Top cyber risk and compliance related news stories and world events, that (for better or for worse) shaped the month's agenda, and what is next

May 2018, cyber risk and compliance in Switzerland

Dear readers,

We have the 26th semi-annual report of the Reporting and Analysis Centre for Information Assurance (MELANI), that addresses the most important cyber incidents of the second half of 2017, both in Switzerland and abroad.

According to the report, in July 2017, the Turla spyware was discovered on several servers of the Federal Department of Defence, Civil Protection and Sport (DDPS). The same malware in December 2015 attacked the technology group RUAG, which is an enterprise associated with the federal government whose responsibilities include securing the equipment of the army.

The Swiss federal agencies were able to carry out the necessary checks in time and take appropriate measures. The cooperation of the individual federal agencies was very good, and made it possible to gather information on the attack methods and technical indicators.

The exchange of such indicators, both nationally and internationally, is a crucial element for detecting current or future attacks. The Federal Council, the members of the Security Committee of the Federal Council, and the chairs of the responsible committees were informed promptly, as is customary for such incidents.

The DDPS also filed criminal charges with the Office of the Attorney General of Switzerland against persons unknown for cyber-attacks on its servers.

The report also discusses cyber parasites. The success of cryptocurrencies offers extremely tempting prospects for cyber criminals.

Mining is the process by which transactions in a cryptocurrency are verified and new cryptocurrency is generated. Complex calculations have to be solved for this purpose, requiring considerable IT resources.

The provision of these resources is compensated with a certain amount of "mined" money, corresponding to the share in the calculation. Mining ultimately contributes to money creation.

Because mining can be used to earn money, certain actors have been looking for ways to abuse it for quite some time. Attacks that abuse computing power for mining have multiplied.

2017 was particularly eventful in this respect – so much so that some experts are wondering whether this may be one of the most lucrative business models for cybercriminals.

Certain types of malware were used for mining, although other criminal options would also have been possible. One example of this is WannaMine: a sophisticated malware that spreads particularly via the EternalBlue exploit, already used by the ransomware WannaCry and NotPetya. Unlike the latter, however, the WannaMine criminals used this to create virtual currency once it is installed, instead of encrypting user data.

In the report there is an interesting definition: Data leaks are security incidents in which unauthorised third parties gain access to personal data, company secrets or other data which is not intended for them.

The definition of the term data leak is very broad and besides data theft and espionage also includes data breaches, in which data will be made available unintentionally.

A common way for criminals to make money with data leaks is certainly blackmailing the company where the data has been breached. One of the first such cases in Switzerland dates back to 2014. A group called Rex Mundi blackmailed a company in French-speaking Switzerland with the publication of data.

Another use of data from data leaks is for targeted attacks. On the underground market, actors have specialised in gathering as much information as possible about a victim. In addition to freely available sources, they also use information originating in data leaks. If the attackers succeed in obtaining a precise picture of the victim with the help of a wide range of data, very targeted attacks are also possible.

The protection of personal data is governed by the Swiss Federal Act on Data Protection (FADP). The aim of the act is to protect the privacy and the fundamental rights of natural and legal persons when their data is processed.

A distinction is made between personal data and sensitive personal data. The latter category includes data on religious, ideological, political, or trade union-related views or activities; health, the intimate sphere, or the racial origin; social security measures; and administrative or criminal prosecutions and sanctions. When processing such data, the express consent of the person concerned must be given.

The Data Protection Act also takes sufficient account of the security aspect and defines that personal data must be protected against unauthorised processing through adequate technical and organisational measures.

The total revision of the Swiss Data Protection Act is currently underway. It can be assumed that the revision will embrace various new elements of the EU General Data Protection Regulation.

The EU General Data Protection Regulation also applies to all Swiss companies, with or without headquarters in the EU, which offer products and services to persons in the EU (which is most likely the case if their website or web shop does this), process personal data of EU citizens, or analyse the behaviour of persons in the EU.

To read the excellent MELANI report:
https://www.melani.admin.ch/melani/en/home/dokumentation/reports/situation-reports/semi-annual-report-2-2017.html

---

I want to share some thoughts about the challenges after the GDPR deadline and the extraterritorial application of EU law.

After the 25th of May, the world must comply with the new General Data Protection Regulation (GDPR) of the EU.

The regulation covers “processing”, data protection, privacy, and information security. The regulation applies to data controllers (firms that collect data from EU residents), and processors (firms that processes data on behalf of data controllers). The regulation applies to organisations based outside the EU, if they collect or process personal data of individuals located in the EU.

Processing covers a wide range of operations performed on personal data. It includes the collection, recording, organisation, structuring, storage, adaptation, alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction of personal data.

In my opinion, one of the most interesting parts of the new regulation follows the words "appropriate" and "state of the art". You wonder which party bears the burden of proof? Well, of course the data controllers and the processors.

Article 32, Security of processing:

"1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

(a) the pseudonymisation and encryption of personal data;

(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

2. In *assessing the appropriate* level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed."

I had enough, now it is time for "The Requiem" by Wolfgang Amadeus Mozart. He composed part of it in Vienna, but it was unfinished at his death. It reminds me that the GDPR compliance implementation is also unfinished in almost all companies and organizations.
Plato believed that music is also a law, a moral law. It gives soul to the universe, wings to the mind, flight to the imagination, and charm and gaiety to life and to everything.

