Deloitte.

Third-party cyber security in Swiss public administration

Contents

About the study

This study is based on interviews with experts from public authorities and administrations, industry and academia on third-party cyber security in Swiss public administration. Responses from experts who wish to remain anonymous have been included in the study on an unattributed basis.

A representative survey on cyber security more broadly was also conducted between 12 April and 13 May 2024. 394 public service employees and 934 Swiss citizens took part.

Cyber security now a major focus for public authorities and administrations

Cyber security is a crucial issue for Swiss public authorities and administrations for two reasons.

First, these bodies hold large volumes of sensitive information and confidential data to which access must be protected and remain secure. This data includes, for example, social security and tax information, medical records and other sensitive data relating to individual citizens. Clear measures on data security and resilient IT services are required to protecting this data against unauthorised access and cyber attack. Second, public authorities and administrations also maintain critical infrastructure and IT services and need to ensure these are operationally resilient. Examples include infrastructure critical to the health service, security and IT, Switzerland's public transport network, and energy and water supply. Public authorities and administrations are also required to ensure public trust and confidence, minimise their financial risk (such as investigation and recovery costs), and comply with legislation, including the Federal Act on Data Protection and the Information Security Act.

"Digital threats are increasing, so cyber security is absolutely crucial to public authorities and administrations in Switzerland. Tight cyber security not only protects sensitive data but also ensures the resilience of critical infrastructure. As digitalisation advances, its success will rely crucially on Swiss citizens having a high level of trust and confidence in the ability of public administrations to keep their personal data secure and keep their IT infrastructure robust."

Christian Dähler, Director, Cyber Risk Services, Deloitte

"Many authorities and administrations using cloud technologies focus strongly on data protection and privacy because their focus is on data back-up. However, they would be well advised to shift their focus to resilience and redundancy: the value that cloud technologies add is actually in ensuring functionality."

Daniel Caduff, CISSP – Principal Security Assurance DACH, Amazon Web Services (AWS)

Over recent years, the advance of digitalisation has heightened the risk of cyber attack, and the incidence of targeted attacks such as ransomware attacks and data theft has grown steadily. Statistics from the Swiss National Cyber Security Centre show that more than 30,000 cyber-related incidents were recorded in the second half of 2023, more than twice as many as in H2 2022.[1] Public authorities and administrations are as vulnerable to the rise in such incidents as the private sector and society generally. The number of phishing incidents in particular has doubled, and there has also been a rise in the number of scam attempts using artificial intelligence (AI). The group of hacktivists involved in distributed denial of service (DDoS) attacks in June 2023 that paralysed the websites of government agencies, the Swiss Parliament, cantons, towns and cities across the country, and the Swiss rail network, continues to be active, meanwhile.[2]

