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

February 2018, cyber risk and compliance in Switzerland

Do you remember the recent WannaCry ransomware attacks? Well, attackers have better options.

State-sponsored hackers, criminals, and others, now prefer WannaMine and other malware variants, that hijack processing power to mine a cryptocurrency called Monero.

A good lawyer and friend has told me: "I want to have the Internet, the whole Internet, and nothing but the Internet." Everything that stands between him and the Internet is a curse. A few days ago, his computers were very slow, and he wondered why.

WannaMine infects computers, uses them to run complex decryption routines that create Monero, and adds the cryptocurrency produced to a digital wallet belonging to the puppet masters that designed the process.

Attackers usually trick victims into loading crypto mining code onto their computers through phishing. If you receive a legitimate-looking email, you may click on a link, no matter how many times you have been advised not to do so.

To make things worse, attackers can inject scripts on legitimate websites. Once victims visit the websites, the script automatically executes.

Can it become worse? Absolutely. What if they persuade you that you save money if you let them mine crypto currencies using your computer? For example, you receive a service for free, if you let them use your processing power while you are browsing a web page. Deal?

There is software available, designed to offer websites an alternative to advertising. Instead of requiring users to tolerate ads, sites offer an ad-free experience, in exchange for some CPU power to mine cryptocurrency. And users opt in.

Are you surprised to hear that the mining doesn't end when a user leaves the website?

How can you avoid that? Awareness, training, countermeasures are all required. For example, you can prevent JavaScript or other website scripts from executing, and you must use adblockers.

No, you cannot have the Internet, the whole Internet, and nothing but the Internet.

What about other devices and cell phones?

As an example, an Android malware called Loapi can lead to all kinds of problems, including cryptocurrency mining.

Trojan.AndroidOS.Loapi is a hidden part of apps, distributed through third-party markets, browser ads, and SMS-based spam. Mobile antivirus apps and, of course, adult-related apps, may hide the Loapi module.

After the installation of the app, Loapi asks for administrator rights. Again, and again, and again, until you give up and do it. You can change it later, right?

If you try to deprive the app of administrator rights, Loapi locks the screen and closes the settings window. And they you try to solve the problem, and you download other apps (antivirus, for example).

In this case Loapi alerts you that these apps are malware, and it demands their removal. Again, and again, and again, until you give up and do it.

And what is Loapi doing on the device? You gave it administrative rights, remember?

- Loads banner and video ads.

- Downloads and installs other apps.

- Visits links, opens web pages, opens Facebook and Instagram to drive up ratings.

- Signs up users to paid services. Even when such subscriptions must be confirmed by SMS, Loapi sends the text message secretly. Then these messages are deleted.

- It turns the phone into a zombie and takes part in DDoS attacks.

- It mines cryptocurrencies (Monero tokens). This activity can overheat the device.

- It downloads new modules to adapt to any new strategy, development, or objective.

I will tell it again. Install apps only from official stores. Disable the installation of apps from unknown sources. (Settings, Security, the Unknown sources check box is not selected).

And, this is just the first line of defense, based on awareness, training and countermeasures.

But there are other interesting developments:

After all these security issues with the Internet of Things, we have even more security issues with the Internet of Bio-Nano Things (IoBNT).

Scientists elaborate on the possibility to combine Internet-enabled devices with miniaturization and biological processes.

It is being envisaged that technology will provide “tools to control, reuse, modify, and reengineer the cells’ structure and function, and it is expected to enable engineers to effectively use the biological cells as programmable substrates”.

In this context an implementation of Bio-Nano Things as biological embedded computing devices is being considered as a main enabler.

If seen together with developments in DNA research, biocomputing and

advances in e-health and medicine, IoBNT opens up numerous avenues for technological breakthroughs where cyber becomes part of and controls vital human biological processes.

It could be good, but what about cyber risks?

Such a development will bring massive challenges to technology, including ethical, social, legal economic and political aspects, to mention the most imminent ones.

Though the effects of these developments are difficult to assess by now, technologist will need to be aware that a lot of work will be necessary in order to cope with such challenges.

Coverage of security issues in IoBNT will bring massive challenges for security and cyber-security: level of protection will be the highest possible, as the assets to be protected are the building blocks of life and health.

Moreover, trust in the functions and in the communication between all involved components will be of great importance.

Finally, requirements of identification, accountability, non-repudiation and integrity functions will be decisive for the development and deployment of IoBNT.

It is good to read the repost from ENISA:

Looking into the crystal ball
A report on emerging technologies and security challenges

The time has come for ENISA to take a look at the crystal ball of technology; In particular looking at what are considered to be emerging technologies and what might be their prospective usage scenarios.

Considering emerging technologies and applications is an important step in assessing future security needs.

ENISA has performed this effort in collaboration with external experts from academia and industry.

Starting with a small number of individuals, it is planned to expand this assessment by engaging additional experts, both within and outside ENISA committees and bodies.

For the time being, the initial sight to emerging technologies has shown that currently top technological challenges are:

- The Internet of Things,
- Autonomous systems,
- Next generation virtualized infrastructures (including SDN and 5G),
- Upcoming societal challenges,
- Virtual and Augmented reality,
- The Internet of Bio-Nano Things,
- AI and Robotics.

Knowing that the above list is not exhaustive, ENISA will continue the dialogue with experts to complement it.

For the above emerging technology areas both technological and cyber-security challenges are presented in this report.

By taking into account the emerging security challenges, the most important cyber security areas have been identified by means of "emerging security related areas".

These are:

- Elaboration on Certification,
- Coordination of actions in cyber space,
- Development of trustworthiness,
- Coverage of complete lifecycle,
- The future of cryptography,
- Future Identification technologies,
- Use of Artificial Intelligence and Machine Learning in cyber security,
- Increasing end-user involvement.

