Cyber Risk GmbH
Handelsregister des Kantons Zürich, Firmennummer: CHE-244.099.341,
Rebackerstrasse 7, 8810 Horgen
Phone: +41 43 810 43 61, Web: www.cyber-risk-gmbh.com

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

July 2017, cyber risk and compliance in Switzerland

According to *The Local:* "Switzerland largely spared from ransomware attack".

Well, no, it is not that simple. *No evidence of a problem, is no evidence or no problem.*

Defensive tactics simply cannot solve problems like NonPetya, ransomware or code that looks like ransomware.

In cybersecurity, we have a highly asymmetric conflict. We must defend against all possible attacks and we must close all possible gaps, even the ones we do not know they exist. The attackers must exploit just one vulnerability.

This asymmetry highly favors the attacker. So, we should attack too. (Does it look insane? Read below.)

Dr Hans-Georg Maaßen, President of the Bundesamt für Verfassungsschutz (BfV, the domestic intelligence service of the Federal Republic of Germany) has said: "We think it's essential that we don't just act defensively, but that we are also able to attack the enemy so that he stops continuing to attack us in the future."

He has also said: “We believe it is necessary that we are in a position to be able to wipe out these servers if the providers and the owners of the servers are not ready to ensure that they are not used to carry out attacks”.

German Defense Minister Ursula von der Leyen has also said that the German military has the authority to respond with "offensive measures" if its computer networks are attacked.

We must consider very carefully our ability to conduct offensive cyber operations, in compliance with the UN Charter’s prohibitions of the threat or use of force contained in Article 2(4), and Article 51’s self-defense provisions.

We have another interesting development – the paper “2016, Internet Crime Report”, from FBI’s Internet Crime Complaint Center IC3. It highlights the IC3’s efforts in monitoring trending scams such as Business Email Compromise (BEC), ransomware, tech support fraud, and extortion.

This past year, the top three crime types reported by victims were non-payment and non-delivery, personal data breach, and payment scams. The top three crime types by reported loss were BEC, romance and confidence fraud, and non-payment and non-delivery scams.

Business Email Compromise (BEC) is defined as a sophisticated scam targeting businesses working with foreign suppliers and/or businesses who regularly perform wire transfer payments.

The Email Account Compromise (EAC) component of BEC targets individuals who perform wire transfer payments.

The techniques used in both the BEC and EAC scams have become increasingly similar, prompting the IC3 to begin tracking these scams as a single crime type in 2017. The scam is carried out when a subject compromises legitimate business email accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers of funds.

Most victims report using wire transfers as a common method of transferring funds for business purposes; however, some victims report using checks as a common method of payment; The fraudsters will use the method most commonly associated with their victim’s normal business practices.

Fraudulent transfers have gone through accounts in many countries, with a large majority traveling through Asia. The scam began to evolve in 2013 when victims indicated the email accounts of Chief Executive Officers or Chief Financial Officers of targeted businesses were hacked or spoofed, and wire payments were requested to be sent to fraudulent locations.

BEC/EAC continued to evolve, and in 2014 victim businesses reported having personal emails compromised and multiple fraudulent requests for payment sent to vendors identified from their contact list.

In 2015, victims reported being contacted by subjects posing as lawyers or law firms instructing them to make secret or time sensitive wire transfers.

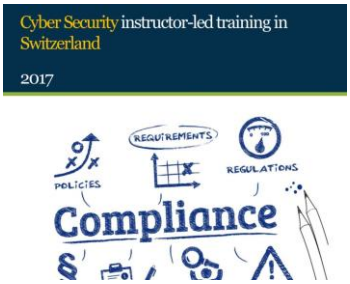
BECs may not always be associated with a request for transfer of funds. In 2016, the scam evolved to include the compromise of legitimate business email accounts and requests for Personally Identifiable Information (PII) or Wage and Tax Statement (W-2) forms for employees.

The BEC/EAC scam is linked to other forms of fraud, including but not limited to: romance, lottery, employment, and rental scams.

