

Cyber Risk GmbH
Handelsregister des Kantons Zürich, Firmennummer: CHE-244.099.341
Dammstrasse 16, 8810 Horgen, Switzerland
Tel: +41 79 505 89 60 Web: <https://www.cyber-risk-gmbh.com>



*July 2023, top cyber risk and compliance related
local news stories and world events*

Dear readers,

Bank regulators are introducing new *cyber resilience testing* requirements and make the existing financial stress testing obligations more complex.



We have an interesting paper from the Financial Stability Institute (FSI) of the Bank for International Settlements (BIS), with title "*Banks' cyber security – a second generation of regulatory approaches*".

The “first generation” cyber regulations, focused on establishing a cyber risk management approach and controls.

Over the last few years, authorities, including those in Emerging Markets and Developing Economies (EMDEs), have issued *new or additional* cyber regulations. These second-generation regulations have a more embedded “**assume breach**” mentality and hence are more aligned with operational resilience concepts.

As such, they focus on improving cyber resilience and providing financial institutions and authorities with specific tools to achieve this.

Managing cyber risks that could arise from connections with third-party service providers has become a key element of the “second generation” cyber security framework. There are now more specific regulatory requirements on cyber incident response and recovery, as well as on incident reporting and cyber resilience testing frameworks.

In addition, regulatory requirements or expectations relating to issues such as cyber resilience metrics and the availability of appropriate cyber security expertise in banks have been introduced.

Read more at number 3 below.



Definitions are very important. George S. Patton has said: “If we take the generally accepted definition of bravery as a quality which knows no fear, I have never seen a brave man”.

We have an interesting definition of *nature-related risk* at the *June 2023 Financial Stability Report*, from the European Insurance and Occupational Pensions Authority (EIOPA), which covers the key developments and risks in the European insurance and occupational pensions sectors. We read:

“*Nature-related risk* refers to the risk of loss of nature, i.e. the loss of natural capital, the reduction of the stock of renewable and non-renewable natural resources, plants and animal species on earth, as well as damage to the way in which they interact with each other (‘ecosystems’).

Nature-related risks are transmitted into society directly (‘first-order’), indirectly (i.e. ‘second order’, for example through value chains) or through spill-over impacts (contagion), affecting citizens, businesses and the economy at large.”

What follows is even more interesting:

“(Re)insurers will thus mostly experience *indirect* nature-related risks through their investments and liabilities in the form of:

1. *Nature-related transition risk*: Misalignment of the asset and liabilities portfolios of (re)insurers with developments (policy, technological, legal,

consumer preferences) aimed at reducing or reversing damage to nature can result in increased counterparty defaults or declining asset values (market risk) for their investments, as well as risks of mispricing and higher claims (underwriting risk).

For example, due to the ‘tightening’ (increase) of legal requirements for due diligence or mandatory liability for environmental damage, transition risks may materialize in liability insurance, credit and suretyship insurance.

2. Nature-related physical risk: Materialization of damage to nature as well as changes in natural stock and flows, can result in losses in investments or higher insurance liabilities.

Where insured goods or activities suffer nature-related damage, insurers may face increasing numbers and amounts of claims, for example in property and business interruption insurance or crop insurance.”

In the same paper, we also read:

“*Cyber underwriting* carries significant risks and insurers may lack the expertise and resources necessary to assess and price cyber risks adequately, leading to under-priced policies and potential large-scale losses. Consequently, there are concerns from the insurance industry about the *insurability of cyber-attacks*.

The insurance industry has previously dealt with systemic risks such as pandemics and climate change, but the pressing risk facing the industry are now cyberattacks. Insurers are used to dealing with large-scale risks such as the formerly mentioned ones, but cyber risks pose new challenges due to their ever-evolving nature.

It seems there are already efforts by the industry to allow investments into cyber risks via insurance-linked securities.”

We also read:

“The *real estate market* in Europe may be at a turning point. After experiencing a prolonged period of increasing real estate prices, there are clear indications that the European real estate market has now peaked.

Several factors have a negative impact on its near-term prospects. The main one is that interest rates have risen significantly, increasing the cost of financing real estate and discouraging investment in the sector.

Additionally, high inflation puts a strain on the disposable income of

households. In the commercial real estate sectors, the slowdown in economic growth reduces demand for property when businesses close or downsize.

Commercial real estate is a cyclical market with price declines during times of crisis. This cyclical development comes on top of the structural change that office attendance is still significantly lower than it was before the pandemic, which reduces demand for offices.”

Read more at number 15 below.

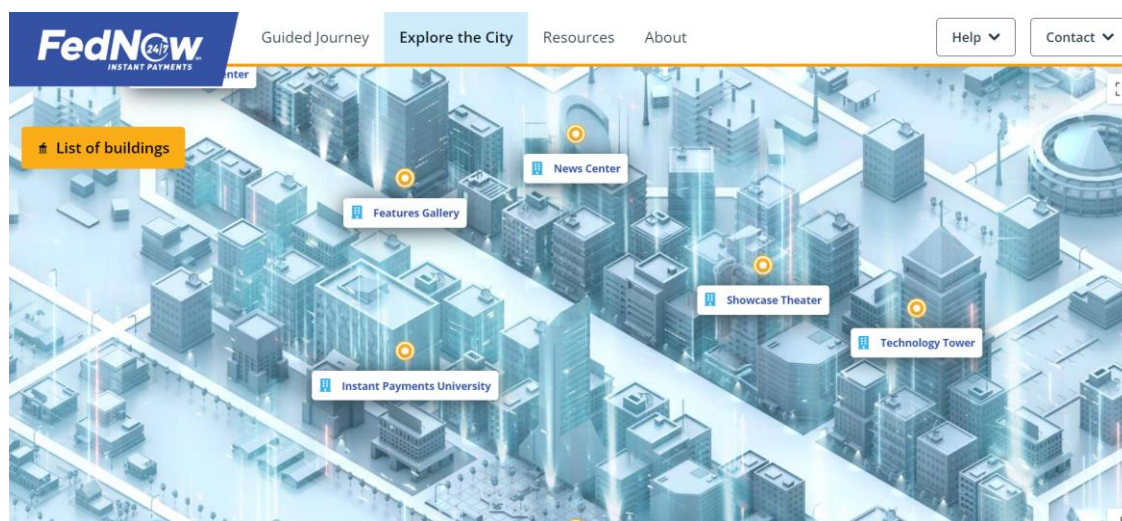


On March 15, the Federal Reserve announced that the *FedNow Service* will launch in **July 2023**. I have spent a couple of days trying to understand it better, and evaluate the Basel 3 compliance benefits.

This is a safe and efficient instant payment infrastructure that will operate around the clock, 365 days a year, and it will enable financial institutions of all sizes to offer customers the ability to send and receive money *immediately*, providing receivers *immediate access to funds*.

I liked the way funds settle between participating financial institutions instantly, *without the buildup of interbank obligations or short-term credit risk*, something great for Basel 3 compliance.