ENISA believes that these cyber security areas will present challenges to the cyber security community in the years to come and hopes that they will be extensively discussed within its stakeholder communities.

Last but not least, in this work input that has been received by the ENISA Permanent Stakeholder Group (PSG) is being mentioned.

In a similar manner, input will be integrated through an interaction with the new PSG that will have its kick-off end of October 2017.

In this manner, both previous and new contributions from PSG will be put in the context of the areas presented in this report, widening thus significantly the number of contributors.

To read more:
https://www.enisa.europa.eu/publications/looking-into-the-crystal-ball

There is a third interesting development this month:

Erich Fromm believed that if a person loves only one other person and is indifferent to all others, his love is not love, but a *symbiotic* attachment, or an enlarged egotism.

Mutualism is a *symbiotic* relationship between individuals of different species in which both benefit from the association.

Commissioner (SEC) Kara M. Stein said that the relationship between a company and its shareholders is rooted in a similar form of *mutualism.* Shareholders invest their savings or capital in a company. The company then deploys the capital to fund its operations.

Kara gave a *great example of mutualism*: The relationship between bees and flowers.

Bees fly from flower to flower gathering nectar to make food. By flying from flower to flower, bees pollinate the plants on which they land. Bees get to eat, and the flowering plants get to reproduce. Bees help plants grow, thus supporting other animals, including us humans. The bee-flower relationship is integral to our entire food chain, and our larger ecosystem.

Kara continues on the relationship between a company and its shareholders:

This corporation-shareholder relationship is likewise part of a larger ecosystem. When all goes well, more employees and managers get hired, and the company produces more products or provides more services, all of which benefits the entire economy.

Unfortunately, the relationship between corporations and their shareholders may be moving away from its origins and becoming *less*

mutualistic. This may harm companies and their shareholders, as well as those who depend on the health of the corporation-shareholder relationship.

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

Our events and *open* instructor-led classes:
www.cyber-risk-gmbh.com/Events.html

Number 1 (Page 12)

From GovCERT.ch

Fake e-mails are currently being sent with the aim of infecting citizens with the eBanking trojan "Retefe"

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Government Computer Emergency Response Team

Number 2 (Page 15)

Cybersecurity built on trust – ENISA supports Member States in establishing PPPs and ISACs

ENISA publishes two reports: Cooperative models for Public Private Partnerships (PPPs) and Cooperative models for Information Sharing and Analysis Centres (ISACs).

enisa *European Union Agency for Network and Information Security*

Number 3 (Page 18)

European Cyber Security Month 2017
Deployment Report, February 2018

5th EUROPEAN CYBER SECURITY MONTH Anniversary

Number 4 (Page 22)

Cryptomining trends

National Cyber Security Centre
a part of GCHQ

News articles have focused recently on the value and volatility of cryptocurrencies, over the past year, most notably Bitcoin which had a peak value of $20,089.00 in December 2017.

Number 5 (Page 24)

IT security
BaFin (Bundesanstalt für Finanzdienstleistungsaufsicht) specifies requirements for the banking industry

BaFin
Federal Financial Supervisory Authority

BaFin has published the Supervisory Requirements for IT in Financial Institutions (Bankaufsichtliche Anforderungen an die IT – BAIT).

Number 6 (Page 26)

Improving recognition of ICT security standards

Recommendations for the Member States for the conformance to NIS Directive

www.enisa.europa.eu European Union Agency For Network and Information Security

This report is a continuation and an extension of previously carried out ENISA work on approaches to the NIS Directive by Member States, which have provided recommendations on standardisation and have outlined the use and management of CSIRTs.

Number 7 (Page 29)

Meltdown and Spectre – Updated Advice

National Cyber Security Centre
a part of GCHQ

Malware making use of Meltdown and Spectre, the two CPU vulnerabilities highlighted back in January, is now being seen in the wild.

Security researchers are reporting they have seen over 140 malware samples based on the proof of concept code.

Number 8 (Page 30)

DARPA Seeks to Improve Military Communications with Digital Phased-Arrays at Millimeter Wave

New program aims to create multi-beam, digital phased-array technology, operating at 18-50 GHz to enhance secure communications between military platforms

DARPA DEFENSE ADVANCED RESEARCH PROJECTS AGENCY

Number 9 (Page 33)

Mutualism: Reimagining the Role of Shareholders in Modern Corporate Governance" Remarks at Stanford University

Commissioner Kara M. Stein

Number 10 (Page 40)

MI6, British Intelligence Explained

Number 1

From GovCERT.ch

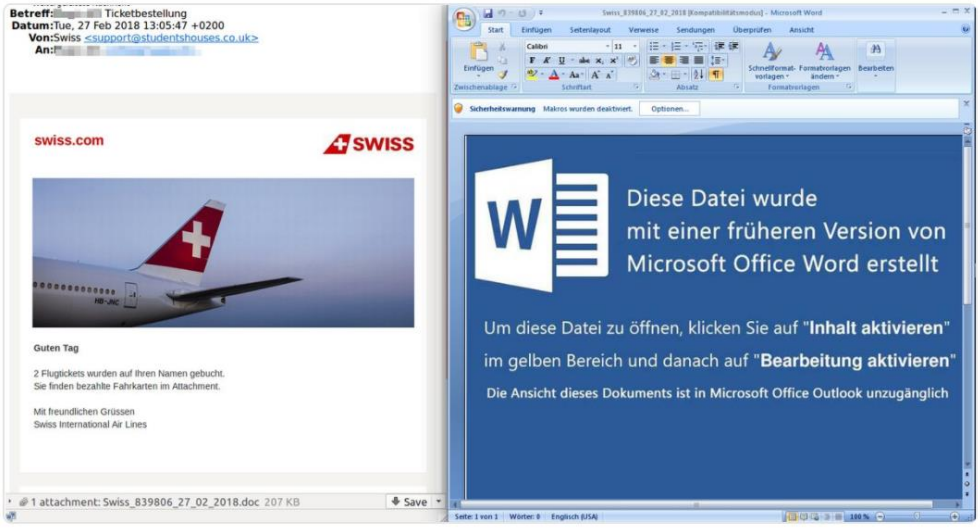
Fake e-mails are currently being sent with the aim of infecting citizens with the eBanking trojan "Retefe"

