Deloitte.

Cyber Flash

A spotlight on cyber and privacy trends

Edition 3, June 2017

Editorial

Edition 3, June 2017

Dear Cyber and Privacy Community

Welcome to the summer Cyber Flash edition.

Looking back at the past three months, it is clear that the year has continued just the way it started - turbulent, with many events to keep risk professionals on their toes in the foreseeable future. Whether it is re-examining the cyber risk maturity of your organisation after the recent global cyber threats, or gearing up for the impact of upcoming global regulatory changes, the road to 2018 is paved with complex, gripping challenges.

With this in mind, we have selected the following topics as summer read:

- **Building a strategic security organisation** – a fresh look at managed security services
- **Board matters** - cyber risk reporting in the UK and Switzerland
- **Privacy by Design** - How to achieve it?
- **GDPR -** implications for the Life Sciences industry

On a side note, I am very pleased to see that our commitment to helping organisations become and stay secure, vigilant and resilient in today's global threat landscape has been recognised by Gartner.

On behalf of our Cyber Risk Services team I wish you a good summer and an interesting read.

Yours sincerely,

Highlights

Cyber security

- A fresh look at managed security services
- Board matters – cyber risk reporting revisited

Privacy and data protection

- Privacy by Design – how to achieve it?
- GDPR - implications for the Life Sciences industry
- Events, conferences and contacts

Mark Carter
Managing Partner
Risk Advisory

Cyber security

A fresh look at managed security services

According to feedback from Deloitte's CISO Labs[1], CISOs consider it one of their top priorities to develop cyber security into an integral and strategic part of business. Managed services can play a central role in this effort.

Over 90% of CISOs hope to improve the strategic alignment between cyber security and the business, yet nearly half (46%) are struggling to accomplish this objective. Why is that?

Our conversations with CISOs identified causes related to the business acumen, skills and experience of CISOs. On the other hand, business leaders may be insufficiently aware of the importance of security. At times, they may have a false sense of security or a misperception that CISOs hinder rather than enable business innovation. However, the number one reason why CISOs stay mired in the weeds is because security teams are too small and there is **not enough experienced talent**. This creates a strong incentive to focus scarce in-house security resources on strategic priorities that add value to the organisation's business. For repetitive operations, organisations are looking increasingly towards managed service providers. Additional reasons for using managed services include the ability to **scale capacity up or down** rapidly, improving **customer satisfaction** via stricter service level agreements, the quest for **cost reduction** and **outcome-based pricing**, and the need to **increase business value.**

The need to increase business value is easily overlooked when approaching managed services with a conventional "your mess for less" mindset. The view is that managed service providers operate existing processes and IT systems at a lower cost. Although managed services can deliver repetitive tasks more efficiently, it could be a mistake to transfer existing operations to an external provider without first considering the business problem that the organisation is trying to solve. In many cases, it turns out that existing operations fail to meet the needs and priorities of the business; therefore, handing them over to managed services providers will rarely deliver the desired value.

Managed services should be considered in the context of **end-to-end business risk management**. In this context, the focus is on building optimal security capabilities that are supported by managed services delivering standardised tasks, while more differentiated or company-specific tasks are performed in-house. Rather than viewing managed services as alternative sourcing models for existing capabilities, we encourage our clients to think of them as building blocks towards the creation of new and optimised security capabilities.

By way of illustration, consider application security. A common approach is to perform penetration tests or static application security tests (SAST) at a gateway before applications go into production. The conventional approach of outsourcing these gateway tests to a Software-as-a-Service (SaaS) or managed services provider leaves important business issues unanswered, such as:

- Are application security tests performed for all 'crown jewel' applications, and do we avoid wasting resources on low-risk/ low-priority applications?
- Do we have an effective follow-up process to address identified application vulnerabilities in a timely, effective and risk-prioritised manner?

[1] The Deloitte CISO Labs are immersive one-day workshops that encourage CISOs to think from a new perspective and develop a plan for success by focusing on the three most important resources a CISO has to manage: time, talent, and stakeholder relationships.

- Do we have a plan to mitigate the impact of application security tests on development budgets and release timelines?
- How do we use the gateway test to drive a 'Security by Design' philosophy throughout the development organisation? How should we modify existing development processes and tooling to achieve that goal?
- How do we protect the confidentiality of application source code and related information about application vulnerabilities?

