. In recent years, two events have brought even more attention to this subject.

The COVID-19 pandemic has driven an unprecedented digital transformation of governments, institutions, and companies. Video calls, electronic identification and signatures, mobile payments, and other technologies

have been widely implemented and adopted as new standards. This, in turn, has increased the possible angles of attack and incentives for data theft and malicious manipulations.

The current geopolitical situation also has implications for the digital space on a global level. Data from Cyber Quant, Mastercard's cybersecurity solution, shows that around two-thirds of politically motivated cyberattacks on European companies can be connected to foreign actors – and the trend is clearly on an upward trajectory.

The increasing shift toward digitalization offers enormous benefits, but also creates an even more attractive environment for cybercriminals.

They are better organized than ever before, and use complex technologies to achieve their financial and/or political goals. At the same time, nation states are trying to increase their influence in cyberspace, as are ideologically, politically, or socially motivated activists.

Within this environment, the financial sector is a particularly attractive target. It is therefore in its interest to be prepared for current and future cyber-threats. This applies in particular to Switzerland as one of the world's most important financial centers.

The following study identifies the main risks and outlines organizational and technical solutions for companies and administrative bodies. Mastercard, the global pioneer in payment innovation and technology, has contributed the experience it has gained from more than 50 years in the industry and from protecting more than two billion cards to this study.



Dr. Daniela Massaro
Country Manager
Mastercard Switzerland



2. Increased Risk Due to Global Upheaval

In recent decades, cybercriminals have already countered every technological development with new, more complex methods of attack. **As digital networks expand, the risk of threat actors using new points of entry for their attacks increases as well.** A high level of cybersecurity and active risk management are therefore key when it comes to defending against these attacks. Previously unknown types of cyberattacks and more opportunities for attacks require organizations to become more resistant and start fully integrating proven methods for cybersecurity into their processes. Malware or ransomware attacks are increasing at an

alarming rate. Switzerland's National Cyber Security Center (NCSC) reported around 34,000 cyber incidents in 2022 – more than 90 per day. This corresponds to a roughly 50 percent increase compared to the previous year. Because these incidents are reported on a voluntary basis, the actual number of attacks could be much higher.

IT system downtime costs companies an average of CHF 5,200 per minute.¹ But a look at the total damages after a data breach is even more revealing. According to a study by IBM, **the total cost of a data breach is CHF 4.1 million on average; for financial institutions, this number rises to CHF 5.8 million** – and that's

before taking reputational damage into account. In the next five years, this survey predicts an **increase of 15 percent annually.**² **Roughly 40 percent of companies that are attacked end up paying hackers a ransom** in order to regain access to their compromised or blocked systems. Affected companies in Switzerland currently pay an average of around CHF 80,000 (globally: CHF 167,000) per incident. Typically, the average cost to fix the technical, organizational, and reputational damage to a company is more than CHF 1.5 million.³

The National Bureau of Economic Research (NBER), a US non-profit research organization, found that the average firm **loses 1.1 percent of its market value and experiences a 3.2 percentage point drop in its year-on-year sales growth rate** after suffering a data breach.⁴ Many Swiss senior executives have already named cyber incidents as one of the greatest risk factors for their companies.⁵

¹ Everbridge, *The Impact of Cybersecurity Risks on Financial Services*, <https://www.everbridge.com/blog/the-impact-of-cybersecurity-risks-on-financial-services/>

² IBM, *Cost of a data breach 2022: A million-dollar race to detect and respond*, <https://www.ibm.com/reports/data-breach>

³ Sophos, *The State of Ransomware, 2022*, <https://assets.sophos.com/X24WTUEQ/at/4zpw59pnkpxnhfhgj9bxgj9/sophos-state-of-ransomware-2022-wp.pdf>

⁴ National Bureau of Economic Research, *Economic and Financial Consequences of Corporate Cyberattacks*, June 2, 2018, <https://www.nber.org/digest/jun18/economic-and-financial-consequences-corporate-cyberattacks>

⁵ Allianz, *Allianz Risk Barometer 2022*, January 18, 2022, <https://www.agcs.allianz.com/news-and-insights/reports/allianz-risk-barometer.html>



Switzerland is not immune to the effects of the geopolitically altered threat landscape either. The Swiss Federal Intelligence Service (FIS) has reported that foreign hackers have likely used Swiss servers to orchestrate cyberattacks in order to influence elections in other Western countries.⁶ Here, too, reputational damage is a cause for concern, as is the loss of the Switzerland's strategic influence.

Nevertheless, many Swiss companies are still not sufficiently equipped to address vulnerabilities in their systems and processes or to eliminate the corresponding risks. In November 2022, the NCSC reported⁷ that

nearly 3,000 companies had not addressed critical vulnerabilities in their IT systems, even though they had known about the issue for months and the patch had been available for two weeks. In addition, the Swiss Financial Market Supervisory Authority (FINMA) reported that around one-quarter of institutions that suffered attacks had been attacked indirectly via a service provider.

