Deloitte.

Cyber Flash

A spotlight on cyber and privacy trends

Edition 2, March 2017

Editorial

Edition 2, March 2017

Dear Cyber and Privacy Community

Welcome to the second edition of our **Cyber Flash.**

The New Year came with a plethora of developments on the global political stage as well as on the regulatory and technological front that all have the potential to impact businesses in Switzerland. Whether it is changes in US policies and directives when it comes to privacy and data protection, or new technologies that may change the way we work – interesting times are coming our way.

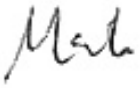
With these developments in mind, we have set the focus of this edition on various cyber risk management topics:

- **Blockchain security** – protecting the distributed ledger.
- **Red Teaming operations** – a holistic approach to information security assessments.
- **Cyber risk reporting** – what to report in the annual report.
- **De-mystifying cyber insurance coverage** – clearing obstacles in a problematic but promising growth market.

As we approach the 'one-year-to-go' milestone of the GDPR effective date, privacy and data protection activities are picking up across Europe. This news flash provides a brief summary of all major updates you need to be aware of this spring.

The **Cyber Risk Services team** and I wish you an interesting read.

Yours sincerely,



Highlights, issue 2

Cyber risk management

- Blockchain security
- Red Teaming operations
- Cyber risk reporting
- De-mystifying cyber insurance coverage

Privacy and data protection

- Privacy and data protection updates
- Events, conferences and contacts

Mark Carter
Managing Partner
Risk Advisory

Cyber risk management

Blockchain security
Protecting the distributed ledger

A Blockchain, or distributed ledger, is a technological protocol that enables data to be exchanged directly between different contracting parties within a network without the need for intermediaries. Each transaction is communicated to all network nodes, and once verified and confirmed, is added to an immutable transaction chain.

Numerous industries are currently researching and piloting Blockchain applications, see our recent white paper **"The Blockchain (R)evolution – The Swiss Perspective"**[1] for a general overview of Blockchain applications in the Swiss market. What most of these new applications have in common is that they need to process and store sensitive data. In the healthcare industry, for instance, these are patient medical records, medical metadata, clinical trial information and PII (Personally Identifiable Information). As a consequence, there is a rising number of inquiries and concerns from our clients about the security aspects of Blockchain and its ability and limitations in protecting such critical data. Based on our experience, three aspects contribute to making Blockchain security difficult to manage:

1. Immaturity and complexity of the technology
Due to the different consensus algorithms available (e.g. proof of work or proof of stake), the Blockchain types (e.g. permissioned or permissionless), and the complex underlying cryptographic protocols, it is difficult for security practitioners to fully understand data flows and potential security weaknesses. In addition, multiple Blockchain platforms and implementations exist and applications must be evaluated for their suitability for integration with a specific Blockchain system.

2. Lack of standards and regulations around Blockchain technology
As of today, Blockchain technology is unregulated, resulting in legal uncertainties and grey areas. An interesting example of the lack of controls and laws regulating Blockchain networks is the DAO hack[2] where a smart contract[3] vulnerability led to the network losing 60 million US dollars[4].

3. Widespread belief that a Blockchain is secure by design
Blockchain technology is built upon public-key cryptography and primitives such as digital signatures and hash functions, which may give a false impression of security. The fact that all cryptographic protocols have their limits and that holistic security includes not only technology, but also people and processes, is often overlooked in a Blockchain security analysis.

To overcome these difficulties, we advise clients to take a risk-based approach to Blockchain security, which ensures that security controls are selected in line with business needs and business use cases. This approach can be summarised as follows:

Understand criticality of data and processes
The first step is to understand the sensitivity of the data that is being stored and processed in a Blockchain. By understanding regulatory implications and performing a business impact analysis, the importance of confidentiality, integrity and availability of data can be determined.

Create a threat model
Secondly, traditional threats related to public key infrastructure and application development, such as key compromise and code bugs, must be factored into the analysis. On top of these, Blockchain-specific attack vectors relevant to the given application need to be identified. These include consensus hijack, Distributed Denial of Service (DDoS), permissioned Blockchain exploitation, smart contract exploitation and wallet hacking[5].

Based on these, risk scenarios can be listed and evaluated for likelihood and impact.

