February 2020, cyber risk and compliance in Switzerland

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

Dear readers and friends,

At its meeting on 29 January, the Federal Council approved Switzerland's foreign policy strategy for the next four years.

The thematic focus areas for 2020–23 are peace and security, prosperity, sustainability and digitalisation.

The strategy also includes clear regional objectives worldwide, with a special focus on the EU, and new objectives for the external network and foreign policy communication.

For the first time, the Federal Department of Foreign Affairs (FDFA) prepared the foreign policy strategy as part of a broad interdepartmental process.

The Federal Council thus intends to increase the coherence, effectiveness and credibility of Swiss foreign policy.

In a world marked by increasing volatility, a strategic framework is essential to guide Switzerland's actions abroad. The Foreign Policy Strategy 2020–23 translates the objectives of the Federal Council's legislative programme into such a framework for foreign policy action.

Based on the Federal Constitution and the principles of consistency, trust and tradition, it defines new focus areas with regard to the previous strategy and proposes new instruments for dealing with a changing global context. The four thematic focus areas set by the Federal Council are:

1. Peace and security

In a spirit of cooperation with other countries, Switzerland is committed to working towards a safe and peaceful world where everyone can live free from want and fear, have their human rights protected and enjoy economic

prosperity. In times of polarisation, demand is growing for Switzerland's specific and wide-ranging expertise, e.g. good offices, humanitarian commitment, bridge-building skills, mediation, military peace support and science diplomacy.

The focus here is on the candidacy for a non-permanent seat on the UN Security Council for the 2023–24 period, which would enable Switzerland to intensify its work towards a peaceful international order.

2. Prosperity

If prosperity is to be assured over the long term, it must be sustainable, shared by all and based on clear and respected international rules. Through targeted international cooperation and sustainable resource management, Switzerland supports this approach by contributing to the development of other countries.

To achieve this, it must also maintain its own prosperity up to 2023 and beyond by working towards a stable global financial, trade and monetary architecture and by creating favourable framework conditions to support the Swiss economy as well as education, research and innovation.

The focus here is on consolidating and expanding the bilateral approach with the EU.

3. Sustainability

Within the framework of the UN 2030 Agenda for Sustainable Development, Switzerland is committed to promoting sustainable development that gives due and balanced consideration to the environment, the economy and society.

It has set up the appropriate administrative structures to this end. It also works at national and international level with all stakeholders to promote environmental protection and sustainability.

The focus here is on implementing the 2030 Agenda and on tackling climate change and protecting the environment.

4. Digitalisation

While continuing to develop its digital foreign policy, Switzerland intends to add a digital dimension to its role as a bridge-builder. Switzerland will also work to ensure that cyberspace activities comply with international law, making people and their needs a priority.

The main focus here is on raising Switzerland's profile in global efforts to consolidate cyber governance. Geneva is to be positioned as a leading hub in this respect.

These four thematic focus areas and the objectives of the Foreign Policy Strategy 2020–23 will be implemented in all regions of the world and at the multilateral level.

Particular emphasis will be placed on relations with the EU. As before, the objectives of Switzerland's EU policy are to consolidate and develop the bilateral approach by means of an institutional agreement and to ensure a partnership that strikes an optimum balance between maximum access to the internal market, wide cooperation in other areas of common interest, and the broadest political autonomy possible.

The Federal Council mandated the FDFA in 2011 to prepare a foreign policy strategy every four years. This is the third such paper to be adopted. For the first time, the strategy has been formulated as part of a broad interdepartmental process. The Federal Council seeks to broaden the consensus on Swiss foreign policy and make sure that it is implemented coherently in line with Switzerland’s national interests and values.

You will find more information at:
https://www.eda.admin.ch/dam/eda/en/documents/publications/SchweizerischeAussenpolitik/Aussenpolitische-Strategie-2020-23_EN.pdf

At its meeting on 19 February 2020, the Federal Council adopted the Dispatch on Switzerland's Strategy for International Cooperation 2021–24 (International Cooperation Strategy 2021–24).

Swiss development cooperation will become more focused, thereby enhancing its effectiveness.

With its International Cooperation Strategy 2021–24, the Federal Council is requesting five framework credits totalling CHF 11.25 billion over four years.

The thematic focus areas of the new strategy are the creation of decent jobs locally, mitigating climate change and adapting to its effects, reducing the causes of irregular migration and promoting the rule of law.

Going forward, still greater use will be made of the potential of the private sector and digitalisation. Multilateralism remains an important pillar of Switzerland's international cooperation.

In terms of economic prosperity, health and quality of life, humanity has made unprecedented progress in recent decades. Thanks to sustained growth in the world economy, social programmes at national level (especially in middle-income countries) and official development assistance (ODA), the proportion of people living in extreme poverty fell from 41% in 1981 to 10% in 2015.

Despite this progress, extreme poverty still affects one in ten people, and in the coming years Africa will have the greatest need to catch up. Challenges such as climate change, lack of food security, economic and financial crises, epidemics, human rights violations and armed conflicts also jeopardise the achievements made to date in combating poverty.

With its International Cooperation Strategy 2021–24, the Federal Council is requesting from Parliament five framework credits totalling CHF 11.25 billion to fund humanitarian aid, development cooperation and the promotion of peace and human security. According to current forecasts, Switzerland's ODA would thus amount to an average of 0.46% of gross national income for the 2021–24 period (ODA/GNI ratio).

The Federal Council seeks to achieve greater harmonisation between the Federal Act on Private Security Services Provided Abroad (PSSA), Goods Control Act (GCA) and War Material Act (WMA).

It has issued instructions to this effect to the Federal Department of Foreign Affairs (FDFA), Federal Department of Justice and Police (FDJP) and Federal Department of Economic Affairs, Education and Research (EAER) at its meeting on 12 February 2020.

The relevant proposals are based on a report produced by an interdepartmental working group.

In addition to achieving greater consistency in the interpretation of the law, the Federal Council is looking to revise the Ordinance on Private Security Services Provided Abroad.

The FDFA and the FDJP have been tasked with submitting relevant amendments to the Federal Council this year, including more precise definitions of the terms 'logistical support', 'advising and training members of armed or security forces' and 'operating and maintaining weapons systems'.

It has also been proposed that the Ordinance should include an EAER consultation mechanism along the lines of the War Material Ordinance and Goods Control Ordinance. The Ordinance as amended should also provide that where the authorities have differing views or the arrangements concerned have far-reaching political implications, the matter should be put before the Federal Council for a decision.

