Deloitte.

Cyber Flash

A spotlight on cyber and privacy trends

Issue 4, December 2017

Editorial

Issue 4, December 2017

Dear Colleagues,

2017 turned out to be another turbulent year in cyber security. We've seen ransomware bring major international organisations to their knees, the largest data breach in history – for the first time affecting over a billion users – was reported, leaked emails were used in an attempt to manipulate the French election, 198 million US voter records were leaked via a publicly accessible database and the countdown to the largest shake-up of data protection laws in almost 20 years has entered its final phase. It is fair to say that cyber attacks are shaking the very foundation of commerce and society. These events also validate the importance of our work and of sharing our latest thinking on how we can best defend our organisations. In this spirit, the final Cyber Flash of 2017 offers a collection of six highly topical articles:

- **Cognitive computing for cyber security**, describing the potential of cognitive computing for better cyber security detection and response capabilities.
- **Third party cyber risk management**, providing leading practice and managing cyber risk from your third party relationships.
- **swissVR Monitor II,** Board-level insights on organisational cyber preparedness.
- **KYE - Know your employees**, or what you need to know about employee monitoring.
- **GDPR benchmarking survey**, offering a representative overview of how companies across Europe prepare for the GDPR.
- **Privacy updates**, summarising the latest privacy developments in Europe and around the world.

On behalf of our Cyber Risk Services team I would like to thank you for your trust and ongoing relationship, and wish you an inspiring read. Season's Greetings and our very best wishes for 2018 from the Cyber Team and myself.

Yours sincerely,

Dr. Klaus Julisch
Lead Partner
Cyber Risk Services

Issue 4 highlights

Cyber security

Privacy and data protection

Cyber security

Cognitive computing for cyber security

The potential of cognitive computing for better cyber security detection and response capabilities.

Old wine in new skins?

Every now and again, a "disruptive" technology captures the imagination of innovators and entrepreneurs. By most standards, the "disruptive" label may be applied to "cognitive computing", which describes a range of technologies that automatically extract concepts and relationships from data, "understand" their meaning, and learn from data patterns and prior experience[1]. For a long time, computers have been able to outperform humans in raw calculative power. Cognitive computing however, is seeing machines encroach into the historically human strengths of thought, reason, and the processing of unstructured data.

In the "Cognitive Computing Era", today's computer systems have evolved into powerful, intelligent systems that can emulate human reasoning[2]. In more technical terms, the field of cognitive computing lies at the intersection of machine learning, image processing, natural language processing, and Big Data, allowing the rapid ingestion of enormous quantities of both structured and unstructured data. The beginning of the Cognitive Computing Era is often marked by the unveiling of IBM's Watson, which won a special edition of the US quiz show Jeopardy in 2011. A quiz show-winning robot doesn't sound useful in itself, but the implications of its abilities are profound and far-reaching. The underlying technology will find use in applications from customer service calls to healthcare, anywhere where structured or, more importantly, unstructured data needs to be sorted and interpreted[1]. Moreover, cognitive computing technologies are considered a game-changer for risk management, by mining often ambiguous and uncertain data to find indicators of known and unexpected risks[3]. The following text provides a brief outlook on how cognitive computing, applied to organisations' cyber security functions, can be expected to be paradigm-shifting.

Applying cognitive computing to the cyber domain

With the increase of data volumes, the growing sophistication of cyber attackers and the shortage of skilled cyber security experts, new approaches are required to keep pace with the modern array of cyber threats. Cognitive computing promises to help.

Enhanced SOC operation

A pillar of a mature cyber security programme is the ability to detect when an attack is occurring. Today, tools already exist to aid first-and second-level support functions in detecting attacks and incidents. However, with increasing sophistication of both IT systems and attackers, the cost of labour required to keep systems safe can increase to untenable levels. Here enters cognitive computing, where the ability to automatically ingest, weigh, discriminate and evaluate immense quantities of data can be expected to represent a centrepiece of modern threat detection. While human attention may fail, and simpler algorithms may misdiagnose threats, the cognitive computer promises to be powerful enough to see the whole system at once, and clever enough to see through subtle anomalies and attack patterns. Moreover, it can not only automatically identify a threat, but also actively scan for vulnerabilities

[1] Deloitte University Press, "Cognitive technologies in the technology sector - From science fiction vision to real-world value," Deloitte University Press, https://www2.deloitte.com/content/dam/Deloitte/tr/Documents/technology-media-telecommunications/Cognitive-Technologies.pdf, 2015.

