May 2019, cyber risk and compliance in Switzerland

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

Dear readers,

The new *Situation Report of the Federal Intelligence Service* is a must-read:

"Our security environment has become more fragmented and more complex and thus more difficult to assess. The significant increase in the number of non-state actors, the possibilities of hybrid warfare, the return of power politics, in some cases with a marked tendency toward unilateralism, heightened tensions between the Western states and Russia, as well as the political and economic challenges in European countries are all part of a situation that increasingly difficult to grasp. The old order is changing under the pressure exerted by political, economic, military but also technological, social and cultural forces. The outcome of these changes is uncertain."

In the report we read that "the use of cyber tools as a key instrument in the exercise of power by nations will probably also continue to grow in importance."

Also, "Espionage operations which have come to light reveal that cyber tools and other communications reconnaissance instruments are being used in parallel and in interaction with human sources. Depending on the objective, information is also being procured exclusively via cyberspace. The latter has gained in importance insofar as the use of cyber-based information-gathering tools has proven successful for many actors.

Cyber espionage is difficult to detect, the perpetrators can hardly be successfully prosecuted, as the purported country of origin does of course not help to elucidate the affair and determination by the means of intelligence of the origins of the cyber-attack ('attribution') can simply be denied based on the lack of provability."

And, of course, we have economic espionage: "Switzerland is an attractive

target for economic espionage. States are increasingly turning to cyber tools in order to engage in economic espionage. Since 2015, the FIS has recorded a growing number of state cyber-attacks on Swiss economic entities. These have tended to involve on the one hand the theft of business and manufacturing secrets and on the other hand the procurement of information ahead of corporate takeovers."

You can download and read the report at:
https://www.vbs.admin.ch/en/current/information-media.detail.nsb.html/75184.html

---

For many years, I study approaches of modelling human behaviour. I have been disappointed many times.

In 2010, Massimo Pigliucci, Professor in the Department of Philosophy at City University New York, published the book "Nonsense on Stilts: How to Tell Science from Bunk". He separates science from pseudoscience and uses the Bentham's term "nonsense on stilts" to describe the worst possible failures of pseudoscience.

A false sense of security is worse than no security at all. *Or,* nothing is worse than providing a false sense of security, as people behave as they are secure.

I have just read a new and very interesting paper, "Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity" from the European Union Agency for Network and Information Security (ENISA).

According to the paper, there is a growing recognition that technical cyber security measures need to operate in harmony with people. This has led to a plethora of academic research that seeks to address the role of the human in cybersecurity.

It is against this backdrop that ENISA has conducted four evidence-based reviews of human aspects of cybersecurity: two based on the use (and effectiveness) of models from social science; one on qualitative studies; and one on current practise within organisations.

Across all four reviews, ENISA found a relatively small number of models, none of which were a particularly good fit for understanding, predicting or changing cyber-security behaviour. Many ignored the context in which much cybersecurity behaviour occurs (i.e. the workplace), and the constraints and other demands on people's time and resources that it causes.

There was little evidence that there are specific links between types of people (e.g. gender, personality) and security behaviours.

Read more at Number 8 below.

I have just read a very interesting presentation, *"Cybersecurity: Where We Are; What More Can be Done? A Call for Auditors to Lean In"* by Kathleen M. Hamm (Board Member, Public Company Accounting Oversight Board, at the Baruch College 18th Annual Financial Reporting Conference, New York).

We read: "What is the role of the auditor as it relates to these and other cybersecurity threats facing our financial reporting system?"

"Today, based on our current standards, an auditor of public company financial statements plays an important, but limited, role with respect to cybersecurity.

The auditor does not broadly evaluate the company's overall cybersecurity risk or the design and effectiveness of operational and other non-financial controls adopted by the company to mitigate that risk.

Instead, as it relates to cybersecurity, the auditor focuses on information technology (IT) that the public company uses to prepare its financial statements.

The auditor also focuses on automated controls around financial reporting, such as the controls around the reliability of underlying data and reports. When doing integrated audits, the auditor also separately evaluates those companies' internal controls over financial reporting (ICFR).

With respect to cybersecurity disclosures by a public company, the financial statement auditor plays two distinct, but likewise limited, roles.

For cybersecurity-related incidents reflected in the financial statements themselves, the auditor evaluates whether those statements taken as a whole are fairly presented in accordance with generally accepted accounting principles, in all material respects."

Read more at Number 3 below.

According to Sun Tzu, to win one hundred victories in one hundred battles is *not* the acme of skill. To subdue the enemy without fighting *is* the acme of skill.

The *"Guidance for individuals in politics, Cyber security tips for individual staff members within political parties"* from the National Cyber Security Centre (NCSC) is excellent. The NCSC has headquarters in London and has brought together expertise from CESG (the information assurance arm of GCHQ), the Centre for Cyber Assessment, CERT-UK, and the Centre for Protection of National Infrastructure.

This guidance has been produced by the NCSC for individuals working in political life, including elected representatives, candidates, activists, and staffers. Cyber-attacks can be designed to influence voters, or to undermine public confidence in democratic processes.

According to the guidance, the three most common types of attack in recent years have been:

- 'Hack and Leak' attacks; where emails (or data) are stolen and published online in an attempt to embarrass or discredit an individual candidate or party. In 2016, a large number of emails belonging to the US Democratic National Convention were accessed by attackers and published online. In 2017, more than 20,000 emails belonging to the Emmanuel Macron campaign were published online.

- 'Hack and Post' attacks; hijacking websites and social media accounts to publish damaging false information. In 2019, two weeks before Tampa's mayoral elections, the twitter account of the Mayor of Tampa, Bob Buckhorn, was compromised by a malicious actor. The hijacker used the account to post a variety of offensive tweets that contained racist comments, child pornography, a bomb threat against Tampa International Airport, and a warning of an incoming ballistic missile strike.

- 'Insider Leak/Malicious insider'; when one recipient on a group message publishes the content of that message in order to expose what others have said. In March 2018, hundreds of WhasApp messages between British MPs discussing Brexit were leaked to the media, exposing numerous disagreements.

Many of these attacks are enabled by phishing, where an attacker aims to lure individuals into inadvertently revealing their login details for both personal and work accounts.

This is a very interesting guidance. We must remember that adversaries follow Sun Tzu's advice:

When using our forces, we must seem inactive;
When we are near, we must make the enemy believe we are far away.

Read more at Number 1 below.

The Border Gateway Protocol (BGP) is the routing protocol of the global Internet. It has been deployed since the commercialization of the Internet, and even version 4 of BGP is over a decade old.

Although the simplicity and the resilience of the protocol is very important for routing, the security of the devices and the infrastructure dedicated to running the protocol is of paramount importance. Unfortunately, there are important vulnerabilities that can be exploited.

I have read a new paper from the European Network and Information Security Agency (ENISA), *"High time to protect the internet route map: Here are 7 basics"*. According to the paper:

"BGP hijacks, hacking the internet route map, continue to happen. Despite years of warnings by security experts.

This spells danger for national security, privacy of citizens, and the resilience of the internet, both in Europe and globally."

"The BGP vulnerabilities can be used in many different ways, from eavesdropping the traffic and silently passing the data forward without disrupting it, to causing internet connection outages which impact the availability of the network.

BGP vulnerabilities can also be used to attack weaknesses in other protocols like DNS hijacks. We distinguish 4 main security risks caused by BGP security vulnerabilities:

1. Eavesdropping internet traffic content: If the internet traffic is unencrypted, BGP attacks can be used to eavesdrop on the content of internet traffic.

This can have severe consequences for subscribers, the endpoints, as well as organization on the server-side.

The impact for subscribers can include financial impact, stealing of credentials and passwords, privacy issues, etc. If carried out carefully, subscribers will not immediately notice an attack is going on.

2. Altering internet traffic content: If the internet traffic is unencrypted, BGP attacks can be used to alter internet traffic, for example redirecting subscribers to spoofed websites, tampering with SSL/TLS certificates, altering DNS responses, etc.

This can have severe consequences for subscribers. A good example is the recent theft of crypto currency by hijacking internet traffic to the Amazon's EC2 cloud.

If carried out carefully, subscribers will not immediately notice an attack is going on.

3. Internet traffic analysis and metadata analysis: If the internet traffic is encrypted, for instance with SSL/TLS, which is increasingly common, BGP attacks can still be used to intercept so-called traffic metadata, i.e. information about which PCs make connections, to which domains and IPs, from where, to which domains, when, etc.

This can be useful for surveillance and espionage.

Capturing, even briefly, a swath of the internet traffic will give the adversary precious information about the kind of applications people are using on their PCs, smartphones, the kind of websites they are visiting, from where, when, etc.

If carried out carefully, subscribers will not immediately notice that an attack is going on.

4. Internet connection outages: Internet traffic can be disrupted using BGP attacks. It is relatively easy to cause large-scale disruptions. Such attacks are obviously visible.

At the same time, considering the dependency of modern society on internet access, disruptions can have severe economic and societal impact.

These risks, depending on the setting and the goals of the attacker, in turn lead to risks of largescale societal and economic disruption (via network outages), privacy risks for citizens using the internet (via eavesdropping of internet traffic metadata or content), risks for national security (via espionage), and so on."

Interesting!

I strongly believe that each vulnerability can be transformed into an opportunity. We know what the adversaries will try to do, so we can use deception, including network topology deception, to mislead them or to attack their ability to harm us.

