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

April 2018, cyber risk and compliance in Switzerland

Dear readers,

According to the Computer Security Incident Response Team of the Swiss Government (GovCERT.ch) and the Melde- und Analysestelle Informationssicherung (MELANI), in April we had massive spam waves for several days, having the look and the feel of well-known Swiss companies like @postschweiz or @ricardo_ch.

The goal: To infect citizens with the eBanking Trojan Retefe.

This is not the first time the Retefe Trojan has targeted Switzerland and German speaking persons. We can find more at: https://www.govcert.admin.ch/blog/33/the-retefe-saga

---

I must confess, I hate the word *interpretation.*

Friedrich Nietzsche believed that all things are subject to *interpretation,* and that whichever interpretation prevails at a given time, is a function of power and not truth.

Marcus Tullius Cicero has said that in doubtful cases, the more liberal *interpretation* must always be preferred.

The European Network and Information Security Agency (ENISA) gives a very interesting definition: "Cyber threat intelligence is the process and product resulting from the *interpretation* of raw data into information that meets a requirement as it relates to the adversaries that have the intent, opportunity and capability to do harm."

According to ENISA, cyber threat intelligence as a discipline has its roots in

incident response and traditional intelligence, and there are various definitions, including the one above. I was surprised to see that ENISA used an unusual (for the EU) reference: "CIA, A Definition of Intelligence, 1995".

Of course, ENISA is right (but the URL leading to the CIA document is wrong, something that is not spooky, it is an error.)

According to the SANS CTI Survey of 2017, 60% of the responders already utilize threat intelligence for detection and response, and 78% of them felt that it had improved their security and response capabilities.

Well … I hope this is neither the result of cognitive bias, nor a systematic error of inductive reasoning.

The table below presents some of the properties of threat intelligence, incident response and security operations practices:

	THREAT INTELLIGENCE	INCIDENT RESPONSE	SECURITY OPERATIONS
Adoption	Early adoption phase	Mainstream since ~2010	Mainstream since ~2005
Focus	External threat monitoring	Security incidents and risk escalation	Notable security event monitoring
Best practices	Evolving best practices	Mature best practices	Mature best practices
Technology enablement	Limited technology enablement	Mature technology enablement	Mature technology enablement

Figure 1: Threat Intelligence, Incident Response and Security Operations practices [11]

Friedrich Nietzsche has also said that necessity is not an established fact, but an *interpretation.*

The full report can be found at:
https://www.enisa.europa.eu/publications/exploring-the-opportunities-and-limitations-of-current-threat-intelligence-platforms

---

According to the Merriam-Webster dictionary, random is something without definite aim, direction, rule, or method.

I am often surprised when I see this word in quotes and articles. Franz Kafka, for example has said: "Self-control means wanting to be effective at some random point in the infinite radiations of my spiritual existence".

What Albert Camus has said is not better: "It is necessary to fall in love… if only to provide an alibi for all the random despair you are going to feel anyway."

Randomness is very important in cryptography. In many cryptographic systems, the generation of random (or pseudorandom) numbers, directly determines the strength of the encryption.

A pseudorandom number generator (PRNG) is an algorithm that generates sequences of numbers, that have properties similar to sequences of random numbers.

The PRNG-generated sequence is not truly random, as it is determined by an initial value (the seed).

PRNGs are also important in simulations, like the Monte Carlo simulations that are used in so many banks for the "measurement" of market risk.

Today we have an interesting development: Researchers at the National Institute of Standards and Technology (NIST) have developed a method for generating numbers guaranteed to be random by quantum mechanics.

The new NIST method generates digital bits (1s and 0s) with photons, or particles of light, using data generated in an improved version of a landmark 2015 NIST physics experiment:

That experiment showed conclusively that what Einstein derided as "spooky action at a distance" *is real.*

In the new work, researchers process the spooky output to certify and quantify the randomness available in the data and generate a string of much more random bits.

"Random" numbers are used hundreds of billions of times a day to encrypt data in electronic networks. But these numbers are not certifiably random in an absolute sense.

That's because they are generated by software formulas or physical devices whose *supposedly* random output could be undermined by factors such as predictable sources of noise.