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Government Computer Emergency Response Team

You can help if you report suspicious emails. Antiphishing.ch is operated by the Reporting and Analysis Centre for Information Assurance MELANI of the Swiss Federal Administration.

The goal is to provide users a simple and easy way to report phishing attempts.



We can read from www.antiphishing.ch/en/about/

What is phishing?

The word phishing is a contraction of the words "Password", "Harvesting" and "Fishing". Fraudsters phish in order to gain confidential data from unsuspecting Internet users.

This may, for example, be account information for e-banking, webmail or social media as well as credit card information.

The fraudsters take advantage of their victim's good faith and helpfulness by sending them e-mails with (often) false sender addresses and company logos.

The e-mails contain a more or less credible scenario according to which recipients are asked to follow a link to a website where they're supposed to log in to a service or indicate personal information.

The links are often "hidden" behind regular text or an unsuspicious address. Instead of leading to the official website of the respective service provider (e.g. the bank), the links direct users towards an imitation of this site that is controlled by the fraudsters.

You can often recognize a fake webpage by the lack of the HTTPS padlock -, a strange looking unusual URL, spelling mistakes or misleading questions about security updates or personal information.

Why should I report phishing attempts?

By reporting phishing attempts, you help protect other people. Your report enables us to take measures in order to prevent users to fall victim to phishing and reduce the chances of success of the fraudsters.

What happens after my report?

MELANI reviews each submission, informs the responsible hosting provider and website owner and asks them to take down the phishing-webpage.

In addition, MELANI shares the URLs with IT security providers, web browser vendors and blacklist providers to achieve a maximum level of protection of the users.

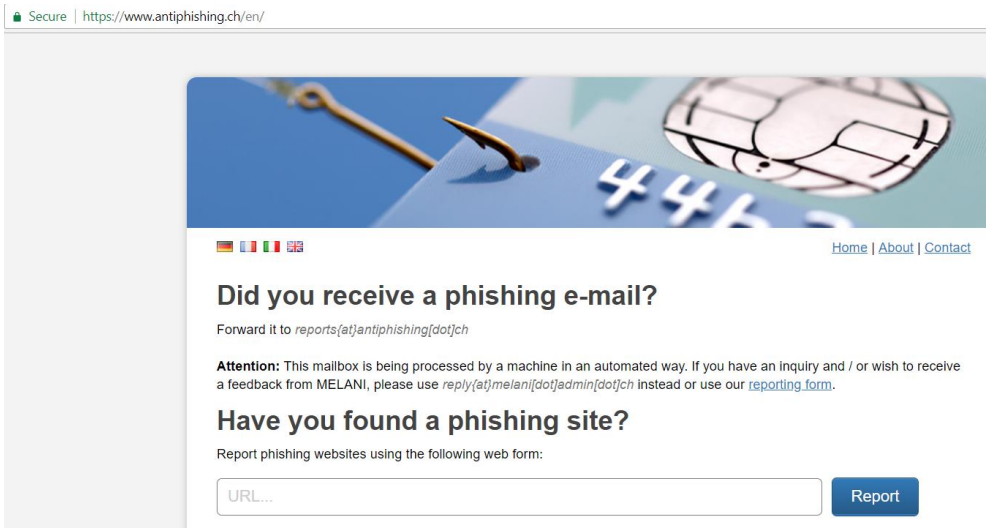
MELANI is not a police unit and does not conduct criminal investigations regarding the submitted phishing attempts.

The task of MELANI resides in averting imminent danger to information security, not the prosecution of criminals.

If you have suffered financial loss or suffered other damage due to phishing, you may press charges at your local police station.

Can I report malware incidents to antiphishing.ch?

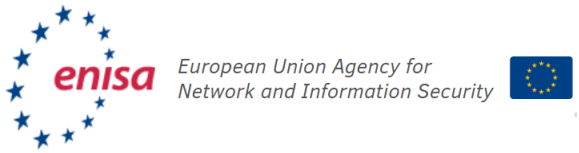
Yes. Submissions to antiphishing.ch related to malware will be analysed and reviewed too. Such submissions help us to spot and identify new malware campaigns.



Number 2

Cybersecurity built on trust – ENISA supports Member States in establishing PPPs and ISACs

ENISA publishes two reports: Cooperative models for Public Private Partnerships (PPPs) and Cooperative models for Information Sharing and Analysis Centres (ISACs).



A common objective of every European national cyber security strategy is collaboration to enhance cyber security across all levels, from threat information sharing to awareness raising.

Collaboration is often achieved through two formal structures: Information Sharing and Analysis Centres (ISACs) and Public Private Partnerships (PPPs).

Since many critical infrastructures are under private jurisdiction, cooperation between public and private sectors is essential to achieve an adequate level of cybersecurity.

Moreover, European legislations like the NIS Directive and the newly announced Cybersecurity Act encourage the creation of sectoral ISACs and PPPs within the EU.