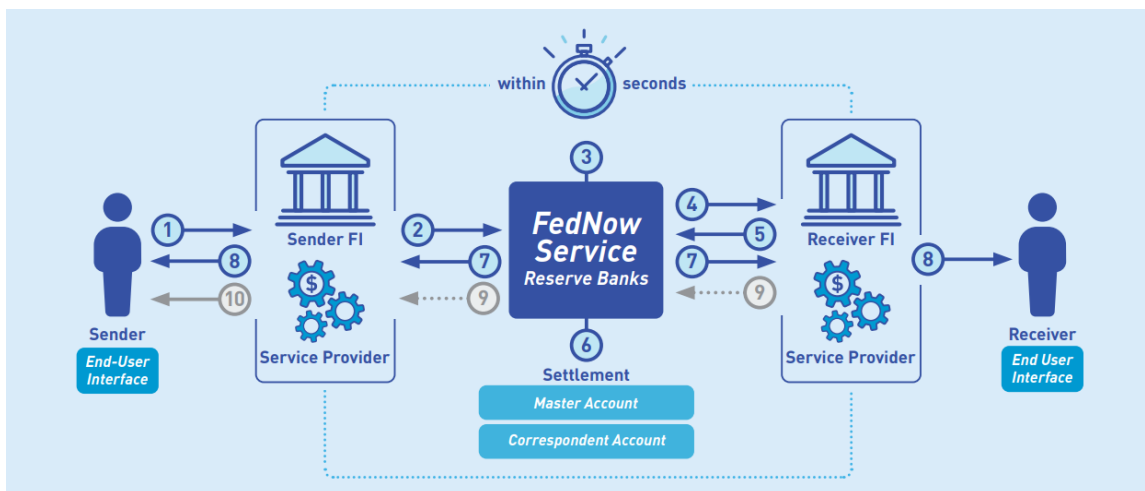
To support and complement the fraud mitigation efforts of each financial institution, the FedNow Service will offer additional fraud management capabilities and will enable security features to protect against threats.



I liked the content and the design of the page:

<https://explore.fednow.org/explore-the-city>

How it works (an overview).



1. A sender (an individual or business) initiates a payment by sending a payment message to its Financial Institution (FI).
2. The sender's FI, or its service provider, submits a payment message to the FedNow Service.
3. The FedNow Service validates the payment message, for example, by verifying that it meets message format specifications.
4. The FedNow Service sends the contents of the payment message to the receiver's FI to seek confirmation that it intends to accept the payment message.
5. The receiver's FI sends a positive response to the FedNow Service, confirming that it intends to accept the payment message.
6. The FedNow Service debits and credits the designated master accounts of the sender's and receiver's FI respectively.
7. The FedNow Service sends a payment message forward to the receiver's FI with an advice of credit and sends an acknowledgement to the sender's FI that settlement is complete.
8. The receiver's FI credits the receiver's account. The receiver's FI makes funds available to the receiver immediately after step 7.

Read more at number 21 and 22 below. Welcome to the Top 10 list.



In Switzerland, we have a very interesting article from the Swiss National Cyber Security Centre (NCSC) with title “Holiday season: what you should consider before you leave home”. We read:

The summer holidays are upon us, and holiday time often means travel time. In an increasingly connected world, where various mobile devices such as mobile phones, laptops and tablets also travel with you, it is important to protect yourself from the dangers present in cyberspace. This is particularly the case when travelling abroad.

In addition to your real-world preparations, such as packing your suitcase, it is important that you also take some measures in the digital world to ensure a relaxed trip. The most important measures that you can take to protect your online security before you travel are outlined below.

Watch out when booking!

In most cases, planning a trip starts with looking for suitable accommodation or booking a flight. While searching the internet, you might discover a tempting travel offer, at an unbeatable price – in this case, caution is advised: if an offer is too good to be true, it usually is.

- Book your stay on trustworthy platforms or directly with the airline, the hotel or via a travel agent
- Check if the airline's and accommodation's websites are genuine by looking at the website's "About us" page
- Check the user reviews
- Only use secure payment sites

Before you leave:

- *Only take essentials with you:* Only take essential devices with you. And make a note of the credit card company's hotline number in case you need to block your card(s).
- *Create a backup:* Your device could be lost or stolen while on

holiday. Back up your data before you leave.

- *Update your software:* Make sure all your devices, including smartphones, laptops and tablets, have the latest operating systems and security updates. Updated software will patch known security vulnerabilities and protect you from potential attacks.
- *Use strong passwords:* Before you leave, review all your passwords and make sure they are strong and unique. Avoid common passwords and use the longest possible combination of letters, numbers and special characters. In addition, use different passwords for each of your online accounts to ensure that one compromised account does not jeopardise all the others.
- *Enable two-factor authentication:* Two-factor authentication adds an extra layer of security by requiring you to complete another verification step in addition to your password, such as receiving a code via text message or using an authentication app. Enable this feature on all your accounts that support it to make unauthorised access more difficult. Be sure to also activate 3D Secure on your credit card(s).
- *Secure your devices:* Make sure you protect all your devices with a PIN, password, fingerprint or facial recognition. If possible, activate encryption for your hard drives to protect your data from unauthorised access. Take only essential devices with you.



The Swiss National Cyber Security Centre (NCSC), in another article with title “Right website, wrong hotline number”, explains something we all must understand. We read:

When holiday season rolls around, the fraudsters are never far behind. They use special tricks to get to their victims' holiday funds. Sometimes these tricks are hard to spot, as illustrated by a case reported to the NCSC last week. Even when you are relaxing on holiday, it is still good to have your wits about you, and to be suspicious too often rather than not often enough.

Sometimes, things can go wrong on holiday. The train isn't running, you've missed your connection, the plane is cancelled or the hotel is overbooked.

In such cases, you need help so that you can continue your journey. It makes sense in these cases to use a search engine to find a number for the tour operator's hotline. However, fraudsters also take advantage of this, as illustrated by a case reported to the NCSC.

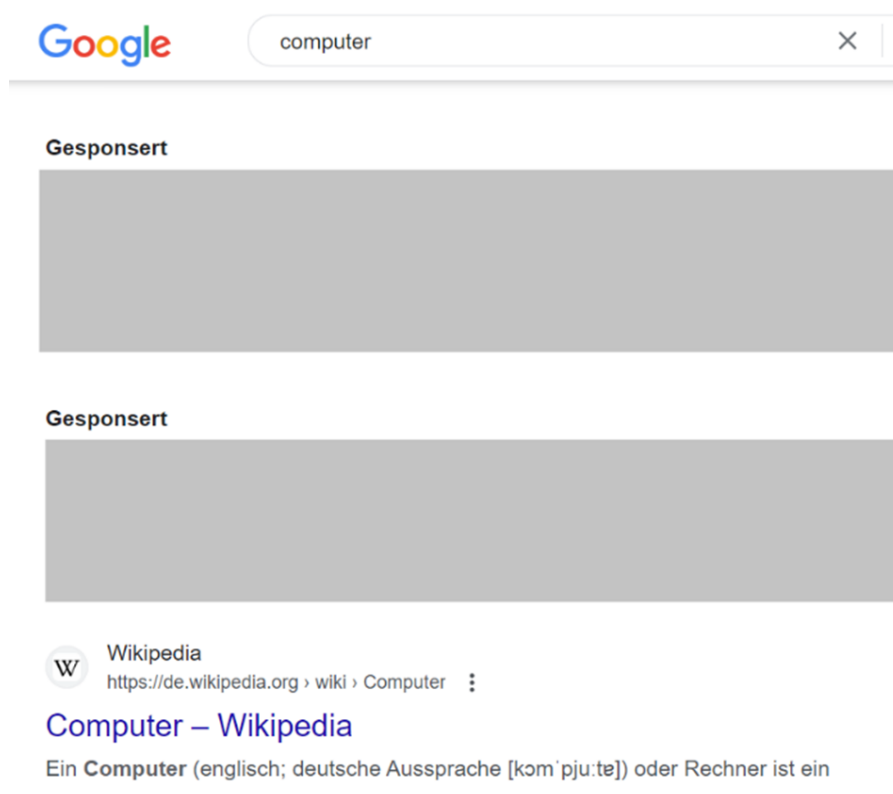
When the first search result sends you to the wrong website

In the Google search results in this case, the entry for a relevant support website of the tour operator was shown in first place. However, the victim did not realise that the first results are not actually search results but are instead adverts, inserted above the real results.