A network defense strategy rooted in deception can provide benefits to network defenders. S. T. Trassare, for example, has developed an interesting paper, "A technique for presenting a deceptive dynamic network topology" (M.S. thesis, Dept. Com. Sci., Naval Postgraduate

School, Monterey, CA, 2013). He has explained how to deploy a network defense tool that deceives an attacker's probes, and how we can present a false network topology.

There are many improvements and ideas based on this paper. An adversary with a false view of a target network's topology can be induced into directing his attack in a way that the defenders choose. No, not toward resilient nodes, non-existent nodes, or low-value targets. The attacker can be induced into directing his attack toward a server that contains disinformation.

Welcome to our monthly newsletter.

Best regards,

George Lekatis

George Lekatis
General Manager, Cyber Risk GmbH
Rebackerstrasse 7, 8810 Horgen
Phone: +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: https://www.cyber-risk-gmbh.com/Cyber_Risk_GmbH_Catalog_2019.pdf

Number 1 (Page 13)

Guidance for individuals in politics
Cyber security tips for individual staff members within political parties.

This guidance has been produced by the NCSC for individuals working in political life, including elected representatives, candidates, activists, and staffers.

Number 2 (Page 17)

The DOD Cyber Exchange

The DoD Cyber Exchange provides one-stop access to Cyber information, policy, guidance and training for cyber professionals throughout the DoD. Formerly the Information Assurance Support Environment (IASE), some portions of the site are also available to the remainder of the Federal Government and the general public.

Number 3 (Page 19)

Cybersecurity: Where We Are; What More Can be Done? A Call for Auditors to Lean In

Kathleen M. Hamm, Board Member, Baruch College 18th Annual Financial Reporting Conference, New York, NY

“Today, I'd like to discuss an emerging area for our oversight: cybersecurity. Specifically, I'd like to explore the dangers posed by cyber and how cybersecurity presents a threat to our financial reporting system and capital markets.”

Number 4 (Page 32)

Ciaran Martin at CYBERUK 2019

Ciaran Martin, CEO of the NCSC, speaking on day two of CYBERUK 2019.

“We had international cooperation with the Five Eyes, we had brilliant technical panels, we had a real buzz in the evening as we showed off collectively the community’s efforts on technological innovation on cyber security, and in a minute, before I introduce our panel, I just wanted to return to that sense of pragmatic optimism about what we can achieve as a community.”

Number 5 (Page 36)

NIST Tool Enables More Comprehensive Tests on High-Risk Software

Updated “combinatorial testing” tool could reduce potential errors in safety-critical applications.

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

We entrust our lives to software every time we step aboard a high-tech aircraft or modern car. A long-term research effort guided by two researchers at the National Institute of Standards and Technology (NIST) and their collaborators has developed new tools to make this type of safety-critical software even safer.

Number 6 (Page 39)

Why the internet of things (IoT) could cause a power cut

Reporting and Analysis Centre for Information Assurance (MELANI)

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

IoT devices can be misused to a large extent for cyber-attacks, successful blackmail attempts (e.g. fake sextortion) as well as money transfer fraud with Office 365 access data and the main topic "Dealing with purchased risks in hardware and software".

Number 7 (Page 41)

Consultation on regulatory proposals on consumer IoT security

The Department for Digital, Culture, Media and Sport (DCMS) is consulting on regulatory proposals regarding consumer Internet of Things security. The UK Government takes the issue of consumer IoT security very seriously. We recognise the urgent need to move the expectation away from consumers securing their own devices and instead ensure that strong cyber security is built into these products by design.

Number 8 (Page 46)

Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity

There is a growing recognition that technical cyber security measures do not exist in a vacuum, and need to operate in harmony with people. This has led to a plethora of academic research that seeks to address the role of the human in cybersecurity.

Number 9 (Page 49)

Researchers recognise MegaCortex ransomware spike

Cyber security researchers at Sophos have reported a spike in a new ransomware named MegaCortex.

The infection targets corporate networks and has reportedly affected customers worldwide, with victims in Italy, the United States, Canada, the Netherlands, Ireland, and France.

Number 10 (Page 51)

Expediting Software Certification for Military Systems, Platforms

Program seeks to develop process for continuous software certification and mission risk evaluation, reducing impediments to developing and fielding new defense capabilities

DARPA DEFENSE ADVANCED RESEARCH PROJECTS AGENCY

Military systems are increasingly using software to support functionality, new capabilities, and beyond. Before a new piece of software can be deployed within a system however, its functional safety and compliance with certain standards must be verified and ultimately receive certification.

Number 11 (Page 54)

The Congressional Cybersecurity Training Resolution

Sponsored by Reps. Kathleen Rice (D-N.Y.) and John Katko (R-N.Y.), would require the chief administrative officer of the House to carry out annual cyber and IT training for House members, officers and employees.

IN THE HOUSE OF REPRESENTATIVES

Miss RICE of New York submitted the following resolution; which was referred to the Committee on _____

RESOLUTION

Amending the Rules of the House of Representatives to direct the Chief Administrative Officer to carry out an annual information security training program for Members, officers, and employees of the House.

This Act may be cited as the "Congressional Cybersecurity Training Resolution of 2019".

Number 12 (Page 55)

EU Elections Update: The Long Game

EU vs Disinfo

With the European parliamentary elections approaching in less than a month's time, we devote this week's Disinfo Review to a brief summary of the ongoing disinformation trends surrounding the elections.

First, a reminder: Russia's disinformation campaign against the EU – and by extension, its electoral process – has been underway for five years. It is not a new feature of the European political landscape.

Number 13 (Page 57)

Revisiting an important article

Preparing for Cyber Incidents with Physical Effects

Joseph W. Pfeifer, Chief of Counterterrorism and Emergency Preparedness for the New York City Fire Department (FDNY).

THE CYBER DEFENSE REVIEW

Cyber weapons have been used to steal billions of dollars of intellectual property, influence elections, manipulate news and damage critical infrastructure.

Yet, we think of cyberattacks as only a technology problem, which are handled by smart computer network technicians capable of discovering a breach and developing patches to mitigate the problem.

Certainly, technical solutions are a big part of cyber preparedness.

Number 1

Guidance for individuals in politics
Cyber security tips for individual staff members within political parties.

National Cyber Security Centre

This guidance has been produced by the NCSC for individuals working in political life, including elected representatives, candidates, activists, and staffers.

It provides information about common cyber-attacks used against those working in politics, and suggests preventative measures that should reduce the likelihood of you becoming the victim.

- This document contains cyber security tips for individual staff members within political parties.

- More technical guidance for IT support staff is available in a separate document. You may visit: https://www.ncsc.gov.uk/guidance/guidance-for-political-parties

How are parties attacked?

Over recent years, there have been reports from several countries of cyber attacks, using a variety of techniques, targeted at political parties, elected representatives, candidates, and their staff. These cyber-attacks can be part of wider activity designed to influence voters, or to undermine public confidence in democratic processes. Attacks have targeted corporately provided and personal IT, both of which can be equally damaging.

Top three cyber attacks

The three most common types of attack in recent years have been:

- 'Hack and Leak' attacks; where emails (or data) are stolen and published online in an attempt to embarrass or discredit an individual candidate or party. In 2016, a large number of emails belonging to the US Democratic National Convention were accessed by attackers and published online. In 2017, more than 20,000 emails belonging to the Emmanuel Macron campaign were published online.

- 'Hack and Post' attacks; hijacking websites and social media accounts to publish damaging false information. In 2019, two weeks before

Tampa's mayoral elections, the twitter account of the Mayor of Tampa, Bob Buckhorn, was compromised by a malicious actor. The hijacker used the account to post a variety of offensive tweets that contained racist comments, child pornography, a bomb threat against Tampa International Airport, and a warning of an incoming ballistic missile strike.

- 'Insider Leak/Malicious insider'; when one recipient on a group message publishes the content of that message in order to expose what others have said. In March 2018, hundreds of WhasApp messages between British MPs discussing Brexit were leaked to the media, exposing numerous disagreements.

Many of these attacks are enabled by phishing, where an attacker aims to lure individuals into inadvertently revealing their login details for both personal and work accounts.

They might send legitimate-looking password reset emails, urgent-sounding messages about financial problems, account change notification requests, or links to documents that require you to log in with passwords.

The NCSC has produced guidance to help you identify the most common phishing attacks at: https://www.ncsc.gov.uk/guidance/avoiding-phishing-attacks

Reducing the risks: top 5 tips for political parties and staff

The cyber security of political parties, elected representatives, candidates, and their staff is difficult due to the increasing number of IT systems now used. However, there are simple steps you can take to significantly reduce the risk of becoming a victim of cyber-attack.

1. Enable two-factor authentication on email and social media accounts

Using two-factor authentication (2FA) means that even if an attacker knows your password, they can't get access to your account.

The website www.turnon2fa.com/tutorials contains up-to-date instructions on how to set up 2FA across popular online services such as Gmail, Facebook, Twitter, LinkedIn, Outlook and iTunes.

Microsoft and Google offer support to people like you to protect your personal accounts - ask your IT department if this is supported by your organisation. The NCSC have also published guidance on setting up two-factor authentication.

2. Use a strong and separate password for email accounts

NCSC have published advice on using strong and separate passwords. You should do this for your most important accounts such as email and social media. A password made of three random words (eg. LlamaPhoneBeach) works well for many purposes, and you'll probably be able to remember it.