ENISA collected information on best practices and common approaches that resulted in two studies, namely Cooperative Models for Public Private Partnership and Information Sharing and Analysis Centres.

Both reports are addressed at policy and lawmakers, national cybersecurity authorities, the CSIRT community, the general public and private organizations with an interest in network and information security.

Prof. Udo Helmbrecht, Executive Director of ENISA, said: “Cybersecurity is a shared responsibility and ENISA, together with the community, is continually working towards making collaboration as well as information and knowledge sharing stronger.

The multi-faceted efforts of ENISA across the cybersecurity spectrum continues to support and promote a safer Europe with better cybersecurity."

PPPs are long-term agreements and collaborations between representatives of public and private sectors.

The study on PPPs identifies four PPP models existing within the EU Member States: Institutional PPPs, goal-oriented PPPs, service outsourcing PPPs and hybrid PPPs.

ISACs are trusted entities, whose purpose is to foster sharing of information and good practices about physical and cyber threats, as well as mitigation.

In the study on ISACs, the most common approaches are categorized into three different models: country focused, sector specific and international structures.

The main finding of both studies is that trust is the most essential factor in establishing and maintaining cooperation between private and public sectors.

Both reports provide some specific recommendations:

For PPPs:

- Legal basis is essential when creating a PPP
- Investment on private-private and public-public collaboration is also critical for PPPs
- Open communication and a pragmatic approach are vital for setting up a PPP
- Small and medium Enterprises (SMEs) should also participate in PPPs

For ISACs:

- Creating a structure which motivates the private sector is essential for an ISAC
- Establishing a facilitator to involve all participants is also crucial for ISACs
- The production of valuable results is key to the success of an ISAC
- Cross sector collaboration is also very important for the effectiveness of ISACs

- Public and private sector stakeholders validated the two studies during the fifth ENISA-NCSS workshop, which was co-organised in October 2017 with NCSC in The Hague, the Netherlands.

The full reports:

https://www.enisa.europa.eu/publications/information-sharing-and-analysis-center-isacs-cooperative-models

https://www.enisa.europa.eu/publications/public-private-partnerships-ppp-cooperative-models

Number 3

European Cyber Security Month 2017
Deployment Report, February 2018

For the fifth consecutive year, last October the European Cyber Security Month (ECSM) campaign was successfully executed across Europe.

The campaign was coordinated and supported by ENISA, the European Commission, Europol's Cyber Crime Centre (EC3), European Banking Federation, the Estonian Information Systems Authority and cyber security organisations from the Member States.

The support for which propelled the campaigns success as measured by both the qualitative and quantitative data compiled.

Although this year's campaign continues to break new records, the conclusions of this report highlight a number of fundamental areas that need to be addressed in the coming years if the campaign is to continue to grow and more importantly influence the security behaviour of citizens online.

Citizens across Europe face similar information security threats and information asset vulnerabilities; this is because most of the platforms, operating systems and devices used are produced by the incumbent global product/service providers.

This applies to mobile phones, email messaging services, laptops and social media channels, since the vast majority of European citizens use similar technologies.

However, citizens of each Member State have different levels of cyber security knowledge and behaviour.

These differences across Member States may be triggered by the disparity of Member States in their commitment to awareness raising.

In particular some Member States have a dedicated team of experts for planning and executing national security awareness campaigns; for example, the BSI in Germany and the ANSSI in France.

Other Member States assign this role to a Ministry or Government CERT alongside their other core activities without a dedicated representative.

The effects of this is that there is a discrepancy between the measures that citizens may apply for the same or similar vulnerability or risk is one Member State compared to that of another Member State.

An example of the situation, the Eurobarometer survey highlights many differences across Member States in the use of cyber security measures,such as firewalls or the awareness of phishing attacks.

Therefore, the different level of citizens' awareness and the potential risk-taking behaviour across Europe in turn leads to an increase in the risk level of Europe as a whole.

The concept for the European Cyber Security Month is to address this disparity across Member States in two stages.

The first stage is to support the Member States so that the awareness and behaviour of citizens in each Member State is raised to a mature baseline.

This becomes the reference baseline across the whole of Europe and thereby the European Cyber Security Month aligns the risk levels across Europe.

The second stage is to further lower this risk by raising the maturity of citizen's behaviour in unison; at the European level.

ENISA and the European Commission can achieve the objectives of the European Cyber Security Month by driving the pan-European campaign so as to ensure all Member States are actively committed to the European Cyber Security Month and that industry is also involved at all levels of the campaign both at the local and European level.

The ground work is in place for the European Cyber Security Month to move to the next level. This next level will be achieved only once a governance structure has been put in place as highlighted in the conclusions of this report.

Furthermore a governance structure will ensure that the campaign is driven by MS as they are ultimately the benefactors of the campaign.

A secondary reason for establishing a governance structure is to achieve another goal raised in the conclusions of this report which is to increase the commitment of the MS to the campaign and to bring on board those MS that have yet to designate a competent body to the campaign.

This report provides an overview of the activities organised and presents a synthesis of findings on the basis of evaluation and performance information gathered via a questionnaire and media monitoring data.

The report is structured into three main parts: an introduction, the implementation phase and an evaluation of the campaign. The introduction will provide readers with the policy context, scope and target audience of the campaign.

The implementation phase of the report highlights the milestones that were achieved during the planning and execution phase of the campaign.

This includes how events were organized and co-ordinated with partners, marketing materials used and insights into the execution of the campaign including results.

The final section of the report deals with the evaluation of the campaign, comparing this year's results with the previous year's and also provides input from the partners that was generated via a questionnaire; and finishes with a conclusion and outlook for the future.

