January 2019, cyber risk and compliance in Switzerland

Top cyber risk and compliance related local news stories and world events

Dear readers,

From January to April 2019, Switzerland chairs the Forum for Security Co-operation (FSC) of the Organization for Security and Co-operation in Europe (OSCE).

The Organization for Security and Co-operation in Europe (OSCE), with 57 participating States in North America, Europe and Asia, is the world's largest regional security organization. The OSCE works for stability, peace and democracy for more than a billion people, through political dialogue about shared values and through practical work that aims to make a lasting difference.

The OSCE is a forum for political dialogue on a wide range of security issues and a platform for joint action to improve the lives of individuals and communities. The organization uses a comprehensive approach to security that encompasses the politico-military, economic and environmental, and human dimensions.

Through this approach, and with its inclusive membership, the OSCE helps bridge differences and build trust between states by co-operating on conflict prevention, crisis management and post-conflict rehabilitation.

The Forum for Security Co-operation (FSC) works to increase military security and stability in Europe, and covers some of the most fundamental politico-military agreements of the OSCE participating States. It helps implement landmark confidence and security-building measures to regulate the exchange of military information and mutual verification between states, as well as the Code of Conduct, a key document ensuring the democratic control of security forces.

The Forum also develops norms and provides practical assistance to address the proliferation of illicit small arms and light weapons; deals with non-proliferation of weapons of mass destruction; and oversees the regular contact, co-operation, and sharing of military information among the participating States.

On 16 January 2019, the FDFA's State Secretary Pascale Baeriswyl travelled to Vienna for the first of a dozen meetings to be held over the next four months within the Forum for Security Co-operation.

The FDFA has joined forces with the DDPS to organize the chairmanship. The Forum's chairmanship changes every four months among the participating States in alphabetical order, with Switzerland taking over from Sweden.

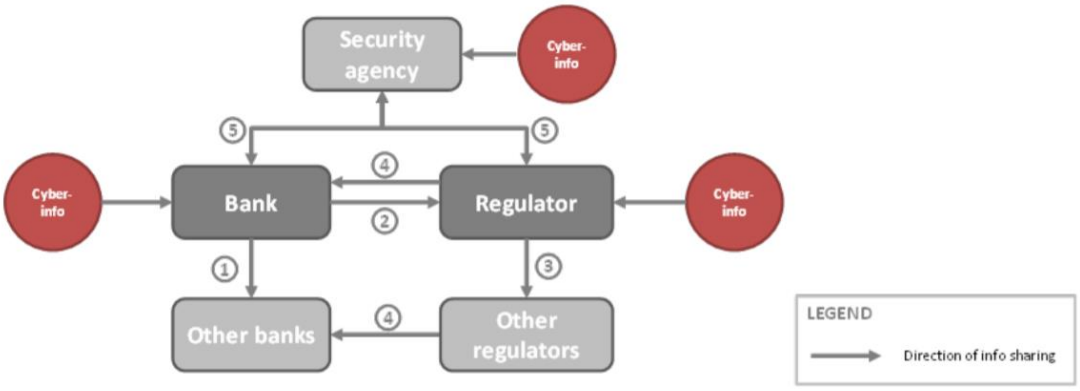
Following its chairmanship of the OSCE in 2014, Switzerland now has an opportunity to actively bring in its interests within the politico-military dimension of the FSC.

Switzerland will contribute in areas in which it has substantial expertise, including small arms, the regulation of private military and security companies, and UN Security Council Resolution 1325 on women, peace and security. Its activities will be guided by the model of its OSCE chairmanship in 2014, which emphasized Creating a security community for the benefit of everyone.

I have just read an interesting new paper from the Basel Committee, with the title *Cyber-resilience: Range of practices*. The paper answers a very important question: Do banks share cyber-security information with regulators?

We read: "The sharing of cyber-security information from a bank to its regulator(s)/supervisor(s) is generally limited to cyber-incidents based on regulatory reporting requirements.

Figure 1: Interlinkage of different types of cyber-security information-sharing practices (1)



(1) the numbered circles next to the arrows indicate the "types" of info sharing as described in section 5.1 and Figure 2
Source: Basel Committe on Banking Supervision.

Such requirements are mainly established to:

(i) enable systemic risk monitoring of the financial industry by regulator(s);

(ii) enhance regulatory requirements or issue recommendations by regulator(s) to adjust policies and strategies based on information collected;

(iii) allow appropriate oversight of incident resolution by regulator(s); and

(iv) facilitate further sharing of information with industry and regulators to develop a cyber-risk response framework.

Reporting requirements are established by different authorities for specific purposes depending on their mandate (eg supervisory and regulatory functions, consumer protection and further distribution of information to national cyber-security agencies for systemic operators).

Incident reporting by banks to regulator(s) is a mandatory requirement in many jurisdictions, with different scopes of requirements and ranges of application.

For jurisdictions already enforcing the requirement in the past, the reporting obligation has a broader operational incident scope, including cyber-incidents.

The perimeter can include all supervised institutions but is more often limited to systemically important institutions.

Nearly all institutions regulated in the EU are required to report cyber-security incidents to the competent authorities.

The requirements stem from supervisory frameworks (such as the Single Supervisory Mechanism (SSM) cyber-incident reporting framework), EU directives (PSD2, NIS) and local law.

Some requirements also include the obligation to submit a root cause analysis for the incident, or a full post-mortem or lessons learnt after the incident.

Different scopes and perimeters may depend on the type of authority (eg supervisors, regulators, national security) and their mandate (ie national cyber-security agencies, consumer protection, banking supervision, etc), sector(s) involved (eg multisector or specific: banks, significant banks, systemic operators, payment) and geographical range (eg national, multiregional).

While many of the supervisors focus only on reporting and tracking incidents that have already taken place, some require proactive monitoring and tracking of potential cyber-threats because concerns about reputational risk may lead to a delay in incident reporting by the regulated entity.

Based on these considerations, different reporting frameworks are also observed.

These range from formal communications to informal communications (eg free-text updates via email or verbal updates over the phone).

Differences are noted in:

(i) taxonomy for reporting;

(ii) reporting time frame (immediately, after two hours, after four hours and after 72 hours are examples of practices observed);

(iii) templates; and

(iv) threshold to trigger an incident reporting."

Read more at Number 4 below.