In the following study, we evaluated **5,935 reports of cyber incidents that affected Swiss companies and public authorities between Q1 2021 and Q2 2022**. The data was generated by Mastercard using its Cyber Quant solution. The primary objective of this study is to gain data-driven insights

into the state of security of Swiss financial institutions in particular within the current threat landscape.

In addition to the selected results and evaluations, the study also includes a typology of the of the most important threat actors, along with their motives, objectives, and attack methods. The final section is comprised of the results of a Mastercard survey of Swiss card issuers and recommendations for ways to reduce risk.

⁶ NZZ, August 28, 2022, <https://www.nzz.ch/schweiz/wie-aktiv-agitiert-der-kreml-von-der-schweiz-aus-ld.1700064>

⁷ National Cyber Security Centre, *Over 2,800 vulnerable Microsoft Exchange servers in Switzerland once again (ProxyNotShell)*, November 18, 2022, <https://www.ncsc.admin.ch/ncsc/en/home/aktuell/im-fokus/2022/schwachstelle-proxynotshell.html>



3. Cyber Risks in the Swiss Financial Sector

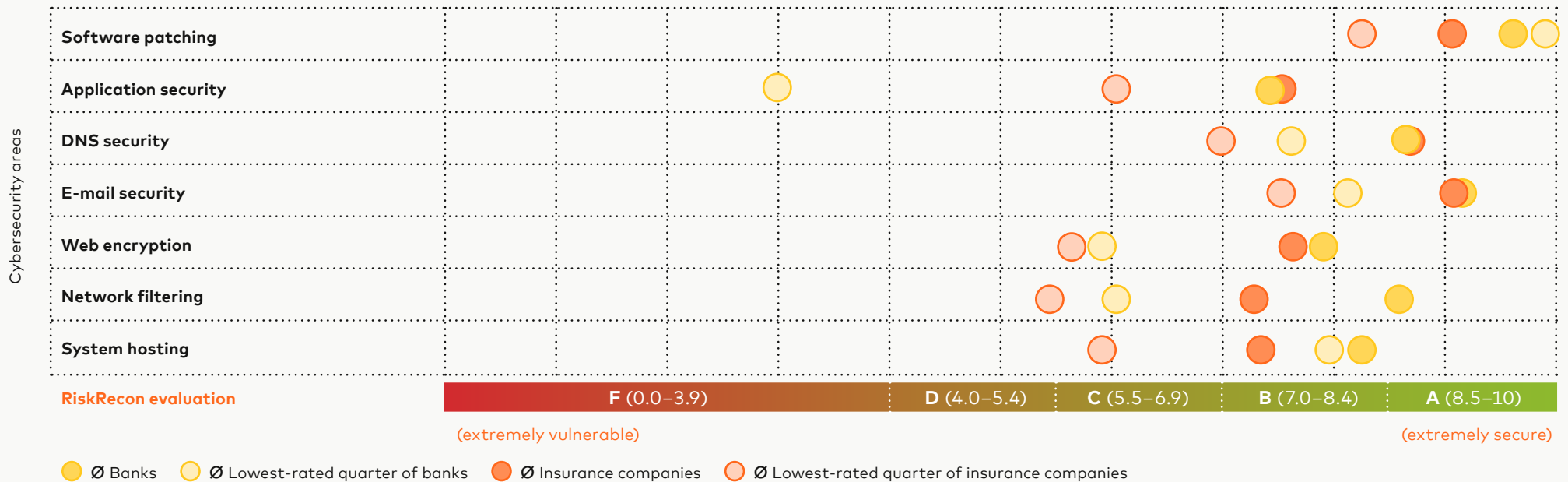
With RiskRecon, Mastercard offers a solution that automatically evaluates the maturity levels of domains (expression of security characteristics). It scans publicly available content under an organization's domain and evaluates it based on security aspects. This solution has been used to evaluate the current state of cyber-

security in the Swiss financial sector and identify common vulnerabilities.

The results show that the degree of cybersecurity varies greatly between the evaluated companies (see Fig. 1 below). **On average, they received 8.5 points on a scale of 0 to 10, which corresponds to the highest grade (A).**

Around 54 percent of the companies received an A (8.5 to 10 points). On the other hand, 7 percent only received a C (5.5 to 6.9 points) due to significant vulnerabilities in several evaluated areas.

Figure 1: Expression of Security Measures by Area and Financial Sector





As the chart above (Fig. 1, p. 6) illustrates, Swiss financial service providers **received the lowest scores in terms of application security (7.4 points), web encryption (7.8 points), system hosting (7.9 points), and network filtering (8.0 points).** Accordingly, these areas present the greatest security-related challenges. Insurance companies received similar scores to the banks. The greatest differences were in the areas of network filtering, software patching, and web encryption.