Documenting the activities of ECSM 2017 will assist in the organization and execution of future ECSM campaigns and allow for comparing the campaign with the results from previous years.

The evaluation results and estimated impact of ECSM activities will provide the opportunity to discuss lessons learned deriving from this exercise and to helps draw attention to related concerns and opportunities for further improvement.

Finally the report is intended to provide a basis for discussion among the Member States, the European Commission and ENISA on how the ECSM can best be organised in the years to come.

All Member States will need to face up to similar challenges, namely how to engage citizens and organizations so as to affect their information security behaviour.

To read more:
https://www.enisa.europa.eu/publications/european-cyber-security-month-2017

European Union Agency For Network And Information Security

Number 4

Cryptomining trends

National Cyber Security Centre
a part of GCHQ

News articles have focused recently on the value and volatility of cryptocurrencies, over the past year, most notably Bitcoin which had a peak value of $20,089.00 in December 2017.

Cryptocurrencies can be earned, or 'mined', by performing computationally intensive operations to support the running of the currency. Malware intended to mine cryptocurrencies on victim computers has been available since at least 2013 and surged in popularity in late 2017 as the currencies' value increased.

Cryptomining malware is attractive to cyber criminals as they are able to use botnets of compromised machines as miners without having to cover the infrastructure costs (e.g. the cost of electricity would be covered by the victim).

Despite the potentially lucrative rewards, cryptomining is becoming increasing economically unviable for some legitimate users as the running costs (hardware and associated electricity costs) often outweigh any potential gains in this increasingly competitive environment.

This has also had real world implications on the price and availability of graphic cards as many are now being purchased specifically for cryptomining.

For cyber criminals, cryptomining malware has some advantages over ransomware. It doesn't rely on the victim being willing and/or capable of making payment. It is also not confrontational but is designed to operate undetected in the background over a long period, potentially earning more money than a ransomware campaign.

More importantly, it can be distributed through same delivery mechanisms as ransomware (e.g. exploit kits) and, once established, a network of mining bots can generate a respectable amount of money with minimal effort (e.g. the Smominru botnet generates 24 XMR per day (approximately £8,500)). Monero is the preferred currency as the

processing power required to mine it is minimal compared to that required to mine Bitcoin.

It is highly likely that the criminal deployment of cryptomining malware will increase during 2018 as cyber criminals either shift their focus away from other forms of malware or run these campaigns alongside their established cyber criminal activities.

Number 5

IT security
BaFin (Bundesanstalt für Finanzdienstleistungsaufsicht) specifies requirements for the banking industry

BaFin
Federal Financial
Supervisory Authority

BaFin has published the Supervisory Requirements for IT in Financial Institutions (Bankaufsichtliche Anforderungen an die IT – BAIT).

The BAIT have now become the cornerstone of IT supervision for all credit and financial services institutions in Germany.

The requirements are directed at the management boards of such companies.

The objective of the BAIT is to create a comprehensible and flexible framework for the management of IT resources, information risk and information security.

They also aim to contribute towards increasing awareness of IT risks throughout the institutions and in relation to external service providers.

Furthermore, they provide transparency about what banking supervisors expect from the institutions with regard to the management and monitoring of IT operations, including the user access management that this necessitates as well as requirements for IT project management and application development.

Overall, the BAIT address those subject areas which BaFin has identified as particularly important based on its experience of IT inspections.

One on the primary objectives of the BAIT is to improve awareness of IT risks at institutions, especially at management levels.

Banking supervisors understand the term "IT risk" as meaning all risks to the institution's financial position and financial performance that arise from deficiencies relating to IT management, the availability, confidentiality, integrity and authenticity of data, the internal control

system for IT organisation, the IT strategy, IT guidelines and IT topics in the rules of procedure, or the use of information technology.

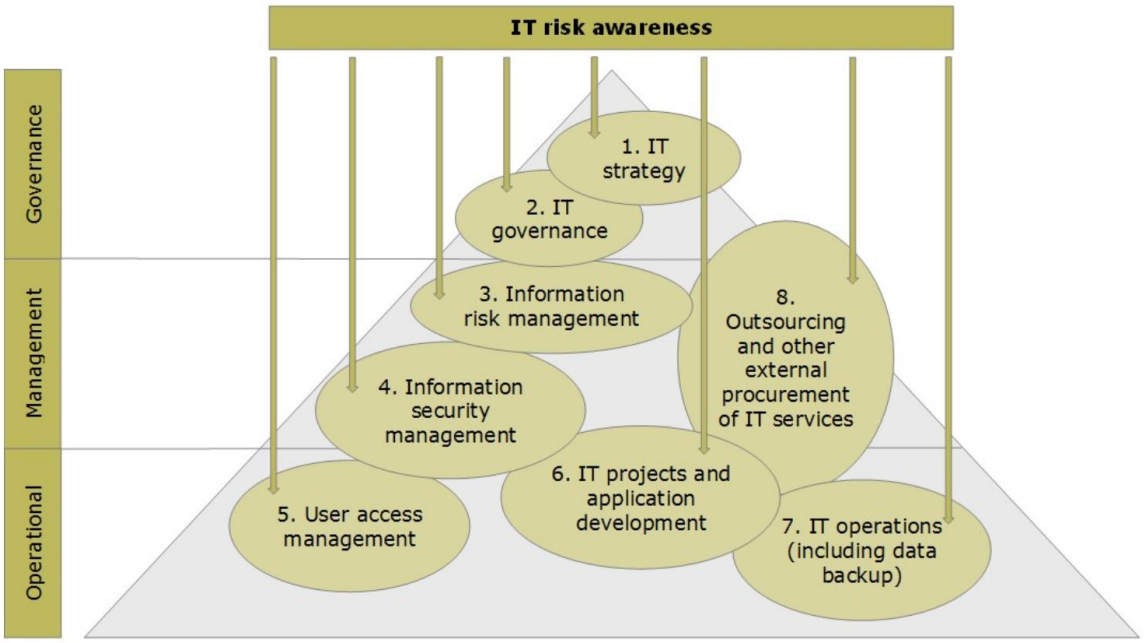


Figure: Improving risk awareness with the BAIT; © BaFin

To read more:
https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Fachartikel/2018/fa_bj_1801_BAIT_en.html