None of these questions are addressed by conventional managed services. However they are at the heart of Deloitte's approach to managed services, which focuses on innovation, risk-based transformation, and the creation of business value. By starting with the business requirements for security, and designing or re-designing security capabilities to meet them, Deloitte's approach elevates the role of CISOs and security leaders to engage with their business counterparts, and it also frees up their time by moving repetitive and standardised work to external managed security providers. Viewed this way, managed security services become a **tool for strategic transformation**, rather than being just an alternative sourcing model for cutting costs.

Dr. Klaus Julisch
Partner
Cyber Risk Services
+41 58 279 6231
Email

Board matters

Cyber risk reporting revisited.

In the previous Cyber Flash, we reviewed how FTSE 100 companies in the UK disclose cyber risks in their annual reports. Specifically, we considered whether FTSE 100 companies identified cyber as a principal risk, how they categorised and described this risk and its impact in on the organisation. Since then, we have applied the same analysis to Swiss SMI companies using their latest annual reports, and found some interesting results:

- **Five of the 20 SMI companies** do not mention cyber risks in their annual reports, and an additional seven companies only make marginal references to it. (They addressed fewer than 10% of the 26 cyber topics that the UK study had identified as good practice, see Appendix).
- **The two large Swiss banks** are the most comprehensive in covering cyber topics, ranging from Board ownership to breach notification (see Appendix)
- The remaining six SMI companies cover only 10%-30% of the good practice cyber topics identified in the UK study.

Turning to the 26 cyber topics that should be considered in annual reports, there are notable differences in the degree to which they are addressed:

- Approximately 25% of SMI companies describe their cyber risks.
- 13% of SMI companies describe the roles of the Board and others in managing cyber risks.
- Only 6% of SMI companies describe the controls they use to manage and mitigate cyber risks.
- No SMI company reported cyber breaches and related remedial actions taken in response to such breaches.

Compared to the UK findings, SMI companies provide notably less detail in their disclosure of cyber-related risks. On many cyber topics, UK FTSE 100 companies are two times more likely than their Swiss peer group to include them in their annual reports. This might suggest that SMI companies are less concerned or less aware of cyber threats.

All SMI companies are, however, global and cyber is a global threat. This begs the question whether SMI companies underestimate cyber threats and whether Boards of Directors may want to consider if cyber threats are covered adequately in their annual reports.

Dr. Klaus Julisch
Partner
Cyber Risk Services
+41 58 279 6231
Email

Cyber insights from Swiss Board members

Stay tuned for the fall edition of swissVR Monitor, Deloitte's bi-annual Swiss Board survey. The report will feature a special section on cyber.

The survey is conducted jointly by swissVR, Deloitte and the Lucerne University of Applied Sciences and Arts. It gauges the outlook members of Swiss company Boards have for the country's economy, their sector and current Board matters.

To receive an electronic copy upon release, register your interest here.

Download the inaugural edition.

In the press

Deloitte ranked #1 by Gartner in Security Consulting for the 5th consecutive year.

Gartner, the world's leading information technology and advisory company, published this ranking in its May 2017 report titled, *Gartner: Market Share: Security Consulting Services, Worldwide, 2016.*

We are pleased to see that our commitment to helping organisations around the globe become and stay secure, vigilant and resilient is being recognised. In a time where cyber threats and security breaches are increasing, we believe this Gartner report provides the assurance to our clients that Deloitte is well-positioned to address their most complex cyber challenges.

For further details visit our webpage or contact Nicole Schmidt, Senior Manager, Communications.

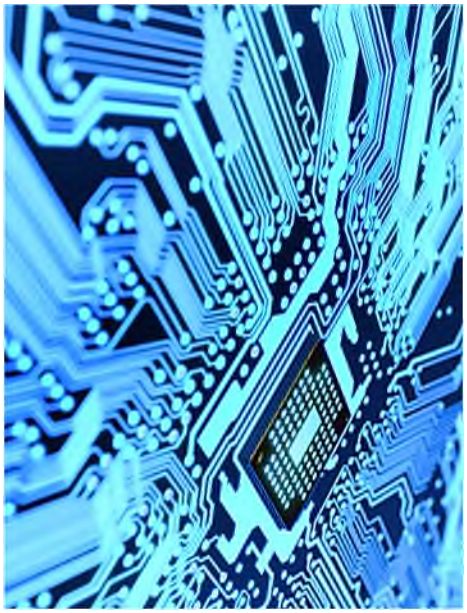
Banking blog

Interested in receiving the latest Swiss banking industry insights?

The Banking blog covers topics ranging from cyber security to regulatory updates, innovation in banking and many more.

Sign up here.

Privacy and data protection



Privacy by Design – how to achieve it?

