Down but not out: Swiss fraudsters are digitalising and diversifying

39%
of Swiss organisations experienced fraud and/or economic crime.

41%
of respondents see cybercrime as the most significant risk over the next 24 months.

92%
of Swiss firms expect to either significantly increase (6%), increase (25%) or maintain (61%) the amount of funds used to combat fraud.

pwc

About the survey

7,228 respondents completed PwC's 2018 Global Economic Crime Survey globally, including 101 respondents from Swiss organisations. We questioned respondents between 21 June 2017 and 28 September 2017 regarding fraud and economic crime within their organisations over the last 24 months. 38% of Swiss respondents' organisations were publicly traded companies while 40% were privately owned. The majority of Swiss respondents were senior management or department heads.

Please note, where charts represent a base of hundred percent, there may be deviations of 1 to 2 percent due to rounding throughout this document.

Contents

Introduction

Welcome to our deep dive into the results of PwC's 2018 Global Economic Crime and Fraud Survey ("the 2018 survey") as they pertain to Switzerland. Over the last 24 months, Switzerland has seen high profile reported instances of layering of the proceeds of crime and bribery and corruption, instances of internal fraud and fallout from global data breaches, and has implemented the Foreign Illicit Assets Act ("FIAA").[1]

Despite high profile fraud[2] cases reported in the media, fraud in Switzerland does not seem to be proliferating – only 39% of our respondents reported that their organisations experienced fraud in Switzerland within the last 24 months, down from 41% in 2016[3] and below 49% reported globally. The mean direct loss attributable to each reported fraud instance in Switzerland was 9.5 million Swiss Francs.

Respondents reported that asset misappropriation (51%) and cybercrime (44%) were the biggest contributors to fraud experienced, with cybercrime the most significant perceived risk going forward.

Perhaps surprisingly, our respondents reported that bribery and corruption has increasingly affected Swiss businesses – 27% of the respondents were asked to pay a bribe in the last 24 months (up from 9%) and 20% lost a business opportunity to a competitor they believed paid a bribe (up from 11%). Firms need to identify and manage bribery and corruption risk without any unnecessary loss of opportunity.

The 2018 survey results indicate that many Swiss firms can develop their systems and controls and better utilise technology to detect, monitor and mitigate fraud risk. We believe that proportional investment in Digital Technology can accelerate fraud reduction in Switzerland.

We hope that you find our analysis both insightful and helpful in your efforts to combat fraud. Our sincere thanks to those who participated within the 2018 survey, without whom this publication would not be possible.

Gianfranco Mautone
Forensic Services and Financial Crime Leader, Switzerland

[1] Federal Act of 18 December 2015 on the Freezing and the Restitution of Illicit Assets held by Foreign Politically Exposed Persons (Foreign Illicit Assets Act, FIAA), implemented 1 July 2016

[2] References to fraud include fraud and/or economic crime

[3] Comparatives provided are against the responses received from PwC's 2016 Global Economic Crime Survey

Reported fraud in Switzerland is less than that reported globally and 6% lower than the average reported across Western Europe

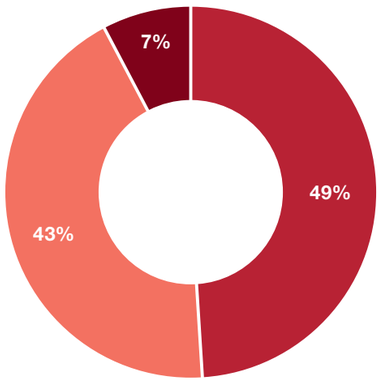
Fraud in retreat?

The 2018 survey identified a small decrease in reported fraud in Switzerland with 39% of Swiss respondents experiencing fraud within the last 24 months, compared to 41% in 2016. Reported fraud in Switzerland was less than that reported globally (49% of global respondents) and 6% lower than the average reported across Western Europe (45%).

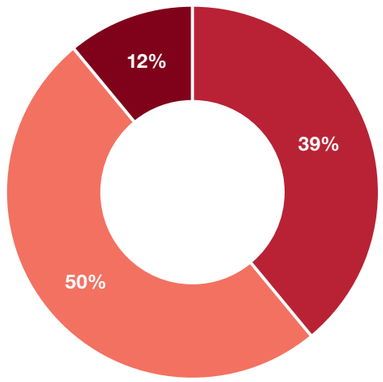
Interestingly, more than one in ten Swiss respondents (12%) did not know whether their organisation had been a victim of fraud in the last 24 months (7% globally). Considering this "known unknown" and the potential for fraud to manifest unnoticed within an organisation, we believe that the level of actual fraud occurrence within Switzerland, and indeed globally, is more than the 39% and 49% reported.

Has your organisation experienced any fraud and/or economic crime in your country within the last 24 months?