Number 6

Improving recognition of ICT security standards

Recommendations for the Member States for the conformance to NIS Directive

www.enisa.europa.eu European Union Agency For Network and Information Security

This report is a continuation and an extension of previously carried out ENISA work on approaches to the NIS Directive by Member States, which have provided recommendations on standardisation and have outlined the use and management of CSIRTs.

This document provides the results of an assessment of the maturity of the implementation of the European Cyber Security Standardisation activities in the EU Member States with respect to the NIS Directive concerning measures for a high common level of security of network and information systems across the Union.

The main assertions this report makes include the following:

- Standardisation for compliance with the NIS Directive is essential;
- Recognition of standardisation in policy is low;
- Utilisation of standards give value to Member States and their infrastructure;
- Utilisation of standards raises Cyber Security levels;
- Utilisation of standards provides sustainability and interoperability at European level.

The current market research has clearly shown that the information security/cyber security standard development ecosystem is healthy and fast moving.

Few gaps actually exist and to implement the NIS Directive choosing the rights ones and implementing them is of paramount importance.

In the scope of this survey a questionnaire was sent to the Member States representatives and used as the basis of data gathering either in the form of interviews, or by directly completing it and sending responses to the authors.

A summary of the responses given have been collated and summarised.

The content of these responses does not allow to identify whether Member States perceive the existence of a gap in current available standardisation.

However, the content, and general limitations in the cohesion amongst Member States suggests that there is insufficient guidance from the specialists in the field (e.g. national normalization institutes, European institutions etc.), on which of the many standards available are to be used.

It is reasonably straightforward and it follows on the current rate on transposition, to suggest that all Member States are aware of the NIS Directive and their responsibilities in implementing it.

What is less clear is the role that standards have in the NIS Directive implementation.

There is insufficient information with regard to the responses to conclude that a lack of knowledge of standards exists.

This suggests however that if an appropriate standard is available, it will be adopted.

For example, even though the ISO27000 series of standards are in the form of broad guidance, there is a well established eco-system that addresses their implementation.

A major concern is that the NIS Directive domain, and compliance with the NIS Directive requirements, is often perceived as a purely national prerogative.

Where international, cross-border, information sharing is required, this has been perceived as in the domain of existing CSIRT relationships used for reporting security incidents and not directly as an element of NIS Directive compliance.
At the operational level there is very little specified for standards-based NIS Directive compliance and this is one area where ETSI, for example, has made some contributions.

However, there are no mandates at either national or European level to guide this activity at the implementation level.

In light of the above, the following solutions are recommended to mitigate the lack of overall awareness and trainings on the role of standards in NIS Directive compliance and to encourage wide deployment of common security platforms in the OES and PDS entities:

• Training initiatives by the European Commission and ENISA through workshops for Member States' relevant agencies

• Promotion of new work items in the European SDOs for some areas (e.g. criteria for defining OES / DSP) or the adoption of appropriate standards in Europe where existing (for example information exchange, where several mature efforts already are in place, like STIX)

• Repeat the information gathering as performed within the elaboration of this study after an adequate interval of time

To read more:
https://www.enisa.europa.eu/publications/improving-recognition-of-ict-security-standards

Number 7

Meltdown and Spectre – Updated Advice

National Cyber Security Centre
a part of GCHQ

Malware making use of Meltdown and Spectre, the two CPU vulnerabilities highlighted back in January, is now being seen in the wild.

Security researchers are reporting they have seen over 140 malware samples based on the proof of concept code.

Whilst there have not been instances of Meltdown and Spectre actually being leveraged to compromise a system, it is a timely reminder that miscreants will take published security vulnerabilities and weaponise them into malware quickly, making it all the more important to patch.

As previously reported by the NCSC, Meltdown and Spectre are two related, side-channel attacks against modern microprocessors that can result in the unprivileged code reading data it should not be able to access.

Most devices may be vulnerable to some extent with many vendors releasing patches to secure systems.

The NCSC have previously advised users and business enterprise users to follow vendor advice and apply patches.

For more detailed advice regarding these vulnerabilities, please see the latest guidance from the NCSC at:
https://www.ncsc.gov.uk/guidance/meltdown-and-spectre-guidance

Number 8

DARPA Seeks to Improve Military Communications with Digital Phased-Arrays at Millimeter Wave

New program aims to create multi-beam, digital phased-array technology, operating at 18-50 GHz to enhance secure communications between military platforms

There is increasing interest in making broader use of the millimeter wave frequency band for communications on small mobile platforms where narrow antenna beams from small radiating apertures provide enhanced communication security.

Today's millimeter wave systems, however, are not user friendly and are designed to be platform specific, lacking interoperability and are thus reserved for only the most complex platforms.

To expand the use of millimeter wave phased-arrays and make them broadly applicable across DoD systems, many technical challenges must be addressed, including wideband frequency coverage, precision beam pointing, user discover and mesh networking.

The use of multi-beam phased arrays as well as advances in digital radio and millimeter wave technology have propelled technology to the current state, and now there is a paradigm shift on the horizon as millimeter wave phased-arrays are poised to change communication and networked mobile platforms.