20% of the evaluated Swiss companies were running at least one system with unpatched web applications that represented a major or critical vulnerability.

In terms of software patching (see the corresponding category in Figure 1), results showed that **20 percent of the companies evaluated were running unpatched versions of application servers on at least one system,** which was classified as a major or even critical vulnerability. For example, web applications were often running on outdated software versions with PHP 5 or lower that no longer received updates to fix vulnerabilities. As a result, these applications offer threat actors attractive points of entry.

In most cases, the unpatched applications were related to subdomains with content of relatively low importance. However, the evaluation also found instances in which primary domains

were affected. Swiss financial service providers should therefore actively search their web servers for non-patched vulnerabilities in order to reduce the potential spread of malware and reputational risks.

30% of the evaluated Swiss companies were using CMS interfaces that exhibited a major or critical vulnerability.

30 percent of the evaluated companies showed major or critical problems in the area of application security (see the corresponding category in Figure

1) that could be traced back to **content management system (CMS)** interfaces. These interfaces were generally accessible from any device and only required a username and a password for authentication without any additional security measures.

Cybercriminals could potentially gain access through these interfaces using simple methods such as brute-force attacks (trying out possible username and password combinations). While the affected web applications often contained content of relatively low importance, in one case, a company's official website with its annual reports could be opened and edited without authorization. CMSs are particularly popular with smaller banks, which were therefore ranked at the bottom of the lowest quarter in terms of application security.



46 %

of the evaluated companies were using vulnerable network services like MySQL that represent a major or critical vulnerability.

Ultimately, **46 of the evaluated financial service providers** demonstrated major or critical vulnerabilities in terms of **network filtering** (see the corresponding category

in Figure 1), in particular **vulnerable network services**. These were mostly database servers and remote access protocols that were considered to be vulnerable and unnecessary. They can allow systems to be compromised using methods such as guessing login information, intercepting communications, and exploiting vulnerabilities.

All financial service providers who were confronted with critical problems in terms of network filtering were using vulnerable data storage systems such as MySQL, PostgreSQL, and Samba. These systems make organizations more vulnerable to attacks because they function as web network ports

that offer points of entry to potential attackers. This vulnerability can be exploited to intercept sensitive data, for example information sent to the company via contact form or data from participants in a contest.

In terms of the **web encryption domain**, 65 percent of the evaluated companies used certificates that were either expired or had invalid subjects, both of which were ranked as moderate risks. Invalid certificate subjects cause browsers to display security warnings to the user, which gives the impression that the website is not secure and negatively impacts the user experience. Expired certificates, on the other hand, make it difficult for users to evaluate the authenticity of the website. The encryption certificate should therefore be continuously updated or replaced as needed.

In terms of the **system hosting domain**, 49 percent of the evaluated financial service providers used shared IP addresses for at least part of their domain. This represents a moderate security problem. Shared IP addresses are more difficult to defend because the control options at the network level, such as options for IP address filtering and attack recognition, are limited. Moreover, after a cyber incident, there is a risk that unaffected domains could also be blocked due to the shared IP address. By using dedicated IP addresses, companies can better control the reputation of their systems and more effectively implement security controls on the network level.

Ultimately, in terms of **DNS security**, at 41 percent of the companies, at least one domain was identified that did not have the basic configuration required to prevent domain hijacking. Without the proper configurations, cybercriminals can gain unauthorized

control over this domain. To prevent this, companies can activate the “clientTransferProhibited” option. This status code tells your domain’s registry to strongly authenticate all protagonists who attempt to make changes to the domain and helps to prevent unauthorized changes to the configuration.



4. Switzerland and Its Threat Space

The data evaluations for this study from Mastercard Cyber Quant show that **93 percent of cyberattacks in Switzerland can be traced back to three** main threat actors: financial hackers, politically motivated cybercriminals, and political activists. They each have different primary motives, methods, and objectives, as depicted below (Fig. 2).

For example, financial hackers mainly use ransomware, malware, and phishing to attack government organizations, software companies, and financial service providers in order to acquire monetizable information.

Politically motivated cybercriminals, on the other hand, use malware, command & control servers (C&C, infecting and using remote servers for attacks), and supply chain attacks. Their preferred targets are government organizations, software companies,




and infrastructure operators in order to obtain intellectual property and trade secrets.

Mastercard Cyber Quant automatically analyzes **thousands of relevant sources, including media reports, the deep web (company databases, streaming servers, and online databases), and the dark web (anonymous, encrypted, and often criminal forums and marketplaces)**. The resulting data reflects the number of reported cyber incidents, not the

number of underlying attempts. Nevertheless, the data can be considered a reliable ballpark figure in terms of attack frequency.

Even though only Swiss financial service providers were evaluated for this study, cybersecurity is a global challenge because the majority of cyberattacks originate outside Switzerland.