Reviewing the effectiveness of the amendments after three years

The FDFA and the FDJP will review the effectiveness of these amendments after three years, in consultation with the EAER and the Federal Department for Defence, Civil Protection and Sport (DDPS), and report their findings to the Federal Council. Suggestions for improvement should also be submitted to the Federal Council where necessary.

As well as measures to achieve greater consistency between the various pieces of legislation, in line with the proposals of the interdepartmental working group (IDWG), the Federal Council has also proposed a review of possible amendments to the PSSA.

The Federal Council believes combining short and medium-term measures is the best way to achieve rapid improvements in key areas for the Swiss export industry and security policy.

IDWG has outlined the need for action and proposed a number of solutions

The PSSA/WMA/GCA interdepartmental working group was set up by the FDFA and EAER on 21 February 2019 and is composed of representatives from the FDFA, EAER, FDJP and DDPS.

It was tasked with assessing similarities and differences between the authorisation and prohibition criteria laid down in the legislation, determining what action was needed, and proposing specific solutions in relation to the PSSA.

The IDWG completed its work at the end of 2019 and presented its report to the heads of the FDFA and EAER. The report was submitted to the Federal Council for consideration at its meeting on 29 January 2020.

I have just read for the second time the report from the US Office of Intelligence & Analysis with title *Strategic Plan for Fiscal Years 2020-2024*. The Office of Intelligence & Analysis is the first federal agency statutorily mandated to share intelligence with state, local, tribal, and territorial law enforcement, as well as the private sector.

We read: "Emerging disruptive technologies continue to outpace legislation and countermeasures across the Homeland.

Unmanned aerial systems (UAS) will continuously enable transnational criminal organizations and criminals to carry out cross-border drug smuggling operations.

Actors will continue to use UAS to conduct surveillance of law enforcement, and potentially facilitate kinetic attacks on stationary, mobile, and high-consequence targets.

Additionally, nefarious actors are increasingly acquiring new capabilities, and enhancing their use of technology previously only accessible to nation-state actors."

I remember a 1970 book, written by Alvin Toffler, with title *Future Shock*. According to Alvin, "It is undeniably true that we frequently apply new technology stupidly and selfishly. In our haste to milk technology for immediate economic advantage, we have turned our environment into a physical and social tinderbox. Our technological powers increase, but the side effects and potential hazards also escalate."

We can see that it is not the first time we are concerned about emerging disruptive technologies. But as we can see in the recent I&A Strategic Plan 2020-2024, during this era of dynamic threats that cross borders in both the physical and digital arenas, we need more and more intelligence and information on transnational organized crime, terrorism, cyber-threat actors, counterintelligence vulnerabilities, economic security, and other developing threats that pose a critical danger to security and the democratic way of life.

Read more at number 1 below.

We can read in *Juvenal's Satires:* “rara avis in terris nigroque simillima cygno” (a bird as rare on the earth as a black swan).

The term *black swan* was used in the 16th century in London, to describe something impossible or at least improbable.

I met Nassim Nicholas Taleb before a couple of years, during the RiskMinds International Conference, at Hotel Okura in Amsterdam. I attended his class after the conference, and we had the opportunity to discuss about his *black swan theory*.

The theory describes a high impact but low likelihood event, for which we are totally unprepared, as we consider it a black swan (we assume that it does not exist as a risk).

Today I read a paper with title *“The green swan. Central banking and financial stability in the age of climate change”* from the Bank of France (Patrick BOLTON, Morgan DESPRES, Luiz Awazu PEREIRA DA SILVA, Frédéric SAMAMA, Romain SVARTZMAN).

According to the paper, the “green swan” concept finds its inspiration in the famous concept of the “black swan” developed by Nassim Nicholas Taleb.

Black swan events have three characteristics:

(i) they are unexpected and rare, thereby lying outside the realm of regular expectations;
(ii) their impacts are wide-ranging or extreme;
(iii) they can only be explained after the fact.

According to the paper (*The green swan*), black swan events can take many shapes, from a terrorist attack to a disruptive technology or a natural catastrophe. These events typically fit fat tailed probability distributions, ie they exhibit a large skewness relative to that of normal distribution (but also relative to exponential distribution).

As such, they cannot be predicted by relying on backward-looking probabilistic approaches assuming normal distributions (eg value-at-risk models). The existence of black swans calls for alternative epistemologies of risk, grounded in the acknowledgment of uncertainty.

For instance, relying on mathematician Benoît Mandelbrot (1924–2010), Taleb considers that fractals (mathematically precise patterns that can be found in complex systems, where small variations in exponent can cause large deviation) can provide more relevant statistical attributes of financial

markets than both traditional rational expectations models and the standard framework of Gaussian-centred distributions (Taleb (2010)).

Read more at number 5 below.

I have read an excellent paper, the *Summary of NCSC's security analysis for the UK telecoms sector*.

The National Cyber Security Center (NCSC) in UK has brought together expertise from the information assurance arm of the Government Communications Headquarters (GCHQ), the Centre for Cyber Assessment, the CERT-UK, and the Centre for Protection of National Infrastructure.

We read in the *Summary of NCSC's security analysis for the UK telecoms sector:*

Supply chain, risk overview - No operator can perform all of the activities required to design, manufacture, install and run an operational telecoms network, and some are not equipped or staffed to operate all the supporting functions that the underlying business requires.

Every operator therefore has a supply chain, which can involve the provision of hardware, software, and managed services.

Supply chain risk breaks down into four risk components:
- risks due to national dependence, supply disruption and sanction,
- risks due to equipment supply (including software),
- risks due to supplier network access and support,
- risks to operator data including SIM supply.

These risks are directly linked, in that mitigating one risk will likely increase another. Consequently, minimising the risk to the UK requires balancing the risk across each risk component.

The extent of supply chain risk depends significantly on the sensitivity of the equipment supplied or accessed. Assuming a properly managed network, the supplier can only directly alter the behaviour of equipment it supplies or supports. Hence the risk of supply is intimately coupled to equipment sensitivity.

The intrinsic risks due to the supply chain are described in the following sections. These are risks that occur absent any mitigating actions by operators or governments.