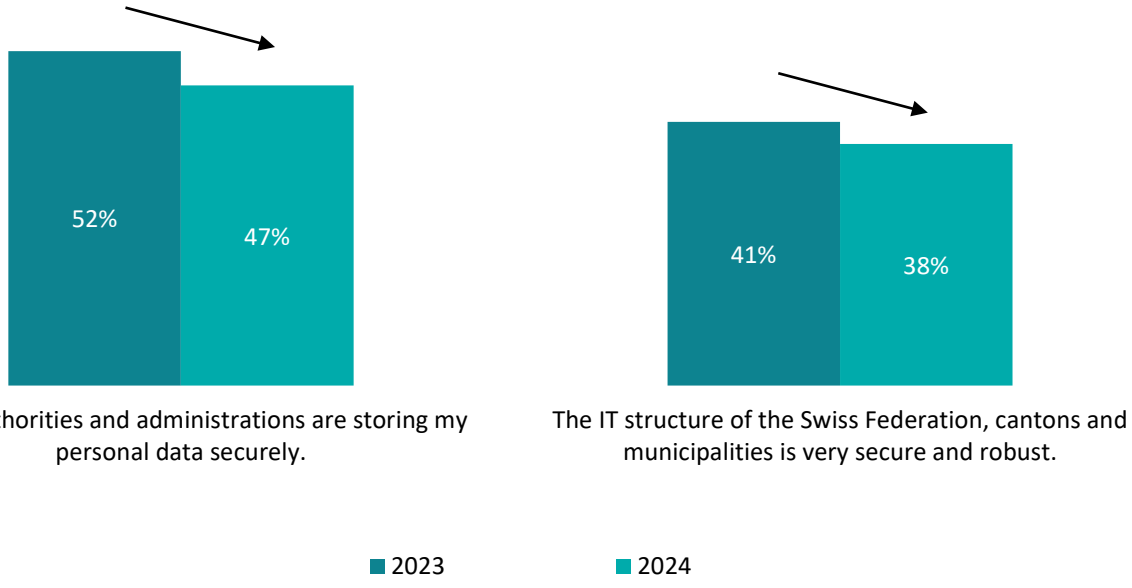
Public authorities and administration are under increasing pressure from the Swiss population to protect sensitive information and confidential data (especially that relating to individual citizens) and to ensure critical infrastructure and services are robust. Deloitte's most recent survey into e-government services finds that fewer than half of citizens surveyed (47%) trust public authorities and administrations to store their personal data securely (see Chart 1). Just 38% also believe that the IT infrastructure of the Swiss Federation, cantons and municipalities is secure and robust. Public trust and the population's rating of government cyber security have therefore declined since Deloitte's 2023 survey: citizens perceive a clear need for action by government.

The problem has become more acute given the accelerating pace of technological change requiring these authorities and administrations to outsource more and more services to third parties; these include AI solutions that rely on massive computing capacity and have to be carried out in the cloud.

This involvement of third parties has massively increased the scope for cyber attacks. One in five public service employees surveyed (21%) believe that there are problems with their organisation's cyber security, and more than a quarter (29%) think that the Swiss government could do more to enhance cyber security.

This study therefore focuses on data security and the resilience of IT services against the backdrop of growing collaboration with third parties. We set out how public authorities and administrations can protect sensitive information and confidential data and the steps they can take to ensure that critical infrastructure and IT services remain robust.

Chart 1. Please rate your agreement with the following statements on how secure and robust the digital services provided by public authorities and administrations are.



Source: 2023 and 2024 Deloitte surveys of Swiss citizens

Third-party cyber-related issues of increasing concern

The May 2023 ransomware attack on Xplain, a Swiss company providing IT services to public security agencies, laid bare the vulnerability of public authorities and administrations and the extent of their reliance on third parties. Among its major clients, Xplain includes the Swiss Federation and individual cantons, and some of the sensitive data published on the dark web by the hackers following the ransomware attack was stolen from Switzerland's Federal Office of Police (fedpol) and the country's Federal Office for Customs and Border Security.[3] The Canton of Aargau and Swiss railways were also affected.[4] The long-term impact of the incident meant, for example, that the app and software operated by Bern's Department of Residential Services, Migration and the Federal Police for Foreigners failed to work properly for months.[5]

It is therefore unsurprising that a significant majority (66%) of Swiss citizens questioned about recent cyber security incidents involving public authorities and administrations express concerns about cyber attacks. This general concern is more marked in French-speaking cantons than in German-speaking ones (76% and 64% of respondents respectively).

Public authorities and administrations increasingly collaborate with third parties and use their services, so third-party risk management is becoming more and more important. Many organisations already have experience of integrating third-party risks into procurement contracts and of due diligence in contract negotiation. However, consistent third-party risk management is not simply about contractual provisions but also requires ongoing monitoring and supervision.

"From a technological perspective, cloud security is high and actually increases when an organisation starts using the cloud. However, users can face problems when they develop their own systems in the cloud rather than using the services provided, which reduces security. By contrast, organisations that adapt their operating model correctly to the cloud find that in most cases, security increases."