The *Cyber Europe 2018 After Action Report* of the European Network and Information Security Agency (ENISA) is very interesting. It describes the simulation of an intense realistic crisis caused by a large-number of cybersecurity incidents that occurred during the two-days, 6-7 June 2018.

The detailed scenario of the exercise consisted of numerous materials including:

- Structured and unstructured, useful and misleading data scattered in simulated online blogs, magazines, forums and file storage infrastructure;

- Thousands of simulated personal and professional social media profiles on multiple simulated platforms;

- A simulated news channel, depicting the event through filmed news in a realistic fashion, supported by simulated formal news websites containing hundreds of news articles and formal news websites;

- Hundreds of tailor-made documents supporting the scenario for participants to analyse, from technical incident material to legal and public affairs documents.

During the exercise, live media pressure was simulated by real journalists who were continually contacting players to ask for information.

Real-time response by the experts was noted, while dynamic media reactions in simulated social media were added by the journalists.

The scenario was set around the concept of the worldwide rise of extremism.

This 'virtually invisible' phenomenon has turned into an open and widespread one with several different facets, from religion to political beliefs, engaging thousands of followers and millions of supporters.

The number of radical websites has increased exponentially since 2013 and extremists are utilising social media to recruit and organise.

The increase of the followers of this extremism lead to their engagement in cyber-attacks. Radical groups could use advanced or less advanced techniques to strike at any time as they revealed the internet to be a hotbed of radicalisation.

A new radicalistic movement, without a central organisation has a powerful arsenal of cyber-attack techniques with capabilities, such as exfiltration, traffic capturing and logging, keylogging, ransomware, hybrid attacks with drones, IoT infectors, worms, etc.

Read more at Number 2 below.

Welcome to our monthly newsletter.

Best regards,

George Lekatis

George Lekatis
General Manager, Cyber Risk GmbH
Rebackerstrasse 7, 8810 Horgen
Phone: +41 43 810 43 61
Mobile: +41 79 505 89 60
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 updated catalog:
https://www.cyber-risk-gmbh.com/Cyber_Risk_GmbH_Catalog_2019.pdf

Number 1 (Page 10)

Switzerland to bring new perspective to politico-military issues during Forum for Security Co-operation Chairmanship, says State Secretary Baeriswyl

Switzerland aims to bring a new perspective to established and current politico-military issues, said the State Secretary of the Swiss Federal Department of Foreign Affairs, Pascale Baeriswyl, as she opened the country's Chairmanship of the Forum for Security Co-operation (FSC) in Vienna.

Baeriswyl added that Switzerland will engage in dedicated discussions and constructive debates to achieve more confidence and transparency on politico-military issues amongst all 57 OSCE participating States.

Number 2 (Page 12)

Cyber Europe 2018 - After Action Report

Cyber Europe 2018 was the fifth pan-European cyber crisis exercise organised by the European Union Agency for Network and Information Security (ENISA).

Number 3 (Page 15)

Zuckerberg's update on addressing abuse from bad actors on Facebook

"For 2018, my personal challenge has been to focus on addressing some of the most important issues facing our community -- whether that's preventing election interference, stopping the spread of hate speech and misinformation, making sure people have control of their information, and ensuring our services improve people's well-being. In each of these areas, I'm proud of the progress we've made."

Number 4 (Page 18)

Cyber-resilience: range of practices

BIS

The Basel Committee on Banking Supervision has published a report that identifies, describes and compares the range of observed cyber-resilience practices across jurisdictions.

Number 5 (Page 21)

Confidential data loss in Denmark

National Cyber Security Centre
a part of GCHQ

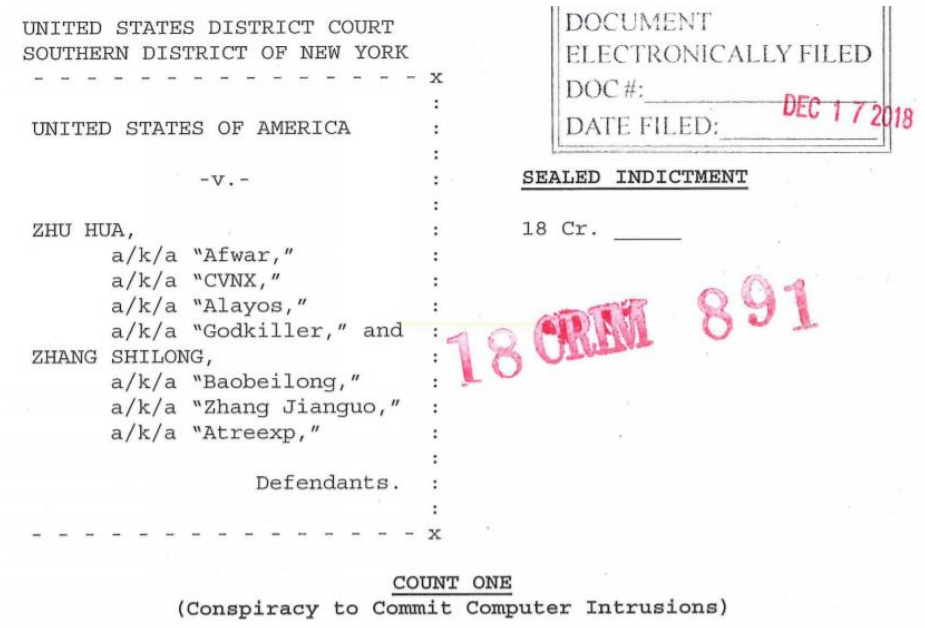
Confidential data of 20,000 residents in Gladsaxe, Denmark has been lost following the theft of a computer from the town's city hall between November 30th and December 3rd.

The data had been saved locally and included information such as registration numbers, age and addresses. Details of social welfare payments and housing were also reported as being affected.

Number 6 (Page 22)

DOJ charges Chinese nationals in cyber espionage campaign

The indictment was filed by prosecutors with the U.S. attorney's office in the Southern District of New York.



UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA

-v.-

ZHU HUA,
a/k/a "Afwar,"
a/k/a "CVNX,"
a/k/a "Alayos,"
a/k/a "Godkiller," and
ZHANG SHILONG,
a/k/a "Baobeilong,"
a/k/a "Zhang Jianguo,"
a/k/a "Atreexp,"

Defendants.