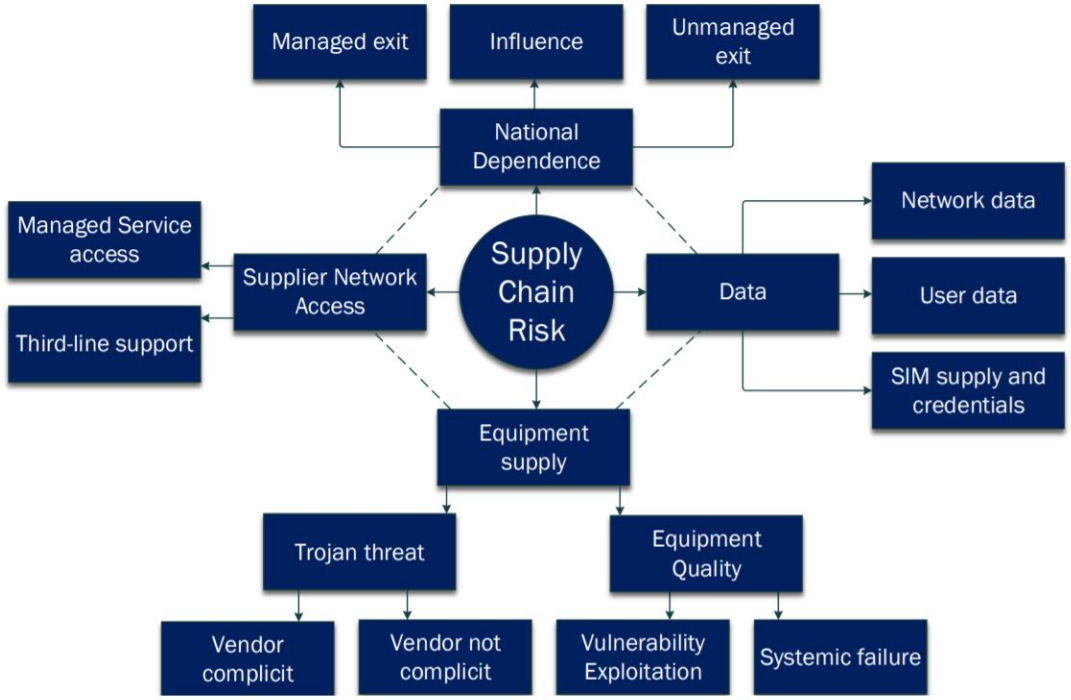


Figure 5.5.1-1: A breakdown of supply chain risk

Read more at number 2 below. Welcome to our monthly newsletter.

Best regards,

George Lekatis

George Lekatis
General Manager, Cyber Risk GmbH
Rebackerstrasse 7, 8810 Horgen
Phone: +41 43 810 43 61
Mobile: +41 79 505 89 60
Email: george.lekatis@cyber-risk-gmbh.com
Web: www.cyber-risk-gmbh.com

Cyber Risk GmbH, Handelsregister des Kantons Zürich, Firmennummer: CHE-244.099.341

Our catalog, *in-house* instructor-led training in Switzerland, Liechtenstein and Germany: https://www.cyber-risk-gmbh.com/Cyber_Risk_GmbH_Catalog_2020.pdf

Number 1 (Page 12)

Office of Intelligence & Analysis
Strategic Plan for Fiscal Years 2020-2024.

Number 2 (Page 14)

Summary of NCSC's security analysis for the UK telecoms sector

Number 3 (Page 16)

Cybercrime Prevention Principles for Internet Service Providers

Number 4 (Page 17)

Election security

DHS Plans Are Urgently Needed to Address Identified Challenges Before the 2020 Elections

Number 5 (Page 21)

The green swan

Central banking and financial stability in the age of climate change (115 pages). Patrick BOLTON - Morgan DESPRES - Luiz Awazu PEREIRA DA SILVA Frédéric SAMAMA - Romain SVARTZMAN, January 2020

Number 6 (Page 23)

NIST Tests Forensic Methods for Getting Data From Damaged Mobile Phones

Researchers put law enforcement hacking tools to the test.

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

Number 7 (Page 26)

What a Pair! Coupled Quantum Dots May Offer a New Way to Store Quantum Information

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

Number 8 (Page 29)

Mitigating Cloud Vulnerabilities

Number 9 (Page 31)

Intentional Use of Audio-Visual Distortions & Deep Fakes

Theodore E. Deutch, Florida
Chairman
Kenny Marchant, Texas
Ranking Member

Grace Meng, New York
Susan Wild, Pennsylvania
Dean Phillips, Minnesota
Anthony Brown, Maryland

John Ratcliffe, Texas
George Holding, North Carolina
Jackie Walorski, Indiana
Michael Guest, Mississippi

ONE HUNDRED SIXTEENTH CONGRESS

U.S. House of Representatives

COMMITTEE ON ETHICS

Thomas A. Rust
Staff Director and Chief Counsel

David W. Arrojo
Counsel to the Chairman

Christopher A. Donesa
Counsel to the Ranking Member

1015 Longworth House Office Buildin
Washington, D.C. 20515–6328
Telephone: (202) 225–7103
Facsimile: (202) 225–7392

Number 10 (Page 33)

Microsoft Releases Security Advisory on Internet Explorer Vulnerability

Cybersecurity and Infrastructure Security Agency (CISA)

Number 1

Office of Intelligence & Analysis
Strategic Plan for Fiscal Years 2020-2024.

Introduction, David J. Glawe, Chief Intelligence Officer, Under Secretary for Intelligence and Analysis.

I am pleased to publish the Office of Intelligence & Analysis Strategic Plan for Fiscal Years 2020-2024.

This document provides a holistic approach that will guide the continued evolution of the Office over the next five years and serves as a foundational document for how DHS Intelligence executes its broad mission and vision.

Following the September 11th, 2001 terrorist attacks, the Homeland Security Act of 2002 created the Department of Homeland Security and the Implementing Recommendations of the 9/11 Commission Act of 2007 established the Office of Intelligence & Analysis as the first federal agency statutorily mandated to share intelligence with state, local, tribal, and territorial law enforcement, as well as the private sector—creating the necessity for a comprehensive approach and strategy to Homeland security.

I&A provides timely, actionable intelligence to a far-reaching base of customers and partners—from the DHS Secretary and Components, policymakers, and the Intelligence Community to an expansive network of state, local, tribal, territorial, and private-sector partners with both national and global influence.

Therefore, this strategy outlines a forward-leaning approach to provide dominant capabilities and anticipatory intelligence to meet the diverse needs of DHS partners, customers, and stakeholders.