Although these entries are marked as "sponsored", this can easily be overlooked in the rush to sort out a holiday problem. The NCSC regularly receives reports about malicious adverts of this kind. They are posted by fraudsters to attract their victims to fraudulent websites.

As a rule, the NCSC recommends that users always check the URL of the visited website, to make sure that they really are on the correct site. In this case, however, this would not have helped, as the fraudsters' method was much more perfidious.

If you Google "computer", the first two results shown are sponsored entries, and only then is the first proper result listed – in this case, the Wikipedia entry.



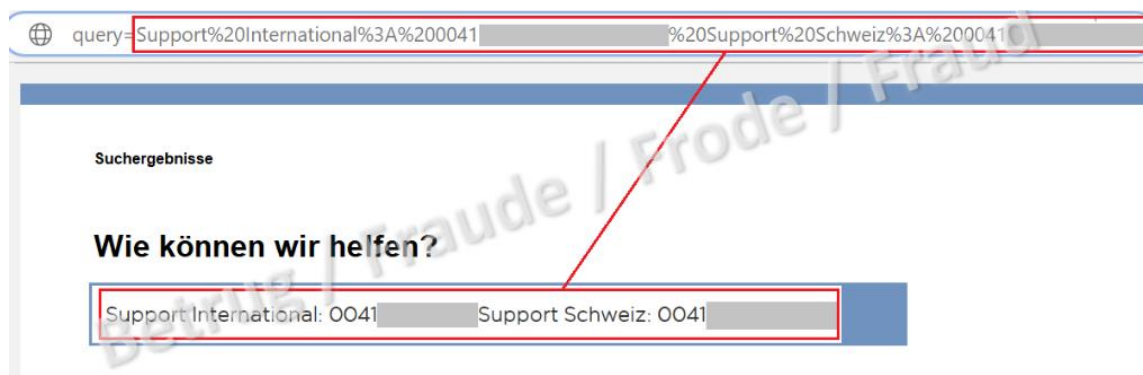
The screenshot shows a Google search interface. At the top, the Google logo is on the left, and a search bar contains the word "computer" with a clear button (X) on the right. Below the search bar, there are two "Gesponsert" (Sponsored) entries, each represented by a grey rectangular placeholder. Below these, the first organic search result is shown: the Wikipedia entry for "Computer". It features the Wikipedia logo, the text "Wikipedia", the URL "https://de.wikipedia.org › wiki › Computer", and the title "Computer – Wikipedia". Below the title, a short description begins: "Ein Computer (englisch; deutsche Aussprache [kɔmˈpjʊːtɐ]) oder Rechner ist ein".

Right website, wrong support hotline

If you click on the advert, it really does direct you to the correct website of the tour operator, where a field shows both the Swiss and international support numbers. However, the number shown leads not to the tour operator but directly to the fraudsters. How could this have happened?

The cause in this case was so-called "content injection". Here, the fraudsters are able to use a doctored link to post any content they like onto a legitimate website. This is possible if, for example, the internet address can be used to upload parameter values which are not checked and are then visible to users on the website.

Even though content injection may appear harmless at first glance, it can be used in combination with social engineering to exploit this content for the purposes of fraud, as the current example illustrates.



When they call the apparent hotline, users are usually asked to install an app and provide a credit card number. Shortly afterwards, money is deducted.

- Take care when using search engines. Do not mistake "sponsored search results" for actual search results.
- Call up the tour operator's website directly and search it for support numbers.
- Never provide your credit card details over the phone.
- If you did provide your credit card details, contact your credit card provider straight away.
- Before you leave on holiday, take the time to note down important hotline numbers. This includes the number of your credit card provider, for example, so that you can have the card blocked in an emergency.

Welcome to our monthly newsletter.

Best regards,

George Lekatis

George Lekatis
General Manager, Cyber Risk GmbH
Dammstrasse 16, 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 reading room: https://www.cyber-risk-gmbh.com/Reading_Room.html



[ABOUT](#) [TRAINING](#) [FOR THE BOARD](#) [ASSESSMENT](#) [READING ROOM](#) [CONTACT](#) [CYBER RISK LINKS](#) [IMPRESSUM](#)

January 2022

Presentations, articles, papers, news

1. Black Hat Asia 2023. Christina Lekati and Samuel Lolagar lead the class: "Fundamentals of Cyber Investigations and Human Intelligence" at Marina Bay Sands, Singapore.

In this class, participants learn a comprehensive methodology for gathering in-depth information on a human target, following three intelligence disciplines:

- Open-source intelligence (OSINT),
- Social media intelligence (SOCMINT), a sub-branch of OSINT,
- Human intelligence (HUMINT), and particularly, virtual HUMINT.

<https://www.blackhat.com/asia-23/training/schedule/#fundamentals-of-cyber-investigations--human-intelligence-29747>



*Number 1 (Page 16)***Malicious Actors Manipulating Photos and Videos to Create Explicit Content and Sextortion Schemes***Number 2 (Page 19)***Betreff | Spionage gegen den Verteidigungssektor (Subject | Espionage against the defense sector).**

From the German Bundesamt für Verfassungsschutz (Federal Office for the Protection of the Constitution)

*Number 3 (Page 21)***Financial Stability Institute, FSI Insights on policy implementation No 50 Banks' cyber security – a second generation of regulatory approaches**

Juan Carlos Crisanto, Jefferson Umehara Pelegrini and Jermy Prenio

*Number 4 (Page 26)***Dismantling encrypted criminal EncroChat communications leads to over 6 500 arrests and close to EUR 900 million seized**
Judiciary and law enforcement present first overview of results

European Union Agency for Law Enforcement Cooperation

*Number 5 (Page 28)***Data Protection: European Commission adopts new adequacy decision for safe and trusted EU-US data flows**

Number 6 (Page 35)

NIS Cooperation Group publication

Threats and risk management in the health sector under the NIS Directive

*Number 7 (Page 40)*

Four companies must stop using Google Analytics

*Number 8 (Page 42)*

Cyber Threat Report: UK Legal Sector

*Number 9 (Page 46)*

The Ethics of Artificial Intelligence Pioneering a New National Security

*Number 10 (Page 50)*

DARPA Seeks a New Gold Standard in Cybersecurity

INGOTS aims to speed up identification and remediation of vulnerabilities using near-full automation

*Number 11 (Page 52)*

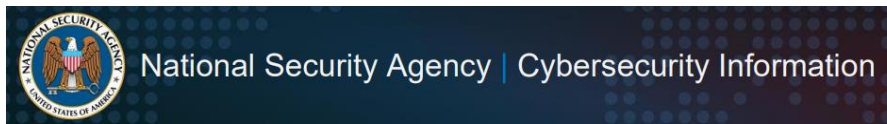
NIST 'Toggle Switch' Can Help Quantum Computers Cut Through the Noise

The novel device could lead to more versatile quantum processors with clearer outputs.



Number 12 (Page 55)

NSA Releases Guide to Mitigate BlackLotus Threat



Number 13 (Page 57)

Homeland Security Acquisition Regulation - Safeguarding of Controlled Unclassified Information



Number 14 (Page 59)

**2023 Common Weakness Enumeration (CWE)
Top 25 Most Dangerous Software Weaknesses**



Number 15 (Page 61)

European insurers and pension funds hold up well despite elevated financial stability risks



Number 16 (Page 64)

National Artificial Intelligence Advisory Committee Releases First Report



Number 17 (Page 66)

Remarks to the Atlanta Commerce and Press Clubs (including Transition to AI, AI as a Tool and a Target of Cybercrime, AI as a Target of Foreign Adversaries)

Christopher Wray, Director, Federal Bureau of Investigation, Atlanta



Number 18 (Page 76)

[High-performing alloy developed to help harness fusion energy](#)
New tungsten-based alloy better withstands fusion energy environments



Number 19 (Page 79)

The European Union Agency for Cybersecurity (ENISA) releases today its first cyber threat landscape for the **health sector**.