Global



Switzerland



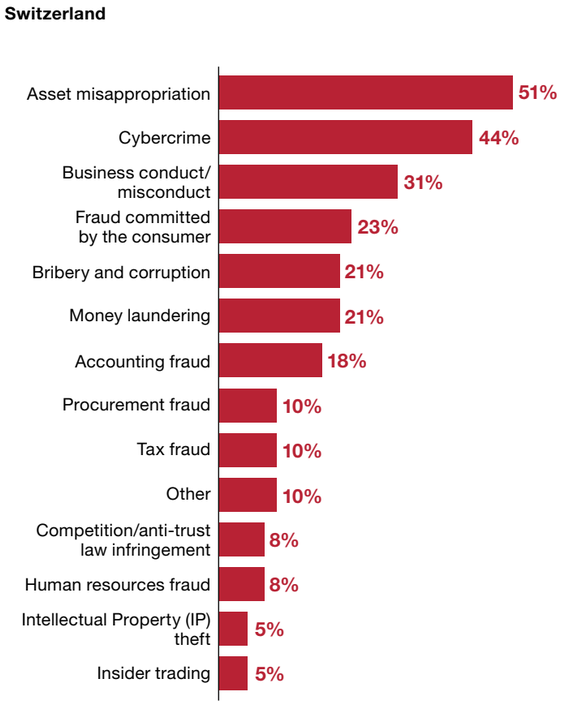
Yes No Don't know

Whilst the 2018 survey illustrates a gap between the reported levels of fraud in Switzerland and globally, the fraud landscape in Switzerland did not depart significantly from that observed globally. In the past 24 months, the two highest number of reported fraud types in Switzerland (and globally) were asset misappropriation (51%, 45% globally) and cybercrime (44%, 31% globally).

What types of fraud and/or economic crime has your organisation experienced within the last 24 months?

Global

Switzerland

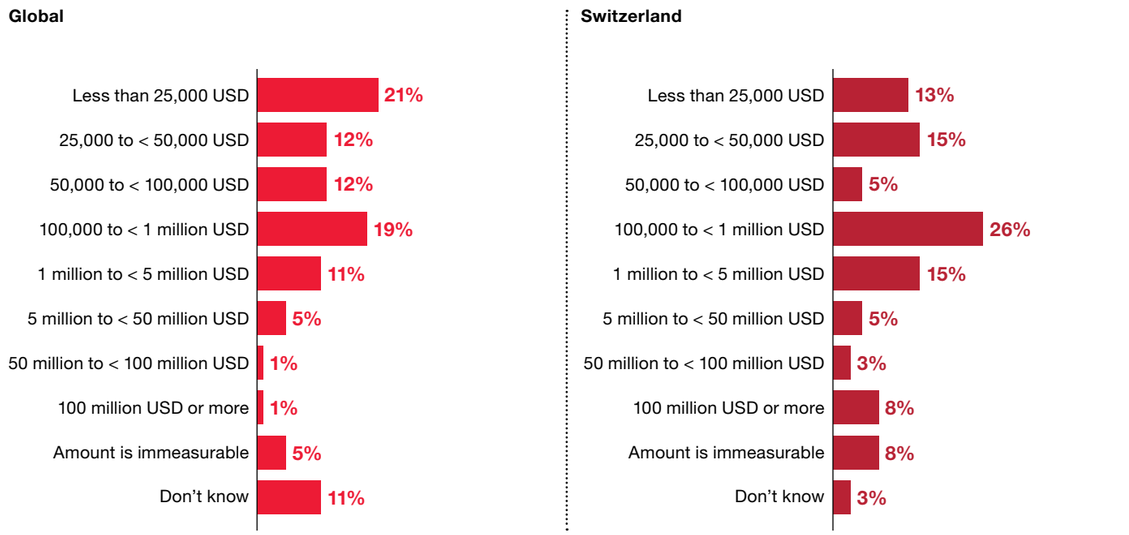


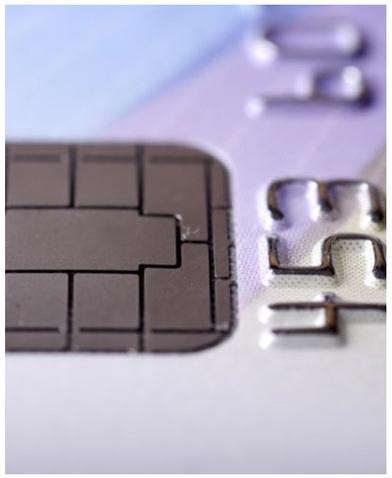
The cost and impact of fraud

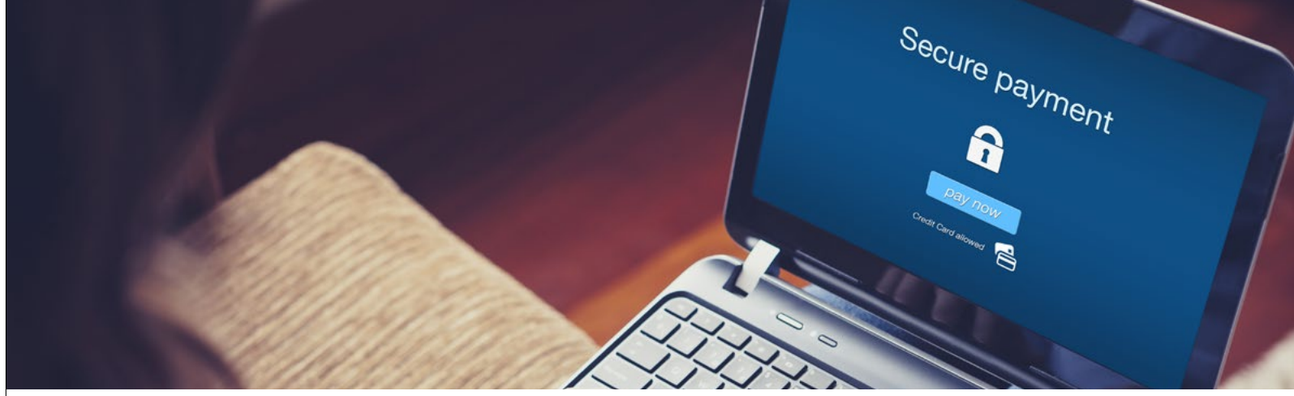
While any decrease in fraud is good news for Swiss organisations, our examination of the survey data reveals some disconcerting facts. The financial impact of fraud on Swiss respondents has been significantly higher than the financial impact observed globally. In Switzerland, the mean direct loss in relation to fraud incidents was 9.5 million Swiss Francs (approximately 10 million USD), compared to only 1.8 million Swiss Francs (approximately 1.9 million USD) globally.