3. Protect your mobile devices

Using a PIN or biometrics (such as fingerprints or face recognition) to unlock mobile devices will help ensure they can't be used if they fall into the wrong hands.

Increasingly, mobile devices use biometrics which provide easy and relatively secure ways of unlocking your device.

Try and use a PIN of at least six digits and avoid using easily guessable PINs like '123456' or '000000'. Be aware that pattern unlocks often leave a mark on the screen, making them easy to guess.

4. Know who you're communicating with

Make sure you know who you're sharing information with. Whilst some messaging apps may use encryption to ensure they can't be intercepted, they don't check that recipients are who they say they are.

Consider using commercially issued IT for communications you want to keep confidential.

When using messaging apps, ensure you know who the recipients are, particularly in group conversations.

Often, information is leaked by a member of a messaging group, and when messaging to a large group, it's hard to know who leaked the information.

5. Avoid sharing passwords and set up multi-user social media accounts

Where you have multiple people managing a social media account, you should avoid sharing the password, if possible.
If you share a password, it is not possible to control who has the password (and therefore who has access to your social media account).

Often business or corporate social media accounts provide security benefits above those available through free accounts.

This includes the ability to create multiple user accounts and manage their access rights.

What to do if you think you've been attacked

If you receive a suspicious email you should not follow any links (or reply to the email) until you're certain that the sender is genuine.

The NCSC has published guidance on how to spot and deal with phishing emails.

If you receive a suspicious email you should report it to your organisation's IT support team, who should be able to offer advice even where it relates to a personal account.

Alternatively, you can report suspicious emails, phone calls or SMS messages to Action Fraud.

If you have clicked on a link or think you've been hacked don't panic, even if you think you made a mistake. If something goes wrong on the IT provided by your organisation report it to IT support.

The security team won't blame you for reporting that something bad happened to you, as it allows them to stop it getting worse and fix things.

To read more:
https://www.ncsc.gov.uk/guidance/guidance-for-individuals-in-politics

Number 2

The DOD Cyber Exchange

The DoD Cyber Exchange provides one-stop access to Cyber information, policy, guidance and training for cyber professionals throughout the DoD.

Formerly the Information Assurance Support Environment (IASE), some portions of the site are also available to the remainder of the Federal Government and the general public.

These resources are provided to enable the user to comply with rules, regulations, best practices and federal laws. DISA is mandated to support and sustain the DoD Cyber Exchange as directed by DoDI 8500.01 and DODD 8140.01.

The DoD Cyber Exchange began as the Information Assurance Support Environment (IASE) which was implemented in May 1997 on the Non-Secure Internet Protocol Router NETwork (NIPRNet) to provide a wide range of Information Assurance services.

In October 1997 it was expanded to the Secret Internet Protocol Router NETwork (SIPRNet) and Releasable (REL) network to authorized DoD foreign coalition partners.

To achieve mission and resource efficiencies IASE REL was decommissioned in March 2018; FVEY partners had accessibility to relevant cybersecurity guidance via IASE SIPR.

The IASE Portals have been a mainstay in the information assurance and cyber communities, and has a usership of over five million annually to include DoD Components, the federal government and general public.

The IASE celebrated its 20th anniversaries in May 2017 and October 2017, and announced plans to modernized IASE Public, IASE NIPR and IASE SIPR to enhance the user interface and user experience; along with the "new look and feel" IASE was rebranded to the DoD Cyber Exchange.

Today's "DoD Cyber Exchange Family of Portals" consists of:

- Public (https://public.cyber.mil), which is accessible to all Internet users,

- NIPR (https://cyber.mil), which requires Public Key Infrastructure (PKI) credentials for access to NIPRNet,

- SIPR (https://cyber.smil.mil), which can only be accessed from the SIPRNet.

The DoD Cyber Exchange is supported by a team of government and contractor staff in the Cyber Directorate at DISA.

The DoD Cyber Exchange web team is charged with Operations Management, Content Management and Web Master Functions, Environment Development and Network Engineering.

The site's content is provided by various Cyber subject matter area content owners, across the DoD through a change request and approval process coordinated and managed by the DoD Cyber Exchange web team.

Number 3

Cybersecurity: Where We Are; What More Can be Done? A Call for Auditors to Lean In

Kathleen M. Hamm, Board Member, Baruch College 18th Annual Financial Reporting Conference, New York, NY

PCAOB
Public Company Accounting Oversight Board

I. Introduction

Good afternoon, everyone. Thank you for that kind introduction. And thank you to Baruch College's Robert Zicklin Center for Corporate Integrity for inviting me to speak here today. It is wonderful to be part of the 18th Annual Financial Reporting Conference.

This center and the Public Company Accounting Oversight Board (PCAOB) have much in common. We were both created at a time when corporate and accounting scandals dominated the headlines, and public confidence in U.S. business was shaken.

By sponsoring forums like this one, the center helps private-sector executives and public-policy makers probe a broad range of complex contemporary issues confronting U.S. corporations and the capital markets.

We at the PCAOB wrestle with many of the same issues. Our mission calls on us to protect investors and the public interest by overseeing one particular aspect of the financial reporting ecosystem: the preparation of informative, accurate, and independent audit reports.

Today, I'd like to discuss an emerging area for our oversight: cybersecurity. Specifically, I'd like to explore the dangers posed by cyber and how cybersecurity presents a threat to our financial reporting system and capital markets.

I'd also like to share my thoughts on what more audit professionals can do to strengthen the cybersecurity and resiliency of our financial reporting system.

But before I do, let me give you a brief update on what the PCAOB accomplished last year and where we are heading.

II. Update on the PCAOB

This April marked the first full year with an entirely new PCAOB board in place.

A board that by design brought together members with diverse expertise, skill sets, and perspectives.

Over much of the past year, my colleagues and I have worked hard, individually and collectively, to understand and assess the PCAOB's core programs and operations.

We have also probed whether and how we can improve the PCAOB's ability to more effectively accomplish our mission.

Last month the PCAOB published our 2018 annual report, the first annual report reflecting the oversight of the new board.

Some of the significant highlights were:

- We completed and approved two long-awaited standards – accounting for estimates, including fair value measurements, and the use of specialists. The public comment period with the Securities and Exchange Commission (SEC) ended last week on both. If approved by the Commission, these two standards will apply to audits of financial statements for fiscal years ending on or after December 15, 2020.

- On our research agenda, we prioritized data and technology and quality control. We tapped into our two advisory groups, the Standing Advisory Group and the Investor Advisory Group, to provide their insights on each topic.

  We also convened a task force of private-sector experts to advise us on emerging technologies and data analytics and their effects on the audit.

- We helped practitioners, investors, and other stakeholders prepare for implementing the last and most significant phase of the new auditor's report, the reporting of critical audit matters.

- We issued our first post-implementation review of a PCAOB standard – AS 1220, Engagement Quality Review.

- We created a new Office of External Affairs to spearhead our efforts to increase our accessibility and engagement with our stakeholders, especially investors, audit committees, and preparers.

- We also began the process of revisiting our approach to conducting and communicating the results of our inspections.

- We awarded $3.32 million in scholarships to 332 accounting students, with funds from penalties collected in our enforcement actions.

These results reflect some of the key priorities identified during a far-reaching strategic planning process that we began last year. That process started with the board querying our personnel bottom to top on what the PCAOB did well and where we could do better.

We also reached out to a broad, diverse set of external stakeholders for their views and suggestions. We conducted a public survey, one-on-one interviews, and board members embarked on listening tours.

After extensive consultation and deliberation inside and outside, last November we published our five-year strategic plan.

That plan has five goals.

Two look inward – becoming more efficient and effective with our resources, and empowering our people for success and prudent risk-taking to promote our mission. The remaining three goals look outward.

These external strategies are:

- One: We are committed to driving audit quality forward through a combination of prevention, detection, deterrence, and enforcement.

- Two: We have pledged to enhance our transparency and accessibility through proactive stakeholder engagement, with a particular focus on reaching out to investors, audit committees, and preparers.

- Three: We have dedicated ourselves to anticipating and responding to a changing environment, and in particular to preparing for the opportunities and risks that emerging technologies present to financial reporting and auditing.

III. The Promise; the Threat

Why is technology a key strategic imperative for us? While we don't know precisely how or when, we do know that emerging technologies and data analytics will fundamentally change the way financial information is reported, how audits are conducted, and ultimately how we at the PCAOB perform our work.

Companies now perform more and more finance tasks using algorithms and robotic process automation.

They are also increasing their use of advanced analytics and artificial intelligence in their financial reporting.

Auditors in turn are exploring new approaches to technology and analytics to perform their assurance function. Today some auditors use drones for inventory observations.

Tomorrow data analytics could replace sampling techniques with analysis of all transactions and accounts. Eventually blockchain and distributed ledger technology could make confirmations a thing of the past.

Technology offers the promise of combining increased efficiencies with improved effectiveness, resulting in enhanced audit quality. Freed from time-consuming manual reviews, technology may provide auditors with more time to exercise their business and financial expertise.

That time could help auditors sharpen their professional skepticism and their ability to more effectively identify indicators of error or fraud. That additional time could also allow auditors to more deeply probe the potential root causes of identified issues and concerns.

But, for all their promise, emerging technologies present real risks. Coding errors present inherent threats. Some occur during development. Others can occur when changes are made after deployment.

Still other errors may lay dormant for extended periods of time. Some experts estimate that between 15 and 50 coding errors exist in every one thousand lines of code.