Figure 2: Characterization of Key Threat Actors

Threat actors	Underlying motive	Typical attack types	Affected industries	Affected information
 Financial hackers	Financial	Ransomware, malware, phishing	Government, software, financial services	Monetizable information (e.g. login data)
 Politically motivated cybercriminals	Political	Malware, C&C, supply chain attacks	Government, software, infrastructure	Intellectual property, trade secrets
 Political activists	Ideological	(D)DoS	Government, media, financial services	Services provided, confidential information

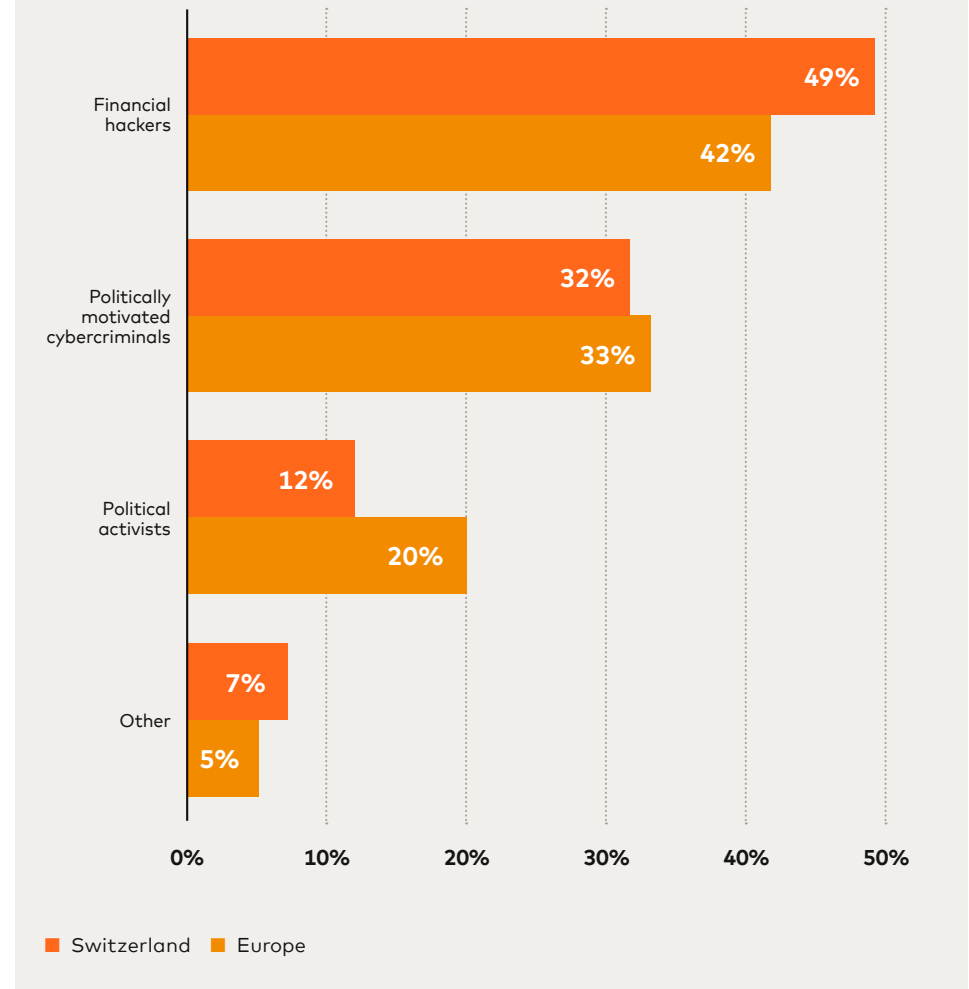


Financial hackers account for the majority (49 percent) of cyber incidents in Switzerland (see Fig. 3) due to the country's unique role as a major financial center. They account for 42 percent of attacks across Europe. Politically motivated cybercriminals were responsible for the second-largest share of attacks in Switzerland, with 32 percent, a number that is similarly high across Europe, with 33 percent. Political activists came in third place, with 12 percent.

7 percent of threat actors (Europe: 5 percent) could not be assigned to any of these three groups. These are mainly traditional fraudsters (Switzerland: 5 percent; Europe: 3 percent). They are financially motivated, but use much simpler methods than financial hackers, for example stealing credit card data through phishing and then using this data for their own purchases.

Only 1 percent of cyber incidents in Switzerland and Europe can be traced back to employees who exploit their authorized access to internal systems; this type of cybercrime is extremely difficult to detect. The share of threat actors in Switzerland and Europe who attack simply for the thrill of it is under 0.5 percent, as is the share of corporate spies trying to obtain information on their competitors.