The new NIST method generates digital bits (1s and 0s) with photons, or particles of light, using data generated in an improved version of a landmark 2015 NIST physics experiment:

https://www.nist.gov/news-events/news/2015/11/nist-team-proves-spooky-action-distance-really-real

"It's hard to guarantee that a given classical source is really unpredictable," NIST mathematician Peter Bierhorst said.

"Our quantum source and protocol is like a fail-safe. We're sure that no one can predict our numbers."

He continues: "Something like a coin flip may seem random, but its outcome could be predicted if one could see the exact path of the coin as it tumbles. Quantum randomness, on the other hand, is real randomness.

We're very sure we're seeing quantum randomness because only a quantum system could produce these statistical correlations between our measurement choices and outcomes."

Pericles has said: "We do not imitate, but we are a *model* to others". Some consultants that build "to do" lists couldn't agree more.

Vincent Van Gogh believed: "Do not quench your inspiration and your imagination; do not become the slave of your *model."*

The UK's National Cyber Security Centre (NCSC) (a part of GCHQ, coming out of the shadows to protect Britain from cyber risks) prefers the Van Gogh's approach, and they are right.

A *maturity model* is a tool for assessing an organization's effectiveness at achieving a particular goal.

According to the NCSC, there are two fundamentally different approaches to using maturity models, and to thinking about an organisation's maturity.

One involves comparing your organisation to how it looked at some point in the past, to track improvements over time.

The other approach involves comparing your organisation with others.

The NCSC has decided to stop its formal support for its Information Assurance Maturity Model (IAMM), with immediate effect.

They believe: "In short, using maturity models to compare your organisation to others is like comparing apples with oranges."

They also believe: “In other words, for some organisations, it became a "tick-box" exercise for compliance purposes, and which really didn't take into account the risk”.

Welcome to our monthly newsletter.

Best regards,

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 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 8)

Maturity models in cyber security: what's happening to the IAMM?

Anne W, Head of Cyber Security Assurance Schemes

National Cyber Security Centre
a part of GCHQ

Number 2 (Page 12)

EU-US Insurance Dialogue Project: New Initiatives for 2017 – 2019 - Focus Areas for 2018

eiopa
EUROPEAN INSURANCE AND OCCUPATIONAL PENSIONS AUTHORITY

Number 3 (Page 14)

Keep America Safe in the Cyber Era

NATIONAL SECURITY STRATEGY
of the United States of America

Number 4 (Page 16)

Signalling Security in Telecom SS7/Diameter/5G

enisa
European Network and Information Security Agency

Number 5 (Page 19)

Cyber Storm VI: Testing the Ability to Respond to a Cyber Incident

Number 6 (Page 21)

Phishing emails deemed number one threat by UK Businesses

Number 7 (Page 23)

Cyber-criminal groups identified on social media

Number 1

Maturity models in cyber security: what's happening to the IAMM?

Anne W, Head of Cyber Security Assurance Schemes

National Cyber Security Centre
a part of GCHQ

What is a maturity model?

Most generally, a maturity model is a tool for assessing an organisation's effectiveness at achieving a particular goal. They enable organisations to identify where their practices are weak or not taken seriously and where their practices are truly embedded.

In the context of cyber security, maturity models can help to distinguish between organisations in which security is baked in and those in which it is merely bolted on.

One of the main reasons that maturity models are used is that organisation-wide improvements can take time; in cyber security a maturity model gives an organisation's leadership a way to measure the progress made in embedding security into its day-to-day and strategic operations.

How do they work?

Generally, a security maturity model describes a range of capabilities that you would expect to see in an organisation with an effective approach to cyber security.

These capabilities will include things like effective leadership and governance or information risk management processes.

Each capability will have a description of the kinds of activities and processes you would expect to see present in the organisation, at different levels of maturity.

An organisation seeking to assess its overall cyber security maturity would compare its own practices against those described in the levels of each capability.

These assessments would need to be backed up by some sort of evidence to justify the assessment made.

That's probably not very clear, so an example should help to explain how this works.

Most cyber security maturity models have a capability around security training. This capability describes the kinds of activity you would expect to see in an organisation at the various levels of maturity.