[Ransomware Accounts for 54% of Cybersecurity Threats](#)



Number 20 (Page 81)

[Microsoft Response to Layer 7 Distributed Denial of Service \(DDoS\) Attacks](#)



Number 21 (Page 83)

[Federal Reserve names organizations certified as ready for FedNow® Service](#)



Number 22 (Page 88)

[FedNow Is Coming in July. What Is It, and What Does It Do?](#)
Michael Lee and Antoine Martin

FEDERAL RESERVE BANK *of* NEW YORK

Number 23 (Page 92)

NCSC marks 20th anniversary of first response to state-sponsored cyber attack



Number 24 (Page 94)

Increased Truebot Activity Infects U.S. and Canada Based Networks



Number 25 (Page 96)

Storm-0978 attacks reveal financial and espionage motives



Number 1

Malicious Actors Manipulating Photos and Videos to Create Explicit Content and Sextortion Schemes



The FBI is warning the public of malicious actors creating synthetic content (commonly referred to as "deepfakes") by manipulating benign photographs or videos to target victims.

Technology advancements are continuously improving the quality, customizability, and accessibility of artificial intelligence (AI)-enabled content creation.

The FBI continues to receive reports from victims, including minor children and non-consenting adults, whose photos or videos were altered into explicit content.

The photos or videos are then publicly circulated on social media or pornographic websites, for the purpose of harassing victims or sextortion schemes.

Explicit Content Creation

Malicious actors use content manipulation technologies and services to exploit photos and videos—typically captured from an individual's social media account, open internet, or requested from the victim—into sexually-themed images that appear true-to-life in likeness to a victim, then circulate them on social media, public forums, or pornographic websites.

Many victims, which have included minors, are unaware their images were copied, manipulated, and circulated until it was brought to their attention by someone else.

The photos are then sent directly to the victims by malicious actors for sextortion or harassment, or until it was self-discovered on the internet.

Once circulated, victims can face significant challenges in preventing the continual sharing of the manipulated content or removal from the internet.

Sextortion and Harassment

Sextortion, which may violate several federal criminal statutes, involves coercing victims into providing sexually explicit photos or videos of

themselves, then threatening to share them publicly or with the victim's family and friends.

The key motivators for this are a desire for more illicit content, financial gain, or to bully and harass others. Malicious actors have used manipulated photos or videos with the purpose of extorting victims for ransom or to gain compliance for other demands (e.g., sending nude photos).

As of April 2023, the FBI has observed an uptick in sextortion victims reporting the use of fake images or videos created from content posted on their social media sites or web postings, provided to the malicious actor upon request, or captured during video chats.

Based on recent victim reporting, the malicious actors typically demanded:

1. Payment (e.g., money, gift cards) with threats to share the images or videos with family members or social media friends if funds were not received; or
2. The victim send real sexually-themed images or videos.

Recommendations

The FBI urges the public to exercise caution when posting or direct messaging personal photos, videos, and identifying information on social media, dating apps, and other online sites.

Although seemingly innocuous when posted or shared, the images and videos can provide malicious actors an abundant supply of content to exploit for criminal activity.

Advancements in content creation technology and accessible personal images online present new opportunities for malicious actors to find and target victims.

This leaves them vulnerable to embarrassment, harassment, extortion, financial loss, or continued long-term re-victimization.

The FBI recommends the public consider the following when sharing content (e.g., photos and videos) or engaging with individuals online:

1. Monitor children's online activity and discuss risks associated with sharing personal content.
2. Use discretion when posting images, videos, and personal content online, particularly those that include children or their information.

2a. Images, videos, or personal information posted online can be captured, manipulated, and distributed by malicious actors without your knowledge or consent.

2b. Once content is shared on the internet, it can be extremely difficult, if not impossible, to remove once it is circulated or posted by other parties.

3. Run frequent online searches of you and your children's information (e.g., full name, address, phone number, etc.) to help identify the exposure and spread of personal information on the internet.

4. Apply privacy settings on social media accounts—including setting profiles and your friends lists as private—to limit the public exposure of your photos, videos, and other personal information.

5. Consider using reverse image search engines to locate any photos or videos that have circulated on the internet without your knowledge.

6. Exercise caution when accepting friend requests, communicating, engaging in video conversations, or sending images to individuals you do not know personally.

Be especially wary of individuals who immediately ask or pressure you to provide them. Those items could be screen-captured, recorded, manipulated, shared without your knowledge or consent, and used to exploit you or someone you know.

7. Do not provide any unknown or unfamiliar individuals with money or other items of value. Complying with malicious actors does not guarantee your sensitive photos or content will not be shared.

8. Use discretion when interacting with known individuals online who appear to be acting outside their normal pattern of behavior. Hacked social media accounts can easily be manipulated by malicious actors to gain trust from friends or contacts to further criminal schemes or activity.

9. Secure social media and other online accounts using complex passwords or passphrases and multi-factor authentication.

10. Research the privacy, data sharing, and data retention policies of social media platforms, apps, and websites before uploading and sharing images, videos, or other personal content.

To read more: <https://www.ic3.gov/Media/Y2023/PSA230605>

*Number 2***Betreff | Spionage gegen den Verteidigungssektor (Subject | Espionage against the defense sector).**

From the German Bundesamt für Verfassungsschutz (Federal Office for the Protection of the Constitution)



The defense sector with its companies, research institutes and the state agencies involved, have traditionally been the focus of espionage by foreign states and their intelligence services.

Increasing geopolitical rivalries as well as the Russian war of aggression against Ukraine exacerbate the risk.

It's about strategic reconnaissance, covert procurement of military technologies and know-how, as well possibly also the preparation of targeted acts of sabotage.



Sicherheitshinweis für die Wirtschaft | 01/2023
Sicherheitshinweis für Politik & Verwaltung | 01/2023

30. Juni 2023

Betreff | Spionage gegen den Verteidigungssektor

Neue Wege
der Spionage

Neben Spionage mit menschlichen Quellen und Cyberangriffen setzt China zuallererst auf legale und legitime Methoden wie z. B. Forschungsk Kooperationen, Joint Ventures oder Unternehmensaufkäufe, um Know-how nach China zu transferieren. Eine Vielzahl staatlich geförderter Talentprogramme spannt gezielt Gastwissenschaftlerinnen und -wissenschaftler oder Werksstudierende zur Beschaffung ein. Solche „Non-Professionals“ verfügen regelmäßig über weitreichende Zugangsmöglichkeiten, ohne Verdacht zu erregen.

To read more (for Google Translate - <https://www.google.com/search?q=german+to+english>) you may visit:

https://www.verfassungsschutz.de/SharedDocs/publikationen/DE/wirtschaftswissenschaftsschutz/2023-30-06-sicherheitshinweis-6.pdf?__blob=publicationFile&v=9

Handlungsempfehlungen

Cybersicherheit

Maßnahmen für (IT-)Sicherheitsverantwortliche:

- Sensibilisieren und schulen Sie Ihre Mitarbeiterinnen und Mitarbeiter regelmäßig mit Blick auf aktuelle Gefahren im Cyberraum.
- Etablieren Sie klare Meldewege. Kommunizieren Sie an die Beschäftigten, was im Notfall zu tun ist.
- Überprüfen Sie in regelmäßigen Abständen die Notwendigkeit von Zugriffsberechtigungen, insbesondere bei neuen Mitarbeiterinnen und Mitarbeitern in administrativen Bereichen, aber auch bei externen Dienstleistern.
- Schaffen Sie für sensible Informationen geeignete Übermittlungswege mit den jeweils notwendigen Vorkehrungen – z. B. Multi-Faktor-Authentifizierung (MFA) und verschlüsselte E-Mail-Kommunikation.
- Führen Sie in geeigneten Abständen Penetrationstests durch, um ein Feedback zum Umsetzungsstand der IT-Sicherheit aus der Sicht von Angreifenden zu erhalten. Beachten Sie dabei auch mögliche Einfallstore in Ihre Netzwerke z. B. über Auslandsniederlassungen.