The threat environment is never static, thus I&A will remain dynamic in its actions to combat the challenges of today, as well as the future, through partnerships, information sharing, and a concrete understanding of the evolving landscape at home and beyond our Nation's borders.

Terrorist networks continue operations to inspire and mobilize those in our country, transnational criminal organizations seek to exploit our borders,

and state and non-state cyber actors target our critical infrastructure, information networks, and the American people; all of these threats will be met with our most forceful and innovative efforts to repel all threats to the Homeland.

This strategy further develops I&A's contributions to national security as a member of the Intelligence Community while simultaneously outlining this Office's activities to integrate and strengthen Department of Homeland Security Intelligence capabilities.

To reiterate my commitment to empowering DHS Intelligence professionals, I&A developed this strategy using vital input of I&A employees as well as contributions from internal and external stakeholders.

I am committed to investing in the DHS workforce to develop premier Homeland Intelligence professionals, truly the most important factor in delivering superior intelligence capabilities in our fight against hostile actions that threaten American security, prosperity, and values that are the fabric of our Nation.

Thank you for your continued support as we work to foster a collaborative environment and continue to bridge the gaps between the federal government, the Intelligence Community, and our state, local, tribal, territorial, and private-sector partners.

It is imperative that we evolve together, as a unified community, to provide the most comprehensive and robust protection possible for the American people.

To read more:
https://www.dhs.gov/sites/default/files/publications/20_0206-oia-strategic-plan-fy20-24.pdf

Number 2

Summary of NCSC's security analysis for the UK telecoms sector

Since the initiation of the DCMS Supply Chain Review in September 2018, the NCSC has performed an extensive and detailed analysis of the security of the telecommunications (telecoms) sector.

The outcomes of that analysis are now being provided through a blog by NCSC's Technical Director (https://www.ncsc.gov.uk/blog-post/the-future-of-telecoms-in-the-uk), our formal advice on the use of High Risk Vendors (HRVs) (https://www.ncsc.gov.uk/guidance/ncsc-advice-on-the-use-of-equipment-from-high-risk-vendors-in-uk-telecoms-networks), and through this document, a summary of NCSC's security analysis for the UK telecoms sector.

Specifically, this document summarises the NCSC's technical recommendations for improving the security of the UK's telecoms sector, alongside a description of our technical security analysis that we used to derive these recommendations. To read more: https://www.ncsc.gov.uk/files/Summary%20of%20the%20NCSCs%20security%20analysis%20for%20the%20UK%20telecoms%20sector.pdf