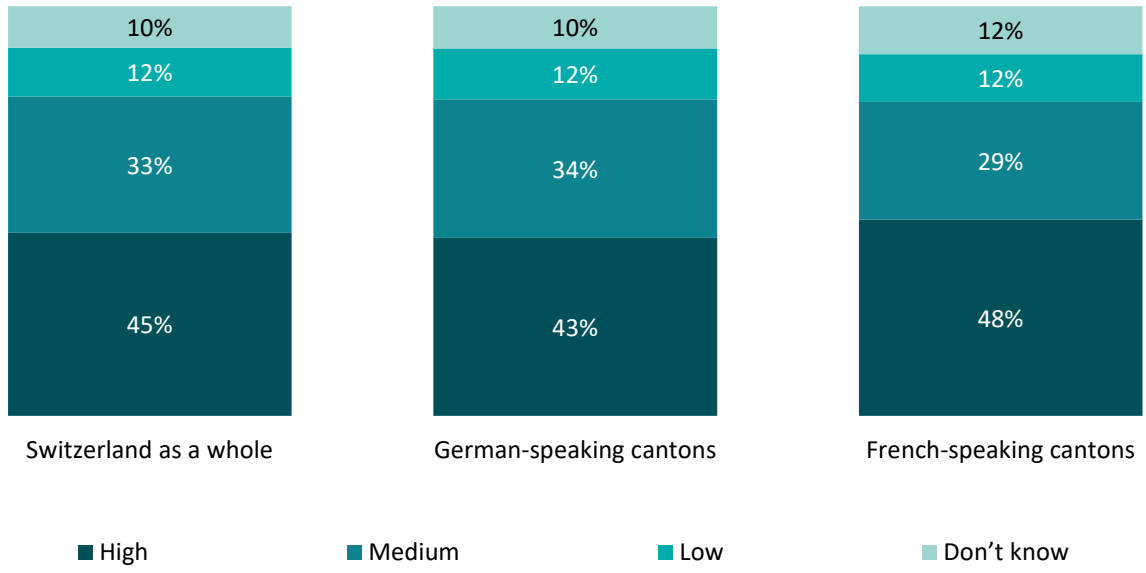
Florian Badertscher, CTO & Co-Founder, Bug Bounty Switzerland

Comprehensive third-party risk management (TPRM)

This study focuses primarily on risks to the cyber security and operational resilience of IT services. However, a comprehensive third-party risk management system should also include other areas of risk:

- **Geography:** risks arising, for example, from the physical location of a third party's headquarters or computing centreGesundheit und Sicherheit: Lieferung von Produkten oder Dienstleistungen von Drittparteien, die zu einem Todesfall beitragen und/oder einen Schaden verursachen.
- **Concentration:** risks posed by excessive and concentrated reliance on a small number of third parties
- **Health and safety:** risks posed by provision of third-party goods or services that contribute to death and/or cause harm
- **Anti-corruption:** risks arising from involvement with third parties whose business practices are unlawful or who engage in criminal activity
- **Environmental, social and governance (ESG):** risks posed by activities with a harmful and unmitigated impact on the environment (e.g. carbon emissions) or individuals (e.g. modern slavery)
- **Compliance:** the risks posed by non-compliance with legislation, regulations or ethical standards
- **Fourth and fifth parties:** risks arising outside the direct relationship with direct third parties where external providers are hidden or unknown
- **Reputation:** risks to an organisation's brand and reputation arising from third parties' actions, statements or business transactions
- **Financial sustainability:** risks in relation to third parties that are financially unprofitable

Chart 2. How do you rate the cyber security risk to Swiss public authorities and administrations of collaborating with third parties (e.g. cloud providers)?



Source: 2024 Deloitte survey of public service employees

45% of public service employees surveyed rate the cyber security risk to public authorities and administrations of collaborating with third parties as high; 33% rate it as medium (see Chart 2). Survey respondents rating the cyber risk of collaborating with third parties as high are substantially more likely to work in French-speaking cantons than in German-speaking ones.