I have just read that "British psychologists found that young adults use their smartphones roughly one-third of their total waking hours." Could you ever see that as an opportunity?

Well, I was surprised with the *next* sentence in the presentation: "Simply put, all of us can now do banking anytime, anywhere. And many segments of our populations are increasingly comfortable going digital, be it for banking, or to purchase goods and services."

Ong Chong Tee, Deputy Managing Director (Financial Supervision) of the Monetary Authority of Singapore, can see some benefits in the behaviour of young adults. I don't know if this is positive thinking, optimism (a mental attitude that interprets situations and events as being optimized), or realism.

Actuaries that have not incorporated in their models that "young adults use their smartphones roughly one-third of their total waking hours" must not feel so happy as Ong Chong Tee feels. Actuaries have a good dose of pessimism and believe in statistics, not monetary authorities.
{Question to an actuary: How many actuaries does it take to change a light bulb? Answer from the actuary: How many did it take the previous five years?}

Ong Chong Tee's presentation continues with some interesting developments, like the UK bank that leverages totally on blockchain and biometrics to provide peer-to-peer financial services with the slogan of "everyone is a bank".

We read: "Open Banking broadly captures the concept that a consumer owns information about himself and should be able to share that information with any third party if he chooses, for example through APIs, and to transfer his money to any third party seamlessly.

The effect is to give consumers ownership over their financial data, to make that data portable, and therefore enables switching and choice among financial service providers. This should promote competition to improve pricing and service quality."

John McAfee has said that our mobile phones have become the greatest spy on the planet. I am sure this is not positive thinking.

James Comey, who has served as the director of the FBI, has said: "Technology has forever changed the world we live in. We're online, in one

way or another, all day long. Our phones and computers have become reflections of our personalities, our interests, and our identities. They hold much that is important to us." I am sure he had a different perspective from Ong Chong Tee.

But it is also true that in Singapore they care about cyber security. We read later in the same presentation: "Recently, we have created an enhanced role of a Chief Cybersecurity Officer as well as appointed a new Chief Data Officer."

Read more at number 7 below.

Albert Camus believed that retaliation is related to nature and instinct, not to law. Law, by definition, cannot obey the same rules as nature.

Perhaps this is the reason the EU has never officially started a retaliation process against UK after the Brexit, but only speaks about "a mechanism allowing the Union to suspend certain benefits deriving for the UK from participation in the internal market".

Of course, lawyers have their way - Quintus Horatius Flaccus (known in the English-speaking world as Horace) believed that lawyers are persons who hire out their words and anger.

The 18th of May, the European Insurance and Occupational Pensions Authority (EIOPA) has issued an opinion on the solvency position of insurers in light of the withdrawal of the United Kingdom (UK) from the European Union (EU).

According to the opinion, the UK's decision to withdraw from the European Union includes the UK leaving the European single market. The UK will become a third country for the purposes of applying the Solvency II framework after the withdrawal date. Until then the European Union legislative framework will remain in force in the UK.

After the withdrawal date, UK banks and investment firms will lose the MiFID passport to provide derivative services in the European Union. This could have an impact on the abilities of derivatives provided by UK banks and investment firms to transfer risk, after the withdrawal date.

UK insurance and reinsurance undertakings may not be able anymore to provide reinsurance services in some EU 27 Member States after the Withdrawal date unless they take measures to secure market access.

The scope of group supervision under Solvency II, depends in particular on whether the parent undertaking of the insurance group is located in the EU. For insurance, groups with a UK parent undertaking and subsidiaries across other Member States, the scope of group supervision will therefore change after the withdrawal date.

Group internal models can be used to calculate both the Solvency Capital Requirements (SCR) at group level, and the SCR at the level of insurance and reinsurance undertakings in the group. Where an insurance group with a UK parent undertaking applies such an internal model, it *cannot be used anymore* to calculate the SCRs of the insurance and reinsurance undertakings in the group that are located in the EU27 Member States, without re-approval by the national supervisory authority. In the absence of any other approved internal model, the SCR for these undertakings would have to be calculated on the basis of the standard formula.

National supervisory authorities should ensure that the insurance and reinsurance undertakings under their supervision identify, measure, monitor, manage and report the risks arising from the UK becoming a third country and include them in their own risk and solvency assessment.

Welcome to our monthly newsletter.

Best regards,

George Lekatis
General Manager, Cyber Risk GmbH
Rebackerstrasse 7, 8810 Horgen
Phone: +41 43 810 43 61
Email: george.lekatis@cyber-risk-gmbh.com
Web: www.cyber-risk-gmbh.com

Cyber Risk GmbH, Handelsregister des Kantons Zürich, Firmennummer: CHE-244.099.341

Our catalog, *in-house* instructor-led training in Switzerland, Liechtenstein and Germany:
www.cyber-risk-gmbh.com/Cyber_Risk_GmbH_Catalog_2018.pdf

Number 1 (Page 12)

NIST Updates Risk Management Framework to Incorporate Privacy Considerations

National Institute of Standards and Technology
U.S. Department of Commerce

The updated version adds an overarching concern for individuals' privacy, helping to ensure that organizations can better identify and respond to these risks, including those associated with using individuals' personally identifiable information.

The update will interest federal agencies and contractors that do business with them, as it connects the RMF with NIST's well-known Cybersecurity Framework (CSF), highlighting relationships that exist between the two documents.