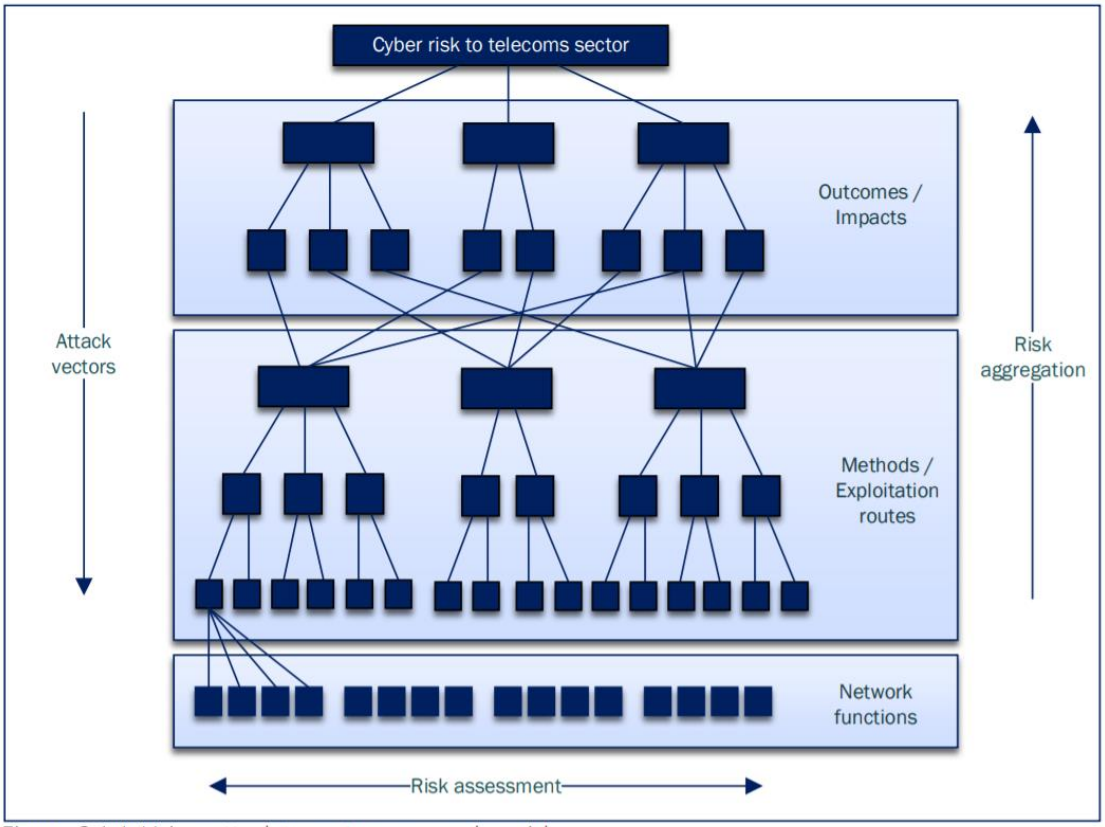


Figure 3.1-1: Using attack trees to assess cyber risk

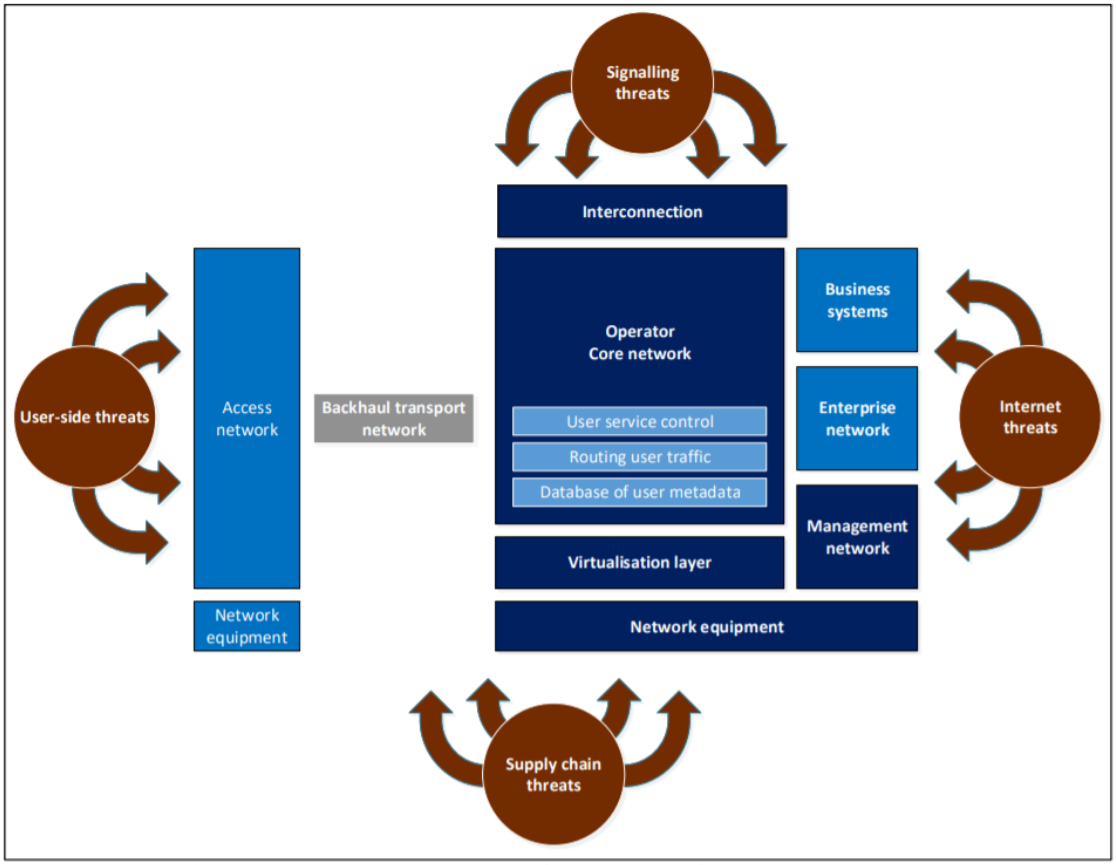


Figure 3.3-1: Attack vectors against a generalised telecoms network

Number 3

Cybercrime Prevention Principles for Internet Service Providers

While certain cyberattacks focus on specific organizations, the majority target the largest number of internet users possible. Such attacks are often relatively easy for cybercriminals to undertake and can cause serious harm. According to Cybersecurity Ventures, the impact of indiscriminate malicious activity online can be significant and carries an estimated global price tag of $6 trillion in 2021.

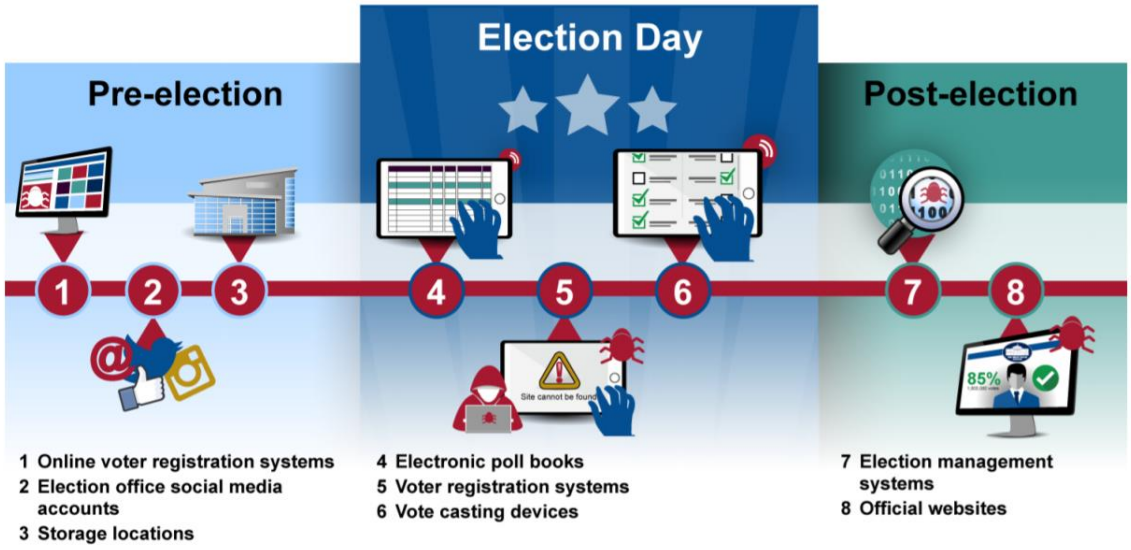
To read more:
http://www3.weforum.org/docs/WEF_Cybercrime_Prevention_ISP_Principles.pdf

Number 4

Election security

DHS Plans Are Urgently Needed to Address Identified Challenges Before the 2020 Elections

Figure: Examples of Election Assets Subject to Physical or Cyber Threats



Source: GAO analysis based on information reported by the Department of Homeland Security, the Harvard University John F. Kennedy School of Government's Belfer Center for Science and International Affairs, and the Center for Internet Security. | GAO-20-267

Since the 2017 designation of election infrastructure as critical infrastructure, the Department of Homeland Security (DHS), through its Cybersecurity and Infrastructure Security Agency (CISA), has assisted state and local election officials in securing election infrastructure through regional support and assistance, education, and information sharing. Such efforts help state and local election officials protect various election assets from threats (see figure above).

In August 2019, the CISA Director identified election security as one of the agency's top five operational priorities.

CISA security advisors, who are located throughout the country, consult with state and local election officials and identify voluntary, no cost services that CISA can provide. According to CISA, as of November 2019, 24 cybersecurity advisors and 100 protective security advisors perform and coordinate cyber and physical security assessments for the 16 critical infrastructure sectors, including the Election Infrastructure Subsector.

Technical teams at CISA headquarters generally provide the services, once requested.

To further assist state and local election officials, CISA conducted two exercises simulating real-world events and risks facing election infrastructure in August 2018 and June 2019.

According to CISA, the 2019 exercise included 47 states and the District of Columbia.

In addition, CISA has funded the Election Infrastructure Information Sharing and Analysis Center (EI-ISAC).