One of the key principles of the new General Data Protection Regulation (GDPR) is that of Privacy by Design; what is it about and how do you achieve it?

The Privacy by Design principle requires that organisations consider privacy from the initial design stages onwards and throughout the entire development process of new products and services that involve the processing of personal data. Although it is a new legal requirement, Privacy by Design (also known as Data Protection by Design) is not a new concept. It is already considered good practice and one of the most effective ways of meeting privacy requirements. Recognising up-front what type of personal information will be used, its purpose, and defining how to protect individuals' rights for privacy, helps to avoid costly remedial work at a later stage. In addition, it promotes awareness of privacy and data protection across organisations, and facilitates overall compliance with privacy principles.

But how can companies implement the Privacy by Design (PbD) principle in practice? The GDPR does not provide specific guidelines on this question, and we are seeing an increasing number of inquiries from clients about ways to tackle this important piece of the GDPR compliance puzzle.

Framework

The starting point for implementing the PbD principle is the definition of a PbD framework. Such a framework typically consists of three elements:

1. Definition of the **process including roles and responsibilities** of designing or modifying systems, products and services. The key questions here are when, how and by whom will the PbD principle be enforced in the course of a change initiative? The corporate functions with privacy responsibilities typically are project managers, engineers, data protection officers (DPO) and information security managers.

2. Design of a GDPR **requirements catalogue**, aimed at identifying the applicable privacy requirements for a system, product or process. This catalogue covers all applicable data protection areas, including lawfulness, consent provisions, fairness and transparency, purpose limitation, data minimisation, and security. The parties identified in the first step above will use this requirements catalogue to perform a gap analysis and define the privacy requirements that apply to a particular change initiative.

3. Definition of the **data protection impact assessment (DPIA)** process, which identifies and assesses privacy-related risks, and defines mitigating privacy and security controls. This also includes defining events that trigger a DPIA, and creating a high-level pre-DPIA analysis that gives a view on the expected level of privacy risks.

Implementation

The implementation of a PbD framework involves activities targeting the three key areas of any organisational design:

1. **People.** This includes defining and executing communication, training and awareness sessions, targeting different user groups. Creating a high level of organisational awareness about privacy ensures that the organisation's employees understand the rules. In addition, specific target groups, such as project managers, engineers and certain control functions, need to understand their roles in implementing the PbD framework.

2. **Processes.** Embedding PbD in an organisation requires well-defined processes and precise guidance. Project management methodology, system development lifecycle (SDLC) and change management processes should be adapted to accommodate different aspects of the PbD framework. Ensuring that a DPIA process is triggered when needed, that data protection compliance requirements are gathered in the requirements collection phase, and that proper security and privacy controls are selected, are crucial for embedding privacy in a design process.

3. **Technology.** Using tools to automate some of the PbD requirements can help with its implementation. For example, the DPIA process can be supported by a tool that prompts a project manager to answer a number of questions relating to volume and sensitivity of personal data, possible transfer of information, and involvement of third parties. The use of automated scanning tools to discover security vulnerabilities in source code or a platform can facilitate the timely definition of mitigation actions.

Certification

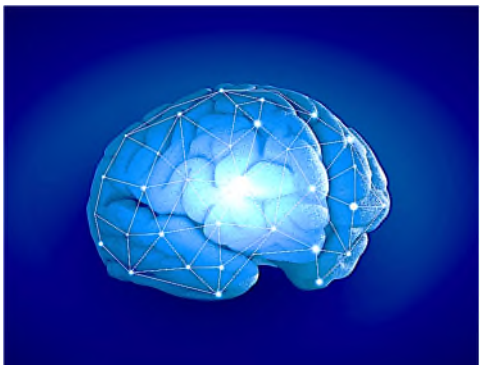
In the context of GDPR compliance, companies need to demonstrate that their practices follow the Privacy by Design principle. One possibility is to obtain a voluntary certification of Privacy by Design practice. The benefits of certification range from gaining competitive advantage and building customer trust – by demonstrating that data privacy is well managed – to minimising the privacy compliance risks.

For an example of a recognised PbD certification, refer to the certification process provided by the Privacy and Big Data Institute in Canada, in collaboration with Deloitte. As part pf this process, products, services or other offerings are tested against the seven foundation principles of Privacy by Design. Deloitte has refined these principles into 30 measurable privacy criteria and 107 illustrative privacy controls. Organisations are assessed against these, using a unique scorecard approach that maps back to each of the foundation principles. The results of this assessment are the basis for certification, which is awarded by Ryerson University.