DOCUMENT
ELECTRONICALLY FILED
DOC #:
DATE FILED: DEC 17 2018

SEALED INDICTMENT

18 Cr. _____

18 CRIM 891

COUNT ONE
(Conspiracy to Commit Computer Intrusions)

Number 7 (Page 23)

Amazon Customers Made This Holiday Season Record-Breaking with More Items Ordered Worldwide Than Ever Before

Customers used Alexa to listen to hundreds of millions more hours of music this holiday season compared to last holiday season, and on even more services – including Amazon Music, Spotify, Tidal, and Apple Music, among others.

Customers asked Alexa to turn on their holiday lights tens of millions of times this holiday season, with the number one request being "Alexa, turn on the Christmas tree."

Number 8 (Page 26)

The State of IT Security in Germany 2018

Federal Office for Information Security

Cyber attack on German authorities

Towards the end of 2017, the BSI received indications of a successful cyber attack via the National Cyber Defence Centre, which purported to affect individual German federal authorities.

The BSI started the incident handling process in coordination with the authorities involved in the National Cyber Defence Centre, informed the authorities that were potentially affected and began the analysis and verification of the information initially available.

Number 9 (Page 28)

Brief summary, 2017 Report on the Protection of the Constitution, Facts and Trends

Federal Ministry of the Interior, Building and Community

Espionage and other intelligence activities

States which strive to gain a knowledge edge in military (particularly strategic) or economic and technological contexts do not hesitate to procure the necessary information secretly and illegally by violating applicable law.

Number 10 (Page 31)

Supporting the Fight Against Cybercrime: ENISA report on CSIRTs and Law Enforcement Cooperation

enisa European Union Agency for Network and Information Security

The fight against cybercrime, requires the involvement of Law Enforcement Agencies, which supported by CSIRTS are likely to be better positioned to investigate complex criminal structures.

This cooperation is incomplete however, unless the judiciary is equally brought into the picture due to the pre-eminent role it plays across the MS in directing criminal investigations.

Number 11 (Page 33)

Hackers threaten to leak 9/11 litigation documents

National Cyber Security Centre
a part of GCHQ

A cyber crime group calling itself 'The Dark Overlord' continues to threaten to release stolen files from US law firms and a London-based plastic surgery clinic if ransom demands are not met.

The FBI is investigating the theft of 18,000 insurance and legal documents relating to the September 11 attacks on the World Trade Centre.

Number 12 (Page 35)

German politicians and celebrities caught in Christmas data leak

National Cyber Security Centre
a part of GCHQ

Over Christmas, personal information and alleged communications belonging to German politicians, journalists, and celebrities were leaked on Twitter, under the username @_orbit. The information was published in the style of an "advent calendar event" each day in December.

The data breach reportedly included politicians' email addresses, mobile phone numbers, identity card photos, direct debit and credit card information, and personal and work communications.

Number 1

Switzerland to bring new perspective to politico-military issues during Forum for Security Co-operation Chairmanship, says State Secretary Baeriswyl

Switzerland aims to bring a new perspective to established and current politico-military issues, said the State Secretary of the Swiss Federal Department of Foreign Affairs, Pascale Baeriswyl, as she opened the country's Chairmanship of the Forum for Security Co-operation (FSC) in Vienna.

Baeriswyl added that Switzerland will engage in dedicated discussions and constructive debates to achieve more confidence and transparency on politico-military issues amongst all 57 OSCE participating States.

In her opening speech, Baeriswyl recognized the unique potential of the FSC as a platform with a wide range of tools at its disposal to approach complex politico-military questions "in an inclusive and pragmatic manner". However, she also acknowledged the difficulty of implementing the Swiss Chair's core principles of co-operation and pragmatism during this currently challenging political climate.

Switzerland plans to encourage openness to new ideas, topics and expertise. New ideas will allow the FSC to explore "the potential of existing tools and commitments," said Baeriswyl.

Moreover, the Swiss State Secretary reminded OSCE participating States to reinforce their adherence to existing commitments, urging them to reflect and remind themselves of the principles of the Helsinki Decalogue and the Charter of Paris, as they build the core of the agreed OSCE principles.

Turning to the programme of the Swiss Chairmanship, which will extend to the end of the Easter recess, Baeriswyl said the focus will be on both established and newer aspects of political and military security: Well-established FSC topics such as small arms and light weapons, stockpiles of conventional ammunition and the Vienna Document on Confidence- and Security-Building Measures and the OSCE Code of Conduct on Politico-Military Aspects of Security will be analyzed from different angles. Emerging topics and challenges, such as the role of private military and security companies, and aspects of modern warfare will also be addressed.

A running theme throughout the Chairmanship will be gender equality in the field of peace and security, she said, adding that Switzerland defines gender equality as "an equal partnership between women and men". As well as chairing a Security Dialogue on UN Security Council Resolution 1325 on Women, Peace and Security, Switzerland would bring gender to the next level of the security debate by replacing the 'why' with the 'how'.

Baeriswyl expressed her thanks to Sweden, which chaired the FSC during the previous trimester, and said that she looked forward to working in the FSC Troika with both the outgoing Chair and Tajikistan, which will chair the FSC in the second trimester of the year.

She said Switzerland will fully coordinate its FSC programme with Slovakia, which is chairing the OSCE in 2019.

Number 2

Cyber Europe 2018 - After Action Report

Cyber Europe 2018 was the fifth pan-European cyber crisis exercise organised by the European Union Agency for Network and Information Security (ENISA).

The exercise engaged around 900 participants, from the public authorities and private companies, mainly in the Aviation sector, from all 28 EU Member States as well as two European Free Trade Association (EFTA) countries, Norway and Switzerland.

The exercise simulated an intense realistic crisis caused by a large-number (over 600 hundred) of cybersecurity incidents that occurred during the two-days, 6-7 June 2018.

The exercise was built on three main pillars:

- The sound use of business continuity and crisis management plans within an organisation

- National-level cooperation and use of contingency plans

- Cross-country cooperation and information exchange

In addition, the exercise gave the opportunity to the technical teams to test their skills in cybersecurity with a vast variety of technical challenges, including malware analysis, forensics, mobile malware, APT attacks, network attacks, IoT device infection, etc.