This difference may be due in part to the size of the Swiss economy and its significant financial services and banking industries. 29% of Swiss respondents operate in the financial services industry, compared to 22% of global respondents, and 6% operate in the insurance business, compared to 4% globally. Due to the nature of their business activities, banks and other financial institutions are an appealing target for fraudsters and are likely to suffer financial losses above those incurred by organisations without such custodian responsibilities.

In financial terms, approximately, how much do you think your organisation may have directly lost through the most disruptive crime over the last 24 months?







Fraud is in the eye of the beholder – we believe fraud awareness is lower than fraud occurrence

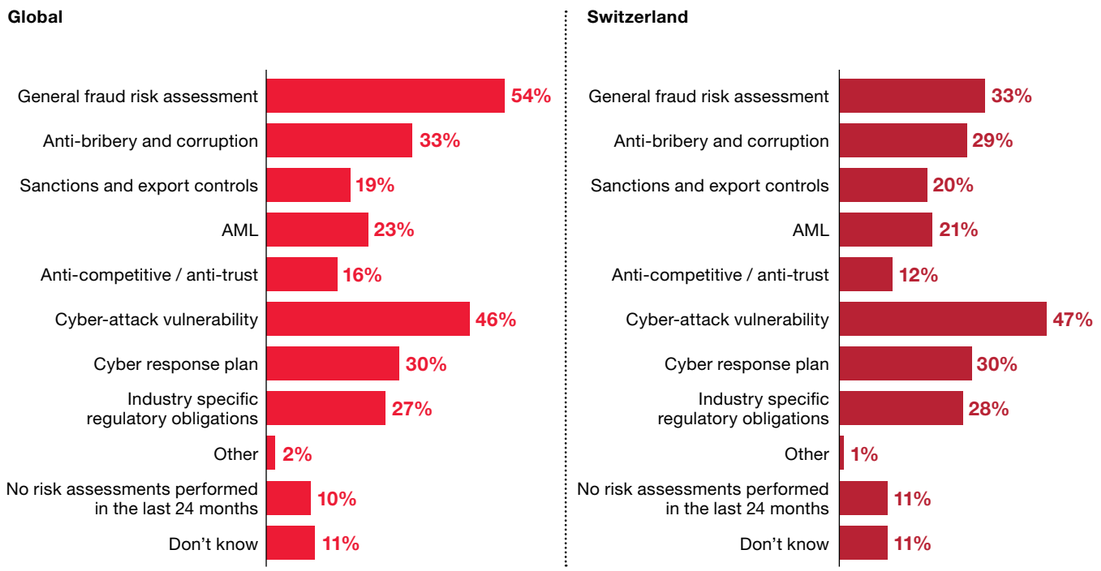
We believe that fraud is occurring unnoticed and unreported within some of the 61% of Swiss respondents who reported observing no instances of fraud within their organisations. Fraud is difficult to identify, to comprehend and to report – it is dynamic and constantly evolving.

Objective and subjective factors may have influenced the identification and the 2018 survey respondents' awareness of fraud within an organisation. Individuals often have their own unique definition, perception and understanding of fraud. Of course, objective factors play a role – a country's legal framework and law enforcement system – however, this is only part of the picture. We believe that a respondent's perception of their organisation and their awareness of fraud influences their response, particularly where a respondent does not have access to management reporting concerning fraud.

The significant gap between reported fraud in Switzerland (39%) to that reported globally (49%) and in Western Europe (45%) may indicate a lower level of fraud awareness amongst the Swiss respondents, a greater perception of the effectiveness of their organisations anti-fraud systems and controls, or a more limited ability to detect fraud.

When asked whether their organisation performed any risk assessments in the last 24 months only one in three Swiss respondents (33%) indicated that they had conducted a general fraud risk assessment, significantly below the 54% of global respondents who had conducted one. General fraud risk aside, the proportion of Swiss organisations who carried out risk assessments of specific fraud areas such as cybercrime, bribery and corruption and money laundering aligned to global results.

In the last 24 months, has your organisation performed a risk assessment on any of the following areas?



These results may reflect a shift in focus of Swiss respondents from general fraud risk management to distinct individual fraud risk areas.

Bribery and corruption – a costly barrier to business

In the past 24 months, Swiss firms have been increasingly mindful of bribery and corruption risks, particularly financial institutions who must guard against the risk that proceeds of bribery and corruption infiltrate and proliferate in the financial system (money laundering). In the last 24 months, both the Swiss Financial Market Oversight Authority ("FINMA") and the Office of the Attorney General of Switzerland ("OAG") have been active in cases against financial institutions for allegedly failing to identify and prevent money laundering with respect to the proceeds of bribery and corruption. Action has also been taken against firms alleged to have actively engaged in bribery and corruption.

It is in this context that Swiss respondents' awareness of, and confidence in acknowledging, attempted bribery and corruption has increased from 2016 to 2018. In 2018, 27% of the Swiss respondents reported that they had been asked to pay a bribe, up from 9% in 2016.

One in five respondents (20%) believe that their firms lost an opportunity to a competitor who paid a bribe within the last 24 months, up from 11% in 2016 – a stark statistic. Interestingly, of these respondents', 70% experienced the lost opportunity globally rather than within the country they primarily do business in. 50% of Swiss organisations that were asked to pay a bribe, experienced this outside the country where they primarily do business in.