If you would like an initial conversation about Privacy by Design under the GDPR, please get in contact with our team.

Dr. Dusko Karaklajic
Manager
Cyber Risk Services
+41 58 279 7386
Email

Dr. Milica Karaklajic
Senior Consultant
Cyber Risk Services
+41 58 279 7049
Email



GDPR and its implications for the Life Sciences industry

The new regulation that comes into effect in May 2018 has far-reaching implications – also for Life Sciences companies.

The GDPR is applicable to all companies that process personal data in the EU, or target/monitor EU residents. As such, it has far-reaching implications, particularly for the Life Sciences industry. This is due to the fact that pharma, medical device and healthcare-related businesses process large amounts of sensitive personal data, such as clinical trials patient data, genetic data used in personalised medicine as well as patient health monitoring data.

With less than a year to go, the clock is ticking on the countdown to address the GDPR requirements and achieve regulatory compliance. Based on a recent survey, numerous meetings and conversations with risk executives in some of Switzerland's largest Life Sciences companies, three topics loom particularly large for the Life Sciences industry.

New provisions: Several new provisions of the GDPR are particularly important for Life Sciences companies. First, the definitions of 'Personal Data' and 'Sensitive Data' have been expanded. The latter now includes genetic and biometric data, as well as data concerning health, which is defined in very broad terms (see Articles 4(15) and 9(1)). This raises the question of whether companies' current security controls over genetic, biometric, and health-related data will be adequate for protecting sensitive personal data in the future.

A related question is whether companies will still have a valid legal basis for processing genetic and biometric data, as well as any other relevant special categories of personal data. Further issues result from the GDPR's new definition of 'pseudonymisation' (see Article 4(5)), which raises questions about whether today's widespread anonymisation and pseudonymisation techniques will be sufficient under the GDPR. The extra-territorial applicability of the GDPR (see Article 3) also means that Life Sciences companies with no operations in the EU will be subject to the GDPR in the future if they run clinical trials or studies in the EU or target EU citizens.

Third-party relationships: Research is fundamental to Life Sciences, and research frequently involves extensive collaboration with start-ups, universities, suppliers, customers and others. Life Sciences companies may feel that these third-party relationships need to be reviewed carefully, and additional legal, contractual or procedural controls are likely to be required in order to comply with the GDPR. This is particularly so in light of stricter processor[2] obligations that are likely to subject previously unaffected third parties to the GDPR.

Fragmentation of laws: Member States are entitled, under Article 9(4) GDPR, to maintain or impose further conditions and restrictions on the processing of genetic, biometric or health data. As a consequence, existing national differences are likely to persist, and further divergence will be permitted. The implication for Life Sciences organisations is that they will have to keep abreast of national laws and achieve compliance with a more diverse set of requirements.

While these issues are particularly relevant for Life Sciences companies, this should not distract from the fact that the GDPR presents organisations with many other challenges, which are not industry-specific but are

nevertheless important. These include the creation of an inventory of processing activities, supporting data subject requests, implementing Privacy by Design and Default, establishing privacy governance and breach notification procedures.

The interplay with other regulations, for example GxP, also needs to be considered – in particular in the area of data retention, which is heavily restricted by the GDPR (see Article 17).