Number 2 (Page 15)

Fake News and ENISA

Strengthening network and information security, protecting against online disinformation ("FAKE NEWS")

enisa European Union Agency for Network and Information Security

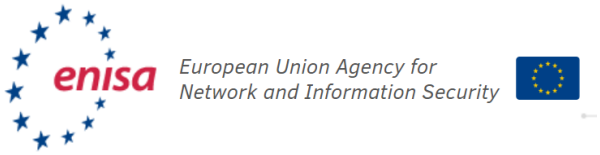
For the purpose of this paper, "online disinformation" is defined as: "false, inaccurate, or misleading online information designed, presented and promoted with malicious intent or for profit".

"Fake news" has recently received a lot of media attention as a potential disruptor of democratic processes globally.

There is a need to initiate a dialogue in the EU around the possible responses to this phenomenon.

Number 3 (Page 17)

The Value of Personal Online Data



A gold rush is ongoing within businesses operating in highly competitive markets looking for data and information about all aspects of human life such as consumer behaviour, social and political orientation, money spending habits, health, lifestyle, etc.

Data has become an important commodity generating profits on its own; and data collection has become the main activity for numerus businesses.

The collection and analysis of personal data is not only important for businesses but for society in general: policy decisions taken based on personal data analysis and medical research using patients and caregivers data to improve healthcare are just few examples. While the benefits from collecting and analysing personal data are evident for a large number of actors/organisation, various interests recurrently challenge its protection.

This cybersecurity info note reviews recent challenges in data protection and the impact to our society on the occasion of the abuse of 87 million Facebook profiles for the purpose of US election campaigns through Cambridge Analytica.

Number 4 (Page 21)

Cyber Security Breaches Survey 2018

The Cyber Security Breaches Survey is a quantitative and qualitative survey of UK businesses and, for the first time in this 2018 release, charities.

The quantitative survey was carried out in winter 2017 and the qualitative survey in early 2018.

Number 5 (Page 22)

NSA declassified document

VENONA - The U.S. Army's Signal Intelligence Service, the precursor to the National Security Agency, began a secret program in February 1943, later codenamed VENONA.

The mission of this small program was to examine and exploit Soviet diplomatic communications but after the program began, the message traffic included espionage efforts as well.

Number 6 (Page 24)

Gremlins on Track for Demonstration Flights in 2019

Airborne launch and recovery of low-cost unmanned aerial systems could enhance combat operations in contested areas, present significant per-mission cost savings

DARPA is progressing toward its plan to demonstrate airborne launch and recovery of multiple unmanned aerial systems (UASs), targeted for late 2019.

Now in its third and final phase, the goal for the Gremlins program is to develop a full-scale technology demonstration featuring the air recovery of multiple low-cost, reusable UASs, or “gremlins.”

Safety, reliability, and affordability are the key objectives for the system, which would launch groups of UASs from multiple types of military aircraft while out of range from adversary defenses.

Once gremlins complete their mission, a C-130 transport aircraft would retrieve them in the air and carry them home, where ground crews would prepare them for their next use within 24 hours.

Number 7 (Page 26)

The future of banking - evolution, revolution or a big bang

Ong Chong Tee, Deputy Managing Director (Financial Supervision) of the Monetary Authority of Singapore, at the German-Singaporean Financial Forum, Singapore.

"(a) Last year, Chancellor Angela Merkel and Prime Minister Lee Hsien Loong met in Berlin in July, and later, President Halimah Yacob hosted President Frank-Walter Steinmeier during his state visit in November.

(b) Singapore was also invited to the G20 meetings in 2017 during Germany's Presidency.

The close partnerships at both government and business levels underscore the many common values and strategic interests that we share. For example, in the area of financial services, there is strong emphasis on financial institutions having high standards of conduct and prudence given the importance of savings and investment in our societies."

Number 1

NIST Updates Risk Management Framework to Incorporate Privacy Considerations

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Augmenting its efforts to protect the nation's critical assets from cybersecurity threats as well as protect individuals' privacy, the National Institute of Standards and Technology (NIST) has issued a draft update to its Risk Management Framework (RMF) to help organizations more easily meet these goals.

The RMF update, formally titled Draft NIST Special Publication (SP) 800-37 Revision 2, is a guidance document designed to help organizations assess and manage risks to their information and systems. Previous versions of the RMF were primarily concerned with cybersecurity protections from external threats.

The updated version adds an overarching concern for individuals' privacy, helping to ensure that organizations can better identify and respond to these risks, including those associated with using individuals' personally identifiable information.

The update will interest federal agencies and contractors that do business with them, as it connects the RMF with NIST's well-known Cybersecurity Framework (CSF), highlighting relationships that exist between the two documents.

"Until now, federal agencies had been using the RMF and CSF separately," said NIST's Ron Ross, one of the publication's authors. "The update provides cross-references so that organizations using the RMF can see where and how the CSF aligns with the current steps in the RMF. Conversely, if you're using the CSF, you can bring in the RMF and give your organization a robust methodology to manage security and privacy risks."

In addition to the RMF-CSF alignment, the update has several important objectives, including:

- Integrating security and privacy into systems development. Building security and privacy into information systems at the initial design stage is a major concern. The RMF also references NIST systems security engineering guidance at appropriate points, including NIST's SP 800-160 (link is external), which addresses the engineering of trustworthy secure systems.