"Bribery and corruption is unjust and stifles fair competition amongst firms. Firms have both a moral and legislative imperative to identify, manage and report[4] bribery and corruption risk."

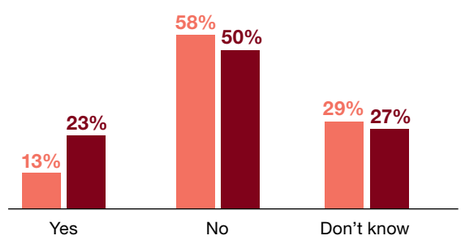
Gianfranco Mautone, Forensic Services and Financial Crime Leader, Switzerland

[4] An online reporting system (https://fedpol.integrityplatform.org/) allows anonymous reporting of bribery and corruption to Swiss law enforcement.

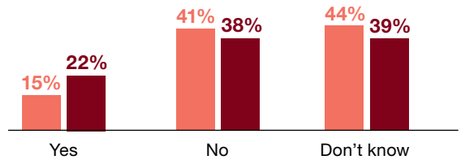
In the last 24 months, has your organisation (comparison to previous years):

Global

Been asked to pay a bribe?

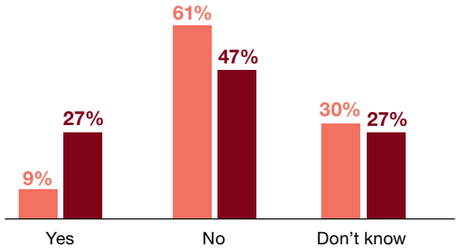


Lost an opportunity to a competitor which you believe paid a bribe?

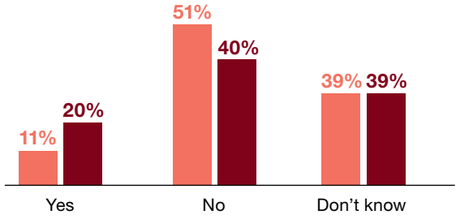


Switzerland

Been asked to pay a bribe?



Lost an opportunity to a competitor which you believe paid a bribe?



While business practices around the world differ, Switzerland's bribery and corruption legislation, the Foreign Corrupt Practices Act and the UK Bribery Act apply uniformly. Swiss businesses and non-governmental organisations must ensure that they have identified and assessed the bribery and corruption risks facing their organisations, and established proportionate mitigating systems and controls.

The threat of cybercrime – the dark cloud that will not move on

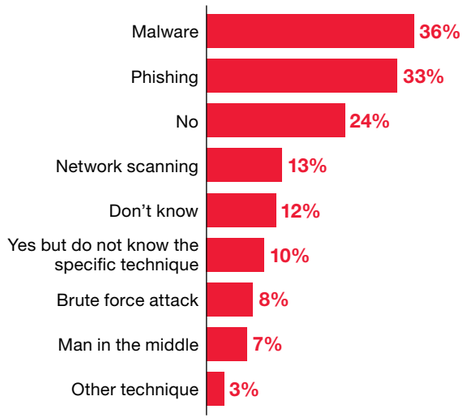
Although the most common type of fraud observed was asset misappropriation, however, when looking to the future, the 2018 survey respondents saw cybercrime as the most disruptive form of fraud over the next 24 months. 44% of the Swiss respondents experienced cybercrime in the last 24 months, compared to 51% who experienced asset misappropriation, while 41% of respondents expected cybercrime to be the most disruptive and significant threat to their organisation over the next 24 months, compared to only 5% of the respondents who identified asset misappropriation.

This result reflects increasing business and consumer digitisation, the increasing sophistication of attacks and heightened data security expectations amongst stakeholders. Cyber security – the mitigation of cybercrime – is now a **boardroom priority.**

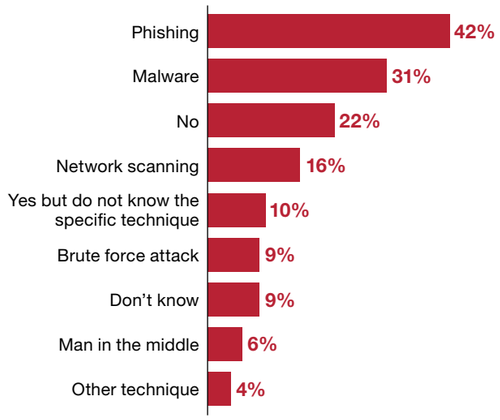
Respondents reported that internal and external actors employed a variety of cyber techniques to commit several different offences against their organisations. Phishing and malware were the most common cyber-attack techniques in Switzerland (42% and 31% respectively) and globally (33% and 36% respectively).

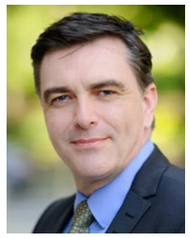
In the last 24 months, has your organisation been targeted by cyber-attacks using any of the following techniques?

Global



Switzerland





"Firms must first understand their security fundamentals in order to effectively build and develop their security architecture"

Reto Haeni, Cybersecurity and Privacy Leader, Switzerland

Contrary to other types of fraud, cybercrime is not a stand-alone offence but rather a means to commit other types of fraud. Three in ten Swiss respondents suffered disruption to their business processes after having been the victim of a cyber-attack. More than a quarter of the Swiss respondents (28%) were the victim of extortion and more than a fifth (23%) reported that a cyber-attack was used as a conduit to commit asset misappropriation against their organisation.

The 2018 survey results show that Swiss firms are taking the clear and present threat of cybercrime seriously and are actively implementing cyber security measures. However, additional efforts are necessary to close the gap indicated within the survey results between the cyber security standards observed in Switzerland and those globally.