You must read the paper at: https://pdf.ic3.gov/2016_IC3Report.pdf

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 - Instructor-led training in Switzerland:
www.cyber-risk-gmbh.com/Cyber_Risk_GmbH_Catalog_2017.pdf

Number 1 (Page 7)

Cyber resilience - a banking supervisor's view

Sabine Lautenschläger, Member of the Executive Board of the European Central Bank and Vice-Chair of the Supervisory Board of the Single Supervisory Mechanism, at the High-Level Meeting on Cyber Resilience, Frankfurt am Main

"In addition to our ongoing supervision we also perform thematic reviews on cyber security and IT outsourcing.

These reviews help us to assess the risks facing each bank as well as the risks that might affect the entire sector. And they also help to raise awareness of cyber risk at Board level."

Number 2 (Page 10)

Developments in China

The Chinese government has asked state-owned telecoms companies to block individuals' access to virtual private networks (VPNs) by 1 February 2018. The ban will greatly restrict individuals' unfettered access to the Internet.

VPNs have often been used to circumvent China's Great Firewall and communicate with servers outside of China.

Number 3 (Page 12)

Password challenges

National Cyber Security Centre
a part of GCHQ

Passwords have been in the news again.

On Friday 23 June, accounts with weak passwords on the UK Parliamentary network were compromised; however less than 1% of the system's 9,000 accounts were directly affected.

Attention was also drawn to router password vulnerabilities, as Virgin Media advised customers with Virgin Super Hub 2 home routers to reset their passwords.

Number 4 (Page 13)

Getting ready for the European Cyber Security Month 2017

EUROPEAN CYBER SECURITY MONTH

Less than three months are left for the launch of the European Cyber Security Month, the EU annual awareness campaign which takes place in October supported by ENISA and EC DG CONNECT with the participation of many partners from all over Europe.

"Cyber Security is a shared responsibility!" is the motto of the ECSM campaign. Preparation for this year's Cyber Security Month kick-off event is in collaboration with the Estonian Information Systems Authority. Taking place during the Estonian Presidency, the Estonian Ministry of Economic Affairs & Communication will be hosting the kick-off event at their premises in Tallinn on the 29th September 2017.

Number 5 (Page 15)

SEC Files Fraud Charges in Bitcoin and Office Space Investment Schemes

U.S. SECURITIES AND EXCHANGE COMMISSION

The Securities and Exchange Commission filed fraud charges against the clandestine founder of a purported Bitcoin platform and a chain of co-working spaces located in former bars and restaurants, alleging that he bilked investors in both companies while hiding his connection given his checkered past with regulators in the U.K.

The SEC alleges that Renwick Haddow, a U.K. citizen living in New York, created a broker-dealer and did not register the firm with the SEC as required under the federal securities laws. Haddow allegedly used sales representatives to cold call potential investors and sell securities in Bitcoin Store Inc. and Bar Works Inc.

Number 6 (Page 17)

A portion of Microsoft Windows 10 Source code leaked online

National Cyber Security Centre
a part of GCHQ

Microsoft have confirmed a portion of its source code has been leaked online.

The initial source of the leak is unknown; however, the content was posted to Beta Archive, one of the largest online 'Beta and Abandonware' repositories for prototype software.

The leaked content was 1.2GB in size and has since been removed from the Beta Archive site.

Number 1

Cyber resilience - a banking supervisor's view

Sabine Lautenschläger, Member of the Executive Board of the European Central Bank and Vice-Chair of the Supervisory Board of the Single Supervisory Mechanism, at the High-Level Meeting on Cyber Resilience, Frankfurt am Main

This week I learnt that the first computer virus dates back to 1971. It spread via the ARPANET, which was a precursor of today's internet.

The ARPANET connected about two dozen universities and government hosts in the United States.

The virus had been written for experimental purposes and was not malicious. It just displayed a simple message on infected computers: "I'm the creeper: catch me if you can".

Things are a bit more complex today, and the outcome of cyber incidents much worse: they can disrupt business, cost a lot of money and destroy reputations.

And indeed, the potential for damage is great, as so much relies on IT and so much happens online - the financial sector is a case in point. As you all know, banks have always been attractive targets for criminals.

Although the damage has been limited so far, we banking supervisors take cyber risk very seriously. And we insist on banks doing the same.

Cyber risk has been a priority for ECB Banking Supervision from day one. In 2015, we established a working group that had three goals.

First, to get an overview of how supervisors deal with such risks both at national and international level.