Figure 3: Types of Threat Actors





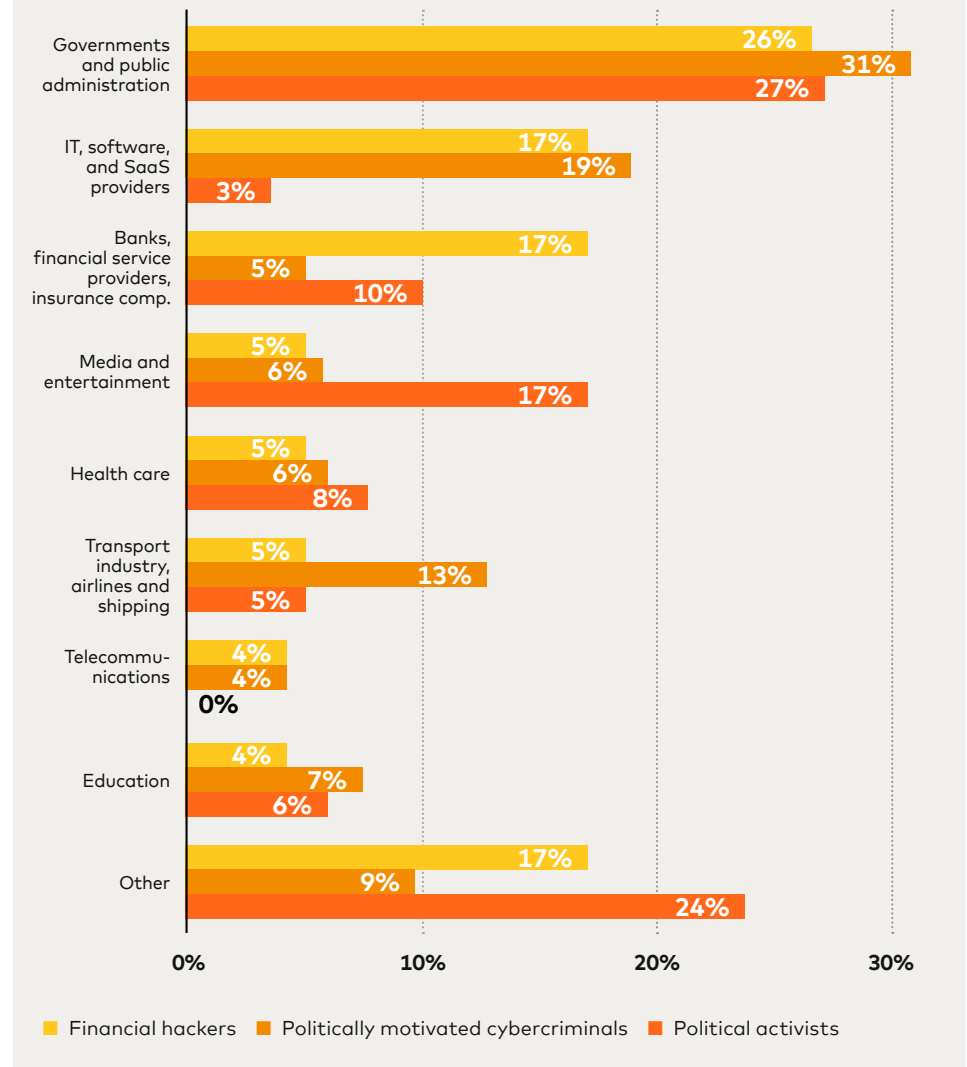
Due to the relatively low incidence of these kinds of attacks – and because we therefore have very little data on these attacks – this study will not be addressing these smaller groups of threat actors. Nevertheless, companies and organizations are still encouraged to consider them during risk assessment and risk prevention because they have the potential to cause just as much damage as the larger groups.

Financial Hackers

Nearly half of the cyber incidents in Switzerland are caused by financial hackers, who are primarily financially motivated. Accordingly, financial service providers – banks in particular, but also card issuers and insurance companies – are their preferred targets, accounting for 17 percent of

attacks (see Fig. 4). Normally, they try to steal and monetize sensitive information. Recently, their methods have become increasingly sophisticated, and are moving toward ransomware attacks (40 percent of attacks; see Fig. 5, p. 12). This method involves encrypting the victim’s data without authorization and then extorting the victim, demanding that they pay a ransom in order to regain access to their data. Cyberattacks by financial hackers pose a threat for all industries and jeopardize operational processes to the highest degree.