Phased-arrays operating at millimeter wave–or very high frequencies–are already an active area of research by the emerging 5G cellular market. Commercial applications are primarily solving the "last mile" problem, where consumers are demanding more bandwidth for high-throughput applications over relatively short ranges at predetermined frequencies and with minimal obstacles to user discovery.

DoD platforms on the other hand create far more complex communications environments. Often separated by tens or even hundreds of nautical miles, today's military platforms are moving in three dimensions with unknown

orientations. This environment is creating unique beamforming challenges that can't easily be solved by applying current communications approaches.

"Imagine two aircraft both traveling at high speed and moving relative to one another," said DARPA program manager Timothy Hancock. "They have to find each other in space to communicate with directional antenna beams, creating a very difficult challenge that can't be solved with the phased-array solutions emerging in the commercial marketplace."

To address these challenges, DARPA is launching the Millimeter-Wave Digital Arrays (MIDAS) program. Announced today, the program aims to develop element-level digital phased-array technology that will enable next generation DoD millimeter wave systems.

To help solve the adaptive beamforming problem and ensure wide application of the resulting solutions, MIDAS seeks to create a common digital array tile that will enable multi-beam directional communications.

Research efforts will focus on reducing the size and power of digital millimeter wave transceivers, enabling phased-array technology for mobile platforms and elevating mobile communications to the less crowded millimeter wave frequencies.

Advances in element-level digital beamforming in phased-array designs is enabling new multi-beam communications schemes—or the use of several beams receiving and transmitting in multiple directions simultaneously—to help significantly reduce node discovery time and improve network throughput. "While critical to the next generation of phased-arrays, today's digital beamforming is limited to lower frequencies, making the resulting arrays too large for use on small mobile platforms," said Hancock.

To reduce the size of the arrays, advances in millimeter wave technology will help push the frequency of operation to higher bands, bringing the capabilities of directional antennas to small mobile platforms. "Through MIDAS, we are seeking proposals that combine advances in millimeter wave and digital beamforming technologies to create radios that will deliver secure communications for our military," said Hancock.

To accomplish its goals, MIDAS is focused on two key technical areas.

The first is the development of the silicon chips to form the core transceiver for the array tile.

The second area is focused on the development of wide-band antennas, transmit/receive (T/R) components, and the overall integration of the system that will enable the technology to be used across multiple applications, including line-of-sight communications between tactical platforms as well as current and emerging satellite communications.

Hancock envisions the four-year program being administered in three phases.

A full program description can be found in the Broad Agency Announcement that was issued on January 23: https://www.fbo.gov/index?s=opportunity&mode=form&id=d8c414aaf7c707bc4f7ac896a7b68b29&tab=core&_cview=0

Number 9

Mutualism: Reimagining the Role of Shareholders in Modern Corporate Governance" Remarks at Stanford University

Commissioner Kara M. Stein

Thank you, Professor [Joe] Grundfest, for that kind introduction. It is a pleasure to be with you this evening, and I would like to thank the Corporations and Society Program and the Rock Center for Corporate Governance for inviting me to visit with you.

In particular, I would like to thank Professors [Anat] Admati and [Joe] Grundfest for extending to me such a warm welcome.

Before I go further, I must state that the views I express today are my own, and do not necessarily reflect those of my fellow Commissioners or the SEC staff.

Tonight, I want to talk to you about something that has been vigorously debated in recent years: What is, and what should be, the role of the corporate shareholder?

In the spirit of being in California, this debate could be summarized as follows: Are shareholders merely extras in the corporate movie? Or are they lead actors that need to be empowered so that they can successfully play their roles?

However, as most people in this room know, it is actually much more complicated than that. It is not, and should not be conceptualized as, a binary choice.

Rather, I would posit that the entire corporate ecosystem's success actually rests on effective communication and collaboration between corporations and their shareholders.

When a company, its management, its shareholders, and its employees work together, companies tend to be more resilient and prosperous. In turn, this benefits companies, their corporate stakeholders, and the economy as a whole.

Today's corporations influence and impact our society in a multitude of ways. Corporations help grow our economy, provide well-paying jobs, and provide earnings to investors saving for retirement, college, or a new home.

Many companies, whether small or large, are helping to drive our society forward, developing new technologies that are raising our living standards, improving our environment, and lengthening our life span.

Corporations hold some of our most precious assets, such as medical histories, consumer bank account information, addresses, and other sensitive information. They also are central players in some of our most immediate problems, such as global warming.

Corporations have shaped, and will continue to shape, our society, our identities, and our relationships with one other. This week's series seeks to promote a discussion of the interrelationship and interdependency between corporations and our society.

Pretty heady stuff, to be sure, but extremely important. Not only from an academic point of view, but from a practical and policy point of view, as well.

So, I thought I would start off our discussion tonight by talking a bit about the science of "mutualism."

For those of you not familiar with the concept, mutualism is a symbiotic relationship between individuals of different species in which both benefit from the association.

One example of mutualism is the relationship between bees and flowers. Bees fly from flower to flower gathering nectar to make food. By flying from flower to flower, bees pollinate the plants on which they land.

Bees get to eat, and the flowering plants get to reproduce. Bees help plants grow, thus supporting other animals, including us humans. The bee-flower relationship is integral to our entire food chain, and our larger ecosystem.

The relationship between a company and its shareholders is rooted in a similar form of mutualism. Shareholders invest their savings or capital in a company. The company then deploys the capital to fund its operations.

This allows the corporation and its shareholders' investments to grow. This corporation-shareholder relationship is likewise part of a larger ecosystem.

When all goes well, more employees and managers get hired, and the company produces more products or provides more services, all of which benefits the entire economy.