Second, to get an overview of how prepared banks are for cyber risk.

And third, to propose to the Supervisory Board a strategic direction and a dedicated work plan on cyber risk.

We have learnt a lot over the past two years. And we have used it to address this risk from several different angles.

For us, one of the first steps was to establish a cyber incident reporting framework. We conducted a successful pilot phase in 2016.

And now we will implement a long-term solution for all those banks that we directly supervise.

As from this summer, they will be required to report all significant cyber incidents.

This will help us to assess more objectively how many incidents there are and how cyber threats evolve. It will also help us to identify vulnerabilities and common pitfalls.

In addition to our ongoing supervision we also perform thematic reviews on cyber security and IT outsourcing.

These reviews help us to assess the risks facing each bank as well as the risks that might affect the entire sector. And they also help to raise awareness of cyber risk at Board level.

The insights that we obtained in 2015 and 2016 were applied in three ways.

First, they informed a dedicated section in our methodology for on-site inspections.

Second, they were used to create new analytical tools for our off-site supervisors.

And third, they were used to produce a cyber risk profile of each bank.

So we are working to obtain a comprehensive picture of what is happening out there.

But how to deal with cyber risk?

Well, the World Health Organization says that the best way of stopping diseases from spreading is basic hygiene: washing your hands. And the same is true for IT.

Basic IT "hygiene" can take banks a long way. Have the latest updates been installed? Are passwords strong enough? Have backups been made and their restoration tested? Such simple things are so important, but often neglected.

So we are taking a close look at our banks to see whether they are following the relevant standards and best practices. And there are plenty of these; I cannot stress this enough.

We also work with the European Banking Authority, the EBA, on how to supervise cyber risk in an effective and harmonised manner across Europe.

As for the euro area, we plan to issue our supervisory expectations on how banks approach IT risks in general. And what we expect clearly goes beyond basic IT hygiene. This will be an important step for two reasons.

First, it will help to forge a common understanding of IT risks between supervisors and banks.

And second, it will help to ensure a harmonised treatment.

To increase awareness and to communicate our expectations, we will organise seminars and discussions with banks.

And we also look beyond the euro area, of course. We cooperate with supervisors worldwide to align priorities and exchange best practices.

To sum up, we take cyber risk very seriously, and we approach it from various angles. My advice to banks is to do the same. It is vital to be alert and ready to react. Thank you for your attention.

Number 2

Developments in China

A virtual private network (VPN) is a tunnel between your computer and the destinations you visit. Your computer is first connected to a VPN server, which can be in any country of the world. Your web traffic passes through that server, and you may fool some third parties into believing that you also browse from the VPN server's country.

Once you are connected to the VPN, it becomes difficult for anyone else to spy on your web-browsing activity. (Difficult means possible). Make no mistake, you are not secure. Even if we forget hackers, keyloggers and many other tools for surveillance, the VPN provider knows where you came from and what you do. And the provider may not be in the "privacy" business.

According to UK's National Cyber Security Centre (NCSC), the Chinese government has asked state-owned telecoms companies to block individuals' access to virtual private networks (VPNs) by 1 February 2018. The ban will greatly restrict individuals' unfettered access to the Internet.

VPNs have often been used to circumvent China's Great Firewall and communicate with servers outside of China. The Chinese government has increasingly cracked down on them in pursuit of "Internet sovereignty", or controlling online activity within China's borders.

The ban on individual access to VPNs follows new rules introduced in June 2017 requiring companies wishing to use VPNs to apply to the government for permission. They also face strict rules on data transfers.

Many foreign businesses have expressed concern at the implications for privacy, data protection and the security of their intellectual property. Possible workarounds may exist for technically proficient individuals, but average Internet users face being cut off from the free and open Internet.

Sources for the NCSC report: Bloomberg News, "China Tells Carriers to Block Access to Personal VPNs by February" (10 July 2017); Washington

Post, “Here’s China’s latest plan to keep its citizens from the open Internet” (10 July 2017).

The internet is changing the way we live, work, produce and consume. Many developed and developing countries will change what the internet is, for their population.

Number 3

Password challenges

National Cyber Security Centre
a part of GCHQ

Passwords have been in the news again.