An assessment might gather evidence of training courses attended, maybe survey or interview the staff, and analyse the impact of that training by looking at specific staff behaviours such as people tailgating through secured swipe-access doors into areas where sensitive information is processed.

The assessment of maturity that comes out of this analysis would form part of the overall assessment of the organisation's maturity; assessments of capability in the individual areas can be used to inform improvements that an organisation may decide to make.

Most maturity models work in this way, including our own IA Maturity Model (IAMM).

"We're mature", but compared to what?

There are two fundamentally different approaches to using maturity models, and to thinking about an organisation's maturity.

One involves comparing your organisation to how it looked at some point in the past, to track improvements over time.

The other approach involves comparing your organisation with others.

A vast number of often complex and hard to measure factors affect the state of cyber security within an organisation.

Factors, which might appear to have nothing to do with cyber security, can have a significant effect on an organisation's maturity in cyber security, so context is essential.

For example, if your organisation has recently moved office, this could significantly change its cyber security maturity.

Equally, in a year of high staff turnover, a workforce's approach to security will change.

If you're using a maturity assessment to track your organisation's improvement you might capture these changes, and then be able to link them to these contextual changes in your organisation.

However, if you, or any 3rd party, are using a maturity model to make a comparison between the maturity rating of your organisation with that of another you are unlikely to have any knowledge of the contextual factors which may have impacted the other organisation.

As such, you're unlikely to know why a given organisation is more or less mature than your own. If that's the case, you're not really going to get any actionable information from making the comparison.

In short, using maturity models to compare your organisation to others is like comparing apples with oranges.

What about the IAMM?

Nearly a decade ago we (as one of our precursor organisations, CESG) produced a maturity model for information assurance (IA); the IA Maturity Model (IAMM).

Its aim was to raise information security and assurance across the UK public sector by helping departments and agencies assess their own levels and then put programmes of work in place to raise their standards.

Although many organisations used the IAMM successfully (and some still use it today), the original intent - to encourage organisations to focus on continual improvement in their IA stance - became blurred.

For some, the focus instead became the assessment itself and not the improvements that maturity level represented.

For others, the focus became comparing their results with others despite us making it clear this wasn't what the IAMM was for.

In other words, for some organisations, it became a "tick-box" exercise for compliance purposes, and which really didn't take into account the risk.

Over this time, NCSC's thinking on how to inform and improve cyber security decision making and investment programmes has matured; over

many years (as CESG) we learned that mandating a specific tool or technique results in unintended consequences. Every organisation has had to make investment decisions about how to protect their technology and services; but every organisation is unique.

We think decision making needs to be more nuanced than looking at the results of a maturity assessment and deciding to spend money on improving a particular score.

As John Y said in his blog last year "there is no single method for doing risk management for cyber security which can be applied universally, to good effect"

The NCSC have therefore decided to stop our formal support for the IAMM with immediate effect.

Instead we would point organisations to our recently published risk management "toolbox".

What does this mean in practice ?

The NCSC will no longer be offering the IAMM independent review or supported self assessment services. We are also withdrawing the IAMM assessment tool. If this causes any particular issues for a public sector organisation, please contact NCSC Enquiries.

We will retain our own IAMM framework on our website but you should be aware that we are not intending to update it now or in the future.

Finally, we know there are organisations who have successfully used maturity models to drive improvements. If that is you, carry on, there are plenty out there ..... just don't use them to compare apples with oranges!!

Number 2

EU-US Insurance Dialogue Project: New Initiatives for 2017 – 2019 - Focus Areas for 2018

The EU-US Insurance Dialogue Project (EU-US Project) began in early 2012, as an initiative by the European Commission, the European Insurance and Occupational Pensions Authority (EIOPA), the Federal Insurance Office of the U.S. Department of Treasury (FIO), and the National Association of Insurance Commissioners (NAIC) to enhance mutual understanding and cooperation between the European Union (EU) and the United States for the benefit of insurance consumers, business opportunity, and effective supervision.

In 2018, the EU-US Project's members will continue the work begun in 2017, focusing on three areas:

1) cybersecurity risk and the cyber insurance market,

2) the use of "big data" in the insurance sector, and

3) group supervision, particularly intra-group transactions.