Unfortunately, the relationship between corporations and their shareholders may be moving away from its origins and becoming less mutualistic.

This, I believe, may harm companies and their shareholders, as well as those who depend on the health of the corporation-shareholder relationship.

So, how do we restore mutualism in the relationship upon which our corporate ecosystem is based?

MUTUALISM AND THE CORPORATION-SHAREHOLDER RELATIONSHIP

Brief History

I recently remarked upon the history of the American corporate form, and I would like to start my talk tonight there, as well.

Don't worry, I won't go as far back as the Dutch East India Company and its participanten, or the tulip bulb market.

Rather, I will quickly touch upon the history of the corporation-shareholder relationship in the United States to inform the rest of our discussion.

From the late-1700s to the mid-1800s, corporations started to flourish in the United States.

American companies typically operated within a single state or community.

The shareholders of a corporation were often members of the same community in which the corporation was located. As a result, they were able to engage and monitor the company's business affairs in a more direct manner than we currently see today.

A corporation also met with its shareholders more frequently, whether in the form of shareholders' meeting or otherwise.

Beginning in the mid-1800s, however, companies started growing larger and the corporate form changed.

Companies began hiring managers—who often had no ownership interest in the companies—to run their affairs.

While this transition created certain efficiencies, it also in many cases separated the ownership of the company from the management of the company.

This had the effect of reducing shareholders' ability to directly influence the company's business.

Mutualism and the Corporation-Shareholder Relationship in Recent Years

A lot has happened since the mid-1800s, and we are now at a tipping point. Instead of being in the midst of an industrial revolution, we are in the midst of a digital revolution.

This new revolution comes with many benefits—speed, efficiency, and innovation, to name only a few.

Coupled with these benefits, however, are also some risks.

I think if we focus on the strengths of the American corporate form, we can successfully reimagine the corporation-shareholder relationship for the Digital Age.

I would like to discuss a few examples of how, in modern corporate governance, the concept of mutualism can help us think through the path forward for corporations, their shareholders, and the larger corporate ecosystem.

Cyberthreats

As we all know, the digital transformation is providing both companies and shareholders with tremendous opportunities. However, one of the biggest challenges facing corporations and their shareholders, their employees and consumers, and our economy as a whole, is cybersecurity.

As we have learned, cyberattacks can affect millions of people at once and potentially compromise our most sensitive personal information. Shareholders have been out front advocating for more information on company practices relating to cybersecurity.

The number of shareholder proposals regarding cybersecurity has increased in recent years.

But good information remains scarce. Unfortunately, corporate disclosures are far from robust and largely consist of boilerplate language that fails to provide meaningful information for investors.

While companies and shareholders agree that cybersecurity is one of the most prominent corporate issues of our time, it is unclear why companies are not doing more to implement robust cybersecurity frameworks and to provide meaningful disclosures regarding the risks of data loss.

Companies and their intermediaries tend to view cyberthreats as a technology problem instead of, more appropriately, a business risk. As we have seen time and time again, cybersecurity, and the related threats of unintentional loss of data, is a governance challenge for all of us, and it requires a change in culture and approach.

Many shareholders seem to understand this and have been urging, and continue to urge, companies to engage.

Regulators are certainly not immune from facing these challenges. In August 2017, I learned for the first time that the Commission's official record system was breached in 2016, and that this breach may have provided the basis for illicit gains through trading.

Clearly, the Commission's enterprise risk management processes failed to adequately address appropriate escalation protocols. Once he was informed, Chairman Clayton immediately launched an investigation into the breach and has focused the Commission and the staff on improving our risk management framework.

Companies, their managers, their boards, as well as their regulators, all need to do a better job in recognizing and addressing the significant risks that can result from the loss of data.

Breaches of security measures can result in theft, reputational harm, or the loss of intellectual property. Simply put, the unintentional loss of data may have material effects on companies. Slowly, regulators around the globe are stepping up to the challenge of issuing data protection laws and regulations.

The approach to these issues continues to evolve with the changing landscape. For example, the European Union's General Data Protection Regulation is set to go into effect in May 2018. China has begun enforcing regulations concerning "critical information infrastructure."

Last March, the New York Department of Financial Services required that regulated firms name a chief information security officer (or CISO). These CISOs must provide an annual report on cybersecurity to the firm's board.

Last year, a bipartisan bill was introduced in the Senate to require publicly traded companies to disclose whether any members of their board have cybersecurity expertise.

We at the Commission have not yet adequately pressed forward. While the Commission's staff has released disclosure guidance for public companies to consider when dealing with cyberrisks and breaches, the Commission can and should do more.

I believe the Commission should consider rules to require disclosure of a firm's enterprise-wide consideration of cyberrisks.

I also believe that we should develop rules to ensure that market intermediaries, including broker-dealers and investment advisers, develop and implement policies and procedures to protect investors' personal information.

The security and integrity of a corporation's assets, like the SEC's, is a great responsibility. As I said earlier, cybersecurity has been viewed by many as simply an "IT" problem, hoisted on the shoulders of a company's chief information officer.

Too often, this has led to a failure to integrate cybersecurity into a firm's enterprise risk management framework. To be sure, some companies are

focused on cyberthreats and recognize their potential economic threat. But companies need to do more than simply recognize the problem.

They need to heed the calls of their shareholders and treat cyberthreats as a business risk.

Corporations and shareholders will both benefit from greater transparency and focus on the risks related to unintended data loss and the collateral consequences.

To read more: https://www.sec.gov/news/speech/speech-stein-021318

Number 10

MI6, British Intelligence Explained

A very interesting page.

You may visit:
https://www.sis.gov.uk/intelligence-explained.html#section-01

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.