The exercise brought up the importance of cooperation between the different actors (victims and authorities) of simulated cybersecurity incidents, security providers and national authorities.

It proved to the participants that only by information exchange and collaboration, it is possible to respond to such extreme situations with a large number of simultaneous incidents.

We have witnessed a large number of instances of public–private and private–private cooperation.

Participants had to follow existing business processes, agreements, communication protocols and regulations to mitigate effectively the situations presented to them.

Nevertheless, the level of preparedness varied significantly between participants, the information flow felt sometimes to be unidirectional and structured private-public cooperation procedures were immature or non-existent.

The EU Network and Information Security (NIS) directive identifies many of the associated shortcomings and proposes measures to improve the situation.

The EU-level cooperation has been undoubtedly improved over the last years.

In particular, the technical-level cooperation has proven mature and effective.

The introduction of the CSIRTs Network (CNW) as defined in the NIS directive has provided EU Member States with an effective formal structure to exchange technical information but also to collaborate in order to resolve complex, large-scale incidents.

The exercise proved that at this level EU is well equipped to respond.

Some minor gaps were identified and have been already tackled by those involved.

On the other hand, the operational-level cooperation was exercised to a lesser extent. It is not so obvious how in real-life these levels will interact and furthermore how they will implement the strategic vision of the political leaders.

Future exercises shall try to test these aspects as well.
Finally, the technical incidents of the exercise provided an excellent opportunity for the cybersecurity teams to enhance their capabilities and expertise to deal with a variety of cybersecurity challenges.

The operational capacity as well as the technical skills in all participating organisation proved to be at the highest level.

Participating teams from non cybersecurity private companies in the Aviation sector analysed the majority of incidents successfully, and proved that their skillset in certainly very high.

The only shortcoming in some cases was not the lack of skills but the actual number of available resources for IT security.

This is a challenge that has be tackled by the higher management, since the return on investment (ROI) in cybersecurity expertise is definitely high for such critical sectors.

To read more:
https://www.enisa.europa.eu/publications/cyber-europe-2018-after-action-report

Number 3

Zuckerberg's update on addressing abuse from bad actors on Facebook

For 2018, my personal challenge has been to focus on addressing some of the most important issues facing our community -- whether that's preventing election interference, stopping the spread of hate speech and misinformation, making sure people have control of their information, and ensuring our services improve people's well-being. In each of these areas, I'm proud of the progress we've made.

We're a very different company today than we were in 2016, or even a year ago. We've fundamentally altered our DNA to focus more on preventing harm in all our services, and we've systematically shifted a large portion of our company to work on preventing harm. We now have more than 30,000 people working on safety and invest billions of dollars in security yearly.

To be clear, addressing these issues is more than a one-year challenge. But in each of the areas I mentioned, we've now established multi-year plans to overhaul our systems and we're well into executing those roadmaps. In the past we didn't focus as much on these issues as we needed to, but we're now much more proactive.

That doesn't mean we'll catch every bad actor or piece of bad content, or that people won't find more examples of past mistakes before we improved our systems. For some of these issues, like election interference or harmful speech, the problems can never fully be solved.

They're challenges against sophisticated adversaries and human nature where we must constantly work to stay ahead. But overall, we've built some of the most advanced systems in the world for identifying and resolving these issues, and we will keep improving over the coming years.

We've made a lot of improvements and changes this year, and here are some of the most important ones:

For preventing election interference, we've improved our systems for identifying the fake accounts and coordinated information campaigns that account for much of the interference -- now removing millions of fake accounts every day.

We've partnered with fact-checkers in countries around the world to identify misinformation and reduce its distribution. We've created a new standard for advertising transparency where anyone can now see all the ads an advertiser is running to different audiences.

We established an independent election research commission to study threats and our systems to address them. And we've partnered with governments and law enforcement around the world to prepare for elections.

For stopping the spread of harmful content, we've built AI systems to automatically identify and remove content related to terrorism, hate speech, and more before anyone even sees it. These systems take down 99% of the terrorist-related content we remove before anyone even reports it, for example.

We've improved News Feed to promote news from trusted sources. We're developing systems to automatically reduce the distribution of borderline content, including sensationalism and misinformation.

We've tripled the size of our content review team to handle more complex cases that AI can't judge.

We've built an appeals system for when we get decisions wrong. We're working to establish an independent body that people can appeal decisions to and that will help decide our policies.

We've begun issuing transparency reports on our effectiveness in removing harmful content. And we've also started working with governments, like in France, to establish effective content regulations for internet platforms.

For making sure people have control of their information, we changed our developer platform to reduce the amount of information apps can access -- following the major changes we already made back in 2014 to dramatically reduce access that would prevent issues like what we saw with Cambridge Analytica from happening today.

We rolled out new controls for GDPR around the whole world and asked everyone to check their privacy settings. We reduced some of the third-party information we use in our ads systems.

We started building a Clear History tool that will give people more transparency into their browsing history and let people clear it from our systems.

And we've continued developing encrypted and ephemeral messaging and sharing services that we believe will be the foundation for how people communicate going forward.

For making sure our services improve people's well-being, we conducted research that found that when people use the internet to interact with others, that's associated with all the positive aspects of well-being you'd expect, including greater happiness, health, feeling more connected, and so on. But when you just use the internet to consume content passively, that's not associated with those same positive effects.

Based on this research, we've changed our services to encourage meaningful social interactions rather than passive consumption. One change we made reduced the amount of viral videos people watched by 50 million hours a day.

In total, these changes intentionally reduced engagement and revenue in the near term, although we believe they'll help us build a stronger community and business over the long term.

To read more you may visit:
https://www.facebook.com/zuck/posts/10105865715850211

Number 4

Cyber-resilience: range of practices

The Basel Committee on Banking Supervision has published a report that identifies, describes and compares the range of observed cyber-resilience practices across jurisdictions.

Based on analysis of authorities' responses to previous international surveys and on exchanges between international experts, the report gains insight into the effective practices and expectations in place.

It also benefited from industry participants' input.

The current challenges and initiatives to enhance cyber-resilience are summarised in 10 key findings and illustrated by case studies which focus on concrete developments in the jurisdictions covered.

1. General Landscape.

Despite convergence in high level expectations, the technical specifications and supervisory practices differ across jurisdictions.