[2] J. E. Kelly, "Computing, cognition and the future of knowing," IBM Corporation, 2015.

[3] Deloitte, "Why artificial intelligence is a game changer for risk management,"https://www2.deloitte.com/us/en/pages/advisory/articles/ai-cognitive-computing-applications-risk-management.html, 2017.

in a systems' configurations, and propose corrective actions. All at speeds that could define the success or failure of a cyber-attack. For example, by using a cognitive computing based platform, a security operations centre ("SOC") provider has been able to reduce the average time for threat investigation and root cause determination from 3 hours to 3 minutes[4]. This may serve to increase the coverage of an organisation's SOC, also helping to bridge the gap in skills and talent that many SOCs experience today, since fewer security engineers are required for triage and first-responses.

Automated threat intelligence

So far, much of cyber security has depended on reactive strategies, responding to threats as and when they manifest. While cognitive technologies can achieve this, they also have the potential to proactively protect their owners' systems by turning their skills of massively parallelised information analysis towards the vast repositories of cyber security information that exist today. Vendors of cognitive technologies promise the ability to ingest data from millions of disparate information sources so as to identify actionable threat intelligence that is meaningful to individual companies, allowing them to prepare proactively. Such intelligence consists in hints and early indicators of threat actors' intentions, targets, and methods used. When the speed and accuracy of your response determines the impact of attacks, the promise of cognitive computing to tap millions of information sources in search of early indicators can be invaluable.

The other side of the coin – applying cyber security to protect cognitive computing

Security plays an equally important but often neglected role as an enabler for cognitive computing. To take full advantage of cognitive computing, it is crucial to build and maintain preventative and detecting cyber security capabilities to ensure the confidentiality, integrity, and availability of underlying systems and data. Medical diagnostics, another strong example of the power of cognitive computing[5], is one such case where the security of information being handled (private medical data), is of paramount importance. Furthermore, solving more complex problems may require additional computing power that needs to be provided by external distributed systems, such as public clouds. Additionally, the effectiveness and accuracy of predictive analyses based on neural networks and associated insights will rely on the availability of correct data sources that are neither corrupted nor manipulated. In all these cases, the implementation and enhancement of well-known cyber security capabilities such as rigorous and fine-granular identity and access controls, data leakage prevention mechanisms, strong encryption technologies, as well as system-health monitoring capabilities remain equally important as any investments in cognitive computing technologies themselves.

Cognitive outlook

At this stage, cognitive computing is still complementing human security specialists by suggesting strategies and calculating probabilities of outcomes. However, major industry players have already launched cognitive-based services for threat detection and security analytics. An example close to home is SIX, the operator of the Swiss financial market infrastructure, who is in the process of deploying IBM Watson for cyber security in a new "Cognitive Security Operations Center"[6].

As humans and computers are learning to collaborate in ways that were impossible in the past, it is expected that more security capabilities based on cognitive computing will evolve over time. One day, such systems may even become capable of protecting themselves from threats, hence addressing the need for security in cognitive computing. While this may still be years out, the journey has definitively begun.

Dr. Thomas Koslowski
Assistant Manager
Cyber Risk Services
+41 58 279 7703
Email

Martin Felle
Consultant
Cyber Risk Services
+41 58 279 7203
Email

[4] IBM Corporation, "Reducing threat investigation and root cause determination from three hours to three minutes," 2017. [Online]. Available: https://www-935.ibm.com/industries/nl-nl/overheid/pdf/IBM-Case-Sogeti-LX-EN_LR.pdf. [Accessed 12 09 2017].

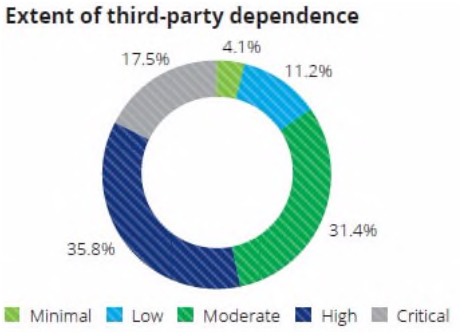
[5] Memorial Sloan Kettering Cancer Center, "Watson Oncology," 2017. [Online]. Available: https://www.mskcc.org/about/innovative-collaborations/watson-oncology. [Accessed 12 09 2017].