Figure 4: Main Attack Targets by Actor

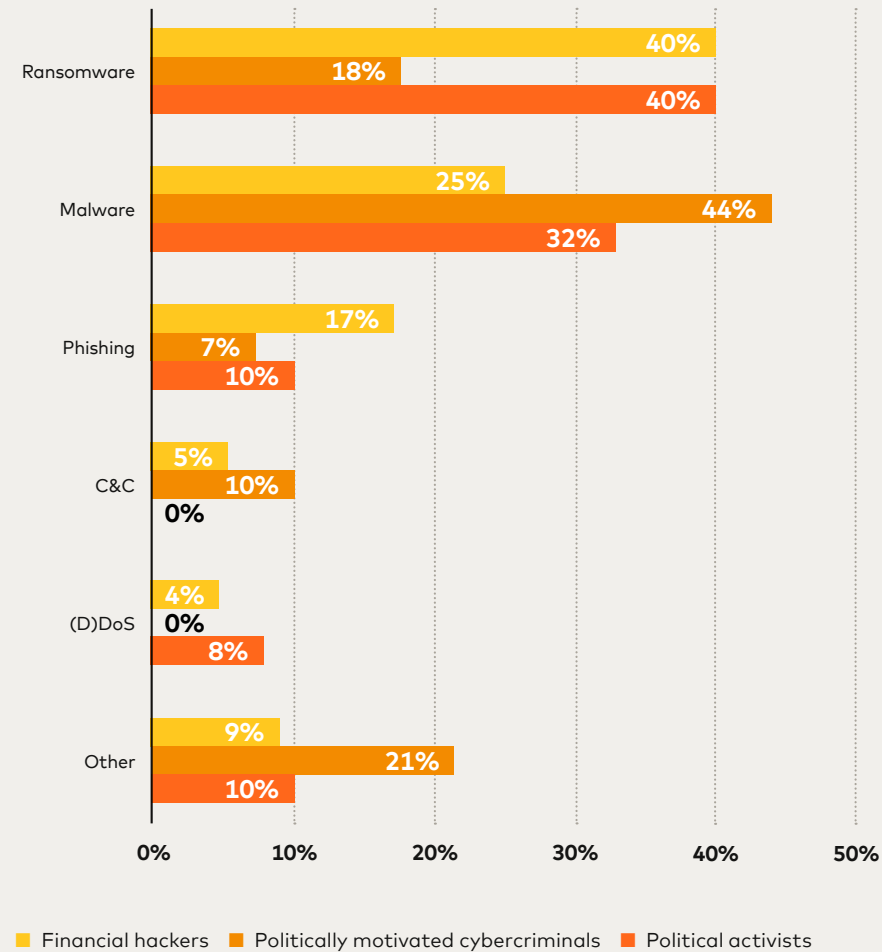




Politically Motivated Cybercriminals

The second-most-active threat actors in Switzerland are **politically motivated cybercriminals**, who account for around one-third of all incidents. Their motives are **political in nature**, and specifically depend on their **national affiliation or backer**. They are usually industrial or nation state spies who target state institutions and strategically important industries, such as companies in the areas of **transport, aviation, shipping, education, media and entertainment, and health care** (see Fig. 4, p. 11). This group's preferred attack methods – malware, C&C servers and supply chain attacks (see Fig. 5) – are **considerably more complex than those of financial hackers**, and are correspondingly difficult to detect.

Figure 5: Preferred Attack Methods by Actor



Political Activists

The third-most-active group of threat actors in Switzerland are **political activists (often referred to as "hacktivists")**. They are characterized by their strong **ideological, political, or social** motives. Political activists are individuals or decentralized groups that want to disseminate their message to the public, often by blocking access to important websites like news websites. Accordingly, they choose their targets based on their political views, ideology, or business model, and tend to act opportunistically depending on the current situation.



Attack Methods

The three groups of threat actors described here use **a variety of attack methods** that they select based on opportunity, motive, and objective. Ransomware (Trojans) and malware (malicious software) are two of the preferred methods. However, once again, different threat actors tend to prefer different methods.

Ransomware

Ransomware is mainly used by financial hackers to attack important systems or data and deny the owner access to said systems or data. Financial hackers generally demand that the companies involved pay them a significant ransom in order to regain access. They are increasingly using a **double-extortion strategy** in which they also threaten to publish confidential data if the company is unwilling to pay the ransom. CipherTrace, a Mastercard company, has determined that double-extortion ransomware attacks increased by nearly 500% between 2020 and 2021.⁸

Ransomware can impact any organization because attackers can use it **regardless of size or industry as soon as they** have gained access to an organization's network and assume that the organization can afford the ransom.

According to an analysis by the Financial Crimes Enforcement Network (FinCEN), a bureau of the U.S. Department of the Treasury, **a total of USD 590 million in ransom** was paid out in connection with ransomware incidents in the US in the first half of 2021 alone.⁹ After tracing cryptocurrency transfers, Chainalysis came to the conclusion that more than 70 percent of ransom payments could be attributed to foreign threat actors.

According to reports, this income is used by the financial hackers to operate more complex and professionally organized "business models" such as **Ransomware as a Service** (analogous to SaaS), which allows less specialized attackers to carry out ransomware attacks.¹⁰ Furthermore, they carry out business-like operations, including "customer service" teams, which interact professionally with victims in order to accelerate negotiations and increase the believability of their intention to restore compromised systems.