Given the complexity of many software applications and solutions, many of which contain millions or tens of millions of lines of code, the risk of material errors is not trivial.

A threat also exists of unintended, or algorithmic, bias. This bias occurs when systematic, repeatable errors in software or computer systems cause unfair outcomes, arbitrarily favoring one result over another.

Bias can emerge from the design of an algorithm itself or through unintended or unanticipated uses of the algorithm.

For example, software designed to automate the analysis of real-estate leases may prove feeble at analyzing equipment leases.
Bias can also occur from the way data is coded, collected, selected, or used to train algorithms. These algorithms underpin machine learning and related artificial intelligence solutions.

Unauthorized access to information systems and data also presents a significant threat. Amplifying this threat is how interconnected we all are to one another through technology and communication networks and systems. This interconnection occurs through domestic and international telecommunication, financial, retail and wholesale payment, and clearing and settlement systems; it also occurs through the internet.

IV. Setting the Stage

a. The Internet and the "Internet of Things"

Today we communicate and engage in commerce through the internet. Organizations of all types – energy, transportation, healthcare, financial services, nonprofits and humanitarian groups, governments – operate on the internet. Vast amounts of personal and other data are accessible there too.

Initially designed in the late 1960s to provide known, trusted users access to one another, interoperability was a key characteristic of the internet: That is, the ability for different networks, systems, devices, and applications to connect, exchange, and use data across organizations and sovereign borders. Security was an afterthought at best.

And now everyday objects, so-called "Internet of things" or "IoT" devices, are connected to the internet as well. Personal computers, smartphones, cars, thermostats, wearable gadgets, lights, and cardiac monitors to name a few – send and receive huge amounts of data largely unfettered by country boundaries.

To fully appreciate the magnitude, scope, and speed of this change, think about this: In 2003 – just a year after the PCAOB and this center were established – a half a billion devices were connected to the internet around the globe.

Fast forward 17 years. By next year, internet-connected devices are expected to have increased 60 fold to almost 31 billion.

This translates into nearly four devices for every man, woman, and child on the planet.

With this unprecedented access and interoperability comes peril. Until recently though, much like the internet itself, little thought was typically given to the security of these devices. This means 31 billion potential access point for criminals, hacktivists, independent digital malcontents, and rogue nation states.

b. Cyber threat

Earlier this year, the U.S. Director of National Intelligence released a report outlining the gravest dangers facing the United States and our intelligence community's proposed response to those dangers.

One of those threats was cybersecurity and resiliency. The threat includes the loss of proprietary and sensitive information, the manipulation and destruction of data, systems, and networks, and even the harming of physical assets, as well as the related costs and undermining of confidence in our institutions.

While acknowledging heightened awareness of cyber threats and improved cyber defenses, the report was sobering in its conclusion that "nearly all information, communication networks, and systems will be at risk."

The report continues that our adversaries – both state and non-state actors – are using cyber access and capabilities to advance their own strategic and economic interests.

As we integrate technology into everything we do – critical infrastructures, communication networks, and consumer devices – the report notes that cyber threats will pose increasing risk to our economic prosperity and public health and safety.

Similarly, last January the World Economic Forum highlighted the rising dependencies of economies on internet connectivity and digital information, citing data fraud or theft and cyber-attacks as the fourth and fifth most likely sources of global risk in 2019.

In its prior year report, the forum highlighted a study that projects that cybercrime will cost businesses $8 trillion over the next five years.

On a related point, reinsurer Munich Re estimates that the market for cyber-risk insurance could reach $8 to $9 billion in premiums by 2020, double the amount of premiums written just two years earlier.[18]

Now let's put a finer point on specifically how cyber threats can affect financial reporting.

i. Data breaches and disclosure obligations

One example: Just over a year ago, the SEC brought a settled enforcement action against the company formerly known as Yahoo! Inc. for misleading investors by failing to disclose one of the world's largest data breaches.[19]

Yahoo's successor, Altaba, paid a $35 million penalty. This was the SEC's first action against a company for a cybersecurity disclosure violation.

To recap, in late 2014, hackers associated with the Russian Federation infiltrated Yahoo's systems and stole personal data relating to hundreds of millions of user accounts.

Within days of the intrusion, Yahoo's information security team understood that the company's so-called "crown jewels" had been ex-filtrated. This stolen data included: the usernames, email addresses, phone numbers, birth dates, encrypted passwords, and security questions and answers for the compromised accounts.

While information on the breach was reported to Yahoo's senior management and legal department, the company failed to properly investigate the incident or adequately consider whether the breach needed to be disclosed to investors. The company also kept its auditors and outside lawyers in the dark.

The breach was only disclosed publicly more than two years later, when Yahoo's operating business was being sold to Verizon Communications, Inc. Ultimately, because of the breach, Verizon lowered its purchase price for Yahoo by $350 million, representing a 7.25 percent discount.

Among other things, the SEC found that Yahoo failed over a two-year period to make required disclosures about the breach and its potential business impact and legal implications in its quarterly and annual reports.

In those filings, instead of disclosing that an actual breach had occurred, the company merely stated that it faced the risk of, and potential negative effects from, data breaches.

Importantly, the SEC also found that Yahoo failed to appropriately design and maintain effective disclosure controls and procedures to ensure the timely assessment and escalation of cyber-incidents.

Relatedly, earlier this year, $29 million was paid to settle a private, derivative lawsuit alleging that the former directors and officers of Yahoo violated their fiduciary duties of care by failing to properly oversee the company's handling of a series of cyberattacks from 2013 to 2016.

These cyberattacks allegedly involved as many as three billion user accounts and included the data breach that formed the basis of the SEC's enforcement action.
Of note, this settlement also represented another first: It was the first monetary recovery in a derivative action involving a data breach.

Until then, settlements of data breach-related derivative lawsuits included governance changes and modest attorney fees, but no cash awards.

ii. Cyber-enabled fraud

Another example: Last October, the SEC issued an investigative report highlighting a specific type of cyber-enabled fraud that victimized nine public companies.

It involved criminals using manipulated – or spoofed – email addresses and domains to impersonate company executives and vendors to dupe employees into making unauthorized payments.

Over the course of weeks or months, each of the nine companies lost at least $1 million, with one losing more than $45 million. Collectively, the companies lost nearly $100 million.

Most of the money was not recovered. In some instances, the frauds were only detected after inquiry from law enforcement or an outside party.

What exactly happened?

The scams came in two varieties. The first type involved criminals masquerading as company executives sending emails to mid-level finance employees with authority to transmit funds.

The emails typically made urgent requests for funds to be wired to the purported foreign bank accounts of well-known law firms to facilitate supposed fast-moving mergers.

The emails also instructed employees to keep the requests secret. Then instead of going to the law firms, the funds were wired to bank accounts controlled by the criminals.

The second more sophisticated variant involved criminals hacking into the actual email accounts of companies' foreign vendors.

After fooling company employees into revealing actual purchase order and invoice information, the hackers then tricked employees into replacing the vendors' payment information with routing information to bank accounts controlled by the hackers.

While declining to bring enforcement actions against the companies, the SEC used the report to underscore the obligations of public companies to devise and maintain sufficient systems of internal accounting controls.

By statute, those systems must provide reasonable assurance that access to company assets and execution of company transactions are only done in accordance with the general or specific authorization of management.

According to the SEC, the hackers succeeded in large part because company personnel were unaware of, or did not understand, their companies' internal controls.

Those employees also failed to recognize multiple red flags indicating that a fraudulent scheme was underway. The Commission further cautioned public companies to be mindful of cyber threats when designing and maintaining internal accounting controls.

To put these threats in context, the FBI estimates that business email compromises have cost companies more than $5 billion over the past five years.

Given the likelihood of underreporting, the actual figure might be higher. In fact, some empirical evidence suggests that companies withhold information from investors on more severe cyberattacks, especially when management appears to believe that the attacks will not be discovered independently.

V. Role of Auditors

What is the role of the auditor as it relates to these and other cybersecurity threats facing our financial reporting system?

a. Limited but important role

First, let's level set.

Today, based on our current standards, an auditor of public company financial statements plays an important, but limited, role with respect to cybersecurity.

The auditor does not broadly evaluate the company's overall cybersecurity risk or the design and effectiveness of operational and other non-financial controls adopted by the company to mitigate that risk.
Instead, as it relates to cybersecurity, the auditor focuses on information technology (IT) that the public company uses to prepare its financial statements.

The auditor also focuses on automated controls around financial reporting, such as the controls around the reliability of underlying data and reports.

When doing integrated audits, the auditor also separately evaluates those companies' internal controls over financial reporting (ICFR).

With respect to cybersecurity disclosures by a public company, the financial statement auditor plays two distinct, but likewise limited, roles.

For cybersecurity-related incidents reflected in the financial statements themselves, the auditor evaluates whether those statements taken as a whole are fairly presented in accordance with generally accepted accounting principles, in all material respects.

For example, if a company establishes a material contingent liability for an actual cyber-incident, then the auditor would need to evaluate, in the overall context of the financial statements, the appropriateness of the disclosure of that liability in the footnotes to those statements.

The auditor plays an even more limited role when cyber-related information is not contained in the financial statements themselves but elsewhere in a company's annual report.

Here the auditor need not corroborate the information in the report. Instead, the auditor need only read and consider whether the cyber-related information in that report, or its presentation, is a material misstatement of fact or materially inconsistent with the information in the financial statements.

b. Risk assessments

Can auditors do more?