According to CISA officials, the EI-ISAC is the primary mechanism for exchanging information about threats and vulnerabilities throughout the election community.

The EI-ISAC director reported that, as of November 2019, its members included 50 states, the District of Columbia, and 2,267 local election jurisdictions, an increase from 1,384 local jurisdictions that were members in 2018.

As a result of its efforts, CISA has provided a variety of services to states and local election jurisdictions in the past 2 years (see table).

Table: Number of Selected Cybersecurity and Infrastructure Security Agency Services Provided to States and Local Election Jurisdictions in 2018 and 2019, as of November 6, 2019

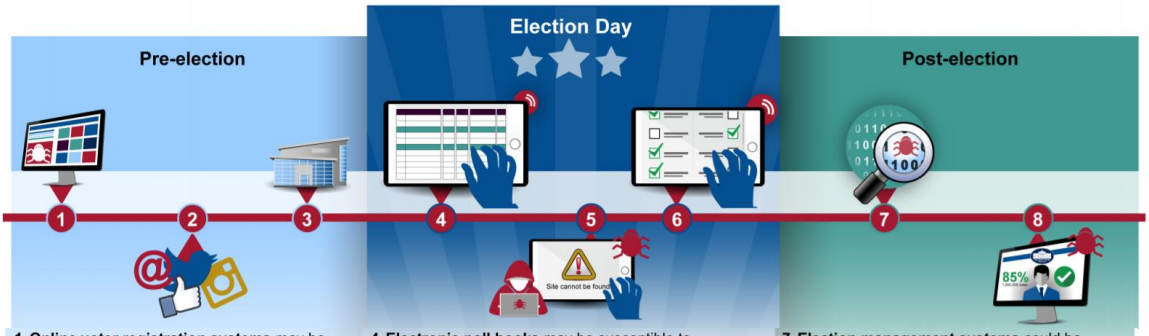
Service	States	Local election jurisdictions
Continuous scanning of internet-accessible systems for known vulnerabilities	40	161
Assessments of potential network security vulnerabilities	26	20
Remote testing of externally accessible systems for potential vulnerabilities	4	44
Assessments of states' and local jurisdictions' susceptibility to malicious emails	10	5
Educational posters on cybersecurity	19	1,202

Source: Cybersecurity and Infrastructure Security Agency. | GAO-20-267

State election officials with whom GAO spoke were generally satisfied with CISA's support to secure their election infrastructure. Specifically, officials from seven of the eight states GAO contacted said that they were very satisfied with CISA's election-related work.

Also, officials from each of the eight states spoke positively about the information that they received from the EI-ISAC.

Figure 1: Examples of Physical and Cyber Threats to the Election Infrastructure and Assets by Stage of the Election Process



1 **Online voter registration systems** may be susceptible to website spoofing as attackers can create a malicious copy of the official website to capture sensitive information or give voters the illusion that their information was updated. Targeted denial of service or outage attacks could prevent voter registration.

2 **Internal communication systems or election office social media accounts** could be compromised as attackers may use legitimate accounts from these systems to send out false information—such as false voting locations and inaccurate dates—to election officials, poll workers, or voters.

3 **Storage locations** may be vulnerable to physical tampering or destruction of voting equipment by attackers with malicious intentions.

4 **Electronic poll books** may be susceptible to compromise by malicious attackers who gain access to the poll books either using a wireless connection or because the physical device is not properly secured. A compromise to a poll book could allow attackers to manipulate the voter rolls—either deleting or altering existing voter registration data resulting in confusion when voters show up to vote on Election Day.

5 **Voter registration systems** access could be blocked and its data and backups could be encrypted or erased through ransomware, a type of malicious software, by attackers until a ransom is paid. This could also result in theft or irreversible encryption of voter registration databases and other sensitive records causing disruption to Election Day activities and potential decline in public trust.

6 **Vote casting devices** may be vulnerable to physical tampering using removable media or remotely using a wireless connection. A compromise to a vote casting device could allow a malicious actor to modify a vote on Election Day.

7 **Election management systems** could be compromised due to commercial software and hardware with security weaknesses or configuration errors in network connections. A successful attack could lead to manipulation of results during electronic transmission of vote tallies.

8 **Official websites** may be susceptible to compromise as attackers may replicate the official state or county website and post opposite results than are being reported—for instance, the winner of a particular race is now the loser.

Source: GAO analysis based on information reported by the Department of Homeland Security, the Harvard University John F. Kennedy School of Government's Belfer Center for Science and International Affairs, and the Center for Internet Security. | GAO-20-267

Further, officials from five states told GAO that their relationship with CISA had improved markedly since 2017 and spoke highly of CISA's expertise and availability.

To guide its support to states and local election jurisdictions for the 2020 elections, CISA reported that it is developing strategic and operations plans.

CISA intended to finalize them by January 2020, but has faced challenges in its planning efforts due to a reorganization within CISA, among other things.

In the absence of completed plans, CISA is not well-positioned to execute a nationwide strategy for securing election infrastructure prior to the start of the 2020 election cycle.

Further, CISA's operations plan may not fully address all aspects outlined in its strategic plan, when finalized.

Specifically, according to CISA officials, the operations plan is expected to identify organizational functions, processes, and resources for certain elements of two of the four strategic plan's lines of effort— protecting election infrastructure, and sharing intelligence and identifying threats.

CISA officials stated that CISA was unlikely to develop additional operations plans for the other two lines of effort—providing security assistance to political campaigns, and raising public awareness on foreign influence threats and building resilience.

To read more:
https://www.gao.gov/assets/710/704314.pdf

Number 5

The green swan

Central banking and financial stability in the age of climate change (115 pages). Patrick BOLTON - Morgan DESPRES - Luiz Awazu PEREIRA DA SILVA Frédéric SAMAMA - Romain SVARTZMAN, January 2020

Climate change poses new challenges to central banks, regulators and supervisors. This book reviews ways of addressing these new risks within central banks' financial stability mandate.

However, integrating climate-related risk analysis into financial stability monitoring is particularly challenging because of the radical uncertainty associated with a physical, social and economic phenomenon that is constantly changing and involves complex dynamics and chain reactions.

Traditional backward-looking risk assessments and existing climate - economic models cannot anticipate accurately enough the form that climate-related risks will take.

These include what we call "green swan" risks: potentially extremely financially disruptive events that could be behind the next systemic financial crisis.