- Connecting senior leaders to operations. The RMF provides guidance on how an organization's senior leaders can better prepare for RMF execution, as well as how to communicate their protection plans and risk management strategies to system implementers and operators.

- Incorporating supply chain risk management considerations. The RMF addresses growing supply chain concerns in the areas of counterfeit components, tampering, theft, insertion of malicious software and hardware, poor manufacturing and development practices, and other potential harmful activities that can impact an organization's systems and systems components.

- Supporting security and privacy safeguards. The RMF update will provide organizations with a disciplined and structured process to select controls from the newly developed consolidated security and privacy control catalog in NIST's SP 800-53, Revision 5.

Aligning the RMF with other NIST guidance and publications will provide clarity for federal agencies, which are required to implement multiple frameworks. While adhering to the CSF is voluntary for private companies, its use for the federal government is mandatory under Executive Order 13800.

Compliance with the RMF is mandatory for federal agencies in accordance with the Federal Information Security Modernization Act (FISMA (link is external)). The RMF is also required and in widespread use in the Department of Defense and the intelligence community.

"It was imperative for us to figure out how these frameworks fit together," Ross said. "Many agencies are trying to follow both."

Ross added that the privacy-enhanced RMF might be valuable to companies and organizations beyond the federal government, considering how high profile the subject of privacy has become of late.

"Many folks are discovering how vulnerable they are with respect to their personal information and may begin to demand some standard level of

protection," he said. "If such a demand occurs, the government will be looking for clearly stated requirements for privacy, privacy safeguards, and a disciplined and structured process on how those controls could be applied. The timing of this publication could not be any better."

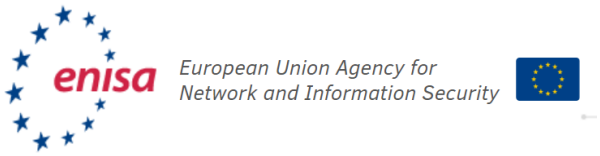
NIST is accepting comments from the public on the draft RMF until June 22, 2018. A final version will be issued in October 2018.

To read more:
https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/draft

Number 2

Fake News and ENISA

Strengthening network and information security, protecting against online disinformation ("FAKE NEWS")



For the purpose of this paper, "online disinformation" is defined as: "false, inaccurate, or misleading online information designed, presented and promoted with malicious intent or for profit".

"Fake news" has recently received a lot of media attention as a potential disruptor of democratic processes globally. There is a need to initiate a dialogue in the EU around the possible responses to this phenomenon.

In this regard, the misuse of:

- a computer connected to the internet,
- a compromised online account,
- a fake online account, or
- online platforms

may be characterised as a weapon, where posting on social media, emails, spam and other online activities can cause damage to others, as well as to society at large.

Recent events suggest that the dissemination of online disinformation is posing an increasing threat to the effective functioning of the democratic process.

This trend is exemplified by the 2016 U.S. presidential elections where, in a December 2016 survey, 64% of U.S. respondents held that fake news caused a great deal of confusion about the basic facts of contemporary events.

Subsequent allegations of cyber meddling in elections in the EU context reported in the media include the French presidential elections and the British EU membership referendum.

A key factor in the dissemination of online disinformation is human behaviour. According to research findings, false claims are shared more than true ones, and false stories gain more attention and are disseminated at a higher speed.

Equally important is the amplifier phenomenom, which concerns accounts that disseminate large amounts of false information aimed at manipulating public opinion.

In this paper, ENISA presents some views on the problem of online disinformation in the EU from a Network and Information Security (NIS) perspective.

A number of recommendations are presented, which relate both to general NIS measures, as well as targeted measures to protect against online disinformation specifically.

This opinion paper was presented as input to the European Commission's Communication "Tackling Online Disinformation: A European Approach", which was published in April 2018.

To read more:
https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/fake-news

Number 3

The Value of Personal Online Data

enisa European Union Agency for Network and Information Security

Introduction

Data is considered to be the gold of the digital age.

A gold rush is ongoing within businesses operating in highly competitive markets looking for data and information about all aspects of human life such as consumer behaviour, social and political orientation, money spending habits, health, lifestyle, etc.

Data has become an important commodity generating profits on its own; and data collection has become the main activity for numerus businesses.

The estimated ARPU (average revenue per user) in digital advertisement, mainly controlled by Google and Facebook, reached $59 per person in 2017.

Multiplying this number by an average 3.8 billion internet active users, we can roughly estimate the size of this business.

The collection and analysis of personal data is not only important for businesses but for society in general: policy decisions taken based on personal data analysis and medical research using patients and caregivers data to improve healthcare are just few examples.

While the benefits from collecting and analysing personal data are evident for a large number of actors/organisation, various interests recurrently challenge its protection.

This cybersecurity info note reviews recent challenges in data protection and the impact to our society on the occasion of the abuse of 87 million Facebook profiles for the purpose of US election campaigns through Cambridge Analytica.

Though this incident is at initial stages of analysis, there are grounds to believe that it is the top of the iceberg with regard to available practices in

harvesting user data, analysing and acting upon the results for a variety of objectives.

Contextual Information

The recent Facebook and Cambridge Analytica incident confirmed what was already known, at least within data privacy experts: online digital services use personal data to monetize their business models and politicians leverage from big data analytics to support election campaigns.