[6] SIX Group, "SIX Leverages IBM Watson for Cognitive Security Operations Center," 2017. [Online]. Available: https://www.six-group.com/about/en/shared/news/2017/ibm.html. [Accessed 18 08 2017].

Third party cyber risk management

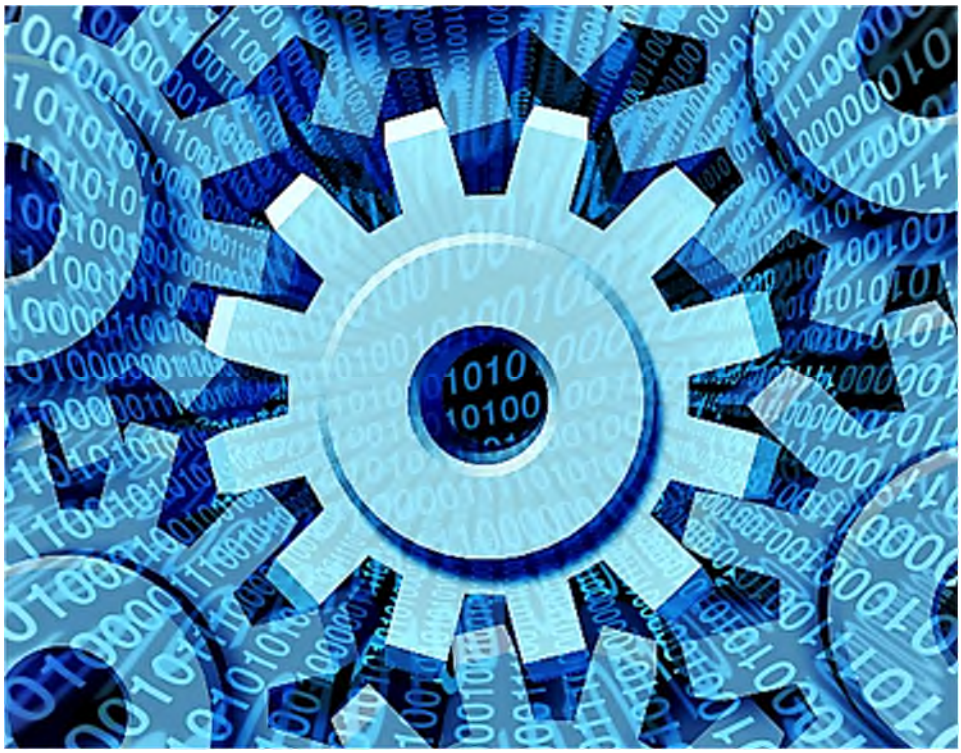
How well are you managing cyber risk from your third party relationships?

In an effort to reduce costs, increase efficiencies and build strategic advantage, organisations are expanding their use of outsourcing and are relying more extensively on third parties for critical business and IT processes. While third parties bring multiple benefits to business, there is a corresponding increase in cyber risk exposure as third parties can access critical systems, sensitive information, and potentially engage sub-contractors. Beyond cyber, there are further third party risks such as the risk of lock-in, regulatory non-compliance, and others, but these exceed the scope of this article. Despite a high dependency on third parties, many organisations are not yet managing cyber risks in a holistic and coordinated manner.



Source: Deloitte 2017 Global Third Party Governance and Risk Management Survey

Additionally, regulated industries are required to strategically think about third party cyber risk management. Potential penalties for managing third party cyber risk insufficiently range from regulatory fines to losing the license to operate. With recent developments in regulations around the globe, such as the cyber regulation by the New York State Department of Financial Services ("NYDFS"), it is expected that regulatory pressure increases on



Swiss organisations to take more proactive measures to manage this risk.

Third party cyber risk management

Third party cyber risk management ("TPCRM") is the process of identifying, evaluating, and preventing or reducing cyber risks associated with third parties to an acceptable level. Determining that level depends on the organisation, the value of the assets, the threat level and budget. A holistic TPCRM framework requires a multi-layered approach covering compliance requirements (e.g. breach notification, support for e-discovery, data location requirements, etc.), security requirements (e.g. multi-factor authentication for remote access, encryption, disaster recovery, etc.), and legal requirements (e.g. right to audit, data ownership, sub-contracting, NDAs, etc.).