I. Cybersecurity Risk and Cyber Insurance Market

A. Introduction

Cyber risk is growing and evolving, both for the insurance sector itself and for those whom it serves. Insurers collect and manage large stores of personally identifiable information and private health information from consumers and are increasingly exposed to cyberattacks by cyber criminals and other hackers, making improved cybersecurity in the insurance sector a priority throughout the EU and the United States.

Additionally, with the growth of the cyber insurance market, some insurers are also increasingly involved in underwriting cyber risks.

Given the potential significance of this evolving threat, and since all EU-US Project members are involved to various degrees in activities to improve cybersecurity in the insurance sector, the EU-US Project Steering Committee has agreed to pursue a bilateral dialogue to share knowledge and information with respect to the dynamic area of cyber risk and the insurance sector.

The EU-US Project will address two main topics:

1) the increased role of insurers, policymakers, and regulators in improving cybersecurity in the insurance sector, and

2) understanding the development of the cyber insurance market, including steps that insurers, policymakers, and regulators are taking to assure that such products are being offered in a sound and prudent manner.

To read more:
https://eiopa.europa.eu/Publications/Other%20Documents/180322_EU_US%20Project%20initiatives_for%20SC_FIO_NAIC_EIOPA_March%2018.pdf

Number 3

Keep America Safe in the Cyber Era

America's response to the challenges and opportunities of the cyber era will determine our future prosperity and security.

For most of our history, the United States has been able to protect the homeland by controlling its land, air, space, and maritime domains.

Today, cyberspace offers state and non-state actors the ability to wage campaigns against American political, economic, and security interests without ever physically crossing our borders.

Cyberattacks offer adversaries low cost and deniable opportunities to seriously damage or disrupt critical infrastructure, cripple American businesses, weaken our Federal networks, and attack the tools and devices that Americans use every day to communicate and conduct business.

Critical infrastructure keeps our food fresh, our houses warm and our citizens productive and safe.

The vulnerability of U.S. critical infrastructure to cyber, physical, and electromagnetic attacks means that adversaries could disrupt military command and control, banking and financial operations, the electrical grid, and means of communication.

Federal networks also face threats. These networks allow government agencies to carry out vital functions and provide services to the American people.

The government must do a better job of protecting data to safeguard information and the privacy of the American people.

Our Federal networks must be modernized and updated.

In addition, the daily lives of most Americans rely on computer-driven and interconnected technologies.

As our reliance on computers and connectivity increases, we become increasingly vulnerable to cyberattacks. Businesses and individuals must be able to operate securely in cyberspace.

Security was not a major consideration when the Internet was designed and launched. As it evolves, the government and private sector must design systems that incorporate prevention, protection, and resiliency from the start, not as an afterthought.

We must do so in a way that respects free markets, private competition, and the limited but important role of government in enforcing the rule of law.

As we build the next generation of digital infrastructure, we have an opportunity to put our experience into practice.

The Internet is an American invention, and it should reflect our values as it continues to transform the future for all nations and all generations.

A strong, defensible cyber infrastructure fosters economic growth, protects our liberties, and advances our national security.

To read more:
https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf

Number 4

Signalling Security in Telecom SS7/Diameter/5G

EU level assessment of the current situation

Telecommunications are key in nowadays societies. They represent the backbone, the primary infrastructure based on which our society works and constitute the main instrument in allowing our democracy (and other EU core values such as freedom, equality, rule of law, human right) to function properly.

As a consequence, here in ENISA (the EU cyber security agency) we consider assuring the security of our infrastructure as a top priority.

The present study has deep dived into a critical area within electronic communications, the security of interconnections in electronic communications (signalling security).

Based on the analysis, at this moment there is a medium to high level of risk in this area, and we do consider that proper attention must be granted by all stakeholders involved so as to find a proper solution.

As mobile technologies evolve so does the threat landscape. Early generations of mobile networks 2G/3G rely on SS7 and its IP Version SIGTRAN, a set of protocols designed decades ago, without giving adequate effect to modern day security implications.

Nobody at that time envisioned the scale that mobile networks could reach in the future, so trust and security were not issues.

Nonetheless at the moment we are still using this legacy set of protocols to assure the interconnection between providers.