Differences between groups of respondents are also evident in responses to the question concerning where responsibility lies for managing the risks of third-party collaboration (see Chart 3). Although almost half of public service employees surveyed (44%) think that responsibility lies with the administrative body itself, the same proportion think that risk management is the responsibility of the third party. This split in opinion reflects two things. First, collaboration with third parties always means shared responsibility since the public authority or administration remains the data owner and retains responsibility for that data even where, for example, it outsources the data to third parties. Second, responsibility for and collaboration with third parties is clearly laid down in the Swiss Information Security Act, so government and other agencies always take responsibility.

This finding – and the broader views of the cyber-related risks posed by third-party collaboration – points to the need for Swiss public authorities and administrations to take substantial action. It also indicates an urgent need for public service employees to be given better information and training.

"Achieving good security in the software as a service (SaaS) sector is a major problem. Many organisations do not have an active third-party risk management system in place and rely instead on certification and trust in their providers. Regular audits are an effective way of maintaining better oversight."

Prof. Dr. Sebastian Höhn, Institute for Public Sector Transformation, Bern University of Applied Sciences

Chart 3. Please rate your agreement with the following statements on the risks of collaboration between Swiss public authorities and administrations and third parties.

Source: 2024 Deloitte survey of public service employees in Switzerland

Key questions, challenges and good practice in third-party cyber security

The cyber security of public authorities and administrations is a fundamental concern for Swiss citizens. Their trust in the cyber security of government bodies at all levels has declined, and these bodies need to take rapid action to restore trust, protect data and ensure robust and resilient services. Third-party cyber security requires these bodies to begin by asking and answering the following four fundamental questions:

1. How can I as a data owner ensure data security?
2. How can I ensure secure collaboration with and outsourcing to third parties?
3. How can I ensure third-party data remains accessible and is resilient?
4. How can I ensure the appropriate skills and resources to collaborate with third parties?

1. How can I as a data owner ensure data security?

Public authorities and administrations face an ongoing challenge to create and maintain a secure IT environment, make timely decisions on enhancing their IT security, and ensure that confidential data is protected. These organisations are data owners and must therefore guarantee the confidentiality, integrity and accessibility of that data at all times. They also need to take regular stock of who has access to data, whether data is correct, complete and authentic, and whether it remains accessible at all times, particularly in the case of system failures.

Given the growing use of third parties, the question also arises of how data flows to these third parties and external access to this data (for example, by external staff) are monitored. Many public service employees are often ignorant of who – or what – a third party is and of the risks posed by collaboration with a third party or use of third-party services.

"The data security of an organization is significantly influenced by the complex networks of partnerships with third parties. As a data owner, I am responsible for ensuring that the third parties with which I collaborate help to keep my data secure. This requires me to understand data flows and to build appropriate supervision and monitoring into the entire data lifecycle."

Florian Widmer, Partner, Cyber Risk Services, Deloitte

Interviews with experts identify the following examples of good practice for Swiss public authorities and administrations wishing to ensure the security of their data:

- **Control data classification:** Clear data classification is crucial to data security and underpins decision-making relating, for example, to what data can be stored locally or in the cloud or what can be outsourced to third parties.
- **Ensure data is catalogued:** Understanding what data is stored and processed where is essential to both data security and data quality. This understanding requires tighter data management throughout the data lifecycle, including data erasure.
- **Instigate secure archiving and back-ups of data:** Data that needs to remain accessible in the long term (e.g. for compliance purposes) must be securely archived. Monitoring mechanisms can help with decision-making on whether data can be amended, manipulated or erased. Back-ups of critical operational data that underpins the company's ability to function in an emergency must also be stored particularly securely.
- **Define responsibility:** Most organisations have dedicated experts to plan and implement the strategy governing the security of their infrastructure, processes, systems and data. The importance of data security right across the organisation must also be prioritised, including training for employees on their responsibilities.
- **Increase third-party risk awareness:** Public service employees must be made more aware of the importance of cyber security, data protection and reliability when collaborating with third parties and using their IT services. This can be achieved, for example, by means of training and awareness-raising campaigns. It is essential that the entire organisation understands third-party cyber risk management not just as a compliance exercise but as part and parcel of organisation's broader approach to risk management (including cyber risk).