⁸ CipherTrace, *CipherTrace Report: Double extortion ransomware jumped by nearly 500% last year*, April 18, 2022, <https://ciphertrace.com/ciphertrace-report-double-extortion-ransomware-jumped-by-nearly-500-last-year/>

⁹ Financial Crimes Enforcement Network, *FinCEN Analysis Reveals Ransomware Reporting in BSA Filings Increased Significantly During the Second Half of 2021*, November 1, 2021, <https://www.fincen.gov/news/news-releases/fincen-analysis-reveals-ransomware-reporting-bsa-filings-increased-significantly>

¹⁰ Microsoft, *Ransomware as a service: Understanding the cybercrime gig economy and how to protect yourself*, May 9, 2022, <https://www.microsoft.com/en-us/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself>

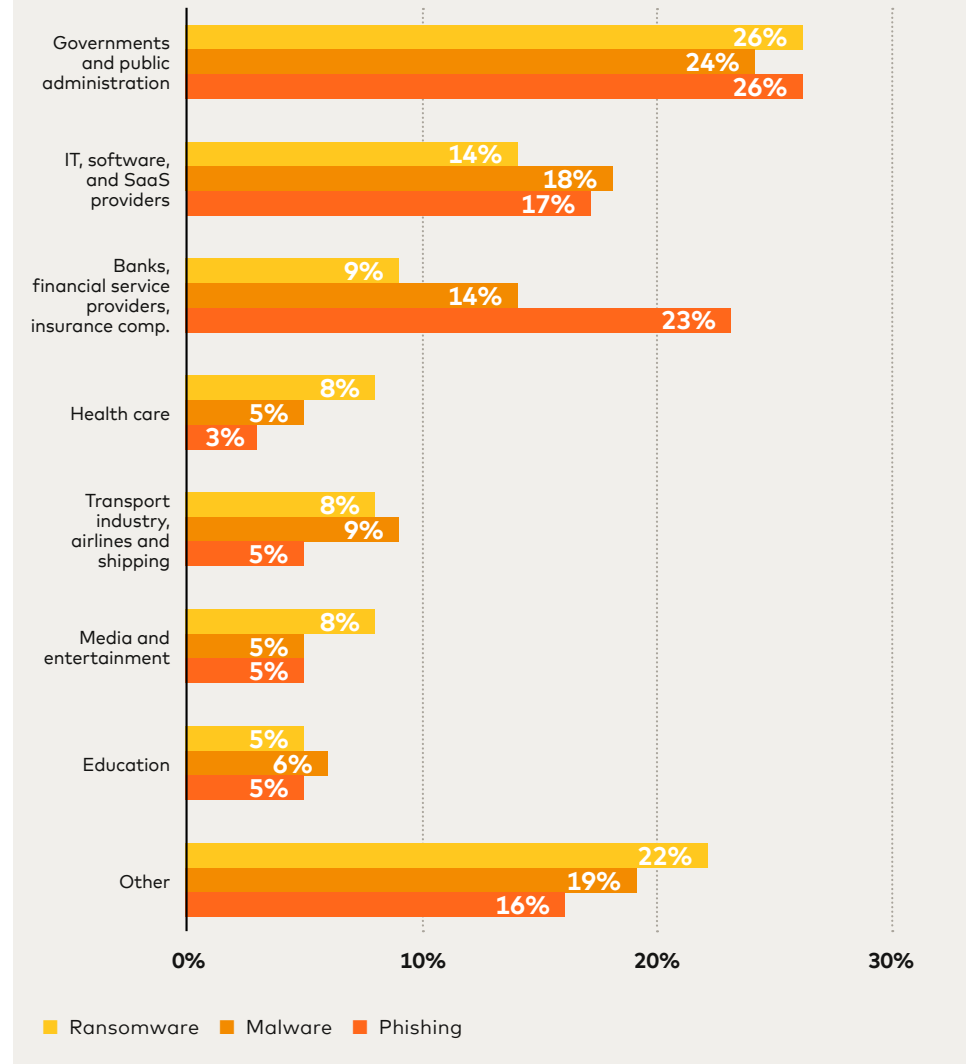


Malware

Malware is especially widespread in the banking industry in particular, accounting for 14 percent of reported cyber incidents (see Fig. 6). This is illustrated by the various Trojans that target customers in the financial sector. One of the most relevant examples that has greatly affected the Swiss banking sector is the Android malware **FluBot**. Financial hackers got consumers to click a link that was sent out via SMS and appeared to track a package or link to a voice message.

Instead, they were tricked into installing a malicious application. The application was then able to intercept the user’s bank data, including two-factor SMS messages, which gave the cybercriminals access to the customers’ online banking accounts and allowed the hackers to make transactions to their own advantage. In a similar fashion, in the case of **TeaBot**, a banking Trojan was mainly spread via the official app stores through what appeared to be a legitimate QR code scanning app.

Figure 6: Main Attack Targets by Attack Method





5. Security-Conscious Card Issuers

Swiss card issuers already give high priority to organizational and technical measures for more cybersecurity. **The majority of them evaluate their controls and security protocols annually with their own resources.** Only a few card issuers outsource this to external service providers. Most of them also carry out security exercises annually. Nearly all of them monitor **the cybersecurity risks of their suppliers** through **manual evaluations.** This was found by a Mastercard survey carried out among card issuers in July 2022.