Outlook

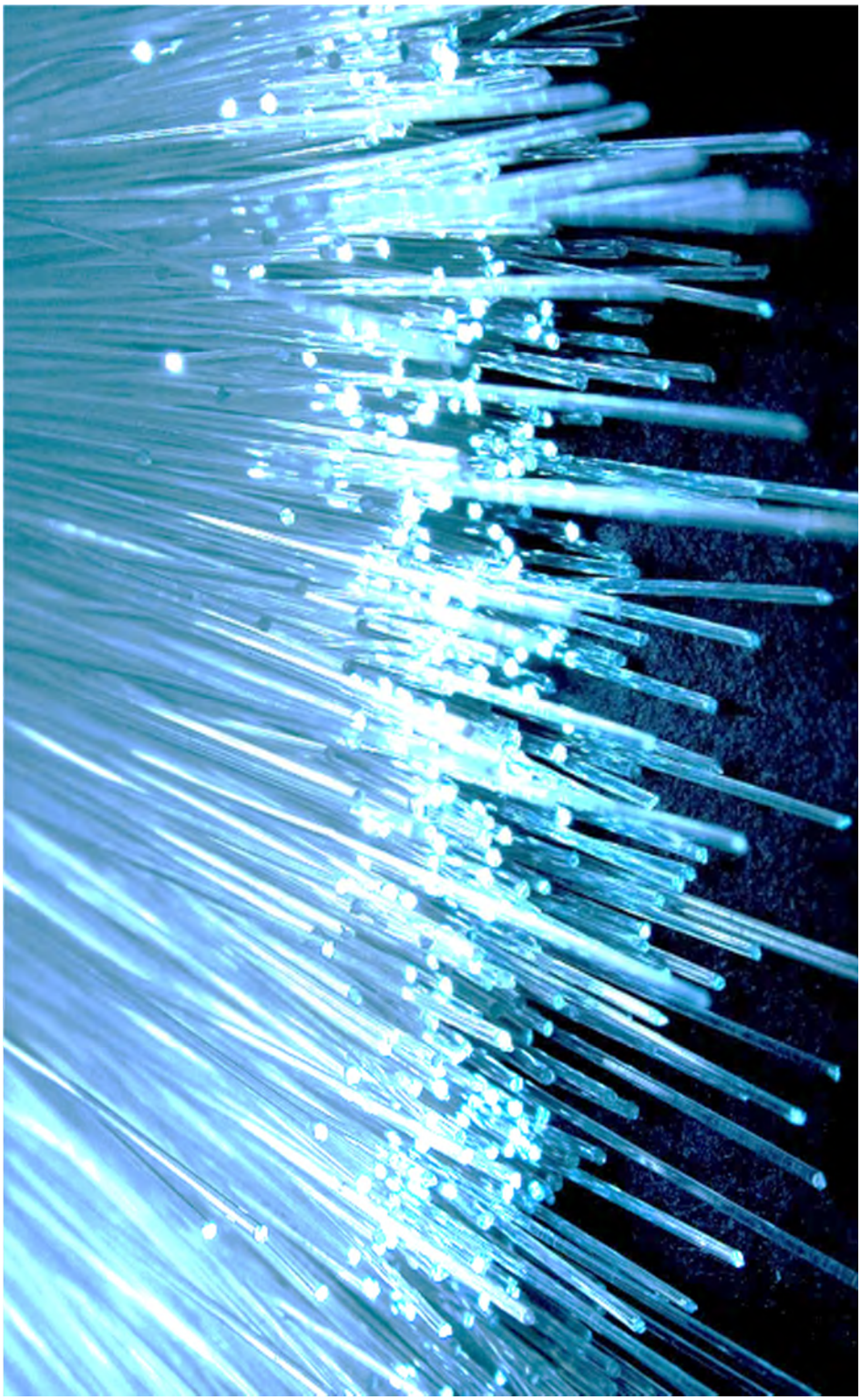
Despite these challenges, it is important not to lose sight of the benefits of the new regulation. For one, the law is there to strengthen the protection of people's privacy, and as individuals we all benefit from this. The GDPR also encourages

[2] In simple terms, the *controller* is an entity to whom individuals entrust their personal data and who determines the means and purpose of processing it; the *processor* is an entity that acts on behalf of a controller and as instructed by the controller to perform certain data processing activities. For example, a company (controller) may outsource the printing and mailing of employee pay slips to another service provider (processor).

organisations to reconsider their data governance. The costs of protecting personal data should discourage indiscriminate data hoarding and encourage companies to devise better ways of managing personal data and deriving economic benefit from it. Lastly, data protection may become a market differentiator, giving a competitive advantage, and some companies are actively pursuing this strategy. Not only are consumers likely to prefer companies that provide superior data protection, they may also be more willing to allow such companies to analyse their personal data in innovative ways, thereby enabling them to understand their clients better and increase their lead over the competition.

Dr. Klaus Julisch
Partner
Cyber Risk Services
+41 58 279 6231
Email

Kishwar Chishty
Director, Life Sciences Risk Advisory
+41 58 279 9180
Email



Events, conferences and contacts

European Privacy Academy
Dolce La Hulpe, Belgium
www.europeanprivacyacademy.com

The European Privacy Academy is a unique training, knowledge and networking centre, focused on the practical day-to-day management of privacy challenges. It provides an on-campus data protection officer course and on-campus or in-house department-specific data protection training. These workshops allow attendees to learn how to manage privacy and security efficiently and in an integrated risk-based manner.

The next European Privacy Academy DPO Course sessions will take place on:
13 - 16 Nov 2017 & 05 Feb 2018
07 - 10 May 2018 & 17 Sep 2018

Key contacts:

Mark Carter
Managing Partner
Risk Advisory
+41 58 279 7380
Email

Dr. Klaus Julisch
Partner
Cyber Risk Services
+41 58 279 6231
Email

Deloitte.