2. How can I ensure secure collaboration with and outsourcing to third parties?

Public authorities and administrations remain data owners and retain responsibility for their data even when third parties are involved with managing that data. This is often forgotten, with outsourcing subject to an 'out of sight, out of mind' mindset. Many employees of such organisations also believe that the third party bears the primary responsibility for manages outsourced risk (see again Chart 3), but this is a dangerous approach: risk remains the responsibility of the public authority or administration, not of third-party providers.

For many public authorities and administrations, increasing trust in third parties is a challenge. Third-party risk management is important both to understanding how secure these third parties are and to understanding their own responsibility as a data owner. Third-party risk management appears to be more effective at federal level than at canton or municipality level, but the situation becomes more complex still when fourth and fifth parties are involved. Typically, the process of assessing cyber security and identifying, evaluating and reducing risks to cyber security arising from third-party providers has been patchy. Many organisations are now starting to include provisions in their contracts to protect themselves against the risks arising from third parties. In other cases, however, day to day business continues largely unchanged.

Interviews with experts identify the following examples of good practice for Swiss public authorities and administrations wishing to ensure safe and secure collaboration with and outsourcing to third parties:

- **Obtain management's agreement/buy-in:** This is the central pillar of a consistent organisation-wide approach. Effective management of the cyber risks posed by third parties requires the whole organisation to manage risks consistently and systematically.
- **Define clear competences and responsibilities:** Many organisations lack a mandate for tackling third party risks as a whole. One of the greatest challenges of third-party risk management is that nobody feels they have overall responsibility, with many decisions and actions taken in silos (finance, IT, legal affairs, etc.). This requires over-arching competences to be defined and consistent responsibilities to be specified.
- **Ensure ongoing discipline and diligence:** Introducing the security measures required is not intrinsically complex: organisations just need to do the hard work. However, few actually do that work. The challenge is to regain control of all elements, including those already in the cloud.
- **Ensure ongoing third-party risk management and make improvements:** The public sector is highly regulated when it comes to procurement, but there are shortcomings in risk management in the post-procurement lifecycle. Ongoing third-party risk management (TPRM) requires a clear framework that encompasses screening, onboarding, risk assessment, risk reduction, monitoring and offboarding of third parties. And this framework needs to form an integral part of the vendor lifecycle management system.
- **Make use of supporting technologies:** Early use of appropriate technologies enables automation of many work processes, boosting acceptance within the organisation and ensuring long-term success.
- **Introduce multi-factor authentication (MFA):** MFA is not just 'nice to have' but an absolute must when it comes to collaboration with external parties. Organisations not insisting on MFA for access to the cloud bear the risk here, not the provider.
- **Centralise for economies of scale:** Individual organisations manage their third parties themselves, missing out on economies of scale . Greater centralisation could see organisations tapping into these economies of scale as part of their third-party risk management and enhancing their maturity.

"Administrative bodies often take an isolated view of cyber security. They need instead to take a holistic view and consider the entire ecosystem of providers and third parties when considering security. Ongoing testing and reviewing of their vulnerability to cyber attack can increase the pressure on third parties to address their own security vulnerabilities."

Sandro Nafzger, CEO & Co-Founder, Bug Bounty Switzerland

3. How can I ensure third-party data remains accessible and is resilient?

It is also important that when organisations collaborate with or make use of third parties, they consider the accessibility of critical data and critical infrastructure and IT services in case of cyber attacks.

The many decentralised structures that impede development of centralised responsibility for third-party risk management may also be a headache for public authorities and administrations. A further challenge may be posed by statutory provisions, for example in relation to procurement.