The industry and security research community has started covering

the topic, by providing good practices and necessary tools. But still, a lot more has to be done.

Basic security measures seem to be implemented by more mature providers, but these measures assure only a basic protection level. More efforts need to be made so that an optimal protection level is achieved.

Current telecommunication mobile generation (4G) uses a slightly improved signalling protocol called Diameter.

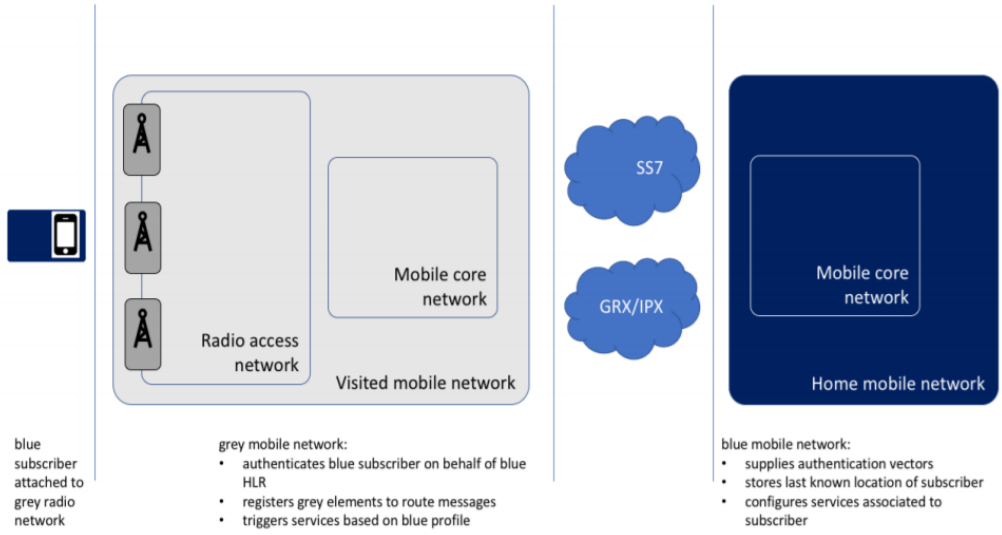

Figure 2 – How visited and home networks interoperate when roaming

Build with the same interconnect principles in mind but on an IP base, the protocol has been proved vulnerable.

The industry is still trying to understand exact implications and to identify possible workarounds.

Attackers are also in the same phase.

It is our impression that the next step will be made soon. As soon as SS7 becomes sufficiently protected their focus will change towards the new attack surface.

5G, the new mobile generation, is still under development. Early releases from some manufacturers are available but the standards are still in their infancy.
Nevertheless there is a certain risk of repeating history.

Given the improvements that 5G will bring (more users, more bandwidth etc.) having the same security risks could be extremely dangerous.
This document represents an EU wide (and not only) assessment of the current situation.

We have analysed areas like types of attacks and their frequencies, security measures in place, available best practices and other constraints so that we can get an overall picture of signalling security in Europe.

As you will notice in the document, further efforts are needed at global level to tackle current threats and prevent future similar situations.

Special attention must be granted by different stakeholders involved so that an adequate level of protection is achieved across EU.

Please find below a set of high-level recommendations that we urge responsible stakeholders to take into account.

For further details, pls. refer to the rest of the document.
To read more:
https://www.enisa.europa.eu/publications/signalling-security-in-telecom-ss7-diameter-5g

Number 5

Cyber Storm VI: Testing the Ability to Respond to a Cyber Incident

Cyber threats to government networks and other critical infrastructure are one of our Nation's most pressing security challenges. Consequences from attacks threaten the safety and security of the homeland, our economic competitiveness, and our way of life.

With the majority of critical infrastructure owned and operated by the private sector, securing cyberspace is only possible through close collaboration, what we described as a "Collective Defense" model of shared responsibility.

Exercises are critical to testing this coordination, and more importantly, to building and maintaining strong relationships among the cyber incident response community. Carried out regularly, these exercises allow us to achieve solutions to some of the biggest challenges facing the homeland as well as raise the overall profile of cyber events and cyberattacks.