This diversity of approaches results in a complex and fragmented landscape, but is also a necessary reflection of actual differences in Members' legal frameworks and degree of digitalisation.

2. Strategy.

Regulators generally do not require a specific cyber strategy, however institutions are expected to ensure that systems are "secure-by-design" and that emphasis is placed on resilience in light of current threats rather than compliance to a standard.

3. Cyber risk management.

In most jurisdictions broader IT and operational risk management practices are more mature and are used to address cyber risk and supervise cyber resilience.

4. Governance / organisation.

Models such as "three lines of defence" are widely adopted, but cyber resilience is not always clearly articulated across the technical, business and strategic lines, which hampers their effectiveness.

5. Workforce.

Skills shortage leads to recruitment challenges. A few jurisdictions have implemented or leveraged specific cyber certifications to address this.

6. Testing.

Protection and detection testing is evolving and prevalent; response and recovery less so.

7. Incident response.

Although an incident management framework is not required, incident response plans are.

8. Metrics.

Although some forward-looking indicators of cyber resilience are being picked up through the most widespread supervisory practices, no standard set of metrics has emerged yet.

9. Information sharing.

The content and use of information collected or shared by banks and supervisors varies widely across jurisdictions. The speed, latitude and security of communications required to cope with a cross-border cyber incident has led a few jurisdictions to take specific formal steps in this area.

10. Third party risk.

Regulatory frameworks for outsourcing activities across jurisdictions are quite established and share substantial commonalities, but there is no common approach regarding third parties beyond outsourced services.

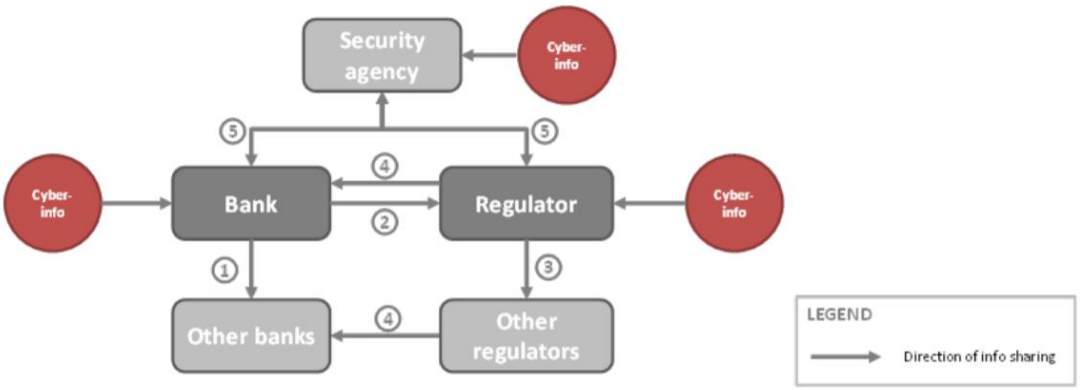
While third parties may provide cost-effective solutions to increase resilience levels, the onus remains on the banks to demonstrate adequate understanding and active management of the third party dependencies and concentration across the value chain.

By describing the diversity of approaches thematically, the report will help banks and supervisors navigate the regulatory environment and will serve as useful input for identifying areas where further policy work by the Committee may be warranted.

Going forward, the Committee will integrate the cyber dimension into its broader operational resilience work.

To read the report:
https://www.bis.org/bcbs/publ/d454.pdf

Figure 1: Interlinkage of different types of cyber-security information-sharing practices (1)



(1) the numbered circles next to the arrows indicate the "types" of info sharing as described in section 5.1 and Figure 2
Source: Basel Committe on Banking Supervision.

Number 5

Confidential data loss in Denmark

National Cyber Security Centre
a part of GCHQ

Confidential data of 20,000 residents in Gladsaxe, Denmark has been lost following the theft of a computer from the town's city hall between November 30th and December 3rd.

The data had been saved locally and included information such as registration numbers, age and addresses. Details of social welfare payments and housing were also reported as being affected.

Local authorities had informed those affected by Monday 3rd blaming the issue on human error following a spreadsheet being saved locally on the computer as a temporary measure.

Ensuring personal data is secure should be at the top of any priority list, and the NCSC has guidance aimed at protecting bulk data at: https://www.ncsc.gov.uk/guidance/protecting-bulk-personal-data-main

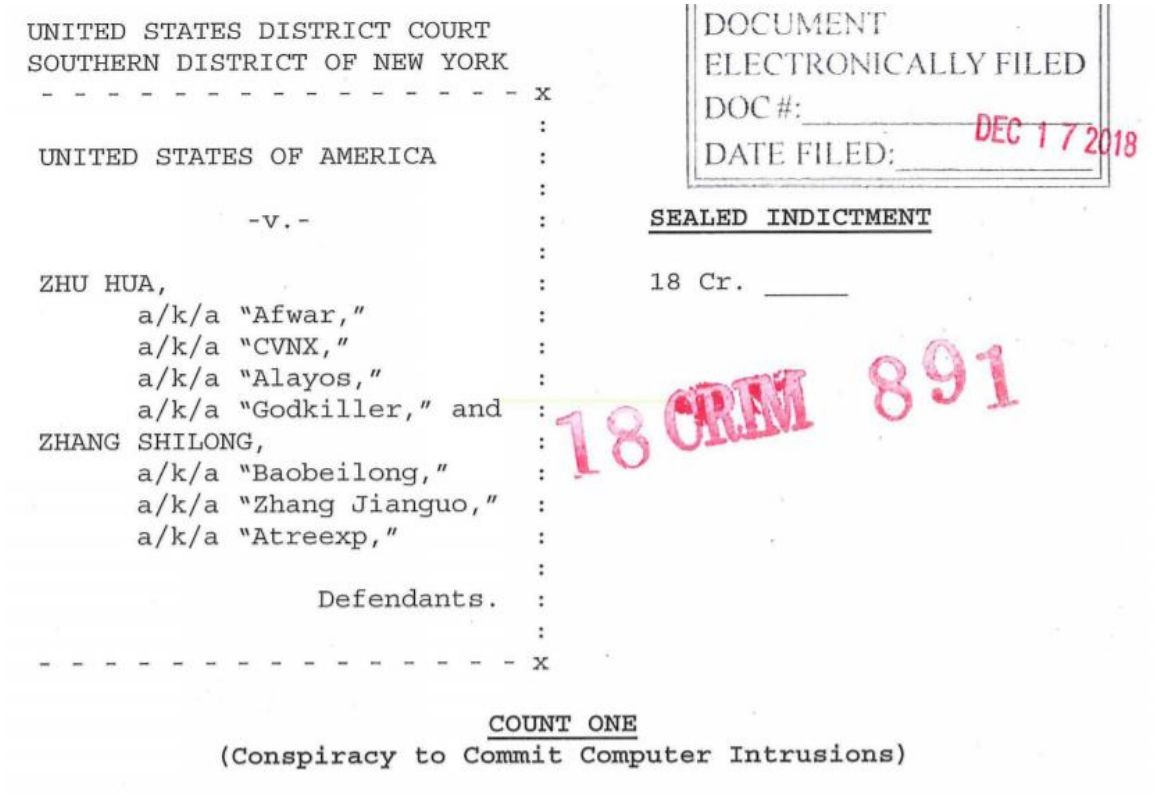
Organisations shouldn't look to pass blame onto employees following this kind of incident. The likelihood is that the employee was acting in good faith to ensure a business need was met. The NCSC encourages adding extra layers of resilience to support employees and use incidents such as this as a learning opportunity.