Number 3

Financial Stability Institute, FSI Insights on policy implementation No 50 Banks' cyber security – a second generation of regulatory approaches

Juan Carlos Crisanto, Jefferson Umebara Pelegrini and Jermy Prenio



BANK FOR INTERNATIONAL SETTLEMENTS

Executive summary

Cyber resilience continues to be a top priority for the financial services industry and a key area of attention for financial authorities.

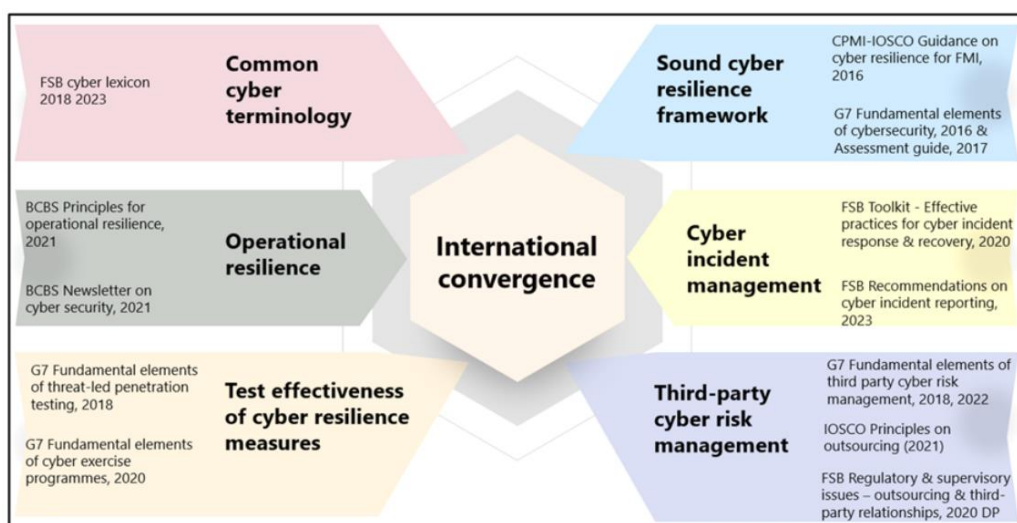
This is not surprising given that cyber incidents pose a significant threat to the stability of the financial system and the global economy.

The financial system performs a number of key activities that support the real economy (eg deposit taking, lending, payments and settlement services).

Cyber incidents can disrupt the information and communication technologies that support these activities and can lead to the misuse and abuse of data that such technologies process or store.

This is complicated by the fact that the cyber threat landscape keeps evolving and becoming more complex amid continuous digitalisation, increased third-party dependencies and geopolitical tensions.

Moreover, the cost of cyber incidents has continuously and significantly increased over the years.



This paper updates Crisanto and Prenio (2017) by revisiting the cyber regulations in the jurisdictions covered in that paper, as well as examining those issued in other jurisdictions.

Aside from cyber regulations in Hong Kong SAR, Singapore, the United Kingdom and the United States, which the 2017 paper covered, this paper examines cyber regulations in Australia, Brazil, the European Union, Israel, Kenya, Mexico, Peru, Philippines, Rwanda, Saudi Arabia and South Africa.

The jurisdictions were chosen to reflect cyber regulations in both advanced economies (AEs) and emerging market and developing economies (EMDEs). This highlights the fact that since 2017 several jurisdictions – including EMDEs – have put cyber regulations in place.

There remain two predominant approaches to the regulation of banks' cyber resilience: the first leverages existing related regulations and the second involves issuing comprehensive regulations.

The first approach takes as a starting point regulations on operational risk, information security etc and add cyber-specific elements to them.

Here, cyber risk is viewed as any other risk and thus the general requirements for risk management, as well as the requirements on information security and operational risks, also apply.

This approach is more commonly observed in jurisdictions that already have these related regulations firmly established.

The second approach seeks to cover all aspects of cybersecurity, from governance arrangements to operational procedures, in one comprehensive regulation.

In both approaches, to counter the risks that might result from having too much prescriptiveness in cyber regulations, some regulations combine broad cyber resilience principles with a set of baseline requirements.

Regardless of the regulatory approach taken, the proportionality principle is given due consideration in the application of cyber resilience frameworks.

Whether as part of related regulations or separate comprehensive ones, recent cyber security policies have evolved and could be described as “second-generation” cyber regulations.

The “first generation” cyber regulations, which were issued mainly in AEs, focused on establishing a cyber risk management approach and controls. Over the last few years, authorities, including those in EMDEs, have issued new or additional cyber regulations.

These second-generation regulations have a more embedded “assume breach” mentality and hence are more aligned with operational resilience concepts.

As such, they focus on improving cyber resilience and providing financial institutions and authorities with specific tools to achieve this.

The “second-generation” regulations leverage existing policy approaches to provide additional specific guidance to improve cyber resilience.

Cyber security strategy, cyber incident reporting, threat intelligence sharing and cyber resilience testing are still the primary focus of the newer regulations.

Managing cyber risks that could arise from connections with third-party service providers has become a key element of the “second generation” cyber security framework.

Moreover, there are now more specific regulatory requirements on cyber incident response and recovery, as well as on incident reporting and cyber resilience testing frameworks.

In addition, regulatory requirements or expectations relating to issues such as cyber resilience metrics and the availability of appropriate cyber security expertise in banks have been introduced in a few jurisdictions.

Authorities in EMDEs tend to be more prescriptive in their cyber regulations.

Cyber security strategy, governance arrangements – including roles and responsibilities – and the nature and frequency of cyber resilience testing are some of the areas where EMDE authorities provide prescriptive requirements.

This approach seems to be connected to the need to strengthen the cyber resilience culture across the financial sector, resource constraints and/or the lack of sufficient cyber security expertise in these jurisdictions.

Hence, EMDE authorities may see the need to be clearer in their expectations to make sure banks’ boards and senior management invest in cyber security and banks’ staff know exactly what they need to do.

International work has resulted in a convergence in cyber resilience regulations and expectations in the financial sector, but more could be done in some areas.

Work by the G7 Cyber Expert Group (CEG) and the global standard-setting bodies (SSBs) on cyber resilience has facilitated consistency in financial regulatory and supervisory expectations across jurisdictions.

This is necessary given the borderless nature of cyber crime and its potential impact on global financial stability.

Another area where there might be scope for convergence is the way in which authorities assess the cyber resilience of supervised institutions. This could, for example, include aligning the assessment of adequacy of a firm's cyber security governance, workforce and cyber resilience metrics.

Lastly, there might be scope to consider an international framework for critical third-party providers, in particular cloud providers, given the potential cross-border impact of a cyber incident in one of these providers.

Contents

Executive summary	4
Section 1 – Introduction	6
Section 2 – International regulatory initiatives.....	8
Section 3 – Design of cyber resilience regulations	11
Section 4 – Key regulatory requirements for cyber resilience.....	14
Cyber security strategy and governance	14
Cyber incident response and recovery	16
Cyber incident reporting and threat intelligence-sharing	17
Cyber resilience testing.....	18
Cyber hygiene.....	20
Third-party dependencies	20
Cyber security culture and awareness	23
Cyber security workforce.....	23
Cyber resilience metrics.....	24
Section 5 – Conclusion	24
References.....	26

Comparative description of the first and second generation of cyber regulations.