In Switzerland, only 54% of the respondents have an operational cyber security programme, 5% below the global average and 7% below the average observed in Western Europe. Some Swiss respondents reported that they had either prepared a programme, but have not yet implemented it (14%), or that they were currently assessing the feasibility of implementing a programme (15%).

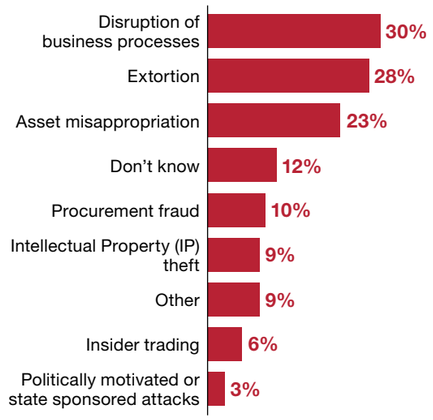
Firms without an operational cyber security programme need to accelerate their planning and implementation. Furthermore, respondents with an existing cyber security framework need to assess whether their framework offers sufficient protection and, if necessary, implement measures aimed at fostering their ability to prevent and detect cybercrime. Cyber-attacks on individual user devices demonstrate that external actors target weak systems and organisations, and are not only attracted to organisations based upon size or industry.

The increasing complexity of fraud and economic crime perpetrated through digital channels is challenging organisations to keep up with the pace of change. Consequentially, we consider that the risk of not knowing all fraud threats and threat vectors exceeds the potential risk associated with managing those fraud risks identified by an organisation.

Which of the following types of fraud and/or economic crime was your organisation victim of through a cyber-attack?

Global

Switzerland



Fraud, quo vadis?

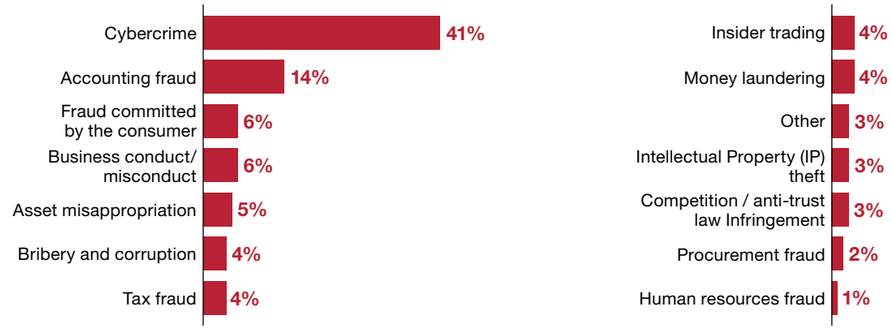
When we asked respondents about what they believed would be the most disruptive type of fraud in terms of the impact on their organisation in the next 24 months, cybercrime was the number one response in both Switzerland (41%) and globally (26%).

Interestingly, the response accounting fraud ranked second in Switzerland (14%) but seventh (6%) amongst global respondents. In recent years, the strength of the Swiss franc has had a negative impact on Swiss organisations' consolidated overseas income. This, together with recent low economic growth over the period may have led Swiss respondents to conclude that the incentive for committing accounting fraud in Switzerland will increase.

Furthermore, whilst asset misappropriation was the most common type of fraud reported in Switzerland in the past 24 months, Swiss respondents are optimistic going forward – only 5% of the respondents named this risk to as the most disruptive type of fraud impacting on their organisation in the next 24 months (compared to 11% globally).

Thinking about the **next** 24 months, which of the following fraud and/or economic crimes is likely to be the **most** disruptive/serious in terms of the impact on your organisation (monetary or otherwise)?

Switzerland



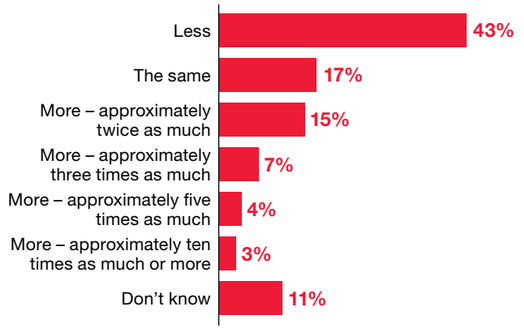
Keeping it simple – building from strong anti-fraud foundations

The mean direct loss attributable to 39% of organisations who reported fraud in Switzerland within the last 24 months was 9.5 million Swiss Francs (approximately 10 million USD) per respondent. In responding to the most disruptive crime experienced, 69% of organisations spent the same or more money on investigations and/or other interventions. Globally, 46% of the respondents spent the same or more money on investigations and/or other interventions than the direct financial loss caused by the most disruptive fraud instance experienced.

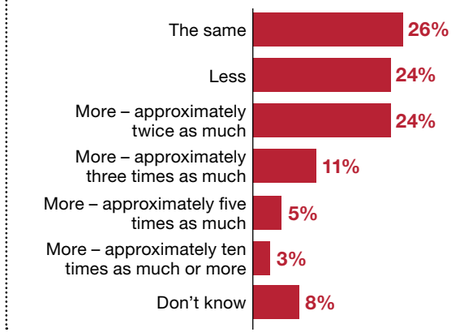
The results in Switzerland are particularly worrying due to the high indirect costs incurred in investigations and other post-fraud interventions conducted by the respondents

As a result of the most disruptive crime experienced in the last 24 months, was the amount spent by your organisation on investigations and/or other interventions, more, less or the same as that which was lost through this crime?

Global



Switzerland



The results in Switzerland are particularly worrying – not only because the average direct financial loss suffered by Swiss organisations was more than five times higher than the average reported globally, but also due to high indirect costs incurred in investigations and other post-fraud intervention activities conducted by the respondents.