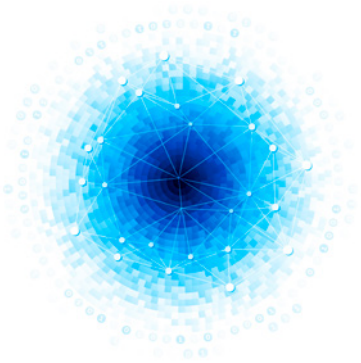
Select security controls
The final step is the selection of security controls that address the identified risks. A number of traditional good security practices can be deployed. These include robust key management, code review, data encryption, access control, and security monitoring. In addition, there are techniques specific to Blockchain technology that can be set up, such as secure wallet management, permissioned chain management, and secure smart contract development. Finally, it is important to keep in mind that people, processes and technology are equally important to ensure that Blockchain applications are properly protected. For instance, the impact of the aforementioned DAO hack could have been contained if proper governance structure and incident response process had been put in place.

If you would like to have an initial conversation about Blockchain security and Deloitte's approach, please get in contact with our team.

Dr. Dusko Karaklajic
Manager
Cyber Risk Services
+41 58 279 7386
dkarakaljic@deloitte.ch

Patricia Egger
Consultant
Cyber Risk Services
+41 58 279 7641
paegger@deloitte.ch

1. Deloitte AG, The Blockchain (R)evolution- The Swiss Perspective, February 2017
2. P. Vessenes, http://vessenes.com/more-ethereum-attacks-race-to-empty-is-the-real-deal/
3. IBM Research, https://developer.ibm.com/clouddataservices/2016/05/19/block-chain-technology-smart-contracts-and-ethereum/
4. Etherscan, https://etherscan.io/address/0x304a554a310C7e546dfe434669C62820b7D83490
5. ENSIA, Distributed Ledger Technology & Cybersecurity – Improving information security in the financial sector, December 2016



Red Teaming operations
A holistic approach to information security assessments

Organisations frequently operate under the assumption that as long as their computer systems are secure, information is secure. In an effort to strengthen the security of their computer systems, they often perform penetration tests – simulated attacks on computer systems aimed at identifying vulnerabilities that could materialize into real risks. However, in reality attackers do not limit themselves to abusing the systems singled out for penetration tests or even any IT system in general. Rather, attackers today are much more sophisticated. They combine different elements that go beyond computer systems, with the objective of finding the path of least resistance. As a consequence, due to their limited and fixed scope, penetration tests alone do not adequately address the risk posed by attackers, and leave organisations vulnerable to realistic attacks.

A realistic attack generally addresses three elements of information security that are linked together. These are:

- **Physical:** Buildings, desks, safes and the physical IT infrastructure.
- **Cyber:** The online world, the Internet as well as corporate Intranets and their interconnectivity with other supplier and business partner networks.
- **Human:** This denotes the employees, customers, clients and third parties that are handling information within an organisation.

Figure 1: Three elements of a realistic attack

Finding the weakest link

The vast majority of cyber breaches in the recent years were caused by human behavioural issues – one of the weakest links that cannot be identified by penetration testing. Red teaming not only tests technical preventative controls, but also the human defence capabilities, which are not tested by traditional penetration tests.

An important aspect of a real attack is the reconnaissance. During this phase an attacker uses various tools and techniques to gather as much information as possible about a victim, in order to make an attack more successful. For example an attacker could use open source intelligence, whereby the web and dark web are being searched for relevant information on an organisation (e.g. user names, passwords, business rules, etc.). Frequently traditional penetration tests do no take this into account, due to their limited and pre-defined scope, and hence could leave an organisation vulnerable.

Red Teaming Operations enable organisations to assess the readiness and awareness against realistic attacks through scenario based controlled incidents that take all elements (human, physical & cyber) within an organisation into account.

Success factors and our recommendation

Successful Red Teaming Operations require thorough planning to create realistic adversarial simulations for an organisation. Random attacks with random objectives will not deliver adequate benefits.
The best planning comes from an in-depth understanding of the business and the organisation, which then translates into realistic scenarios, combining risk and threat management approaches. As part of the planning phase it is important to identify the key risks of an organisation. These are unique to each organisation and serve as a basis to create realistic scenario-based controlled incidents.

Our experience shows that successful Red Teaming Operations are built upon three principles.

1. Knowledge Mix
Red teaming exercises need to combine the right amount of technical and business understanding to become useful and representative.

2. Understanding of Adversary
A successful red teaming exercise requires a thorough understanding of a potential attacker. Meaning, that aside from possessing the skills and knowledge of a potential attacker, the team needs to have the ability to think like one as well. In short, the attacker's objectives need to match the risks to the organisation and have to be incorporated into the defined scenarios driving the red teaming exercise.