Phishing – the theft of user data via fake websites, e-mails, or text messages – was seen as **a common attack method.** For this reason, employee training courses focused on phishing and were generally held on a quarterly basis. This applied in particular to employees with customer contact, because phishing generally targets customer data. A number of card issuers **also expanded these training courses to include select suppliers** in order to reduce indirect risk.

Respondents cited perimeter security, which means reducing risk in the boundaries between the company network and the public network, **along with identity and access management as the most important areas of IT investment.** However, with overall IT budgets remaining largely unchanged compared to the previous year, the **proportion of expenditure on cybersecurity was less than 10 percent,** thus remaining constant among the majority of respondents. Only a minority increased their cybersecurity expenditures.

Many card issuers had added the specialized position of **Chief Information Security Officer (CISO);** however, in many cases, this position did not report directly to the CEO. Most of the companies that participated in the survey had **calculated the possible financial impacts of cybersecurity risks** and regularly included this consideration in business decisions.



6. Real-World Recommendations

On the whole, the level of security awareness was encouraging, giving us cause to hope that Swiss financial service providers will continue to consider cybersecurity an extremely relevant topic in the future in order to continuously reduce their risks. The **combination of quick fixes and complex, long-term measures** enables the constant and necessary focus on cybersecurity in an environment in

which threat actors are continually developing new attack methods.

This includes gearing **employee and supplier training toward the most common security risks** like those listed in this study. In terms of budgeting, we recommend **creating a separate cost center for cybersecurity** so that it does not have to compete with other IT investments that have an

easier-to-understand ROI and therefore could be subconsciously favored.

Cyber risks in the supply chain can be further reduced through **routine security checks and by training suppliers and service providers**. If a company has a large number of partners, it makes sense to supplement manual security evaluation with **time-saving automated evaluations**.

Last but not least, we recommend incorporating cybersecurity into all corporate decision-making processes as a potential business risk alongside other measured quantities, KPIs, and success factors.



Highest Strategic Priority

- Assign cybersecurity to the CEO as a staff unit
- Consider cybersecurity as an investment, not a cost factor



Prevention and Defense

- Continually develop cybersecurity measures
- Carry out regular attack simulations



Cooperation

- Establish transparency in terms of current threats
- Exchange knowledge within the financial sector



Organizational measures could include assigning the **Chief Information Security Officer to the CEO as a staff unit** instead of completely externalizing this department.

Many vulnerabilities are the result of insufficiently secured domains and IT systems from acquired subsidiaries. We therefore recommend that companies **carry out cyber due diligence before any acquisition, and introduce and enforce guidelines for acquired companies** that ensure they meet

the same security standards as the parent company.

Even though the likelihood of an attack may seem low at first, given the enormous damage risks and costs, it is advisable to take cybersecurity measures further than simple security checks. Instead, companies and organizations need to consider **simulating standard attacks themselves** in order to recognize and address existing vulnerabilities in their systems and in third-party systems early on.

Companies that see **cybersecurity as an investment** – not just as a cost factor – are laying the foundation for a secure and successful future. Greater cooperation between Swiss financial service providers could further increase the effectiveness of these individual measures.



7. Solutions from Mastercard

Mastercard helps companies to detect potential security risks early on and to continually reduce them over time. A two-pronged approach has emerged and proven itself in practice.

Mastercard solutions actively evaluate digital networks in terms of vulnerabilities, monitor all transactions, and limit fraud from the "outside in." From the "inside out," they evaluate and strengthen the company's internal processes, technologies, and practices in terms of its risk exposure.

The following three solutions are particularly effective in helping companies increase cybersecurity and trustworthiness within a digitally networked economy:

Cyber Quant ("Inside Out")

Cyber Quant is a solution for the **risk assessment of a company's security processes and practices as well as its technological infrastructure.** Cyber Quant assesses the maturity level of 50 types of security measures in the areas of infrastructure, prevention,

and discovery. This solution helps companies select and prioritize their cybersecurity measures based on the threats they face.

Cyber Front ("Outside In")

Cyber Front evaluates how resistant an organization's security mechanisms are. To do this, Cyber Front **imitates the behavior of organized cybercriminals**, who attack systems in multiple ways simultaneously. The program evaluates the effectiveness of every security check, such

as Firewalls and attack-detection systems, and offers recommendations for ways to further strengthen existing configurations.

RiskRecon ("Outside In")

RiskRecon automatically monitors the cyber environment of every company with an online presence – thereby saving time and reducing the manual workload – in order to identify cyber risks and vulnerabilities before they can be exploited. Through the **effective, ongoing evaluation of third-party risks**, companies are able to further minimize their risk of becoming the victim of indirect cyberattacks via external business partners.