Cyber Storm VI was led by the Department of Homeland Security (DHS) and involved more than 1,000 members of the private industry, government and international partners who participated in a three-day distributed exercise that focused on the critical manufacturing and transportation sectors.

The exercise evaluated and improved the capabilities of the cyber response community, informed preparedness and resilience planning efforts, and evaluated the effectiveness of the National Cyber Incident Response Plan in guiding response.

Growth in this community of partners acknowledges the increasing value of information sharing and the benefits of exercising their organizations cyber response plans.

During the exercise, participants faced a simulated cyber crisis of national and international consequence that required them to use their training,

policies, processes, and procedures for identifying and responding to a multi-sector cyberattack targeting critical infrastructure. The Cyber Storm VI scenario was an environment where no single organization was is in a position to stop or mitigate the impacts of the attack by itself.

Thus, the scenario promoted cooperation and information sharing across the United States government, states, the private sector, and international partners.

The DHS National Cybersecurity and Communications Integration Center (NCCIC) served as the focal point for federal response and coordination during the event.

NCCIC is a 24x7 cyber situational awareness, incident response, and management center that is a national nexus of cyber and communications integration for the Federal Government, intelligence community, and law enforcement.

The NCCIC is also designated as the federal interface for private sector information sharing, cross-sector coordination, and incident response.

A comprehensive after-action process will take place to discuss initial, high-level findings. An after-action conference will also be held to validate these findings and inform the development of an after action report.

This information, along with the lessons from previous exercises and real-world incidents, is integral for strengthening the Nation's capacity to respond to a cyber incident.

It also assists DHS in creating more challenging scenarios to test the security and resiliency of their partners in the years to come.

For more information about the Cyber Storm exercise series, and to view the final reports from Cyber Storms I-V, you may visit: https://www.dhs.gov/cyber-storm

Number 6

Phishing emails deemed number one threat by UK Businesses

National Cyber Security Centre
a part of GCHQ

Industry research by security company Clearswift has reported that malicious links within emails are perceived as posing the biggest cyber threat to UK businesses, with 59% of business decision makers highlighting this as their chief concern.

This is indicated to be far more than any other cyber threat.

The research surveyed 600 senior business decision makers and 1,200 employees across the UK, US, Germany and Australia.

When asked what they see as the biggest threat to their organisation, business decision makers ranked phishing emails as the top threat in all four surveyed regions:

Cyber Threatscape Top 10

1. Malicious links within emails – 59%
2. Employees sharing usernames/passwords – 33%
3. USB memory sticks/removable storage – 31%
4. Users not following protocol/data protection policies – 30%
5. Ex-employees retaining access to network – 28%
6. Infection via malware from personal devices – 26%
7. Hackers – 25%
8. Employees using non-authorised tools/applications for work purposes (personal email drives/file sharing) – 25%
9. Social media viruses – 24%
10. Critical information on stolen devices – 23%

The survey findings are aligned to previous NCSC assessments; email remains a popular tool for attackers to launch cyber attacks, distribute ransomware and other forms of malware, or to commit fraud via business email compromise.

Number 7

Cyber-criminal groups identified on social media

National Cyber Security Centre
a part of GCHQ

Facebook deleted around 120 private discussion groups - equating to more than 300,000 members - that were promoting a host of illicit cyber-criminal activities, including spamming, selling stolen debit and credit account credentials, phony tax refunds, DDoS-for-hire services and botnet creation tools.

The groups had reportedly been operating on Facebook for an average of two years, although some had been in operation for up to nine years. The deletions were a result of analysis work carried out by a cyber security researcher using common terminology for this type of activity and it is likely that there are many more sites of this nature on Facebook and other social media platforms.

The use of social media to advertise illicit goods and services is perhaps not as well reported as the use of darknet criminal marketplaces (such as Alphabay and Hansa that were taken down by law enforcement last year) but it is of no surprise that criminals will seek to utilise whatever means available to peddle their wares.

From past experience, Facebook's deletion of these groups is unlikely to have a long term impact, as the activity will likely be displaced elsewhere, or the groups will use names that are less obviously associated with cyber crime, to make their detection more difficult.

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 on this website. The inclusion of links to other 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 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.