At a first glance, it has become public – revealed by a whistle-blower - that Facebook deliberately opened a door in 2013 for a third-party app to harvest personal data without the user's consent.

Cambridge Analytica - a British political consulting firm – obtained access to a database with personal data from 87 million Facebook accounts (initially estimated in 50 million) collected via a third-party app offering a free personality test quiz.

The owner of the app, Aleksandr Kogan a Cambridge University Psychology Professor, took advantage of a Facebook privacy breach and legally obtained consent from 200,000 users to access their personal data, including details about their friends who in any case were not in a position to provide their consent.

This way, the app owner increased the number of Facebook accounts accessed and the amount of personal data harvested by ca. 250 times. Moreover, according to the whistle-blower, a database with the harvested data was later shared with Cambridge Analytica, utilized for political analysis and Facebook advertisement in support of political campaigns.

In the attempt to apologise for the incident, Facebook CEO could not confirm which other third-party apps took advantage of this privacy breach between 2013 and 2015, and if other copies of the data possessed by Cambridge Analytic were distributed.

Furthermore, Facebook recently acknowledged a breach in its search engine and account recovery functions that it said could have exposed "most" of its 2 billion users to having their public profile information harvested.

Investigations over Facebook conduct and practices with regards of processing personal data (PII) and free movement of such data are not new.

In the past the Canadian Privacy Regulator, US Federal Trade Commission and EU Data Protection Authorities from UK, Ireland, Belgium, Norway and Germany scrutinized the practices of the social media giant imposing significant changes to its software. The European Union data protection acts, 1988 and 2003 - EU Data Protection Directive 95/46/EC - adopted in 1995 introduced important legislation into EU Member States legal systems, allowing the investigation of such incidents and consequent legal prosecution.

The General Data Protection Regulation (GDPR), due to come in force May 2018 superseding this directive, will have significant impact on companies such as Google, Facebook and Twitter who if proven, could face huge fines for this type of incidents.

Nonetheless, in the realm of this incident, there are some further investigations regarding various data collection activities that have been performed by Facebook in the past; and some debates are coming up regarding the consistency/coverage of privacy issues mentioned in user agreements.

Furthermore, a news media investigation uncovered the actions of Cambridge Analytica that included the use of personal data analytics to format political messages published in the social media in an attempt to manipulate the public opinion towards specific electoral candidates.

This revelation occurs while the civil society still debates and the judiciary investigates alleged foreign interference in the 2016 US presidential elections and UK Brexit referendum using social media adds and fake news.

This incident also demonstrated the power of big data analysis: service offerings go beyond traditional statistics and may support any objective related to human behaviour, such as supporting of election campaigns.

Cambridge Analytica publicly announced how their services influenced elections around the world.

Though formally lawful, such interventions may move usage of user data in grey zones.

The incident has made clear that a lot of discussion is still pending about data privacy issues and about potential regulation needs in the usage of big data.

Such regulation come to complement data protection regulation to cover appropriateness and legitimation of data analysis campaigns.

Recommendations

Users are advised to reevaluate their privacy settings in the digital world by taking the following actions:

- Avoid subscribing or installing suspicious third-party apps - Those are common on the network and most request access to personal data without the user noticing.

- Review which services or apps are sharing personal data – Digital platforms offer third-party authentication services to other applications. Users are advised to review which applications and services are connected to their accounts.

- Change privacy settings – Digital platforms have many privacy settings available to control who can have access to personal information.

- Review the privacy policy before subscribing to digital applications and services – Policies are long and hard to read but these are meant to inform users about their commitment to privacy protection.

Closing Remarks

People's confidence in digital players to protect their privacy has been recurrently undermined by these type of incidents, with serious impact in credibility and trust in the digital economy.

We cannot expect that data carers will proactively revert this situation by regulating themselves putting an end to a situation that ultimately generates large profits for them.

Since the start of this incident, Facebook already lost US $80 billion in market value (ca. 18% depreciation in stock price) followed by other social media giants Google (ca. 7%) and Twitter (ca. 20%).

The way the story evolves, it is premature to anticipate what will be the result and predict what will be the outlook of companies and business models that rely exclusively in the monetization of personal data.

Number 4

Cyber Security Breaches Survey 2018

Department for Digital, Culture, Media & Sport

Ipsos MORI Social Research Institute

University of Portsmouth

The Cyber Security Breaches Survey is a quantitative and qualitative survey of UK businesses and, for the first time in this 2018 release, charities.

The quantitative survey was carried out in winter 2017 and the qualitative survey in early 2018.

It helps these organisations to understand the nature and significance of the cyber security threats they face, and what others are doing to stay secure. It also supports the Government to shape future policy in this area.

Figure 3.2: Updates given to senior management on cyber security

To read more:
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/702074/Cyber_Security_Breaches_Survey_2018_-_Main_Report.pdf

Number 5

NSA declassified document

VENONA - The U.S. Army's Signal Intelligence Service, the precursor to the National Security Agency, began a secret program in February 1943, later codenamed VENONA.

The mission of this small program was to examine and exploit Soviet diplomatic communications but after the program began, the message traffic included espionage efforts as well.