Table 1

	1st generation (2017 paper)	2nd generation (2023 paper)
Conceptual underpinning	Focus on building "strong perimeter"	More embedded "assume breach" mentality
Scope	Aligned with IT/ICT and information security framework	In addition, aligned with operational resilience framework
Requirements	Emphasis on enhancing security capabilities	Emphasis on improving resilience capabilities
	Guidance/expectations regarding cyber risk management and (typical) security controls	In addition, guidance/expectations regarding key aspects of cyber resilience framework
	Third-party dependencies largely managed through outsourcing lens	Third-party dependencies increasingly becoming a key part of cyber resilience framework
Types of rules	(i) Leverage existing regulations and (ii) "all-in-one" cybersecurity frameworks	In addition, (iii) principles plus baseline requirements
Tailoring	Apply proportionality approach	
References	In addition to SSB & G7 guidance, well-established technical standards on cyber & information security	

To read more:

<https://www.bis.org/fsi/publ/insights50.pdf>

Number 4

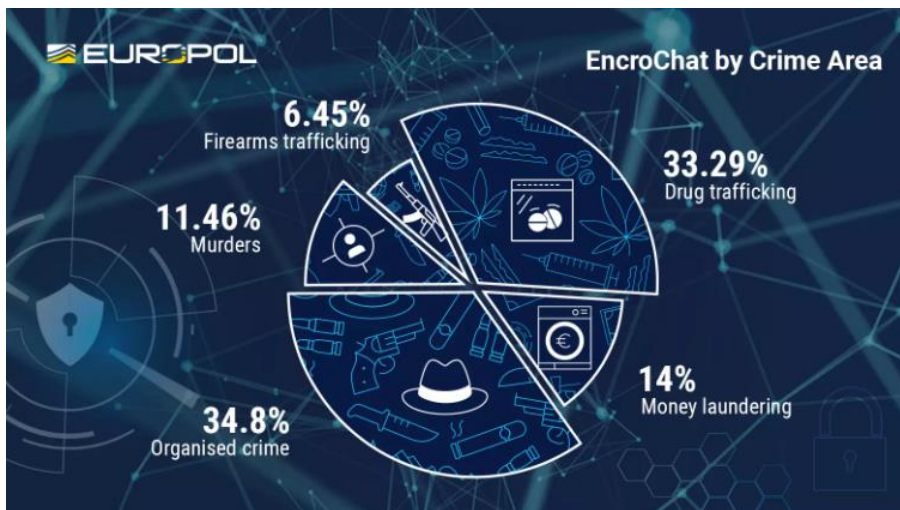
Dismantling encrypted criminal EncroChat communications leads to over 6 500 arrests and close to EUR 900 million seized Judiciary and law enforcement present first overview of results



European Union Agency for Law Enforcement Cooperation

The dismantling of the encrypted communications tool EncroChat, widely used by organised crime groups (OCGs), has so far led to 6 558 arrests worldwide. 197 of those arrested were High Value Targets. This result is detailed in the first review of EncroChat, which was presented today by the French and Dutch judicial and law enforcement authorities in Lille.

The successful takedown of EncroChat followed the efforts of a joint investigation team (JIT) set up by both countries in 2020, supported by Eurojust and Europol. Since then, close to EUR 900 million in criminal funds have been seized or frozen.



What is EncroChat?

EncroChat phones were presented to customers as guaranteeing perfect anonymity (no device or SIM card association on the customer's account, acquisition under conditions guaranteeing the absence of traceability) and perfect discretion both of the encrypted interface (dual operating system, the encrypted interface being hidden so as not to be detectable) and the terminal itself (removal of the camera, microphone, GPS and USB port).

It also had functions intended to ensure the 'impunity' of users (automatic deletion of messages on the terminals of their recipients, specific PIN code intended for the immediate deletion of all data on the device, deletion of all data in the event of consecutive entries of a wrong password), functions that apparently were specially developed to make it possible to quickly erase compromising messages, for example at the time of arrest by the police. In addition, the device could be erased from a distance by the reseller/helpdesk.

EncroChat sold the cryptotelephones (at a cost of around EUR 1 000 each) at international scale and offered subscriptions with a worldwide coverage, at a cost of 1 500 EUR for a six-month period, with 24/7 support.

To read more: <https://www.europol.europa.eu/media-press/newsroom/news/dismantling-encrypted-criminal-encrochat-communications-leads-to-over-6-500-arrests-and-close-to-eur-900-million-seized>

*Number 5***Data Protection: European Commission adopts new adequacy decision for safe and trusted EU-US data flows**

The European Commission adopted its adequacy decision for the EU-U.S. Data Privacy Framework.

The decision concludes that the United States ensures an adequate level of protection – comparable to that of the European Union – for personal data transferred from the EU to US companies under the new framework.



Brussels, 10.7.2023
C(2023) 4745 final

COMMISSION IMPLEMENTING DECISION

of 10.7.2023

**pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council
on the adequate level of protection of personal data under the EU-US Data Privacy
Framework**

On the basis of the new adequacy decision, personal data can flow safely from the EU to US companies participating in the Framework, without having to put in place additional data protection safeguards.

The EU-U.S. Data Privacy Framework introduces new binding safeguards to address all the concerns raised by the European Court of Justice, including limiting access to EU data by US intelligence services to what is necessary and proportionate, and establishing a Data Protection Review Court (DPRC), to which EU individuals will have access.

The new framework introduces significant improvements compared to the mechanism that existed under the Privacy Shield. For example, if the DPRC finds that data was collected in violation of the new safeguards, it will be able to order the deletion of the data.

The new safeguards in the area of government access to data will complement the obligations that US companies importing data from EU will have to subscribe to.

President Ursula von der Leyen said:

“The new EU-U.S. Data Privacy Framework will ensure safe data flows for Europeans and bring legal certainty to companies on both sides of the Atlantic. Following the agreement in principle I reached with President Biden last year, the US has implemented unprecedented commitments to establish the new framework.

Today we take an important step to provide trust to citizens that their data is safe, to deepen our economic ties between the EU and the US, and at the same time to reaffirm our shared values. It shows that by working together, we can address the most complex issues.”

US companies will be able to join the EU-U.S. Data Privacy Framework by committing to comply with a detailed set of privacy obligations, for instance the requirement to delete personal data when it is no longer necessary for the purpose for which it was collected, and to ensure continuity of protection when personal data is shared with third parties.

EU individuals will benefit from several redress avenues in case their data is wrongly handled by US companies. This includes free of charge independent dispute resolution mechanisms and an arbitration panel.

In addition, the US legal framework provides for a number of safeguards regarding the access to data transferred under the framework by US public authorities, in particular for criminal law enforcement and national security purposes. Access to data is limited to what is necessary and proportionate to protect national security.

EU individuals will have access to an independent and impartial redress mechanism regarding the collection and use of their data by US intelligence agencies, which includes a newly created Data Protection Review Court (DPRC). The Court will independently investigate and resolve complaints, including by adopting binding remedial measures.

The safeguards put in place by the US will also facilitate transatlantic data flows more generally, since they also apply when data is transferred by

using other tools, such as standard contractual clauses and binding corporate rules.

Next steps

The functioning of the EU-U.S. Data Privacy Framework will be subject to periodic reviews, to be carried out by the European Commission, together with representatives of European data protection authorities and competent US authorities.

The first review will take place within a year of the entry into force of the adequacy decision, in order to verify that all relevant elements have been fully implemented in the US legal framework and are functioning effectively in practice.