Steps to consider for the implementation of an effective TPCRM

To implement an effective, value-adding TPCRM, the programme must be embedded in your company's vendor lifecycle management, starting from the due diligence process to the on-boarding and contracting, to the continuous monitoring and, finally, to the off-boarding and termination. The core of each TPCRM framework is the approach to assessing third party cyber risk, where a two-tier approach is considered leading practice.

First, an inherent risk assessment is used to categorise the third party into low, medium or high inherent risk vendors based on the nature of its services and without accounting for its controls. **Secondly**, based on the inherent risk rating, organisations are advised to assess if their vendor has sound security controls in place that meet their risk appetite. The 'tell me' exercise is performed using questionnaires to obtain insights on the current level

of security risk among suppliers. **Finally**, one would use these insights to plan and initiate on-site reviews or remote assessments adopting a 'show me' approach to controls testing.

In some organisations, the number of vendors is equal to, or higher than the number of employees. To manage third party cyber risk on scale, organisations need to think about staffing and an agile, scalable execution model. Using a managed service here is increasingly common for a number of reasons:

- It allows organisations to benefit from economies of scale and associated cost benefits.
- It provides the ability to quickly scale up and down depending on demand.
- An external assessor is often preferred by regulators and usually comes with a high level of trust and independence.
- The concern of finding skilled security professionals with an audit mind-set can be reduced that way.

Key takeaways

With the rapid adoption of cloud computing solutions and outsourcing of business processes, the dependency of businesses on third parties will further increase. Based on our experience, organisations are encouraged to consider:

1. Defining a TPCRM programme that improves security and provides value beyond just addressing compliance.

2. Implementing third party risk management solutions fully integrated in the vendor life-cycle to be least disruptive for business.

3. Executing third party risk assessments in a scalable manner to ensure a high degree of consistency and standardisation of the assessments.

4. Getting a complete picture of the cyber risks associated with third parties by also looking into the effectiveness of your company's internal control framework (e.g. access re-certification, data protection measures, patch management, etc.).

5. Including third party cyber risk management into your company-wide risk and security awareness as well as training programmes.

Patrick Lechner
Manager
Cyber Risk Services
+41 58 279 7780
Email

swissVR Monitor II

Board-level insights on organisational cyber preparedness

According to our latest swissVR Monitor survey, Board awareness of cyber security topics has increased, compared to previous years: **78% of the 464 surveyed Board members** report that cyber security issues are now on the Board's agenda. A reassuring outcome in light of the recent wave of ransomware attacks organisations faced in Switzerland and globally.

However, **only 35% of surveyed Board members** report that their companies have a clear cyber security strategy and action plan in place. Followed by **a third of respondents** reporting that a strategy and plan are currently being devised. This leaves **one third of businesses with no strategy or action plan at all**; a surprising result considering the looming threats and expected rise of cyber-attacks in today's increasingly digitalised and automated business environment.

The outcome might suggest that some companies in Switzerland are less concerned or less aware of cyber threats. Which begs the question whether these organisations underestimate cyber threats and the potential impact of an attack on their companies. To be prepared for eventualities, Boards of Directors may want to consider adding cyber risk to the Board's agenda and integrating cyber security in their companies' risk management approach.

To find out more and to read the interview on the topic with Heinz Karrer, President of economiesuisse, download the PDF. For a hard copy of the report in English or German please contact:

Cornelia Bade
Marketing Manager
Risk Advisory
+41 58 279 6504
Email

Privacy and data protection

KYE – Know your employees

What you need to know about employee profiling.

Planting the KYE seed

In the early 1900s, Henry Ford hired a team of private investigators to monitor his employees, inside and outside of his factory. These investigators, who worked for Ford's sociological department, would visit employees' homes not only to make sure that personal issues were not interfering with their work, but also to ensure that they were living according to Ford's values.