> Further analysis showed that each one of the five systems was used exclusively by one of the following subscribers (listed in descending order according to the volume of message traffic which had been collected):
>
> 1. trade representatives – Lend-Lease, AMTORG, and the Soviet Government Purchasing Commission
>
> 2. diplomats – i.e., members of the diplomatic corps in the conduct of legitimate Soviet embassy and consular business
>
> 3. KGB – the Soviet espionage agency, headquarters in Moscow and residencies (stations) abroad
>
> 4. GRU – the Soviet Army General Staff Intelligence Directorate and attachés abroad
>
> 5. GRU-Naval – Soviet Naval Intelligence Staff

Although it took almost two years before American cryptologists were able to break the KGB encryption, the information gained through these transactions provided U.S. leadership insight into Soviet intentions and

treasonous activities of government employees until the program was canceled in 1980.

The VENONA files are most famous for exposing Julius (code named LIBERAL) and Ethel Rosenberg and help give indisputable evidence of their involvement with the Soviet spy ring.

The first of six public releases of translated VENONA messages was made in July 1995 and included 49 messages about the Soviets' efforts to gain information on the U.S. atomic bomb research and the Manhattan Project. Over the course of five more releases, all of the approximately 3,000 VENONA translations were made public.

To read more:
https://www.nsa.gov/news-features/declassified-documents/venona/

Note from the NSA:

"As NSA/CSS reviews records under the Freedom of Information Act or Mandatory Declassification Review provisions of Executive Order 13526, we will make the material available to the public via the NSA.gov website on the Internet. In addition, NSA/CSS periodically conducts "Special Topical Reviews" of categories of records, such as the Gulf of Tonkin, USS Liberty, UKUSA, and posts those records to this site. Lastly, in accordance with the federal Open Government initiative, we will identify subjects and records for which there is a general public interest. We will meet transparency goals by reviewing those records and including them on this web page."

Number 6

Gremlins on Track for Demonstration Flights in 2019

Airborne launch and recovery of low-cost unmanned aerial systems could enhance combat operations in contested areas, present significant per-mission cost savings

DARPA is progressing toward its plan to demonstrate airborne launch and recovery of multiple unmanned aerial systems (UASs), targeted for late 2019.

Now in its third and final phase, the goal for the Gremlins program is to develop a full-scale technology demonstration featuring the air recovery of multiple low-cost, reusable UASs, or "gremlins."

Safety, reliability, and affordability are the key objectives for the system, which would launch groups of UASs from multiple types of military aircraft while out of range from adversary defenses.

Once gremlins complete their mission, a C-130 transport aircraft would retrieve them in the air and carry them home, where ground crews would prepare them for their next use within 24 hours.

A recent flight test at Yuma Proving Ground provided an opportunity to conduct safe separation and captive flight tests of the hard dock and recovery system.

"Early flight tests have given us confidence we can meet our objective to recover four gremlins in 30 minutes," said Scott Wierzbanowski, program manager in DARPA's Tactical Technology Office.

In addition to preliminary flight tests, the team has focused on risk reduction via extensive modeling and simulation. The team looked at how fifth generation aircraft systems like the F-35 and F-22 respond to threats, and how they could incorporate gremlins in higher risk areas.

The gremlins' expected lifetime of about 20 uses could provide significant cost advantages by reducing payload and airframe costs, and by having lower mission and maintenance costs than conventional platforms, which are designed to operate for decades.

The C-130 is the demonstration platform for the Gremlins program, but Wierzbanowski says the Services could easily modify the system for another transport aircraft or other major weapons system. Modularity has made Gremlins attractive to potential transition partners.

“We are exploring opportunities with several transition partners and are not committed to a single organization. Interest is strong with both the roll-on/roll-off capability of the Gremlins system -- as it does not require any permanent aircraft modification -- and a wing-mounted system to provide greater flexibility to a wider range of aircraft,” said Wierzbanowski.

Gremlins also can incorporate several types of sensors up to 150 pounds, and easily integrate technologies to address different types of stakeholders and missions.

DARPA recently awarded a contract to a Dynetics, Inc.-led team to perform the Phase 3 demonstration. The DARPA program team currently is exploring the possibility of demonstrating different sensor packages with potential integration partners prior to program completion in 2019.

Number 7

The future of banking - evolution, revolution or a big bang

Ong Chong Tee, Deputy Managing Director (Financial Supervision) of the Monetary Authority of Singapore, at the German-Singaporean Financial Forum, Singapore.

Dr Johannes Beermann, Member of the Executive Board of the Deutsche Bundesbank, His Excellency Dr Ulrich Sante, Ambassador of the Federal Republic of Germany, Dr Claus Trenner, President of the Singaporean - German Chamber of Industry and Commerce, Distinguished Guests, Ladies and Gentlemen

It is my pleasure to join you this morning at the inaugural German - Singaporean Financial Forum.

Bilateral relations

Singapore and Germany have strong bilateral relations at many levels.

(a) Last year, Chancellor Angela Merkel and Prime Minister Lee Hsien Loong met in Berlin in July, and later, President Halimah Yacob hosted President Frank-Walter Steinmeier during his state visit in November.

(b) Singapore was also invited to the G20 meetings in 2017 during Germany's Presidency.

The close partnerships at both government and business levels underscore the many common values and strategic interests that we share. For example, in the area of financial services, there is strong emphasis on financial institutions having high standards of conduct and prudence given the importance of savings and investment in our societies.

MAS and our German counterparts, the Bundesbank and BaFin, participate in many international forums and standard-setting bodies including the Financial Stability Board, the Basel Committee on Banking Supervision, the International Association of Insurance Supervisors, and the International Organisation of Securities Commission.