Interviews with experts identify the following examples of good practice for Swiss public authorities and administrations wishing to ensure the accessibility and resilience of data when using third parties:

- **Focus on the right issues:** Organisations need to ensure that they are focusing on the right issues. This requires the capacity to act and governance that specifically identifies and addresses risks as well as ensuring that responsibility is consistent.
- **Find a balance between diversification and the risks posed by concentration:** Organisations that diversify make their IT landscape more complex and more vulnerable. However, from the perspective of the risks posed by concentration, diversification is an advantage. Finding the right balance between diversification and concentration needs a clear risk analysis and ongoing third-party risk management.

"Improving cyber security and resilience in an organisation requires redundancy – that is, offline storage of data alongside storage by additional cloud providers. It also requires zone concepts. 'Zero trust networks', which require authentication and authorisation for data access, are as important in a cloud environment as ongoing log-in management and encryption."

Daniel Caduff, CISSP – Principal Security Assurance DACH, Amazon Web Services (AWS)

4. How can I ensure the appropriate skills and resources to collaborate with third parties?

Public authorities and administrations

are good at governance and documentation but perform less well outside these areas. They often lack expertise, resources and technical skills – such as the skills to use technology to monitor what data is being used and where – and this is a particular challenge for cantons and municipalities. It is generally true that the smaller the organisation, the greater the problem it has with these skills and resources.

Interviews with experts identify the following examples of good practice for Swiss public authorities and administrations wishing to ensure that they have the right skills and resources to tackle the use of third parties:

- **Build expertise and talent within the organisation:** Organisations need to invest more and build their own expertise. Strong performance in relation to cyber activities must be underpinned by recruiting employees with skills, experience and a cyber orientation. It is now crucial to look beyond traditional professional profiles when recruiting the right staff. Public authorities and administrations must also take steps to retain experienced staff.
- **Create strategic partnerships in procurement:** Organisations cannot achieve maturity solely through their own efforts; building the necessary skills in the long term and implementing a consistent and comprehensive third-party risk management system (e.g. identifying the risks of excessive concentration, third-party risks, etc.) also means adapting elements such as procurement practices. This requires strategic partners who not only provide skills and resources but can also assume and cover risks.
- **Collaborate with other administrations on third-party risk management:** Municipalities lacking appropriate resources could consider delegating third-party risk management to cantons as a centralised function.

"It is inefficient for small organisations to act independently in tackling cyber security and their shortcomings in this area. It makes more sense to pool resources: that way, all stakeholders can derive mutual benefit. Cantons are already regularly sharing their experience in the area of cyber security, but multi-party collaboration is a challenge for smaller administrations, such as municipalities."

Florian Badertscher, CTO & Co-Founder, Bug Bounty Switzerland

Four recommendations for action by public authorities and administrations

Our discussion of key issues and good practice gives rise to four overarching recommendations for action that public authorities and administrations can take to ensure third-party cyber security.

1. **Improve proactivity in the area of cyber security**

   Public authorities and administrations are often reactive when it comes to cyber security, taking action only once a security issue actually arises. Greater proactivity is needed. In particular, a much more proactive culture will ensure appropriate responses to cyber security risks. Cyber security is an ongoing process rather than a one-off achievement. Day to day improvement and ongoing adaptation form the basis of maturity in this area, and organisations need to be constantly asking themselves the crucial questions about their own vulnerability – how resilient are we, and how can we tackle shortcomings in our cyber security?

2. **Increase general awareness of the cyber risks of using third parties**

   Better awareness of the cyber risks involved in using third parties needs to be underpinned by a comprehensive third-party risk management system that consciously takes calculated risks, creates added value for the organisation, and is not merely compliance-oriented. Ongoing third-party risk management needs to be an integral part of vendor lifecycle management systems and offer a comprehensive risk profile that also includes the effectiveness of the organisation's internal monitoring mechanisms (e.g. recertification of access rights, data protection measures, patch management systems, etc.). And because the root cause of many cyber security issues is inappropriate use of systems, organisations need to use targeted staff development and systematic training to raise their employees' awareness of how important cyber security is across the board.