On Friday 23 June, accounts with weak passwords on the UK Parliamentary network were compromised; however less than 1% of the system's 9,000 accounts were directly affected.

Attention was also drawn to router password vulnerabilities, as Virgin Media advised customers with Virgin Super Hub 2 home routers to reset their passwords.

This followed concerns that the routers had a relatively weak eight-character default password consisting of lower case letters that could be cracked in four days, potentially allowing access to other home devices.

Routers supplied by other service providers may also come with default passwords.

Passwords also featured in Ciaran Martin's interview with BBC's Today programme (Friday 30 June, 0810) where he recommended that two-factor authentication be used so that a stolen password is much less valuable to a criminal.

You may visit: http://www.bbc.co.uk/programmes/b08vwn8b#play

NCSC password guidance can be found there:
https://www.ncsc.gov.uk/guidance/password-collection

Number 4

Getting ready for the European Cyber Security Month 2017

Less than three months are left for the launch of the European Cyber Security Month, the EU annual awareness campaign which takes place in October supported by ENISA and EC DG CONNECT with the participation of many partners from all over Europe.

"Cyber Security is a shared responsibility!" is the motto of the ECSM campaign. Preparation for this year's Cyber Security Month kick-off event is in collaboration with the Estonian Information Systems Authority.

Taking place during the Estonian Presidency, the Estonian Ministry of Economic Affairs & Communication will be hosting the kick-off event at their premises in Tallinn on the 29th September 2017.

The ECSM runs for the entire October, with each of its four weeks focusing on a different topic. During each week, ENISA and its ECSM partners will be organising events and activities centred on each of these themes.

Events may have an emphasis on education material, strategy summits, general presentations to users, online quizzes, etc. 2017 marks the 5 year anniversary of the ECSM campaign.

Check out the themes planned for this year's ECSM:

Week 1: Oct. 2-6
Theme: Cyber Security in Workplace
Targeting businesses, the aim of the theme is to raise awareness amongst company employees, IT professionals & senior management about threats such as Ransomware, Phishing, Malware and to provide general cyber "Hygiene" advice.

Week 2: Oct. 9-13
Theme: Governance, Privacy & Data Protection

Countdown to compliance: Ensure you're ready!!! The aim of this theme is to uncover how to prepare your organization for the new EU Directives and Regulations such as the NIS Directive and the GDPR.

Week 3: Oct. 16-20
Theme: Cyber Security in the Home
The aim of the theme is to raise awareness amongst general users of threats from IoT, online fraud / scams and provide guidance on how protect their home network and protect their online privacy.

Week 4: Oct. 23-27
Theme: Skills in Cyber Security
The theme seeks to support the young with gaining Cyber Security skills via training and education so as to grow the next generation of skilled Cyber Security professionals.

Find out more about the activities and how to get involved at:
https://cybersecuritymonth.eu/

About ECSM: ECSM is the EU's annual awareness campaign taking place in October, which aims to raise awareness on cyber security threats, promote cyber security among citizens and provide up to date security information, through education and sharing of good practices.

The ECSM video about all you need to know:

https://www.youtube.com/watch?v=Rr-gVUG9koM

Number 5

SEC Files Fraud Charges in Bitcoin and Office Space Investment Schemes

U.S. SECURITIES AND EXCHANGE COMMISSION

The Securities and Exchange Commission filed fraud charges against the clandestine founder of a purported Bitcoin platform and a chain of co-working spaces located in former bars and restaurants, alleging that he bilked investors in both companies while hiding his connection given his checkered past with regulators in the U.K.

The SEC alleges that Renwick Haddow, a U.K. citizen living in New York, created a broker-dealer and did not register the firm with the SEC as required under the federal securities laws. Haddow allegedly used sales representatives to cold call potential investors and sell securities in Bitcoin Store Inc. and Bar Works Inc.

According to the SEC's complaint, offering materials presented to investors in both companies touted the backgrounds of senior executives who do not appear to exist.

The materials also misrepresented other key facts about both companies' operations. Haddow allegedly diverted more than 80 percent of the in funds raised by the broker-dealer for the Bitcoin Store, and sent more than $4 million from the Bar Works bank accounts to one or more accounts in Mauritius and $1 million to one or more accounts in Morocco.