For some organisations, responses to the survey indicate that monies spent on investigations and/or other interventions could be used more effectively – on fraud prevention.

At least 78% of Swiss organisations performed a risk assessment encompassing one or more fraud and economic crime areas. Firms can maximise their risk assessment by including all major risks together and evaluating them holistically. For example, firms in all industries should assess the following risks:

- Fraud risk;
- Anti-bribery and corruption;
- Sanctions compliance;
- Anti-trust; and
- Cyber risk.

22% of the Swiss respondents and 21% of the respondents globally have not performed a risk assessment in the past 24 months or could not answer the question.

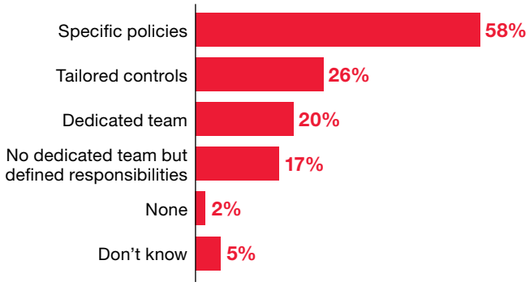
Both in Switzerland as well as globally, respondents' ethics and compliance programs focus mainly on general fraud, anti-bribery and anti-corruption as well as industry-specific regulatory compliance. A low proportion of the respondents in Switzerland and globally reported that their ethics and compliance programs addressed further fraud risk areas, such as sanctions and export controls, anti-money laundering, anti-competition and anti-trust or cyber behaviour.

The ethics and compliance programs of the Swiss respondents and the respondents globally largely consist of specific policies. The reported use of tailored controls, dedicated teams or defined responsibilities to address the aforementioned risk categories is below our expectation and our view of best practice ethics and compliance programs.

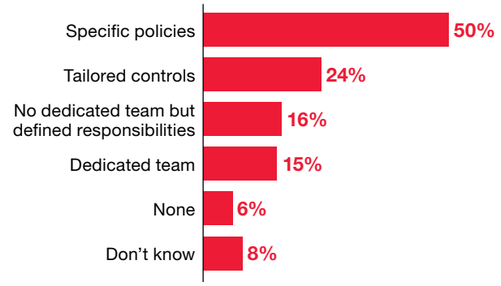
In what ways does your organisation's formal business ethics and compliance program address the following risk categories?