Questions & Answers: EU-US Data Privacy Framework

1. What is an adequacy decision?

An adequacy decision is one of the tools provided under the General Data Protection Regulation (GDPR) to transfer personal data from the EU to third countries which, in the assessment of the Commission, offer a comparable level of protection of personal data to that of the European Union.

As a result of adequacy decisions, personal data can flow freely and safely from the European Economic Area (EEA), which includes the 27 EU Member States as well as Norway, Iceland and Liechtenstein, to a third country, without being subject to any further conditions or authorisations. In other words, transfers to the third country can be handled in the same way as intra-EU transmissions of data.

The adequacy decision on the EU-U.S. Data Privacy Framework covers data transfers from any public or private entity in the EEA to US companies participating in the EU-U.S. Data Privacy Framework.

2. What are the criteria to assess adequacy?

Adequacy does not require the third country's data protection system to be identical to the one of the EU, but is based on the standard of 'essential equivalence'. It involves a comprehensive assessment of a country's data protection framework, both of the protection applicable to personal data and of the available oversight and redress mechanisms.

The European data protection authorities have developed a list of elements that must be taken into account for this assessment, such as the existence

of core data protection principles, individual rights, independent supervision and effective remedies.

3. What is the EU-U.S. Data Privacy Framework?

In its adequacy decision, the Commission has carefully assessed the requirements that follow from the EU-U.S. Data Privacy Framework, as well as the limitations and safeguards that apply when personal data transferred to the US would be accessed by US public authorities, in particular for criminal law enforcement and national security purposes.

On that basis, the adequacy decision concludes that the United States ensures an adequate level of protection for personal data transferred from the EU to companies participating in the EU-U.S. Data Privacy Framework. With the adoption of the adequacy decision, European entities are able to transfer personal data to participating companies in the United States, without having to put in place additional data protection safeguards.

The Framework provides EU individuals whose data would be transferred to participating companies in the US with several new rights (e.g. to obtain access to their data, or obtain correction or deletion of incorrect or unlawfully handled data). In addition, it offers different redress avenues in case their data is wrongly handled, including before free of charge independent dispute resolution mechanisms and an arbitration panel.

US companies can certify their participation in the EU-U.S. Data Privacy Framework by committing to comply with a detailed set of privacy obligations. This could include, for example, privacy principles such as purpose limitation, data minimisation and data retention, as well as specific obligations concerning data security and the sharing of data with third parties.

The Framework will be administered by the US Department of Commerce, which will process applications for certification and monitor whether participating companies continue to meet the certification requirements. Compliance by US companies with their obligations under the EU-U.S. Data Privacy Framework will be enforced by the US Federal Trade Commission.

4. What are the limitations and safeguards regarding access to data by United States intelligence agencies?

An essential element of the US legal framework on which the adequacy decision is based concerns Executive Order on 'Enhancing Safeguards for United States Signals Intelligence Activities', which was signed by President Biden on 7 October and is accompanied by regulations adopted

by the Attorney General. These instruments were adopted to address the issues raised by the Court of Justice in its Schrems II judgment.

For Europeans whose personal data is transferred to the US, the Executive Order provides for:

- Binding safeguards that limit access to data by US intelligence authorities to what is necessary and proportionate to protect national security;
- Enhanced oversight of activities by US intelligence services to ensure compliance with limitations on surveillance activities; and
- The establishment of an independent and impartial redress mechanism, which includes a new Data Protection Review Court to investigate and resolve complaints regarding access to their data by US national security authorities.

5. What is the new redress mechanism in the area of national security and how can individuals make use of it?

The US Government has established a new two-layer redress mechanism, with independent and binding authority, to handle and resolve complaints from any individual whose data has been transferred from the EEA to companies in the US about the collection and use of their data by US intelligence agencies.

For a complaint to be admissible, individuals do not need to demonstrate that their data was in fact collected by US intelligence agencies. Individuals can submit a complaint to their national data protection authority, which will ensure that the complaint will be properly transmitted and that any further information relating to the procedure—including on the outcome—is provided to the individual.

This ensures that individuals can turn to an authority close to home, in their own language. Complaints will be transmitted to the United States by the European Data Protection Board.

First, complaints will be investigated by the so-called 'Civil Liberties Protection Officer' of the US intelligence community. This person is responsible for ensuring compliance by US intelligence agencies with privacy and fundamental rights.

Second, individuals have the possibility to appeal the decision of the Civil Liberties Protection Officer before the newly created Data Protection Review Court (DPRC).

The Court is composed of members from outside the US Government, who are appointed on the basis of specific qualifications, can only be dismissed for cause (such as a criminal conviction, or being deemed mentally or physically unfit to perform their tasks) and cannot receive instructions from the government.

The DPRC has powers to investigate complaints from EU individuals, including to obtain relevant information from intelligence agencies, and can take binding remedial decisions. For example, if the DPRC would find that data was collected in violation of the safeguards provided in the Executive Order, it can order the deletion of the data.

In each case, the Court will select a special advocate with relevant experience to support the Court, who will ensure that the complainant's interests are represented and that the Court is well informed of the factual and legal aspects of the case. This will ensure that both sides are represented, and introduce important guarantees in terms of fair trial and due process.

Once the Civil Liberties Protection Officer or the DPRC completes the investigation, the complainant will be informed that either no violation of US law was identified, or that a violation was found and remedied. At a later stage, the complainant will also be informed when any information about the procedure before the DPRC—such as the reasoned decision of the Court—is no longer subject to confidentiality requirements and can be obtained.

6. When will the decision apply?

The adequacy decision entered into force with its adoption on 10 July.

There is no time limitation, but the Commission will continuously monitor relevant developments in the United States and regularly review the adequacy decision.

The first review will take place within one year after the entry into force of the adequacy decision, to verify whether all relevant elements of the US legal framework are functioning effectively in practice. Subsequently, and depending on the outcome of that first review, the Commission will decide, in consultation with the EU Member States and data protection authorities, on the periodicity of future reviews, which will take place at least every four years.

Adequacy decisions can be adapted or even withdrawn in case of developments affecting the level of protection in the third country.

7. What is the impact of the decision on the possibility to use other tools for data transfers to the United States?

All the safeguards that have been put in place by the US Government in the area of national security (including the redress mechanism) apply to all data transfers under the GDPR to companies in the US, regardless of the transfer mechanism used. These safeguards therefore also facilitate the use of other tools, such as standard contractual clauses and binding corporate rules.

To read more:

https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3721

<https://commission.europa.eu/system/files/2023-07/Adequacy%20decision%20EU-US%20Data%20Privacy%20Framework.pdf>

Number 6

NIS Cooperation Group publication

Threats and risk management in the health sector under the NIS Directive



Executive Summary

The “Threats and risk management in the health sector – Under the NIS Directive” shines a light on the different cybersecurity threats targeting the health sector of the European Union in times of ever-growing interconnections between traditional health care services and internet-connected networks and information systems.

Starting with the analysis of the cyber threat landscape and the most relevant threat taxonomies and cyber incident data, this report highlights the main current and emerging cyber threats which the European health sector is likely to be confronted with.

In this sense, the report also presents a set of business continuity and mitigation recommendations to limit the likelihood and impacts of a cyber related incident.

Finally, the present document provides an analysis of the results of a questionnaire that was disseminated by Member States to Operators of Essential Services and that focused inter alia on the cybersecurity and risk management culture, cybersecurity awareness, cybersecurity measures currently in place and the cyber threat perceptions of institutions of the European healthcare sector.

In conclusion, this “Threats and risk management in the health sector – Under the NIS Directive” aims to enhance the awareness of the European health sector with regards to the cyber threats it faces and to enhance the general cybersecurity posture of institutions being part of the European health sector.