Central banks have a role to play in avoiding such an outcome, including by seeking to improve their understanding of climate-related risks through the development of forward-looking scenario-based analysis.

But central banks alone cannot mitigate climate change. This complex collective action problem requires coordinating actions among many players including governments, the private sector, civil society and the international community.

Central banks can therefore have an additional role to play in helping coordinate the measures to fight climate change. Those include climate mitigation policies such as carbon pricing, the integration of sustainability into financial practices and accounting frameworks, the search for appropriate policy mixes, and the development of new financial mechanisms at the international level.

All these actions will be complex to coordinate and could have significant redistributive consequences that should be adequately handled, yet they are essential to preserve long-term financial (and price) stability in the age of climate change.

To read more you may visit: https://www.bis.org/publ/othp31.pdf

Number 6

NIST Tests Forensic Methods for Getting Data From Damaged Mobile Phones

Researchers put law enforcement hacking tools to the test.

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

Criminals sometimes damage their mobile phones in an attempt to destroy evidence.

They might smash, shoot, submerge or cook their phones, but forensics experts can often retrieve the evidence anyway.

Now, researchers at the National Institute of Standards and Technology (NIST) have tested how well these forensic methods work.

A damaged phone might not power on, and the data port might not work, so experts use hardware and software tools to directly access the phone's memory chips.

These include hacking tools, albeit ones that may be lawfully used as part of a criminal investigation.

Because these methods produce data that might be presented as evidence in court, it's important to know if they can be trusted.

"Our goal was to test the validity of these methods," said Rick Ayers, the NIST digital forensics expert who led the study. "Do they reliably produce accurate results?"

The results of the NIST study will also help labs choose the right tools for the job. Some methods work better than others, depending on the type of phone, the type of data and the extent of the damage.

The study addresses methods that work with Android phones. Also, the study covered only methods for accessing data, not decrypting it.

However, they can still be useful with encrypted phones because investigators often manage to get the passcode during their investigation.

To conduct the study, NIST researchers loaded data onto 10 popular models of phones. They then extracted the data or had outside experts extract the data for them. The question was: Would the extracted data exactly match the original data, without any changes?

For the study to be accurate, the researchers couldn't just zap a bunch of data onto the phones.

They had to add the data the way a person normally would.

They took photos, sent messages and used Facebook, LinkedIn and other social media apps.

They entered contacts with multiple middle names and oddly formatted addresses to see if any parts would be chopped off or lost when the data was retrieved.

They added GPS data by driving around town with all the phones on the dashboard.

After the researchers had loaded data onto the phones, they used two methods to extract it.

The first method takes advantage of the fact that many circuit boards have small metal taps that provide access to data on the chips.

Manufacturers use those taps to test their circuit boards, but by soldering wires onto them, forensic investigators can extract data from the chips.

This is called the JTAG method, for the Joint Task Action Group, the manufacturing industry association that codified this testing feature.

Chips connect to the circuit board via tiny metal pins, and the second method, called "chip-off," involves connecting to those pins directly.

Experts used to do this by gently plucking the chips off the board and seating them into chip readers, but the pins are delicate.

If you damage them, getting the data can be difficult or impossible.

A few years ago, experts found that instead of pulling the chips off the circuit board, they could grind down the opposite side of the board on a lathe until the pins were exposed.

This is like stripping insulation off a wire, and it allows access to the pins. "It seems so obvious," said Ayers. "But it's one of those things where everyone just did it one way until someone came up with an easier way." The chip-off extractions were conducted by the Fort Worth Police Department Digital Forensics Lab and a private forensics company in Colorado called VTO Labs, who sent the extracted data back to NIST. NIST computer scientist Jenise Reyes-Rodriguez did the JTAG extractions.

After the data extractions were complete, Ayers and Reyes-Rodriguez used eight different forensic software tools to interpret the raw data, generating contacts, locations, texts, photos, social media data, and so on. They then compared those to the data originally loaded onto each phone.

The comparison showed that both JTAG and chip-off extracted the data without altering it, but that some of the software tools were better at interpreting the data than others, especially for data from social media apps. Those apps are constantly changing, making it difficult for the toolmakers to keep up.

The results are published in a series of freely available online reports. This study, and the resulting reports, are part of NIST's Computer Forensics Tool Testing project. Called CFTT, this project has subjected a wide array of digital forensics tools to rigorous and systematic evaluation. Forensics labs around the country use CFTT reports to ensure the quality of their work.

"Many labs have an overwhelming workload, and some of these tools are very expensive," Ayers said. "To be able to look at a report and say, this tool will work better than that one for a particular case — that can be big advantage."

This research was funded by NIST and the Department of Homeland Security's Cyber Forensics Project (https://www.dhs.gov/science-and-technology/forensics).

Background information is available on the CFTT website (https://www.nist.gov/itl/ssd/software-quality-group/computer-forensics-tool-testing-program-cftt).

The JTAG and chip-off reports are available on the DHS website (https://www.dhs.gov/publication/st-binary-image-jtag-chip-decoding-and-analysis-tool-paraben-s-electronic-evidence)

Number 7

What a Pair! Coupled Quantum Dots May Offer a New Way to Store Quantum Information

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

Researchers at the National Institute of Standards and Technology (NIST) and their colleagues have for the first time created and imaged a novel pair of quantum dots — tiny islands of confined electric charge that act like interacting artificial atoms.

Such "coupled" quantum dots could serve as a robust quantum bit, or qubit, the fundamental unit of information for a quantum computer.

Moreover, the patterns of electric charge in the island can't be fully explained by current models of quantum physics, offering an opportunity to investigate rich new physical phenomena in materials.

Unlike a classical computer, which relies on binary bits that have just one of two fixed values — "1" or "0" — to store memory, a quantum computer would store and process information in qubits, which can simultaneously take on a multitude of values.

Therefore, they could perform much larger, more complex operations than classical bits and have the potential to revolutionize computing.

Electrons orbit the center of a single quantum dot similar to the way they orbit atoms. The charged particles can only occupy specific permitted energy levels.

At each energy level, an electron can occupy a range of possible positions in the dot, tracing out an orbit whose shape is determined by the rules of quantum theory.

A pair of coupled quantum dots can share an electron between them, forming a qubit.

To fabricate the quantum dots, the NIST-led team, which included researchers from the University of Maryland NanoCenter and the National Institute for Materials Science in Japan, used the ultrasharp tip of a scanning tunneling microscope (STM) as if it were a stylus of an Etch A Sketch.