Unless an organization runs entirely on manual processes without using technology or the internet, I believe auditors should consider cybersecurity as part of their audit risk assessment.

While Benedictine nuns and monks in a monastery atop a mountain copying the Bible by hand on vellum, using quills, and natural-made inks comes to mind, few other enterprises are totally devoid of cybersecurity risk, particularly public companies.

We know some auditors are laser focused on cybersecurity and have taken steps to specifically consider cyber when assessing the risk of material misstatements in the financial statements of public companies.

Whether or not a cyber-incident has occurred, during the planning process an auditor must perform a risk assessment, and I believe that assessment

should consider any cybersecurity risks that could have a material effect on the company's financial statements.

If the auditor identifies a risk related to cybersecurity that could have a material effect on a company's financial statements, the auditor should then design and execute procedures to address those risks.

For an integrated audit, this work would include testing relevant controls.

To begin the risk assessment, an auditor must obtain an understanding of the company and its external and internal environment.

This understanding, of course, includes the company's IT systems relevant to financial reporting, along with any related subsystems.

This also includes understanding the potential access points into these systems, as well as the logical access controls over the systems.

As part of the risk assessment, I believe the auditor should also understand the methods used by the company to prevent and detect cyber-incidents that could have a material effect on the financial statements: the company's processes that block and identify attempted unauthorized transactions or access to assets, as well as employees' familiarity with those processes.

Other areas of focus should include the company's processes to assess and address material cyber-incidents once identified.

This includes understanding, for example, how the company ensures timely evaluation and reporting up the management ladder of material cyber-incidents.

It also includes how the company ensures appropriate escalation to the board and timely consideration of disclosure obligations to investors and others.

When performing these risk assessments, I encourage auditors to think broadly. Why? As companies become more and more digitally linked with their vendors, customers, and employees, the potential entry points and attack surfaces multiple.

We also know that threat actors usually target the weakest link to gain entry, a website or an email account. And once inside, threat actors typically seek to move laterally throughout an organization's IT architecture looking to gain access to systems they can exploit.

As a result, an auditor should be clear-eyed about the risk that attackers can operate under the guise of legitimate users, ultimately accessing a company's systems or subsystems that support the financial reporting process.

c. Responding to cyber-incidents

Even if a specific cybersecurity incident has not been identified, it is important for an auditor to remain professionally skeptical throughout the audit. Why? According to a recent study, the average time to identify a breach is 196 days – more than six months.

Therefore, a real possibility exists that a breach has occurred and has not yet been identified or disclosed to the engagement team.

What is the auditor's responsibility if a company experiences a cyber-incident? Of course, the auditor must assess the nature and extent of the breach, including what was stolen, altered, or destroyed.

The auditor should also consider the expected effect of the breach on the company's operations. Armed with this information, the auditor should consider the financial implications of the breach.

The financial effects could include the loss of revenue from disrupted operations and the costs associated with securing, reconfiguring, and replacing systems.

Costs could also include the fees associated with conducting forensic inquiries and defending against enforcement investigations and civil actions, as well as the payment of regulatory fines and monetary penalties to harmed private parties.

Beyond that, the auditor should also assess whether the incident resulted from a deficiency in the company's internal controls over financial reporting and whether the company has put in place procedures to prevent similar future incidents.

The auditor should also explore with management and the audit committee the nature and type of disclosures that the company is considering in its financial statements or the notes to those statements.
The auditor's obligation to assess the risk of material misstatement continues throughout the audit.

Therefore, if during the audit, the auditor obtains information about a cyber-incident, then the auditor should evaluate whether that incident has an effect on the previously performed risk assessment.

If so, the auditor would need to revise the risk assessment and appropriately modify the planned audit procedures; potentially performing additional procedures.

Regardless of the effect on the risk assessment, the auditor would need to document relevant considerations of the cyber-incident on the audit.

Finally, even when a cyber-incident may appear not to be material to the financial statements, if the auditor becomes aware of a possible illegal act related to the incident, the auditor would need to assure themselves that the company's audit committee was adequately informed as soon as practical.

Such an instance could occur if management, notwithstanding a legal requirement, failed to timely disclose a breach of customers' personally identifiable information.

VI. Conclusion

Cybersecurity represents one of the most significant economic, operational, and national security threats of our time. It is a key risk to investors and our capital markets as well.

So, how do we respond? One thing is for sure: We all must take responsibility. The government, private institutions, and individuals each share responsibility for protecting our individual and collective assets and each other from cyber threats.

Public companies and their officers and directors have important roles as well. So do auditors.

Thank you for giving me the opportunity to share my views on this important topic.

Number 4

Ciaran Martin at CYBERUK 2019

Ciaran Martin, CEO of the NCSC, speaking on day two of CYBERUK 2019.

Thank you for coming back.

We know you have other options such as hotel room beds, nice walks along the river. It's easy to come here on day one. It's really quite admirable after a very inspiring but very demanding day to have everyone back. We had a fantastic day yesterday.

We had international cooperation with the Five Eyes, we had brilliant technical panels, we had a real buzz in the evening as we showed off collectively the community's efforts on technological innovation on cyber security, and in a minute, before I introduce our panel, I just wanted to return to that sense of pragmatic optimism about what we can achieve as a community.

Looking around and seeing so many people I spoke to yesterday, there's that real spirit of challenge, of fixing things, that spirit of just speaking truth unto power, a sort of equality and egalitarianism.

And I was remembering this because I think we'll probably all struggle a bit for energy levels today.

And I once said to one of my team: 'Why am I struggling? Why am I in such a bad mood today?'

And in the best spirit of the NCSC, she said: 'Maybe it's because you're a 44-year-old man and none of your childhood dreams have come true.'

But anyway, this is a spectacular and wonderful event, and I just wanted to set the tone.

This is the last CYBERUK of the decade.
So what's it going to be like – what's it going to feel like for us and our successors in 10 years time?

And I want to set a tone and capture a spirit of being optimistic because I think we're at an important point in the history of technology.

If you think back 15 or 20 years, you think of the narrative around new technology, around the information age, the fourth industrial revolution – whatever fancy term you want to use.

We were changing the world. Everything was getting easier. Everything was being better and faster, more connected.

We could do more.

We were on a relentless trajectory to better. And it was going to fix everything. And it was going to free up everything. And nothing could get in the way.

And we don't talk like that anymore.

I remember – I'm not going to say too much about other countries this morning; I think this is a very domestic focus – but I remember on a visit to China of all places – I'm not going to say much about China because you may have noticed I had to speak an awful lot about China in the course of yesterday – but I remember on one visit having a fascinating discussion with a leading Chinese opinion former about the way the internet was going.

And he said: 'Twenty years ago, you were telling us that our model of the internet wasn't going to work. It wasn't practical. You couldn't really control the internet. But also it wasn't desirable. Twenty years on, you're beginning to talk a bit like we are. You're talking about harms all the time.'

And it's absolutely right we talk about harms.

You look at, as Director Fleming said yesterday, you look at the excellent DCMS online harms paper. A really grown-up, groundbreaking, realistic look at the sort of challenges we face with the way technology has evolved. Obviously, our field is the vulnerabilities of technology that can be exploited to our detriment.

There is the horrors of terrorist radicalisation, harmful material, child sexual exploitation, cyber crime, and so forth. And this Chinese opinion former was saying: 'That's what we were warning you about. And you need to do something about it.'

So it is the case that whilst these new technologies – and a new generation of technologies – still offer these unparalleled opportunities to make all our

lives so much better – our healthcare, our economies, our societies – but we have to think about managing the risks and managing the harm.

And that's the challenge for this community – and the opportunity.

We can fix these problems. We can get ahead of the problem. We can look at the way technology is evolving. We can avoid the mistakes of 20 years ago where we allowed new technology to develop but in a way that didn't always incentivise good security. And we can make it safe enough so we can all enjoy it and use it safely.

But I think for all of us, there is a question every so often – maybe on a daily basis – about why we're getting out of bed and doing what we do.

And for me – and I think for this community – it is spectacularly motivating to be able to get out of bed – to come to work – and say: there are a set of things happening across the world, a set of innovations, a set of products and services that are changing the way we live.

And we're going to make them safer, still usable, but safer so we can have confidence in them.

Because at a time when confidence in the way the western internet works, it's not collapsing – but it's pretty obvious that in some areas it's wobbling.

Let's get that confidence back. Let's do these fixes. Let's get after these problems. Nothing particularly ideological about it.

I love the approach that we have in this event of having the sessions – the breakout sessions – ranked by chillis in order of technical complexity.

This talk – as with all my talks – is zero chillis, a new category all of my own.

But whether it's highly technical or actually quite general, just about the way people behave – whether it's behavioural science, economics, whether it's product design, or whether it's a really complex mathematical or engineering problem, I think everyone in this room – and everyone in our organisations – has his or her part to play in making sure that when we vacate this stage – literally and metaphorically – and give way to the next generation, that we are handing over to them a technological economy and society with confidence.

So that's all I really want to say this morning.

But we have a mission – it is an historic mission – to secure our society for the next generation.

Our children get this. They're digital natives. They know about the risks. But when they take control of the country, what are we leaving them?

Are we leaving them a technological legacy that's imbued with confidence, optimism, that fundamentally works in a safe way? Or are we leaving them with an absence of confidence, with concerns and doubt?

Let's make sure we win this.