It's well worth reading a blog post written on the NCSC website back in November 2016 at: https://www.ncsc.gov.uk/blog-post/security-breaches-communication-what-are-your-users-telling-you

Number 6

DOJ charges Chinese nationals in cyber espionage campaign

The indictment was filed by prosecutors with the U.S. attorney's office in the Southern District of New York.



UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA

-v.-

ZHU HUA,
a/k/a "Afwar,"
a/k/a "CVNX,"
a/k/a "Alayos,"
a/k/a "Godkiller," and
ZHANG SHILONG,
a/k/a "Baobeilong,"
a/k/a "Zhang Jianguo,"
a/k/a "Atreexp,"

Defendants.

DOCUMENT
ELECTRONICALLY FILED
DOC #:
DATE FILED: DEC 17 2018

SEALED INDICTMENT

18 Cr. _____

18 CRIM 891

COUNT ONE
(Conspiracy to Commit Computer Intrusions)

You may visit:
https://www.justice.gov/opa/press-release/file/1121706/download

Number 7

Amazon Customers Made This Holiday Season Record-Breaking with More Items Ordered Worldwide Than Ever Before

Amazon has announced a record-breaking holiday season thanks to its customers all around the world, with more items ordered worldwide than ever before.

Amazon customers shopped at record levels from a wide selection of products across every department, discovering top holiday gifts and trending products offered at deep discounts and low prices.

Some of the best-selling products this season included, all-new Echo Dot, L.O.L. Surprise! Glam Glitter Series Doll, fashion items from Carhartt, and Bose QuietComfort Wireless Headphones, among others.

Prime membership continued to grow this holiday season, with tens of millions of people starting Prime free trials or paid memberships, to benefit from FREE Same-Day, One-Day or Two-Day shipping, in addition to FREE two-hour delivery with Prime Now, and exclusive shopping and entertainment benefits.

Prime members enjoyed shopping a wide selection of products with fast and free shipping throughout the season – in fact, this holiday millions of unique items in the U.S. shipped with Prime FREE Same-Day, Prime FREE One-Day or FREE two-hour delivery with Prime Now.

“This season was our best yet, and we look forward to continuing to bring our customers what they want, in ways most convenient for them in 2019.

We are thrilled that in the U.S. alone, more than one billion items shipped for free this holiday with Prime,” said Jeff Wilke, CEO Worldwide Consumer. “Thank you to our employees all around the world who are committed to bringing our customers the widest selection of products with low prices and fast and free delivery options throughout the holidays and all year long.”

Amazon Devices & Alexa

- Customers purchased millions more Amazon Devices this holiday season compared to last year – the best-selling Amazon Devices this

holiday included all-new Echo Dot, Fire TV Stick 4K with all-new Alexa Voice Remote, and Echo.

- It was a record holiday season for Amazon's Kids Edition devices; customers purchased more Echo Dot Kids Edition and Fire Kids Edition tablets than ever before.

- Customers purchased millions of Amazon Fire TV, Fire Tablet, and Kindle products this holiday season.

- Ring and Blink sold more devices this holiday season than ever before, as more and more customers are keeping their homes safe.

- Customers made their homes even smarter this year with a record number of smart home devices sold on Amazon.com; best-selling smart home devices included Amazon Smart Plug, Ring Video Doorbell 2, TP-Link Kasa Smart Plug Mini Outlet, and the iRobot Roomba 690.

- Customers used Alexa to listen to hundreds of millions more hours of music this holiday season compared to last holiday season, and on even more services – including Amazon Music, Spotify, Tidal, and Apple Music, among others.

- Customers asked Alexa to turn on their holiday lights tens of millions of times this holiday season, with the number one request being "Alexa, turn on the Christmas tree."

- Alexa delivered 8x as many reminders this holiday season compared to last.

- Alexa set more than one hundred million timers this holiday season.

- Customers requested nearly 3x as many recipes this holiday season compared to last and asked Alexa for cooking-related advice twice as much.

- Alexa helped mix hundreds of thousands of cocktails this holiday season – with eggnog and Moscow Mule being the most requested drinks.

- From carolers to delivery drivers and holiday guests, customers received millions of doorbell and motion announcements via Alexa this holiday season.

- Customers were in to the festive spirit with Alexa Skill Blueprints – popular Blueprints this holiday season were The Holiday Story, Santa's Letter, and the Hallmark Holiday Greeting.

- The number one holiday song that customers requested this holiday season was “All I Want for Christmas is You” by Mariah Carey.

- This holiday season, customers listened to more than one million holiday stories from Amazon Storytime on Alexa – the most popular holiday story was Rapping Paper.

- Customers around the world asked Alexa how many days or sleeps until Christmas this holiday season – customers in the United Kingdom were the most excited, asking twice as much as customers in any other country.

- Customers used Alexa nearly twice as much on Fire TV devices this holiday season compared to the same time period last year.

Number 8

The State of IT Security in Germany 2018

Federal Office
for Information Security

Cyber attack on German authorities

Situation

Towards the end of 2017, the BSI received indications of a successful cyber attack via the National Cyber Defence Centre, which purported to affect individual German federal authorities.