Fast forward 100 years

Although such methods may seem ludicrous today, the idea and practice of companies profiling their employees is gaining ground, enabled in part by the daily use of technology and connected devices. While Ford's motivations were related to his employees' efficiency and moral values, one reason for the trend today is that insider threats are becoming increasingly common. According to IBM's Cyber Security Intelligence Index[7], the financial services sector saw **58% of their attacks come from insiders** in 2016 – both malicious and inadvertent. In the same year, 71% of attacks in the healthcare industry were due to insiders. During this same period, Gartner reported that its clients increasingly inquired about how to address and mitigate insider threats[8].

Although the risk culture in many organisations mainly targets external threats, companies must invest in protecting themselves from internal threats as well.

The potential of KYE

Thanks to technological advances and the digitisation of information, one solution companies turn to in order to mitigate insider threats is employee profiling. Employee profiling is an umbrella term for algorithms tailored to each company's objectives that learn from available input feeds such as:

- Activity logs e.g. email and phone communication, internet browsing history, host and network activity logs and physical movement of employees.
- Usage behaviour logs, e.g. time spent on applications and software and time of day at which applications and software are used.
- Data usage logs, e.g. use of external drives, copied, moved and/or deleted data.

They then compare employee behaviour against profiles of normal behaviour or patterns of known abuse. The idea is that by monitoring its employees' behaviour, a company may be able to detect attacks and attack pre-cursors and take informed action in a timely manner.

Catalysing a paradigm shift

As it turns out, many techniques now exist that can create baseline profiles for individuals and detect and flag deviations from them. Pushing the concept further, some companies see employee profiling as a catalyst for a shift in the way they ensure that employees only access data to which they have permitted access. Indeed, instead of setting up controls to enforce access control policies, why not simply build

[7] IBM, "Cyber Security Intelligence Index," 2016

[8] Gartner, "Understanding Insider Threats," 2016.

profiles for each employee to detect and block abnormal behaviour? For example, assume HR staffer Bob is flagged when he accesses software development resources that have recently been added to the company's network. Looking into this event, his manager Alice finds that these resources were put online before the appropriate access controls were set up. Because it is never possible to fully secure systems, this approach could prove to be more effective in preventing insider attacks, as compared to traditional methods.

The main hurdle: privacy laws and regulations

In many geographies, there are laws and regulations that must be understood and followed when considering the monitoring of employees. For instance, Europeans will see their privacy enhanced as the new General Data Privacy Regulation ("GDPR") comes into effect in May 2018. Similarly, the Swiss government is due to publish a revision of the Federal Act on Data Protection ("FADP") next year, a draft of which is already available online (in French, German and Italian)[9]. The FADP is being updated specifically to take into account advances in technology and societal changes and specifically addresses the issue of employee profiling.

Why you should care

Employee profiling is becoming increasingly important as the occurrence of insider threats occupies a significant portion of attacks today and have the potential to cause serious damage. In addition, progress in technology (e.g. IoT devices and sensors) and computer science (e.g. data mining and machine learning) now allow the efficient creation of profiles and (near) real-time detection of deviations, thus rendering employee profiling feasible.

Patricia Egger
Consultant
Cyber Risk Services
+41 79 856 2462
Email

GDPR Benchmarking Survey

How are European organisations preparing for the GDPR?

The results of our recent GDPR Benchmarking Survey indicate that organisations are taking **a wide range of readiness approaches**, driven by the combination of potentially significant fines, the increased obligation to demonstrate proactive compliance and the complexity and ambiguity of some of the requirements.

Approaches to compliance and remedial spending vary widely; 39% of respondents report spending less than €100,000, whilst 15% report spending more than €5 million. No correlation was found between the size of the organisations (by headcount or revenue) and their spend, nor any clear trends in different industry segments. Among the results we found examples of organisations with fewer than 10,000 employees spending over €2.5 million, but also examples of organisations with more than 50,000 employees spending less than €250,000.

Overall, only 15% of organisations surveyed expect to be fully compliant by May 2018, with the majority instead targeting a risk-based, defensible position. The results of the survey also give an insight into what respondents consider as the most challenging GDPR requirements. **The top 5 (in order of difficulty) are:**

1. Consent
2. Right to erasure
3. Developing and maintaining a personal data register
4. The accountability principle
5. Data portability

This report examines these and other GDPR compliance related matters and makes pragmatic recommendations on how to comply with the areas respondents feel present the greatest challenges. Most importantly, this report considers how privacy can become more than a compliance exercise; **how it can become a real business asset and enabler, and maybe even a competitive advantage.**

Download the report here

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

[9] Swiss Government, "Stärkung des Datenschutzes," [Online]. Available: https://www.bj.admin.ch/bj/fr/home/staat/gesetzgebung/datenschutzstaerkung.html. [Accessed August 2017].