Global

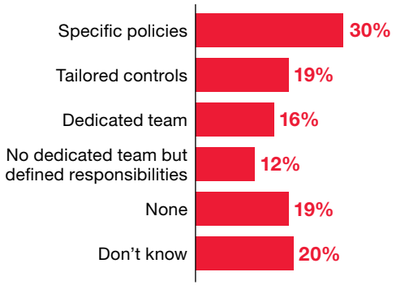
General fraud



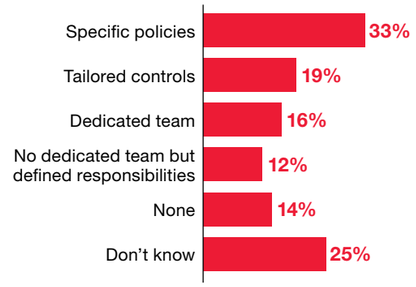
Anti-bribery and corruption



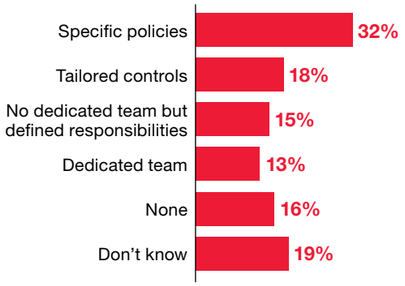
Sanctions and export controls



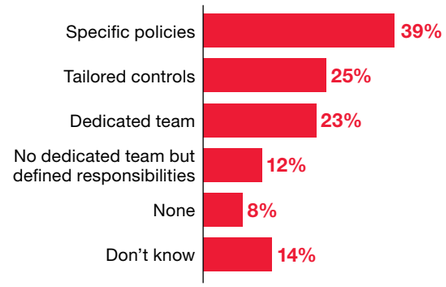
AML



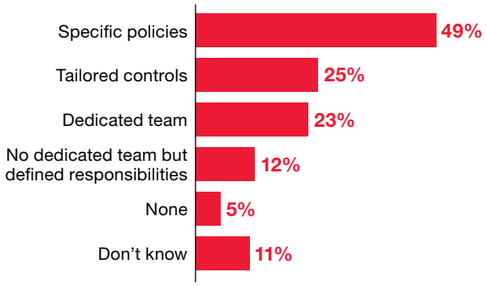
Anti-competitive / anti-trust



Cyber behaviour

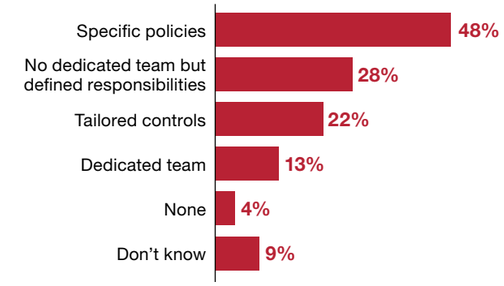


Industry-specific regulatory compliance

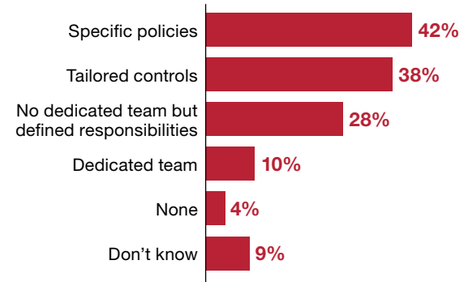


Switzerland

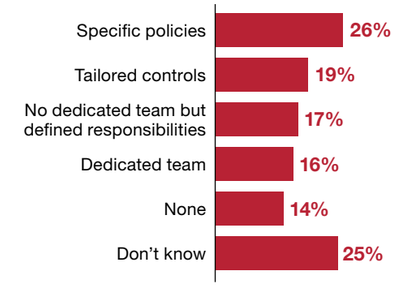
General fraud



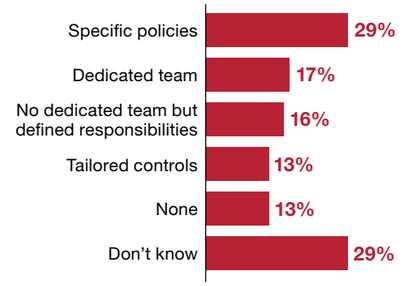
Anti-bribery and corruption



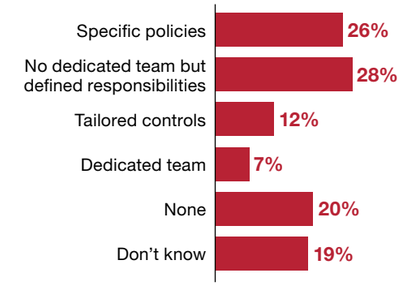
Sanctions and export controls



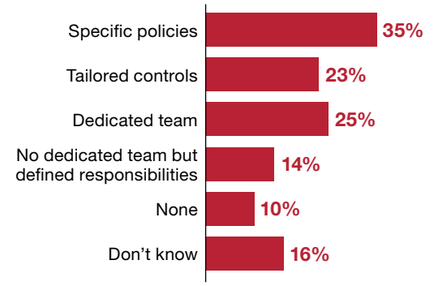
AML



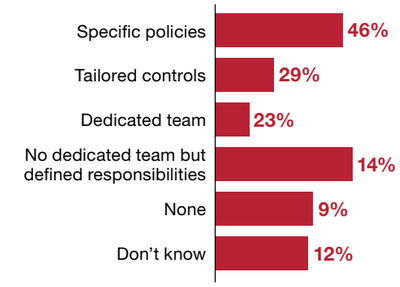
Anti-competitive / anti-trust



Cyber behaviour

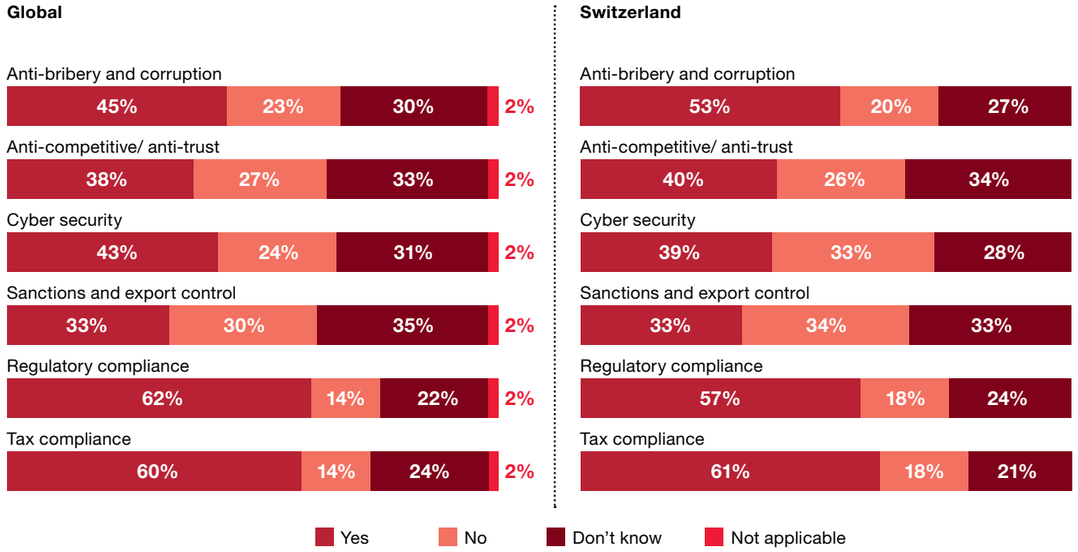


Industry-specific regulatory compliance



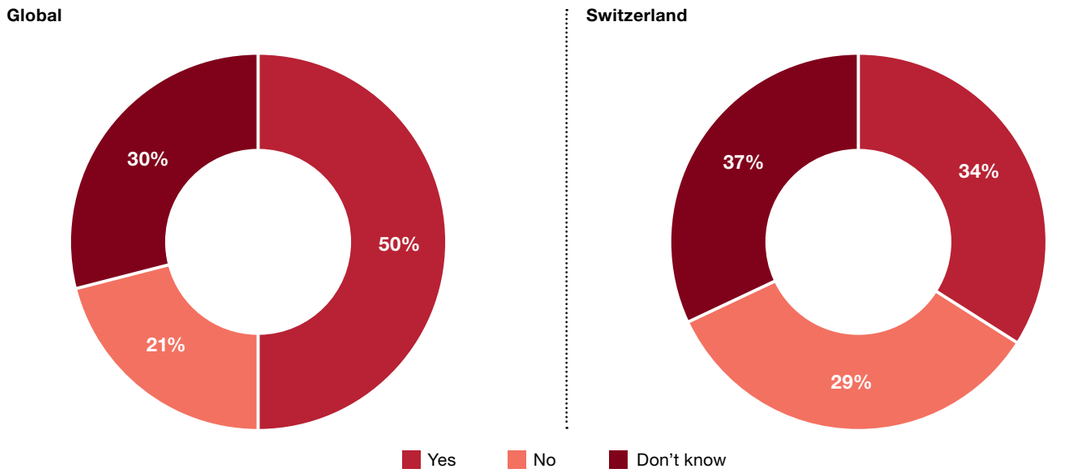
Reoccurring and/or unchecked fraud in a company can be financially costly or worse, indicative of a weak control environment and a poor tone at the top –factors that are important considerations in any acquisition. Our survey has identified that the majority of respondents consider fraud and/or economic crime risks as part of acquisition due diligence.