The BSI started the incident handling process in coordination with the authorities involved in the National Cyber Defence Centre, informed the authorities that were potentially affected and began the analysis and verification of the information initially available.

Cause and Damage

The primary target of the attack was the Foreign Office. A learning platform operated by the Federal University of Applied Sciences was attacked in order to gain access to the Federal Foreign Office network via this intermediate step. This was because established protection measures had prevented attackers from accessing the network of the Foreign Office directly.

This put the attacker in a position to successfully infect some client systems at the German Foreign Office and to extract internal documents in small numbers. However, the attack was not directed against the government networks as a whole.

Reaction

In close cooperation between the authorities concerned, the National Cyber Defence Centre and BSI responded with the following measures, among others:

- analysis of the impact
- identification and protection of infected systems
- forensic analysis

• protocols and log data evaluation for those affected and at central points in government networks

In addition, the BSI has deployed a mobile incident response team (MIRT, within the meaning of Section 5a of the BSIG) to support incident handling on site for those affected, at weekends as well.

In consultation with those affected, the attack was observed undercover in order to first analyse the attackers‘ actions and then to maximise the effectiveness of the measures to be taken.

The findings gained have already been incorporated into the Federal Administration‘s protective measures during the analysis.

After press reports had publicised CLASSIFIED information on the incident on 28 February 2018, immediate corrective action was taken.

Additional protective measures to prevent attacker communication have been established.

The affected systems of the Federal University of Applied Sciences were subsequently also switched off.

Recommendation

The situation clearly shows the current threat potential posed by targeted attacks on the Federal Administration.

The financial, time and technical resources invested by the attacker in the preparation and execution of the attack demonstrate the attacker‘s great interest in its target.

The incident underscores the need for multi-level protection concepts and consistent implementation of protection measures against targeted attacks.

However, the incident also proves the effectiveness of these measures: Similar incidents have had a far more serious impact on those affected in the past.

To read more:
https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2018.pdf?__blob=publicationFile&v=3

Number 9

Brief summary, 2017 Report on the Protection of the Constitution
Facts and Trends

Federal Ministry
of the Interior, Building
and Community

Espionage and other intelligence activities

States which strive to gain a knowledge edge in military (particularly strategic) or economic and technological contexts do not hesitate to procure the necessary information secretly and illegally by violating applicable law.

In this context, their governments political agenda dictates the priority areas of the individual intelligence services‘ activities.

Germany is of interest in its role as a geopolitical player, as a member of NATO and the EU and on account of its economic strength and innovative businesses.

Oppositional groups from foreign intelligence services’ home countries in Germany are another target of espionage activities.

The consequences for Germany range from a weakening of its negotiating position to high material and economic damage and a potential impairment of its national sovereignty.

The Russian Federation, the People’s Republic of China and the Islamic Republic of Iran are the major players behind espionage activitiesthat are directed against Germany.

Apart from that, other countries (including western countries) also play a role.

The Russian intelligence services invest a lot of organisational and financial effort to engage in espionage activities against Germany.

With the use of cyberspace the extent of espionage has increased many times over.

It is targeted at all areas of politics, economy, research and technology, with a focus on the political position of the Federal Government vis-à-vis the Russian Federation.

The efforts of the Russian intelligence services focus in particular on those policy areas where decisions with a potential impact on Russian interests are taken.

These policy areas include the alliance policy within NATO and the EU and Germany's foreign policy.

The tense relationship between the EU and Turkey and the resulting potential impact on the accession negotiations and the future of the EU – in particular after the so-called BREXIT vote – and the orientation of the Common Foreign and Security policy have been of particular interest to the Russian intelligence services.

Owing not least to the dwindling public interest, the Ukraine crisis which was very much in the fore in 2014 and 2015,has been overshadowed by other areas of tension such as the conflict in Syria.

Nevertheless the question as to whether the political and economic sanctions which were imposed on Russia in the course of the Ukraine crisis in 2014, are going to be lifted or extended continues to be of high interest to the Russian intelligence services.

As regards German home affairs policy, the services tried to gather information on party-political structures and developments, on the views of individual political parties and on the potential impact of electoral outcomes.

Apart from their espionage interests the Russian services strive to influence the political and public opinion in Germany.

As in previous years, pro-Russian propaganda was disseminated in numerous ways.

Important tools include social networks, the microblogging service Twitter, government-funded and private institutes (such as think tanks) and Russian state media.

TV, radio and Internet channels which broadcast around the world run targeted propaganda and disinformation campaigns.

Such disinformation and propaganda campaigns are aimed at destabilising the Federal Republic of Germany and at weakening its position as an advocate for an extension of the EU-sanctionsimposed on Russia.

The situation in Russia, by contrast, is being glossed over while the sole responsibility for the economic and social hardships is attributed to the western governments.

The focus of Chinese intelligence activities is shifting towards political espionage.

They are now making great efforts to obtain information about supranational entities such as the EU and about international conferences such as the G20 Summit.

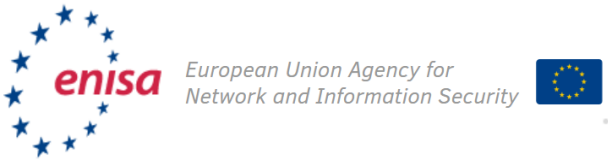
Moreover, the country is very interested in policy positions on China, e.g. recognition as a market economy or territorial disputes in the region of the South China Sea.

In Germany, Chinese intelligence services continue to focus on industry, research, technology and the armed forces (in particular information on the structure, armament and training of the Bundeswehr and on modern weapons technology) as well as on policies which– from the Chinese perspective – threaten national unity and the Communist Party's monopoly on power ("Five Poisons").

To read more:
https://www.verfassungsschutz.de/en/download-manager/_annual-report-2017-summary.pdf

Number 10

Supporting the Fight Against Cybercrime: ENISA report on CSIRTs and Law Enforcement Cooperation



The fight against cybercrime, requires the involvement of Law Enforcement Agencies, which supported by CSIRTS are likely to be better positioned to investigate complex criminal structures.

This cooperation is incomplete however, unless the judiciary is equally brought into the picture due to the pre-eminent role it plays across the MS in directing criminal investigations.

While collecting evidence is important warranting its admissibility in a criminal trial is equally so.