So with that, enjoy the day. We've an excellent first panel of senior figures in journalism and in public regulation and law enforcement – and me, I'm afraid.

We then have the second most senior member of the government, we have excellent sessions later on, and I hope you enjoy the day.

And with that, thank you, and it is my pleasure to welcome to the stage our panel headed by the editor of the Financial Times, Mr Lionel Barber.

Thank you.

The video:
https://www.youtube.com/watch?v=tXgusGn5YC0&feature=youtu.be

Number 5

NIST Tool Enables More Comprehensive Tests on High-Risk Software

Updated “combinatorial testing” tool could reduce potential errors in safety-critical applications.

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

We entrust our lives to software every time we step aboard a high-tech aircraft or modern car.

A long-term research effort guided by two researchers at the National Institute of Standards and Technology (NIST) and their collaborators has developed new tools to make this type of safety-critical software even safer.

Augmenting an existing software toolkit, the research team’s new creation can strengthen the safety tests that software companies conduct on the programs that help control our vehicles, operate our power plants and manage other demanding technology.

While these tests are often costly and time-consuming, they reduce the likelihood this complex code will glitch because it received some unexpected combination of input data.

This source of trouble can plague any sophisticated software package that must reliably monitor and respond to multiple streams of data flowing in from sensors and human operators at every moment.

With the research toolkit called Automated Combinatorial Testing for Software, or ACTS, software companies can make sure that there are no simultaneous input combinations that might inadvertently cause a dangerous error.

As a rough parallel, think of a keyboard shortcut, such as pressing CTRL-ALT-DELETE to reset a system intentionally.

The risk with safety-critical software is that combinations that create unintentional consequences might exist.

Until now, there was no way to be certain that all the significant combinations in very large systems had been tested: a risky situation.

Now, with the help of advances made by the research team, even software that has thousands of input variables, each one of which can have a range of values, can be tested thoroughly.

NIST's ACTS toolkit now includes an updated version of Combinatorial Coverage Measurement (CCM), a tool that should help improve safety as well as reduce software costs.

The software industry often spends seven to 20 times as much money rendering safety-critical software reliable as it does on more conventional code.

The peer-reviewed findings of the research team appear in two papers the team will present on April 23 at the 2019 IEEE International Conference on Software Testing, Verification and Validation in Xi'an, China.

The research includes collaborators from the University of Texas at Arlington, Adobe Systems Inc. and Austria's SBA Research.

NIST mathematician Raghu Kacker said that CCM represents a substantial improvement to the ACTS toolkit since its last major addition in 2015.

"Before we revised CCM, it was difficult to test software that handled thousands of variables thoroughly," Kacker said. "That limitation is a problem for complex modern software of the sort that is used in passenger airliners and nuclear power plants, because it's not just highly configurable, it's also life critical. People's lives and health are depending on it."

Software developers have contended with bugs that stem from unexpected input combinations for decades, so NIST started looking at the causes of software failures in the 1990s to help the industry.

It turned out that most failures involved a single factor or a combination of two input variables—a medical device's temperature and pressure, for example—causing a system reset at the wrong moment. Some involved up to six input variables.

Because a single input variable can have a range of potential values and a program can have many such variables, it can be a practical impossibility to test every conceivable combination, so testers rely on mathematical strategy to eliminate large swaths of possibilities.

By the mid-2000s, the NIST toolkit could check inputs in up to six-way combinations, eliminating many risks of error.

"Our tools caught on, but in the end, you still ask yourself how well you have done, how thorough your testing was," said NIST computer scientist Richard Kuhn, who worked with Kacker on the project. "We updated CCM so it could answer those questions."

NIST's own tools were able to handle software that had a few hundred input variables, but SBA Research developed another new tool that can examine software that has up to 2,000, generating a test suite for up to five-way combinations of input variables.

The two tools can be used in a complementary fashion: While the NIST software can measure the coverage of input combinations, the SBA algorithm can extend coverage to thousands of variables.

Recently, Adobe Systems Inc. contacted NIST and requested help with five-way testing of one of its software packages. NIST provided the company with the CCM and SBA-developed algorithms, which together allowed Adobe to run reliability tests on its code that were demonstrably both successful and thorough.

While the SBA Research algorithm is not an official part of the ACTS test suite, the team has plans to include it in the future. In the meantime, Kuhn said that NIST will make the algorithm available to any developer who requests it.

"The collaboration has shown that we can handle larger classes of problems now," Kuhn said. "We can apply this method to more applications and systems that previously were too hard to handle. We'd invite any company that is interested in expanding its software to contact us, and we'll share any information they might need."

The ACTS test suite contains research tools, not commercial products, and the toolkit is not intended to compete with products in the private sector, Kuhn said.

To read more: https://www.nist.gov/news-events/news/2019/04/nist-tool-enables-more-comprehensive-tests-high-risk-software

Number 6

Why the internet of things (IoT) could cause a power cut

Reporting and Analysis Centre for Information Assurance (MELANI)

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

IoT devices can be misused to a large extent for cyber attacks, successful blackmail attempts (e.g. fake sextortion) as well as money transfer fraud with Office 365 access data and the main topic "Dealing with purchased risks in hardware and software".

The 28th semi-annual report of the Reporting and Analysis Centre for Information Assurance (MELANI) published on 30 April 2019 deals with the most important cyber incidents of the second half of 2018 in Switzerland and abroad.

The rapidly advancing digitalisation can only be mastered with corresponding hardware and software.

The market is clearly dominated by US companies, with China in the fast lane and isolated global players in hardware and software, for example from Korea, Russia or Germany.

The potential access to ICT manufacturers by the respective host countries leads to questions about how to deal with these risks properly.

The 28th semi-annual MELANI report is dedicated to this problem in the key topic and deals with other current topics such as those described below.

Household appliances as triggers for a power failure

With the Internet of Things (IoT) all kinds of devices such as heaters and air conditioners are connected to the internet for remote control.

This is practical, but also involves certain risks.

According to a study published by Princeton University in 2018, it is quite possible that malicious actors could hack inadequately protected IoT devices, merge them into a botnet and misuse them for cyber attacks, such as a power failure. The semi-annual report highlights the problems and contains recommendations.

Extortion using fake sextortion

Since March 2018 countless fake sextortion emails have been circulating. In an email, the attackers claim to have compromising images showing recipients looking at pornographic websites.

As "proof" for the authenticity of the claim, passwords or mobile phone numbers from previous data leaks are often mentioned in the email.

The semi-annual report deals with this problem and shows the development of the various fake sextortion waves.

Office 365-access data used for transfer fraud

With over 100 million monthly users, Office 365 accounts have become a popular target for attackers.

In the second half of 2018, so-called wire fraud occurred with Office 365 access data obtained in this way.

This is what happens when fraudsters search for existing electronic invoices in compromised accounts, then copy them, add a different IBAN and redeliver them.

The 28th MELANI semi-annual report is published at:
https://www.melani.admin.ch/melani/en/home/dokumentation/reports/situation-reports/semi-annual-report-2018-2.html

Number 7

Consultation on regulatory proposals on consumer IoT security

The Department for Digital, Culture, Media and Sport (DCMS) is consulting on regulatory proposals regarding consumer Internet of Things security.

The UK Government takes the issue of consumer IoT security very seriously. We recognise the urgent need to move the expectation away from consumers securing their own devices and instead ensure that strong cyber security is built into these products by design.

Having worked with stakeholders, experts and the National Cyber Security Centre (NCSC), we are now consulting on proposals for new mandatory industry requirements to ensure consumer smart devices adhere to a basic level of security.

The proposals set out in this consultation seek to better protect consumers' privacy and online security which can be put at risk by insecure devices.\

Who is this consultation for?

- Device Manufacturers: The entity that creates an assembled final internet-connected product. A final product may contain the products of many other different manufacturers.

- IoT Service Providers: Companies that provide services such as networks, cloud storage and data transfer which are packaged as part of IoT solutions. Internet-connected devices may be offered as part of the service.

- Mobile Application Developers: Entities that develop and provide applications which run on mobile devices. These are often offered as a way of interacting with devices as part of an IoT solution.

- Retailers: The sellers of internet-connected products and associated services to consumers.

- Those with a direct or indirect interest in the field of consumer IoT security, including consumer groups, academics and technical experts.

Executive Summary

As the technological advances of the 21st century continue to accelerate, consumers are bringing more and more 'smart' devices (i.e. consumer IoT products) into their homes, such as smart TVs, internet connected toys, smart speakers and smart washing machines.

The Internet of Things (IoT, also known as 'internet-connected' or 'smart' products) is already being used across a range of industries and it is delivering significant benefits to the lives of its users.

In the future, we expect an ever increasing number of more developed consumer Internet of Things products and services.

These devices will be able to anticipate and meet their users' needs and will be able to tailor information specifically to them across everything from home energy to security.

This will offer users the opportunity to live more fulfilling lives; saving time, effort and money.

As with all new technologies, there are risks. Right now, there are a large number of consumer IoT devices sold to consumers that lack even basic cyber security provisions.

This situation is untenable. Often these vulnerable devices become the weakest point in an individual's network, and can undermine a user's privacy and personal safety.

Compromised devices at scale can also pose a risk for the wider economy through distributed denial of service (DDOS) attacks such as Mirai Botnet in October 2016.

The UK Government takes the issue of consumer IoT security very seriously. We recognise the urgent need to move the expectation away from consumers securing their own devices and instead ensure that strong cyber security is built into these products by design.