Does your organisation perform any of the following additional due diligence as part of your acquisition process?



Interestingly, given that Switzerland is not currently implementing a publicly available ultimate beneficial owner register[5], Swiss respondents were undecided if the implementation of Global Beneficial Ownership standards would ultimately benefit their organisation in combatting fraud (37% did not know, 34% responded "yes" and 29% "no").

In your business/industry, would the implementation of Global Beneficial Ownership standards be beneficial to your organisation in combatting economic crime?



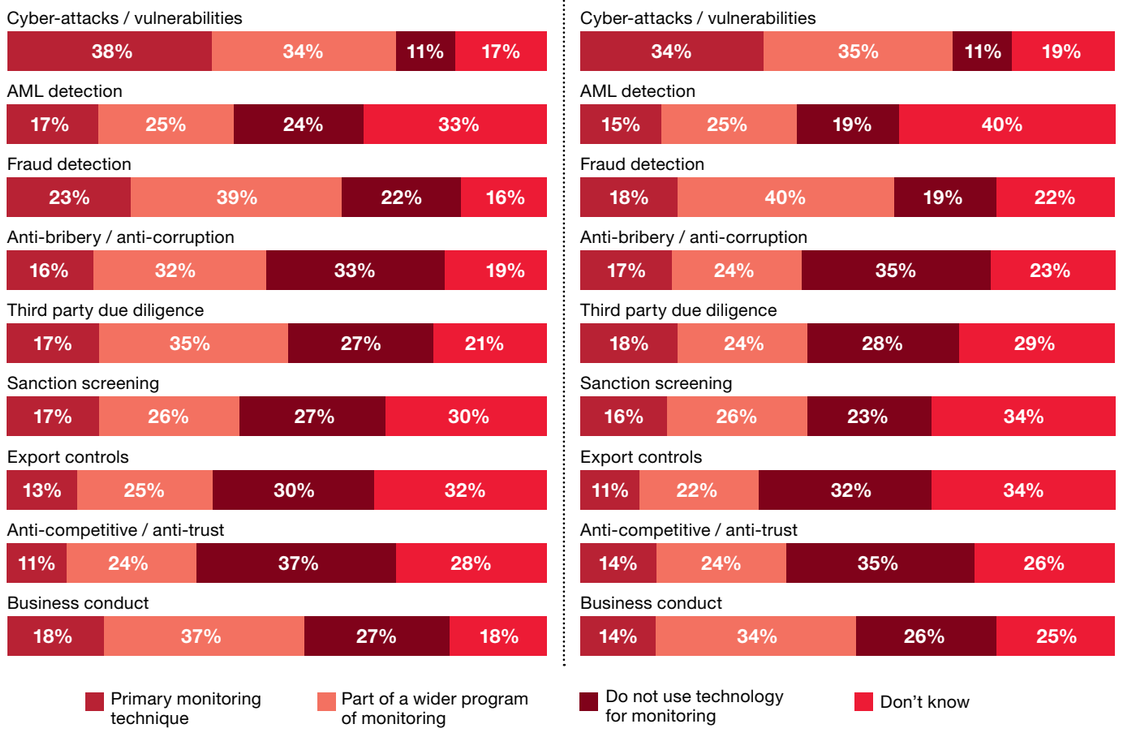
[5] Non-listed Swiss public limited corporations ("AG") are obligated to keep records of their shareholders and substantial beneficial owners. Members of Swiss limited liability companies ("GmbH") are listed in the Register of Commerce.

The leading role of digital technology in fraud prevention and detection

Digital technology is key to combatting fraud. 69% of the Swiss respondents indicated that technology was either the primary tool to monitor potential cyber-attacks and vulnerabilities or it was part of a wider monitoring program, compared to 72% globally. More than half of the Swiss respondents (58%) leveraged technology for fraud detection, compared to 62% globally.

Digital technology is underutilised within the mitigation of several fraud and economic crime risks: Less than half of the Swiss respondents reported having used technology for business conduct monitoring (48%), third party due diligence (42%), sanction screening (42%), anti-bribery and anti-corruption (41%), AML detection (40%), anti-competition and anti-trust (38%) or export controls (33%).

To what extent do you use technology as an instrument to monitor fraud and/or economic crime in each of the following areas?



Contacts

Gianfranco Mautone
Partner
Forensic Services and Financial Crime Leader, Switzerland
+41 58 792 17 60
gianfranco.mautone@ch.pwc.com

Ralf Baumberger
Partner
Forensic Services
+41 58 792 17 63
ralf.baumberger@ch.pwc.com

Selma Della Santina
Senior Manager
Forensic Services
+41 58 792 20 86
selma.della.santina@ch.pwc.com

Silvia Svihrova
Senior Manager
Forensic Services
+41 58 792 46 82
silvia.svihrova@ch.pwc.com

Alister Smith
Senior Manager
Forensic Services
+41 58 792 47 96
alister.smith@ch.pwc.com