On many issues, we share common interests and positions. In 2010, MAS and Bundesbank established a cross-border collateral arrangement to enhance liquidity provision by widening the pool of eligible collateral for banks.

MAS has a Supervisory Memorandum of Understanding (MOU) with BaFin that provides for mutual assistance and sharing of supervisory information in banking and insurance.

MAS also participates in the annual Deutsche Bank Supervisory College for non-EU regulators and we are pleased to have hosted the most recent one last November.

Given that financial activities are often cross-border in nature, such international co-operation will be of increasing importance, including to facilitate innovative services as well as to mitigate the risks that some these may present.

It is also in this spirit that I congratulate the establishment of this partnership forum. It is an excellent example of a co-operation platform that allows our industry players to engage one another in open discussions, to identify common challenges and working opportunities.

This forum also provides for perspectives from government, central bank, regulator and academia.

Future of banking

Allow me now to share some thoughts on the conference theme around the future of banking.

This is clearly a topical subject in the face of the ongoing Technology Revolution around us.

Many of us will probably have heard of the famous quote by Bill Gates, that "people do not need banks, they need banking".

In other words, with the rise of new FinTech players, activities that are considered banking services need not be provided by traditional banks alone.

Technology or e-commerce giants like Alibaba and Tencent have moved into the financial services space, as they seek to strengthen their customer-centric propositions and services.

Business disruptions need not be led only by the large firms. Smaller nimble start-ups have also sought to un-bundle the banking value chain by focusing on niche areas such as financial advisory services and consumer finance.

There are two underlying factors:

(a) One, is the arrival of the smartphones that launched a new era of mobile apps. Banking has moved from physical branches, to the desks, and now to the palm.

Recently, I read a report that British psychologists found that young adults use their smartphones roughly one-third of their total waking hours.

Simply put, all of us can now do banking anytime, anywhere. And many segments of our populations are increasingly comfortable going digital, be it for banking, or to purchase goods and services.

(b) Second, the accessibility afforded by technology has led banks to shift away from a production-consumption model. Traditional banking models are based on making available the range of the services that a customer need.

Today, competition centres on the customer experience. One of our local Singapore banks has a tag line on making banking joyful.
The notion of delighting a customer opens up a whole field of competitive ideas as to how to generate that positive experience. This is what the FinTech players have sought to do, and this is what banks are fighting back on. Banks will have the advantage of being highly regulated and trusted, that smaller and newer players may find it hard to challenge.

The general consensus is that many FinTechs and the established financial institutions will collaborate.

There is a natural synergy here:

(a) Collaboration with financial institutions enables FinTech players and technology firms to broaden their reach.

(b) On the flip side, FinTech solutions present established financial institutions with opportunities to enhance their product offerings or to improve operational productivity.

McKinsey estimated that enhancing digital capacity and adopting technologies could result in productivity gains worth roughly US$350 billion for the global banking industry by 2025.

But the competition will remain intense. Large internet-based firms with their massive customer base can be serious contenders for customer mind-share and wallets including in the area of financial services.

There is another development that has gained traction. We see the emergence of fully digital banks that operate entirely online with no physical branches, but are able to provide similar services as the traditional brick-and-mortar banks.

Fidor Bank, founded in Germany, is one such example. WeBank in China is another.

DBS' Digibank, a mobile-only bank in India, is also completely branchless and in less than two years, have signed up more than 1.5 million customers. All three have different origins and operate very different business models. I am sure the panellists later will discuss these further when they talk about the future of banking.

Let me turn to this forum's theme question on whether we will witness an evolution or revolution in banking. I believe it will be both. A lot of attention and excitement have been created by services going digital.

This digitisation of services have transformed the customer experience say for on-boarding or transactional purposes; but frankly, are not ground-breaking in themselves.

As one commentary noted, this is no different from reading an actual newspaper or reading the news online.

But a revolution is also happening when new digital services or business models emerge that employ say, artificial intelligence (AI) or blockchain technologies. These can fundamentally change how we borrow, save, pay, invest or insure.

As an example, there is a UK bank BABB that leverages totally on blockchain and biometrics to provide peer-to-peer financial services with the slogan of "everyone is a bank".

Time will determine the winners and losers as this cycle of technology disruption takes it course.

Open banking

Open Banking broadly captures the concept that a consumer owns information about himself, and should be able to share that information with any third party if he chooses, for example through APIs, and to transfer his money to any third party seamlessly.

The effect is to give consumers ownership over their financial data, to make that data portable, and therefore enables switching and choice among financial service providers. This should promote competition to improve pricing and service quality.

The EU has started on this journey by making payment and data interconnectivity between banks and non-banks mandatory, through the Payment Services Directive 2.

Australia has also announced that it will legislate a national Consumer Data Right in 2018, allowing consumers open access to all their data including banking-related ones.

While these hold a lot of promise by promoting consumer interests and welfare, there are other details to consider. For example, what primary data rightfully belongs to the customer, and what about secondary data about the customer that a bank had made sense of? How should a customer's data be packaged for onward sharing? How do we develop technical standards to share this information efficiently and securely? Who should pay for these?

In Singapore, we subscribe to the notion of banks sharing their data openly as a larger good. Some of the operational details have to be worked out. In MAS' engagement with the banking industry, there is broad consensus as to the benefits of open banking.