We have previously stated our preferred an approach whereby industry self-regulate to address these issues, but that we would consider regulation where necessary.

In October 2018 we published a Code of Practice for IoT Security, alongside accompanying guidance, to help industry implement good security practices for consumer IoT.

Despite providing industry with these tools to help address these issues, we continue to see significant shortcomings in many products on the market.

We recognise that security is an important consideration for consumers. A recent survey of 6,482 consumers has shown that when purchasing a new consumer IoT product, 'security' is the third most important information category (higher than privacy or design) and among those who didn't rank 'security' as a top-four consideration, 72% said that they expected security to already be built into devices that were already on the market.

It's clear that there is currently a lack of transparency between what consumers think they are buying and what they are actually buying.

Our ambition is therefore to restore transparency within the market, and to ensure manufacturers are clear and transparent with consumers by sharing important information about the cyber security of a device, meaning users can make more informed purchasing decisions.

Having worked with stakeholders, experts and the National Cyber Security Centre (NCSC), we are now consulting on proposals for new mandatory industry requirements to ensure consumer smart devices adhere to a basic level of security.

The proposals set out in this document seek to better protect consumers' privacy and online security which can be put at risk by insecure devices.

We are mindful of the risk of dampening innovation and applying a strong burden on manufacturers of all shapes and sizes.

This is why we have worked to define what baseline security looks like, in line with the 'top three' guidelines of the Code of Practice. Our ambition is for the following security requirements to be made mandatory in the UK.

These are:

- All IoT device passwords shall be unique and shall not be resettable to any universal factory default value

- The manufacturer shall provide a public point of contact as part of a vulnerability disclosure policy in order that security researchers and others are able to report issues

- Manufacturers will explicitly state the minimum length of time for which the product will receive security updates.

Meeting these practical and implementable measures would protect consumers from the most significant risks (such as the Mirai attack in 2016). This would also restore transparency in the sector and allow consumers to identify products that will meet their needs over the lifespan of the product.

In addition, mandating vulnerability disclosure policies will enable an effective feedback mechanism to operate, between the security research community and manufacturers.

One of the core aims of the consultation is to listen to feedback on the various implementation options we have developed in partnership with industry and stakeholders.

These include the following three options:

- Option A: Mandate retailers to only sell consumer IoT products that have the IoT security label, with manufacturers to self declare and implement a security label on their consumer IoT products

- Option B: Mandate retailers to only sell consumer IoT products that adhere to the top three guidelines, with the burden on manufacturers to self declare that their consumer IoT products adhere to the top three guidelines of the Code of Practice for IoT Security and the ETSI TS 103 645

- Option C: Mandate that retailers only sell consumer IoT products with a label that evidences compliance with all 13 guidelines of the Code of Practice, with manufacturers expected to self declare and to ensure that the label is on the appropriate packaging

Later this year, the security label will initially be run on a voluntary basis until regulation comes into force and the government will make a decision on which measures to take forward into legislation following analysis of the responses received through this consultation.

We recognise that any regulation will need to mature over time, and additional information for this approach is within the consultation stage impact assessment 'mandating security requirements for consumer IoT products'.

To learn more:

https://www.gov.uk/government/consultations/consultation-on-regulatory-proposals-on-consumer-iot-security/consultation-on-the-governments-regulatory-proposals-regarding-consumer-internet-of-things-iot-security

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/798722/Secure_by_Design_Consultation_Stage_Regulatory_Impact_Assessment.pdf

Number 8

Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity

There is a growing recognition that technical cyber security measures do not exist in a vacuum, and need to operate in harmony with people.

This has led to a plethora of academic research that seeks to address the role of the human in cybersecurity.

It is against this backdrop that ENISA has conducted four evidence-based reviews of human aspects of cybersecurity: two based on the use (and effectiveness) of models from social science; one on qualitative studies; and one on current practise within organisations.

These reviews are published online as a technical annex.

Across all four reviews, ENISA found a relatively small number of models, none of which were a particularly good fit for understanding, predicting or changing cyber-security behaviour.

Many ignored the context in which much cybersecurity behaviour occurs (i.e. the workplace), and the constraints and other demands on people's time and resources that it causes.

At the same time, there was evidence that models that stressed ways to enable appropriate cybersecurity behaviour were more effective and useful than those that sought to use threat awareness or punishment to urge users towards more secure behaviour.

There was little evidence that there are specific links between types of people (e.g. gender, personality) and security behaviours.

However, by systematically approaching and analysing the current cybersecurity stance of the organisation, and carrying out an in-depth analysis of the causes of any problem(s), ENISA proposes that practitioners can take significant steps towards helping employees to act in a more secure way.

This may involve skills-based training and support but may also require the restructuring of security practises and policies to better align with people's workplace goals and/or capabilities.

ENISA proposes a model of awareness, analysis and intervention for organisations to systematically plan and implement changes to address human aspects of cybersecurity.

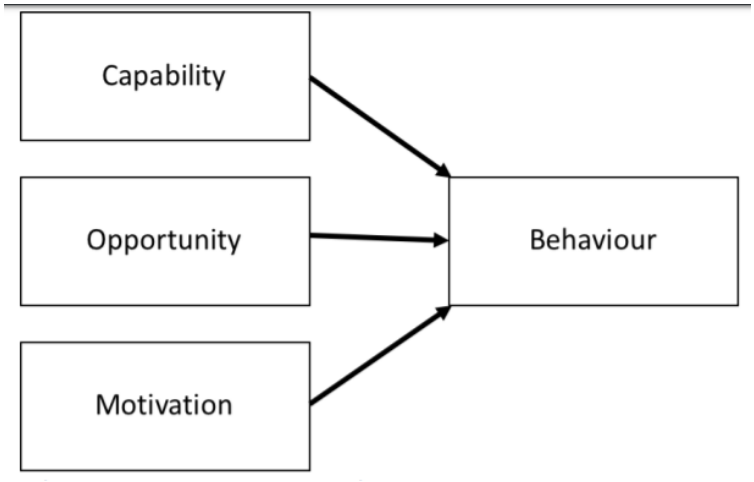
The role of metrics is discussed, in particular the importance of using multiple measures in order to triangulate findings, and the avoidance of over-reliance on self-report measures and simple behavioural metrics.

Organisations should strive for adherence (active participation) rather than compliance - rapidly emerging threats require employees who are engaged and willing to step up.

Organisational leadership has a key role in developing effective and workable security - by helping security specialists to fit security into the business, breaking down silos and leveraging other organisational capabilities (safety, HR, communications) - but not least by setting the tone and leading by example.

Measures to improve security behaviour should be an ongoing, iterative process - the human factor in cyber-security is never 'solved', and there is no simple 'solution', but human skills and knowledge, rather than vulnerabilities, can be made to work in favour of an organisation's defensive cybersecurity.

The report concludes with recommendations for specific groups such as policy makers, management and organizational leaders, CISO and security specialists, CSIRT / CERT community, software developers and awareness raising managers.



The report: https://www.enisa.europa.eu/publications/cybersecurity-culture-guidelines-behavioural-aspects-of-cybersecurity

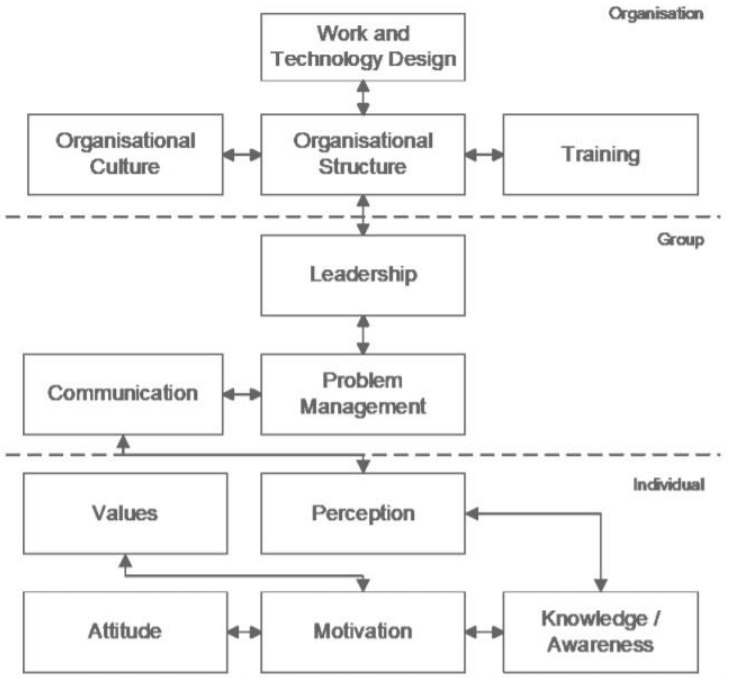


Figure 3: Organisational behaviour model to assess cybersecurity culture (arrows are only exemplary to demonstrate interconnections between domains)

Number 9

Researchers recognise MegaCortex ransomware spike

Cyber security researchers at Sophos have reported a spike in a new ransomware named MegaCortex.

The infection targets corporate networks and has reportedly affected customers worldwide, with victims in Italy, the United States, Canada, the Netherlands, Ireland, and France.

The report: https://news.sophos.com/en-us/2019/05/03/megacortex-ransomware-wants-to-be-the-one/

Sophos said the ransomware appears to have been designed to target large enterprise networks as part of carefully planned targeted intrusions.