Admissibility of evidence relies on compliance with certain technical and legal requirements as well as the conditions laid down in criminal procedure.

In 2018, ENISA confirmed that CSIRTs, law enforcement and the judiciary have complementary roles and structure and that incident handling varies across Member States.

The data CSIRTs and Law Enforcement Agencies have access to varies, and it affects information sharing between them when they seek to respond to cybercrime.

CSIRTs interact frequently with the Law Enforcement Agencies rather than with the prosecutor.

CSIRTs offer support to Law Enforcement Agencies to collect and analyse different types of evidence. CSIRTs are called rarely as witness in courts but the material they collect during the incident handling might be used to decide on cybercrime cases.

Cooperation challenges concern data retention, the sharing of personal data (including IP addresses) and the confidentiality around criminal investigations as well as evidential admissibility of digital evidence.

Legal challenges are followed by cultural, technical and organisational ones.

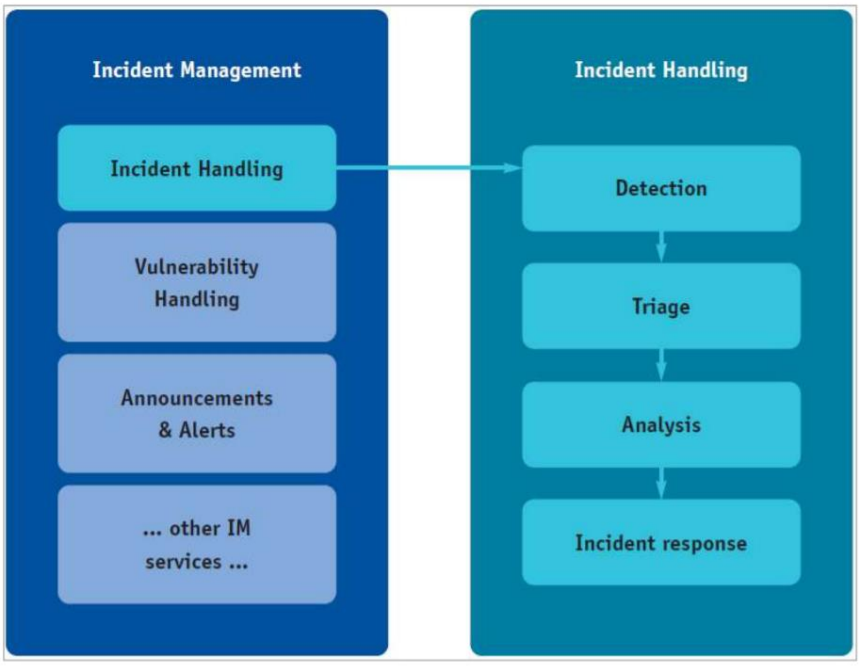
ENISA recommendations include:

- Gather further knowledge and study interactions across the three communities;

- Analyse the legal and policy framework shaping this cooperation;

- Seek to better understand tools and methods used for the cooperation between CSIRTs and LE and their interaction with the judiciary and improve via training opportunities.

For the full report:
https://www.enisa.europa.eu/publications/csirts-le-cooperation



Number II

Hackers threaten to leak 9/11 litigation documents

National Cyber Security Centre
a part of GCHQ

A cyber crime group calling itself 'The Dark Overlord' continues to threaten to release stolen files from US law firms and a London-based plastic surgery clinic if ransom demands are not met.

The FBI is investigating the theft of 18,000 insurance and legal documents relating to the September 11 attacks on the World Trade Centre.

The group reportedly obtained access to the documents after compromising a specialist law firm in the U.S. that provided advice to global insurance firm Hiscox. The insurance firm has confirmed that their own systems were unaffected by this incident.

In October 2017, the Met police confirmed that it was investigating the group for stealing data from a London cosmetic surgery clinic popular with celebrity clients. The group continue to threaten the release of this historic, personal data for money.

After distributing a small preview set of files, the group has publicly released a decryption key for more files, in a bid to bolster their extortion efforts.

The news gives insight into how hacking groups may be evolving in their extortion efforts; opting to drip out stolen material bit by bit, while generating public interest through the media and their own announcements, all to exert pressure on the ransom victim.

The NCSC has previously highlighted this tactic as one which is used by criminals to blackmail organisations.

You may visit:
https://www.ncsc.gov.uk/report/weekly-threat-report-3rd-november-2017

Open source reporting suggests that there has been a recent surge in activity by 'The Dark Overlord' which began in September 2018.

Any organisation that deals with sensitive personal information (e.g. medical institutions, law firms) is at a higher risk of being targeted.

The NCSC has published 15 good practice measures for the protection of bulk personal data.

To read it:
https://www.ncsc.gov.uk/guidance/protecting-bulk-personal-data-main

The NCSC strongly encourages anyone who believes they have been a victim of this or other similar activity to report it to Action Fraud at https://www.actionfraud.police.uk/

Number 12

German politicians and celebrities caught in Christmas data leak

National Cyber Security Centre
a part of GCHQ

Over Christmas, personal information and alleged communications belonging to German politicians, journalists, and celebrities were leaked on Twitter, under the username @_orbit. The information was published in the style of an "advent calendar event" each day in December.

The data breach reportedly included politicians' email addresses, mobile phone numbers, identity card photos, direct debit and credit card information, and personal and work communications.

A 20-year-old student has admitted to carrying out the hack.

The private information seems to have been acquired over a substantial period of time in 2018 in what German officials called a "sophisticated" operation, and added to publicly available information.

Investigators said that the hacker "exploited several vulnerabilities", although they have confirmed that several such security gaps have since been fixed. Officials also said there was no evidence to suggest that government systems had been compromised.

The BSI information security agency said it was contacted by a member of the German parliament in early December about suspicious activity on private email and social media. In a statement, the agency said it was linked to the @_orbit leaks only when the account's existence became known in early January.

German Interior Minister Horst Seehofer has subsequently confirmed that he will introduce new measures to improve cyber security and an existing security law with more protections for industry and citizens.

Data breaches such as this highlight the need for individuals who believe their data may be comprised to remain vigilant to phishing emails.

The NCSC has published guidance on the phishing threat following data breaches at: https://www.ncsc.gov.uk/guidance/phishing-threat-following-data-breaches

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.