Hovering the tip above an ultracold sheet of graphene (a single layer of carbon atoms arranged in a honeycomb pattern), the researchers briefly increased the voltage of the tip.

The electric field generated by the voltage pulse penetrated through the graphene into an underlying layer of boron nitride, where it stripped electrons from atomic impurities in the layer and created a pileup of electric charge.

The pileup corralled freely floating electrons in the graphene, confining them to a tiny energy well.

But when the team applied a magnetic field of 4 to 8 tesla (about 400 to 800 times the strength of a small bar magnet), it dramatically altered the shape and distribution of the orbits that the electrons could occupy.

Rather than a single well, the electrons now resided within two sets of concentric, closely spaced rings within the original well separated by a small empty shell.

The two sets of rings for the electrons now behaved as if they were weakly coupled quantum dots.

This is the first time that researchers have probed the interior of a coupled quantum dot system so deeply, imaging the distribution of electrons with atomic resolution (see illustration), noted NIST co-author Daniel Walkup.

To take high-resolution images and spectra of the system, the team took advantage of a special relationship between the size of a quantum dot and the spacing of the energy levels occupied by the orbiting electrons: The smaller the dot, the greater the spacing, and the easier it is to distinguish between adjacent energy levels.

In a previous quantum dot study using graphene, the team applied a smaller magnetic field and found a structure of rings, resembling a wedding cake, centered on a single quantum dot, which is the origin of the concentric quantum dot rings.

By using the STM tip to construct dots about half the diameter (100 nanometers) of dots that they had previously studied, the researchers succeeded in revealing the full structure of the coupled system.

The team, which included Walkup, Fereshte Ghahari, Christopher Gutiérrez and Joseph Stroscio at NIST and the Maryland NanoCenter, describes its findings today in Physical Review B.

The way in which the electrons are shared between the two coupled dots can't be explained by accepted models of quantum dot physics, said Walkup.

This puzzle may be important to solve if coupled quantum dots are eventually to be used as qubits in quantum computing, Stroscio noted.

Number 8

Mitigating Cloud Vulnerabilities

While careful cloud adoption can enhance an organization's security posture, cloud services can introduce risks that organizations should understand and address both during the procurement process and while operating in the cloud.

Fully evaluating security implications when shifting resources to the cloud will help ensure continued resource availability and reduce risk of sensitive information exposures.

To implement effective mitigations, organizations should consider cyber risks to cloud resources, just as they would in an on-premises environment.

This document divides cloud vulnerabilities into four classes (misconfiguration, poor access control, shared tenancy vulnerabilities, and supply chain vulnerabilities) that encompass the vast majority of known vulnerabilities.

Cloud customers have a critical role in mitigating misconfiguration and poor access control, but can also take actions to protect cloud resources from the exploitation of shared tenancy and supply chain vulnerabilities.

Descriptions of each vulnerability class along with the most effective mitigations are provided to help organizations lock down their cloud resources.

By taking a risk-based approach to cloud adoption, organizations can securely benefit from the cloud's extensive capabilities.

This guidance is intended for use by both organizational leadership and technical staff. Organizational leadership can refer to the Cloud Components section, Cloud Threat Actors section, and the Cloud Vulnerabilities and Mitigations overview to gain perspective on cloud security principles.

Technical and security professionals should find the document helpful for addressing cloud security considerations during and after cloud service procurement

To read more: https://media.defense.gov/2020/Jan/22/2002237484/-1/-1/0/CSI-MITIGATING-CLOUD-VULNERABILITIES_20200121.PDF

Number 9

Intentional Use of Audio-Visual Distortions & Deep Fakes

This memorandum serves as a reminder that Members must exercise care in communicating, especially when using electronic communication, such as email, websites, Facebook, Twitter, Instagram, or YouTube.

All House Members, officers, and employees must conduct themselves at all times in a manner that reflects creditably on the House.

As Members of the House of Representatives, we are widely recognizable public servants.

Communicating with our constituents and the public is one of our most important duties.

Electronic communication has drastically improved our ability to communicate directly and in real-time with our constituents at a minimal cost.

The fast pace and wide dissemination of electronic communication can lead to mistaken transmissions; for example, emailing the wrong person, posting a private message publicly, or sharing the wrong video.

All of these examples of mistakes may be embarrassing and have unintended consequences.

However, intentional distortions of audio and/or visual representations can be far more damaging.

Members have a duty, and a First Amendment right, to contribute to the public discourse, including through parody and satire.

However, manipulation of images and videos that are intended to mislead the public can harm that discourse and reflect discreditably on the House.

Moreover, Members or their staff posting deep fakes “could erode public

trust, affect public discourse, or sway an election."

Accordingly, Members, officers, and employees posting deep fakes or other audio-visual distortions intended to mislead the public may be in violation of the Code of Official Conduct.

Prior to disseminating any image, video, or audio file by electronic means, including social media, Members and staff are expected to take reasonable efforts to consider whether such representations are deep fakes or are intentionally distorted to mislead the public.

The Committee has long held that Members are responsible for the actions of their staff.

Further, Members must take reasonable steps to ensure that any outside organization over which the Member exercises control—including a campaign entity—operates in compliance with applicable law.

Accordingly, Members should ensure their official and campaign staff are familiar with the rules and regulations regarding electronic communications that those staff are involved in preparing or disseminating.

If you have any questions regarding this guidance, please feel free to contact the Committee's Office of Advice and Education at (202) 225-7103.

Number 10

Microsoft Releases Security Advisory on Internet Explorer Vulnerability

Cybersecurity and Infrastructure Security Agency (CISA)

Microsoft has released a security advisory to address a critical vulnerability in Internet Explorer. A remote attacker could exploit this vulnerability to take control of an affected system.

According to the advisory, “Microsoft is aware of limited targeted attacks.”

The Cybersecurity and Infrastructure Security Agency (CISA) encourages users and administrators to review Microsoft’s Advisory ADV20001 and CERT/CC's Vulnerability Note VU#338824 for more information, implement workarounds, and apply updates when available.

Consider using Microsoft Edge or an alternate browser until patches are made available.

Microsoft’s Advisory ADV20001, you may visit:
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV200001

CERT/CC's Vulnerability Note VU#338824, you may visit:
https://kb.cert.org/vuls/id/338824/

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.