Researchers note how MegaCortex "leverages both automated and manual components, and appears to involve a high amount of automation to infect a greater number of victims".

The researchers have also suggested that there a correlation between the MegaCortex attacks and a pre-existing, ongoing infection on the victims' networks with both Emotet and Qbot.

The malware's name is a reference to the corporation where the character Neo worked in the first Matrix movie.

The ransom note has also been said to have been written in the voice of the film's character, Morpheus.

It reads: "Your companies (sic) cyber defence systems have been weighed, measured and have been found wanting. The breach is the result of grave neglect of security protocols."

The most important thing an organisation can do is regularly create a backup copy of important files.

This reduces the leverage of the attacker. The NCSC has published guidance on how to prevent a ransomware incident, and what to do if your organisation is infected.
The guidance: https://www.ncsc.gov.uk/guidance/protecting-your-organisation-ransomware

The NCSC has also launched a free tool, Exercise in a Box, to help SMEs test and practise their response to a cyber attack.
You may visit:
https://www.ncsc.gov.uk/information/exercise-in-a-box

Number 10

Expediting Software Certification for Military Systems, Platforms

Program seeks to develop process for continuous software certification and mission risk evaluation, reducing impediments to developing and fielding new defense capabilities

Military systems are increasingly using software to support functionality, new capabilities, and beyond.

Before a new piece of software can be deployed within a system however, its functional safety and compliance with certain standards must be verified and ultimately receive certification.

As the rapid rate of software usage continues to grow, it is becoming exceedingly difficult to assure that all software considered for military use is coded correctly and then tested, verified, and documented appropriately.

“Software requires a certain level of certification – or approval that it will work as intended with minimal risks – before receiving approval for use within military systems and platforms,” said Dr. Ray Richards, a program manager in DARPA’s Information Innovation Office (I2O). “However, the effort required to certify software is an impediment to expeditiously developing and fielding new capabilities within the defense community.”

Today, the software certification process is largely manual and relies on human evaluators combing through piles of documentation, or assurance evidence, to determine whether the software meets certain certification criteria.

The process is time consuming, costly, and can result in superficial or incomplete evaluations as reviewers bring their own sets of expertise, experiences, and biases to the process.

A lack of a principled means of decomposing evaluations makes it difficult to create a balanced and trustworthy process that applies equally to all software.

Further, each subsystem and component must be evaluated independently and re-evaluated before it can be used in a new system. “Just because a subsystem is certified for one system or platform does not mean it is unilaterally certified for all,” noted Richards. This creates additional time delays and review cycles.

To help accelerate and scale the software certification process, DARPA developed the Automated Rapid Certification Of Software (ARCOS) program. The goal of ARCOS is to create tools and a process that would allow for the automated assessment of software evidence and provide justification for a software's level of assurance that is understandable.

Taking advantage of recent advances in model-based design technology, "Big Code" analytics, mathematically rigorous analysis and verification, as well as assurance case languages, ARCOS seeks to develop a capability to automatically evaluate software assurance evidence to enable certifiers to rapidly determine that system risk is acceptable.

"This approach to reengineering the software certification process is well timed as it aligns with the DoD Digital Engineering Strategy, which details how the department is looking to move away from document-based engineering processes and towards design models that are to be the authoritative source of truth for systems," said Richards.

To create this automated capability, ARCOS will explore techniques for automating the evidence generation process for new and legacy software; create a means of curating evidence while maintaining its provenance; and develop technologies for the automated construction of assurance cases, as well as technologies that can validate and assess the confidence of an assurance case argument.
The evidence generation, curation, and assessment technologies will form the ARCOS tools and processes, working collectively to provide a scalable means of accelerating the pathway to certification.

Throughout the program's expected three phases, evaluations and assessments will occur to gauge how the research is progressing. ARCOS

researchers will tackle progressively more challenging sets of software systems and associated artifacts. The envisioned evaluation progression will move from a single software module to a set of interacting modules and finally to a realistic military software system.

Interested proposers will have an opportunity to learn more during a Proposers Day on May 14, 2019, from 8:30AM to 3:30PM (EST) at the DARPA Conference Center, located at 675 N. Randolph Street, Arlington, Virginia, 22203. The purpose of the Proposers Day is to outline the ARCOS technical goals and challenges, and to promote an understanding of the BAA proposal requirements.

For details about the event, including registration requirements, you may visit:
https://www.fbo.gov/index?s=opportunity&mode=form&id=6a8f03472cf43a3558456b807877f248&tab=core&_cview=0

Additional information will be available in the forthcoming Broad Agency Announcement, which will be posted to www.fbo.gov

Number II

The Congressional Cybersecurity Training Resolution

Sponsored by Reps. Kathleen Rice (D-N.Y.) and John Katko (R-N.Y.), would require the chief administrative officer of the House to carry out annual cyber and IT training for House members, officers and employees.

IN THE HOUSE OF REPRESENTATIVES

Miss RICE of New York submitted the following resolution; which was referred to the Committee on _____

RESOLUTION

Amending the Rules of the House of Representatives to direct the Chief Administrative Officer to carry out an annual information security training program for Members, officers, and employees of the House.

This Act may be cited as the "Congressional Cybersecurity Training Resolution of 2019".

Clause 4 of rule II of the Rules of the House of Representatives is amended by adding at the end the following new paragraph:

"(e)(1) The Chief Administrative Officer shall carry out an annual information security training program for Members (including the Delegates and Resident Commissioner), officers, and employees of the House.

"(2) A new Member, Delegate, Resident Commissioner, officer, or employee of the House shall receive training under this paragraph not later than 30 days after beginning service to the House.

"(3) Not later than January 31 of each year, each officer and employee of the House shall file a certification with the Chief Administrative Officer that the officer or employee completed an information security training program as established by this paragraph.".

To read more:
https://kathleenrice.house.gov/uploadedfiles/cyber_training_res_2019.pdf

Number 12

EU Elections Update: The Long Game

With the European parliamentary elections approaching in less than a month's time, we devote this week's Disinfo Review to a brief summary of the ongoing disinformation trends surrounding the elections.

First, a reminder: Russia's disinformation campaign against the EU – and by extension, its electoral process – has been underway for five years. It is not a new feature of the European political landscape.

The Kremlin's efforts to undermine public support for the EU, promote populist and Eurosceptic parties and candidates, increase polarisation and fragment European unity began in earnest in 2014, and have not relented since.

Russia is playing a long game in Europe: its objective is not merely to influence the outcome of any particular election, but rather to broadly subvert the efficacy of our democratic institutions, fuel widespread social fragmentation and mistrust, and ultimately paralyse our ability to act in our own self-interest and to defend our values.

The Snowball Effect

Using various tactics and disinformation narratives, the Kremlin has been sowing the seeds of this discontent now for nearly half a decade.

It has habitually supported populist, anti-EU parties and candidates on both the far right and the far left, attacked the integrity of mainstream politics and media, and emphasised the illegitimacy and futility of elections in a system it alleges to be fundamentally corrupt.

Through these efforts, the Kremlin has empowered and amplified other venal and anti-democratic actors to grow their influence in Europe, creating a snowball effect for its anti-Western agenda.

Due to this meticulous groundwork and the long-term integration (and normalisation) of anti-EU narratives in the public sphere, the Kremlin's attempted manipulation of the EP elections looks far less sensational than

other more infamous cases, such as #MacronGate or the 2016 US presidential election.

But this doesn't mean that no manipulation is taking place – on the contrary, the pro-Kremlin media continues to persistently attack the EU, its values, and its democratic mandate whilst simultaneously promoting Eurosceptic voices.

For example, Sputnik systematically features interviews with and updates of anti-EU parties as well as their candidates and positions.

Sputnik Poland headlines anti-EU politicians, giving them space and promoting their narratives, while Sputnik Italy has given exclusive attention to the national-conservative Fratelli d'Italia (Brothers of Italy) party.

Questioning the legitimacy of European elections on grounds of corruption and the EU's alleged capture by special interests is another common trope aimed at discouraging voter turnout.

To read more:
https://euvsdisinfo.eu/eu-elections-update-the-long-game/

https://euvsdisinfo.eu/methods-of-foreign-electoral-interference/

Number 13

Revisiting an important article

Preparing for Cyber Incidents with Physical Effects

Joseph W. Pfeifer, Chief of Counterterrorism and Emergency Preparedness for the New York City Fire Department (FDNY).

THE CYBER DEFENSE REVIEW

Cyber weapons have been used to steal billions of dollars of intellectual property, influence elections, manipulate news and damage critical infrastructure.

Yet, we think of cyberattacks as only a technology problem, which are handled by smart computer network technicians capable of discovering a breach and developing patches to mitigate the problem.

Certainly, technical solutions are a big part of cyber preparedness.

But what if cyberattacks combine denial of services in cyberspace with targeted attacks on critical infrastructure, causing massive damage and loss of life in the physical world?

This article will explore how federal, state, and local agencies, as well as private corporations, are using tabletop exercises, functional simulations and war gaming to prepare for significant cyberattacks.

These programs examine how public and private sectors adapt to extreme cyber events.

In a connected world, adaptive incident managers quickly form networks to exchange ideas, align core efforts and foster public communication.

To read the article:
https://cyberdefensereview.army.mil/Portals/6/Documents/CDR_V3N1_SPRG2018_Complete.pdf

Disclaimer

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

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

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

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

This information:

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

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

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

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

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

- is in no way constitutive of interpretative;

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

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

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

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