3. **Cooperate across authority and beyond administration boundaries**

   Most large organisations have better awareness of their cyber security risks and better access to the necessary resources to analyse and address them than smaller organisations, which often rely on external support and expertise. Greater cooperation between differing levels of government (such as cantons and municipalities) helps to strengthen third-party risk management for smaller organisations, but this external collaboration is important for large organisations too, as it is often the only way problems are identified and improvements implemented. Modern organisations are already benefiting from crowdsourcing and collective intelligence to tackle cyber security issues, including the use of 'ethical hackers'.

4. **Be aware of unresolved risk management in relation to fourth and fifth parties**

   Ensuring good third-party risk management also means improving recognition of the potential risks represented by third-party providers. Moreover, third parties frequently sub-contract to further providers, giving rise to what are sometimes known as 'fourth parties' and even, when yet another level is involved, 'fifth parties'. Each additional level of dependency multiplies the number of organisations involved, leading in some cases to extensive networks within an ecosystem. Not all risks posed by fourth and fifth parties will impact on an organisation – but some will, and while it is very difficult to retain complete control of the risks arising from this extended ecosystem, using risk assessment tools and expert providers can help organisations better to assess the risks they face. Nonetheless, where organisations rely on a variety of data sources without appropriate correlation and analysis, they risk overlooking risks and threats.

Endnotes

1. National Cyber Security Centre, Twice as many cyber incidents reported and rise in AI scam attempts, press release, 6 May 2024. https://www.ncsc.admin.ch/ncsc/en/home/dokumentation/medienmitteilungen/newslist.msg-id-100926.html.
2. Inside IT, Bundesanwaltschaft untersucht DDoS-Angriff auf Parlamentsdienste [Federal Prosecutor investigates DdoS attack on Swiss Parliament services], 12 June 2023. https://www.inside-it.ch/bundesanwaltschaft-untersucht-ddos-angriff-auf-parlamentsdienste-20230612 (in German only). Watson, Prorussische Hacktivisten greifen weiter websites des Bundes an [Pro-Russian hacktivists continue to attack Swiss government websites], 14 June 2024. https://www.watson.ch/digital/schweiz/322045086-prorussische-gruppe-noname057-16-greift-weiter-websites-des-bundes-an (in German and French only).
3. Federal Office of Police (fedpol) website, Hacker attack on Xplain: Impact on fedpol and measures taken, 11 September 2023. https://www.fedpol.admin.ch/fedpol/en/home/aktuell/informationen/2023-09-11.html. Federal Office for Customs and Border Security website, Hacker attack on Xplain: Impact on the Federal Office for Customs and Border Security and measures taken. https://www.bazg.admin.ch/bazg/en/home/teaser-homepage/focus-teaser/hacker-attack-on-xplain.html.
4. Inside IT, Auch SBB und Kanton Aargau vom Xplain-Hack betroffen [Swiss railways and Canton of Aargau also hit by Xplain hacking attack], 12 June 2023. https://www.inside-it.ch/auch-sbb-und-kanton-aargau-vom-xplain-hack-betroffen-20230612 (in German only).
5. Schweizer Radio und Fernsehen (SRF), Folgen grösser als bekannt - wegen Hackerangriff auf Xplain Polizeisoftware teils offline [Impact greater than realised: hacking on Xplain takes Swiss police software partially offline], 4 October 2023. https://www.srf.ch/news/schweiz/folgen-groesser-als-bekannt-wegen-hackerangriff-auf-xplain-polizeisoftware-teils-offline (in German only).

Authors and contacts

Rolf Brügger
Partner
Government & Public Services Industry Leader
Tel: +41 58 279 77 14
rbruegger@deloitte.ch

Florian Widmer
Partner
Cyber Risk Services

Tel: +41 58 279 69 10
fwwidmer@deloitte.ch

Steffen Pietz
Partner
Third Party and Supply Chain Risk

Tel: +41 58 279 64 94
spietz@deloitte.ch

Christian Dähler
Director
Cyber Risk Services

Tel: +41 58 279 5274
cdaehler@deloitte.ch

Deloitte.