3. Joint teams
Teaming is key – a successful exercise outcome comes from working together and combining efforts and expertise of both, the red and the defending team. Working in such a collaborative setup enables outstanding red teaming exercises that matter, are focused, agile, cost-effective and as a result enhance defensive capabilities.

And here is how a cyber-attack happens

How often do we get to watch how an actual cyber-attack happens, and see the consequences unfold before our eyes in real-time? Hopefully never. We developed two videos to provide a sneak-peak of what you could face. Experience the speed and intensity of a cyber-attack; as the plot unfolds, learn how companies can defend themselves, take control of the situation, and effectively fight back.

Watch:

- Companies like yours
- Cyber security evolved

If you would like to have an initial conversation about Red Teaming Operations and Deloitte's approach to making it a success, please get in contact with our team.

Gianni Crameri
Senior Consultant
Risk Advisory
+41 58 279 6413
gcrameri@deloitte.ch

Cyber risk reporting

What to report in the annual report

On the back of growing cyber regulation globally, Deloitte has surveyed the full FTSE 100 in the UK to better understand how these companies disclose cyber risks in their annual filings.

The results show a varied picture and should serve Swiss companies as a benchmark and impetus to reassess their approach to cyber reporting.

The survey examined whether the FTSE 100 are identifying cyber as a principal risk, and how they are categorising and describing this risk and its impact. It further considered how clearly companies are describing the ownership of cyber risk and whether the board is leading the way and demonstrating that they provide appropriate challenge to management. Some interesting conclusions emerge regarding today's common practice in cyber reporting:

- Every sector, although not every company, identifies cyber as a principal risk – think carefully if you have not done so.
- The value destruction capability of cyber risk is very high, ranging from remediation demands to huge reputational damage. Detailed disclosure is therefore worthwhile to highlight the risks to shareholders and let them know you are taking it seriously.
- Boards and board committees are increasingly educating themselves about the cyber threat and challenging management on how they are dealing with the risk.
- While many organisations have a CISO, CTO or CIO there often seems to be a lack of Board leadership, with only 5% of FTSE 100 boards having a director with direct specialist expertise.
- Companies should take credit for their cyber security activities, including describing who has executive responsibility, board level responsibilities, the policy framework, internal controls, and disaster recovery plans.
- Finally, if your disclosure does not look strong enough after taking credit for what the company is doing already, it is time to ask whether you are actually doing enough to manage cyber risk.

The full report is available **online** and its Appendix also contains a helpful summary of "good practice" cyber reporting topics that will enable you to identify potentially worthwhile additions for inclusion in your existing annual reporting.

Dr. Klaus Julisch
Director
Cyber Risk Services
+41 58 279 6231
kjulisch@deloitte.ch

De-mystifying cyber insurance coverage

Clearing obstacles in a problematic but promising growth market

Organisations continue to invest heavily in cyber security efforts to safeguard themselves against threats, but far fewer have signed on for cyber insurance to protect their firms after an attack. Why not? What are the roadblocks, and what steps could the industry take to help clear them?

Our recent Deloitte University Press **publication** seeks to answer these critical questions with a thorough analysis of the cyber insurance landscape. By identifying and examining obstacles to the industry's development from both the insurer and buyers' perspectives, and presenting a number of strategies to overcome them, we provide a roadmap for cyber insurers seeking to crack the code of this challenging yet promising emerging market.

The next figure provides an overview of the most significant obstacles we identified that carriers face when contemplating the sale of cyber insurance, as well as issues causing many prospects to hesitate when considering a transfer of at least part of their risk to third parties.

Figure 2: Obstacles to meeting demands for cyber coverage

Insurers will likely need to overcome these obstacles to fully realise the upside potential of this problematic yet promising market.

Existing cyber insurers should consider the following strategies:

- **Data-challenged insurers could buy time** with alternative approaches including leveraging internal cybersecurity expertise and focusing on specific areas of exposure.
- **Insurers could go beyond risk transfer** and offer holistic cyber risk management programmes.
- **Insurers should pave the way for growth** by raising risk awareness and standardising policy language.

With the more frequent global news coverage on cyber-attacks and being in the business of risk, the industry has a prime position to capitalise on what is likely to be increasing interest in the purchase of cyber insurance. That is, if they can crack the code and overcome the roadblocks that are preventing the growth of cyber insurance coverage. Read the full article **here**.