Privacy updates – what you need to know before the end of this year.

The puzzle pieces regarding the exact interpretation and ramifications of the GDPR continue to fall into place.

In Germany, The Data Protection Authority (DPA) of Bavaria has distributed a questionnaire to 150 organisations to help them assess how far they have come in their preparation for 25 May 2018. In the associated press release, the DPA clarified that the questionnaire should give companies an idea of how the DPA plans to use the new audit powers it will receive in less than a year's time. As organisations across Europe wonder how the GDPR will play out in practice, this may provide a useful indication of things to come.

Germany also passed a new Data Protection Act on 12 May 2017. The new law makes use of the so-called "opening clauses" in the GDPR, which allow Member States to enforce stricter rules (e.g. regarding the mandatory DPO appointment) or to relax certain requirements (e.g. minimum age for valid consent). As expected, Germany will continue to require organisations to appoint a DPO if they employ more than 10 persons who are permanently engaged in the automated processing of personal data. On the other hand, the German act goes beyond the GDPR in defining specific rules in the areas of video surveillance, consumer credit and creditworthiness. In addition, it creates rules allowing for the sanctioning of individuals, which could lead to personal liability risks for employees of data controllers.

The Spanish Data Protection Authority (Agencia Española de Protección de Datos, or AEPD) has published a new set of guidelines to help companies prepare for the GDPR, which will become enforceable in 25 May 2018. While addressed to small and medium companies, the documents can be used by organisations of any size, and are likely to constitute an important reference point in their interactions with a Data Protection Authority that is known for being active in the field of enforcement.

Since early 2017, the Article 29 Working Party ("WP29") produced several pieces of important guidance surrounding the impact and implementation of the GDPR. Specifically, the WP29 published its final guidance on data protection officers, lead authorities, data protection impact assessments ("DPIA"), administrative fines and the right to data portability. The Article 29 Working Party further published the draft guidance on consent and draft guidance on transparency under the GDPR. These two documents are subject to public consultation. The deadline to submit comments is 23 January 2018.

It also becomes apparent that many of the principles of the GDPR become more widely adopted, either outside Europe or outside the specific context of privacy. This development is highly relevant as many organisations have been debating whether GDPR should be treated as a "European problem" or a global issue. The latter might turn out to be the better answer as the desire to align with the GDPR creates a cascading effect where countries such as Switzerland, Poland, India and Argentina revise their data protection laws.

Moreover, certain aspects of the GDPR, such as breach notification, are becoming a common regulatory requirement as evidenced, for example, by the Network Information Security Directive, which also comes into force in May 2018 and requires operators of essential services to report significant incidents without undue delay. Amending the Privacy Act of 1988, the Australian Senate has also introduced a mandatory data breach notification scheme on 13 February 2017. Agencies and companies will, from a set moment in time communicated by the Federal Government, be obliged to notify data breaches to the Australian Data Protection Authority (i.e. Australian Information Commissioner). Additionally, the affected data subjects have to be informed about all data breaches that provide a high risk to the rights and freedom of the data subjects and are most likely to result in a serious harm for the data subjects affected.

While none of these developments are conclusive when taken in isolation, in aggregate they show that the GDPR has ramifications beyond its original scope. To read the complete articles on the above and additional topics, download the latest Privacy Flash issues from July and October. For further insights into how we are helping clients navigate the difficult landscape of data protection, visit our website.

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

Privacy Flash

For more insights on global regulatory developments in the field of data protection and privacy visit our website.

Key contact:

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

Events and conferences

IAPP Global Privacy Summit 2018
Washington DC, USA
25–28 March 2018
https://iapp.org/conference/global-privacy-summit-2018/

True to its three day format consisting of workshops and conferences, the IAPP Global Privacy Summit offers an unparalleled forum for lively debate, interaction, and exchange between regulators, data protection experts and privacy professionals from across the globe.

European Privacy Academy
Dolce La Hulpe, Belgium
DPO course dates:
07-10 May 2018 & 17 Sep 2018
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.

Deloitte.