What we see is an opening up of customer data as a ground-up process led by the banks themselves. We believe this is a constructive development, that industry players themselves see the value in doing so.

Role of financial regulators

In my remarks so far, it should be obvious that financial regulators will have active roles in the business and technology transformation in the banking industry.

Regulators need to have a sharp understanding of emerging technologies and new business models, and to be alert to potential risks. Only then are we able to exercise thoughtful judgment.

There will be a balance between supporting innovation and technology use, while pre-empting new or heightened risks that these may present.

MAS takes an even-handed approach by providing a regulatory regime that is risk-proportionate across the range of institutions involved in regulated financial activities.

We seek to provide the environment, and even to encourage new FinTech and other players to establish themselves to compete, collaborate and innovate.

We allow for adoption of technology and innovation in financial services, especially those that hold promise in raising efficiency, in creating new opportunities, in enabling new or value-adding services or simply to manage risks better.

MAS adopts a "materiality and proportionality" test, and seeks to right-size regulations to be fit-for-purpose; for both traditional as well as new business models, according to the risks the activity poses.

For example, in the new Payment Services Bill that MAS has consulted on, regulatory requirements for payment activities will be differentiated according to the risks that specific activities pose rather than apply a uniform set of regulations on all payment service providers.

Regulation comes in when the risk posed becomes material or crosses a threshold. The weight of regulation must be proportionate to that risk. Singapore is one of the first jurisdictions to have established regulatory sandboxes where firms can experiment their innovative solutions in a contained environment, with access to a limited pool of actual customers.

What we will diligently protect is the trust and credibility in our financial system. We will also be paying closer attention to financial institutions' management of cyber-threats and to new forms of financial stability vulnerabilities as digitisation blurs the boundaries across geography and industries.

Recently, we have created an enhanced role of a Chief Cybersecurity Officer as well as appointed a new Chief Data Officer. I believe there is much we

can share and learn from other central banks, financial regulators and even law enforcement agencies, such as our European counterparts.

Looking ahead

Finally, there are other areas that should matter to all of us amidst the ongoing transformations in the banking industry.

One is the important issue of financial inclusion. In the quest to innovate and as banks develop the sophistication to sharpen the profile of each customer, we should not overlook the need for financial inclusion - especially access to basic banking and financial services for under-served communities.

Another area is in the responsible use of technology tools. Earlier this month, MAS announced the setting up of a regulator-industry grouping to co-create a guide to promote the responsible and ethical use of AI and data analytics by financial institutions.

This Committee is known by its acronym FEAT - which stands for Fairness, Ethics, Accountability and Transparency. This gives you a good idea of its mandate. The key is as technology and data analytics usage become more prevalent, the responsible use of these is equally paramount.

Conclusion

To conclude my remarks, allow me to resurrect a quote from a speech by President Kennedy in 1966, which I thought is apt even in current times.

[quote] There is a Chinese curse which says 'May he live in interesting times'. Like it or not we live in interesting times. They are times of danger and uncertainty; but they are also more open to the creative energy of men than any other time in history. [unquote]

Many will agree that we are living in interesting times; and a forum like this will be useful in bringing together the constructive and creative energy of experts like yourselves to share, to understand and to co-operate.

Ultimately, it falls on all of us to do our part to make the future more promising and enriching for this and the generation that follows.

Thank you

Disclaimer

Despite the great care taken to prepare this newsletter, we cannot guarantee that all information is current or accurate. If errors are brought to our attention, we will try to correct them, and we will publish the correct information to the LinkedIn and Facebook pages of Cyber Risk GmbH.

Readers will make their own determination of how suitable the information is for their usage and intent. Cyber Risk GmbH expressly disclaims all warranties, either expressed or implied, including any implied warranty of fitness for a particular purpose, and neither assumes nor authorizes any other person to assume for it any liability in connection with the information or training programs provided.

Cyber Risk GmbH and its employees will not be liable for any loss or damages of any nature, either direct or indirect, arising from use of the information provided on this newsletter, or our web sites.

We are not responsible for opinions and information posted by others. The inclusion of links to other web sites does not necessarily imply a recommendation or endorsement of the views expressed within them. Links to other web sites are presented as a convenience to users. Cyber Risk GmbH does not accept any responsibility for the content, accuracy, reliability, or currency found on external web sites.

This information:

- is of a general nature only and is not intended to address the specific circumstances of any particular individual or entity;

- should not be relied on in the particular context of enforcement or similar regulatory action;

- is not necessarily comprehensive, complete, or up to date;

- is sometimes linked to external sites over which the association has no control and for which the association assumes no responsibility;

- is not professional or legal advice (if you need specific advice, you should always consult a suitably qualified professional);

- is in no way constitutive of interpretative;

- does not prejudge the position that the relevant authorities might decide to take on the same matters if developments, including Court rulings, were to lead it to revise some of the views expressed here;

- does not prejudge the interpretation that the Courts might place on the matters at issue.

Please note that it cannot be guaranteed that these information and documents exactly reproduce officially adopted texts. It is our goal to minimize disruption caused by technical errors. However, some data or information may have been created or structured in files or formats that are not error-free and we cannot guarantee that our service will not be interrupted or otherwise affected by such problems.

Readers that are interested in a specific topic covered in the newsletter, must download the official papers, must find more information, and must ask for legal and technical advice, before making any business decisions.