"As alleged in our complaint, Haddow created two trendy companies and misled investors into believing that highly-qualified executives were leading them to quick profitability. In reality, Haddow controlled the companies from behind the scenes and they were far from profitable," said Andrew M. Calamari, Director of the SEC's New York Regional Office.

The SEC alleges that materials provided to Bitcoin Store investors claimed it was "an easy-to-use and secure way of holding and trading Bitcoin" and had generated several million dollars in gross sales. In fact, the SEC alleges that Bitcoin Store has never had any operations nor generated the gross sales it touted.

In 2015, for example, Bitcoin Store's bank accounts allegedly received less than $250,000 in incoming transfers, none of which appear to reflect revenue from customers. According to the SEC's complaint, the corporate address used for Bitcoin Store was Haddow's residential address minus the apartment number.

According to the SEC's complaint, Bar Works claimed to bring "real vibrancy to the flexible working scene by adding full-service workspaces to former bar and restaurant premises in central city locations." Bar Works primarily sold leases coupled with sub-leases that together functioned like investment notes. The company also allegedly sold leases for more workspaces than actually existed in at least two locations. Among false claims made to investors, who invested more than $37 million in the Bar Works scheme, were that a location was profitable within months of opening and that Bar Works had engaged an auditor.

In a parallel action, the U.S. Attorney's Office for the Southern District of New York announced criminal charges against Haddow.

The SEC's complaint filed in federal district court in Manhattan charges Haddow, Bitcoin Store, Bar Works, and another Haddow-controlled company called Bar Works 7th Avenue, Inc. with violating Section 17(a) of the Securities Act of 1933 and Section 10(b) of the Securities Exchange Act of 1934 and Rule 10b-5. The complaint further alleges that Haddow is liable for aiding and abetting Bitcoin Store, Bar Works, and Bar Works 7th Avenue's violations and as a control person for the registration violations of his brokerage firm InCrowd Equity Inc.

The SEC has obtained an emergency asset freeze against all defendants and relief defendants in the case.

The SEC's investigation is being conducted by Maureen P. King, Preethi Krishnamurthy, Neil Hendelman, and Sandeep Satwalekar. The case is being supervised by Lara Shalov Mehraban. The litigation will be handled by Ms. Krishnamurthy, Ms. King, and Christopher J. Dunnigan. The SEC appreciates the assistance of the U.S. Attorney's Office for the Southern District of New York and the Federal Bureau of Investigation.

Number 6

A portion of Microsoft Windows 10 Source code leaked online

National Cyber Security Centre
a part of GCHQ

Microsoft have confirmed a portion of its source code has been leaked online.

The initial source of the leak is unknown; however, the content was posted to Beta Archive, one of the largest online 'Beta and Abandonware' repositories for prototype software.

The leaked content was 1.2GB in size and has since been removed from the Beta Archive site.

Microsoft already shares some of its source code with industry partners and government through its Shared Source Initiative. However, this instance represents an unauthorised leak.

A number of theories about who is responsible are currently circulating.

Was it one of Microsoft's trusted partners who already had access to the source code?

Or was it a criminal who illegitimately obtained access to the code before leaking it?

There is no evidence to confirm either way at this stage.

The leak occurred one day after two men were arrested in the UK for unauthorised access to Microsoft's network, however there is no evidence that these two incidents are related.

Some reports have highlighted the risks of malicious actors using the leak to identify vulnerabilities in the code before developing exploits to target them.

However, when a similar leak occurred in 2004 of Microsoft's Windows 2000 code, similar claims were made, but did not result in a significant up-

tick in related attacks. Also, white hat hackers may use the leaked code as an opportunity to investigate it for vulnerabilities before reporting them to Microsoft for fixing.

While Microsoft has responded to this incident, questions have been raised about how the source code was originally obtained.

Disclaimer

Cyber Risk GmbH enhances public access to information about cyber risk and compliance in Switzerland.

Our goal is to keep this information timely and accurate. If errors are brought to our attention, we will try to correct them.

This information:

- is of a general nature only and is not intended to address the specific circumstances of any 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 Cyber Risk GmbH has no control and for which Cyber Risk GmbH assumes no responsibility;

- is not professional or legal advice);

- is in no way constitutive of an interpretative document;

- 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.