Sam Friedman
Insurance Research Leader
Center for Financial Services
Deloitte Services LP
+1 212 436 5521
samfriedman@deloitte.com

Marco von Arb
Manager
Risk Advisory
+41 58 279 6738
mvonarb@deloitte.ch

Privacy and data protection

The **General Data Protection Regulation (GDPR)** is at the heart of some of this spring's most important developments:

- On December 22, 2016, the **Swiss Federal Department of Justice and Police** published a draft revision of its Data Protection Act. The Act anticipates the application of the GDPR and aims at maintaining Switzerland's status as an adequate country for international data transfers in the GDPR universe. It strengthens the Commissioner's role, with administrative fines reaching up to 500,000 CHF. In related news, the Swiss government has also announced its own Privacy Shield agreement with the US.

- The European Commission published two draft regulations (one for ePrivacy and the second one for the protection of personal data by EU institutions) in order to **align Europe's wider data protection laws with the GDPR**.

- On 13 December 2016, the **Article 29 Working Party published guidance** on three core GDPR requirements: The appointment of the Data Protection Officer (DPO); the right to data portability and how to identify the lead DPA in case of cross-border personal data processing. Additional guidance is expected throughout 2017 to further clarify the requirements of the GDPR.

- In anticipation of the Article 29 WP guidance due to be published in 2017, the Belgian DPA has recently published a **recommendation on Data Protection Impact Assessments**.

With respect to data breaches, the **Dutch DPA released its assessment of one year of data breach notifications**. The Netherlands had introduced a mandatory data breach notification in early 2016. In an evaluation of its statistics, the Dutch DPA notes over 5,500 breaches, 4000 of which were given a closer look.

On this basis, over 100 organisations received a warning. In a few tens of cases, a deeper investigation was started by the DPA. Interestingly, the sectors where most breaches took place were healthcare, financial services and public administration.

In additional to several smaller fines, the following **fines and enforcement actions** made headlines:

- A multinational general insurance company has been fined £150 000 by the ICO for losing personal data belonging to almost 60,000 customers.

- The FTC and dating site AshleyMadison have come to a settlement after the 2015 data breach. The site will implement a data security program, and pay a fine of $1.6 million.

- The US Department of Health and Human Services' Office for Civil Rights settles first HIPAA enforcement action for $475 000 with a large home health company for a breach of unsecured protected health information.

Dr. Klaus Julisch
Director
Cyber Risk Services
+41 58 279 6231
kjulisch@deloitte.ch

Please refer to our latest **Privacy Flash** for additional details on the above and other developments.

Privacy Flash
For a detailed view of the latest privacy and data protection trends across Europe, download the PDF documents below:

- Issue 10, Feb 2017
- Issue 9, Dec 2017

Events, conferences and contacts

European Privacy Academy

Dolce La Hulpe, Belgium
Dates below
europeanprivacyacademy.com

The European Privacy Academy is a unique training, knowledge and networking centre, focused on practical day-to-day management of privacy challenges.

The next sessions of the European Privacy Academy's DPO Course will take place on:

- **8-11 May 2017 & 18 Sept 2017**
- **13-16 Nov 2017 & 5 Feb 2018**
- **7-10 May 2018 & 17 Sept 2018**

IAPP Europe Data Protection Intensive

London, United Kingdom
13-16 March 2017
iapp.org/conference/iapp-europe-data-protection-intensive

The Data Protection Intensive of the International Association of Privacy Professionals (IAPP) returns to London and offers the opportunity to deep dive into today's critical data privacy topics and the coming challenges. The Intensive is divided into a two-day training and workshop, taking place as from 13 to14 March. These practical sessions are followed by the actual conference on 15 and 16 March.

Global Privacy Summit 2017

Washington DC, USA
17-20 April 2017
iapp.org/conference/global-privacy-summit

The Global Privacy Summit in April 2017, offers perspectives from around the globe for in-depth discussion and gold-standard education, big-picture inspiration and valuable connections. The Summit starts with a two-day Training and Active learning on 17 and 18 April, followed by a conference on 19 and 20 April.

Cyber Risk Services contacts

For further information or an individual consultation on how our Cyber Risk experts can help you, please do not hesitate to contact us.

Dr. Klaus Julisch
Director
Cyber Risk Services
+41 58 279 6231
kjulisch@deloitte.ch

Mark Carter
Managing Partner
Risk Advisory
+41 58 279 7380
markjcarter@deloitte.ch

Deloitte.

Designed and produced by The Creative Studio at Deloitte, London. J11527