Context

The most valuable asset to any healthcare organisation is the patient, who expects from healthcare organisations and professionals help to get better, saving or sustaining his life.

But health organisations are also comprised of digital and technological systems and tools that enable them to increase patients' safety and care.

Thus, electronic health data is also the lifeblood of a healthcare organisation, and this data must be kept confidential, its integrity must be preserved, and it must be made available on demand wherever and whenever it is needed.

Healthcare is increasingly the target of malicious cyberattacks, which result not only in data breaches but also increased healthcare delivery costs, and they can ultimately affect provision of care.

Health information systems, networks and medical devices are particularly targeted and vulnerable because they host and process information such as patients' protected health information, personal identifiable information, and intellectual property related to medical research and innovation which represents high monetary and intelligence value to cyber thieves and nation-state actors.

On the other hand, more and more cybersecurity incidents arise because of the lack of maintenance and technological updates of these systems, even if there is no targeted attack.

Table 4 – Motivation

ETL MOTIVATION	DESIRED END STATE
Monetisation	Conquer Acquire Survive
Geopolitics/Espionage	Conquer Acquire Defend Survive
Geopolitics/Disruption	Prevent Maintain Defend Survive
Ideological (e.g., hacktivism)	Prevent Maintain Defend

Often, healthcare providers rely on legacy systems, outdated computer systems that are still in use and provide less protection and increased susceptibility for an attack.

Cybersecurity incidents on electronic health records and other health information systems stand out when we talk about health cyberattacks and incidents, but the attack surface of a hospital is much broader, considering the supply chain, cloud-based infrastructures, the building automation systems (HVACs, for example), the internet of medical things, etc. It is crucial that the health ecosystem actors (people, manufacturers and facilities) work together to manage the risks and to protect patient safety.

The connection between cybersecurity and patient safety may be naively seen as somewhat abstract as the impacts of cyber-attacks do not seem to immediately present harm or mortality to patients, however there are plenty of examples that disprove this.

Losing access to medical records and lifesaving medical devices, such as a ransomware attack holding them hostage, disrupts the ability to effectively care for the patients.

Hackers' access to private patient data not only opens the door for them to steal the information, but also to either intentionally or unintentionally alter the data, which could lead to serious effects on patient health and outcomes.

It is crucial that healthcare organisations understand that cybersecurity is directly related to patient safety and know how to keep health data ecosystems secure.

Aligning these two domains and initiatives not only will help health organisations to protect patient safety and privacy but will also ensure the continuity of effective high-quality delivery of care by mitigating disruptions that can have a negative impact on clinical outcomes and business continuity.

Another important consideration is that cyber risks need to be incorporated into the overall enterprise risk management governance and receive the attention and support of executive leadership, including the C Suite and Board.

The Board of health organizations must lead and support all the necessary efforts to ensure the existence of resilient and secure services with the IT department performing an important role since, as we have seen, a cybersecurity incident can have a direct impact on the provision of healthcare or the organisation's business.

Hospital leaders generally do recognize the importance of safety culture; thus, one needs to extend this awareness to cybersecurity.

Contents

1. Executive Summary	4
2. Context	5
2.1. Scope, target audience and objectives of the document.....	6
2.2. Methodology	6
3. Cybersecurity Threats.....	7
3.1. ENISA Threat Landscape	7
3.2. Cyber Threat Taxonomies.....	10
3.2.1. ISO 27005:2022 cyber threat taxonomy.....	11
3.2.2. ENISA cyber threat taxonomy	13
3.2.3. Key takeaways	14
4. Cybersecurity incidents	17
4.1. Cybersecurity incidents with a significant impact reported.....	17
4.2. Health cybersecurity incidents in 2021, 2022 and early 2023	23
4.2.1. Main Threat Actors	24
4.3. Other relevant health cybersecurity incidents.....	25
4.4. Key takeaways	26
5. Current and Emerging Healthcare Cyber Threats and Vulnerabilities	28
I. Ransomware.....	28
II. Threats against data	28
III. Distributed Denial of Service (DDoS) attacks	29
IV. Supply Chain Attacks	29
V. Malware.....	30
VI. Social engineering threats (phishing)	30
5.1. Related vulnerabilities	30
I. Insiders	30
II. Legacy Systems	31
5.2. Key takeaways	31
6. Business Continuity & Mitigation recommendations.....	32
I. Incident Response	32
II. Access Control	32
III. Backup and Restore	32

IV.	IT preparedness	32
V.	Physical Security	32
VI.	Patch Management and Anti-malware Protection	32
VII.	Awareness Training	33
VIII.	Supplier Management	33
IX.	Compliance	33
X.	Knowledge Sharing	33
6.1.	Key takeaways	33
7.	Cybersecurity context by health organisations	34
7.1.	Identification	34
7.2.	Risk Management	36
7.2.1.	Cybersecurity and Risk Management Culture	36
7.2.2.	Risk Assessment and Analysis	38
7.2.3.	Quality Control and Internal Audits	41
7.2.4.	Health assets	41
7.3.	Threats and Types of incidents	42
7.4.	Certification, Barriers and Guidance	45
7.5.	Key takeaways	47
8.	General Conclusions	48
9.	Additional ENISA Relevant Materials	49
10.	Annex	50

4.2.1. Main Threat Actors

The majority of cyber incidents affecting the European healthcare sector remain unattributed and likely some of them can be State sponsored APTs (Advanced and Persistent Threats) targeting of this sector due to espionage purposes.

To read more:

<https://ec.europa.eu/newsroom/ECCC/redirection/document/97124>

Number 7

Four companies must stop using Google Analytics



Note: The Swedish Authority for Privacy Protection (IMY) is an agency ensuring that people are protected against their personal privacy being violated through processing of personal data.

The Swedish Authority for Privacy Protection (IMY) has audited how four companies use Google Analytics for web statistics.

IMY issues administrative fines against two of the companies. One of the companies has recently stopped using the statistics tool on its own initiative, while IMY orders the other three to also stop using it.

IMY has audited how four companies transfer personal data to the US via Google Analytics, which is a tool for measuring and analysing traffic on websites.

The companies audited are CDON, Coop, Dagens Industri and Tele2. The audits concerns a version of Google Analytics from 14th of August 2020.

The audits are based on complaints from the organisation None of Your Business (NOYB) in the light of the Schrems II ruling by the European Court of Justice (CJEU). The complaints allege that the companies, in violation of the law, transfer personal data to the United States.

According to the data protection regulation, GDPR, personal data may be transferred to third countries, i.e. countries outside the EU/EEA, if the European Commission has decided that the country in question has an adequate level of protection for personal data that corresponds to that within the EU/EEA.

However, the CJEU ruled through the Schrems II ruling that the United States could not be considered to have such an adequate level of protection at the time of the ruling.

In its audits, IMY considers that the data transferred to the US via Google's statistics tool is personal data because the data can be linked with other unique data that is transferred.

The authority also concludes that the technical security measures that the companies have taken are not sufficient to ensure a level of protection that essentially corresponds to that guaranteed within the EU/EEA.

By the fact that IMY has decided on these cases at the same time, it is made clear what requirements are placed on technical security measures and other measures when transferring personal data to a third country, in this case the United States, says legal advisor Sandra Arvidsson, who led the audits of the companies.

If there is no decision on an adequate level of protection by the European Commission, data may be transferred based on standard contractual clauses that the European Commission has decided on. However, according to the CJEU, such standard contractual clauses may need to be supplemented with additional safeguards if it is necessary for the protection that the clauses are intended to provide to be maintained in practice.

All four companies have based their decisions on the transfer of personal data via Google Analytics on standard contractual clauses. From IMY's audits, it appears that none of the companies' additional technical security measures are sufficient.

IMY issues an administrative fine of 12 million SEK against Tele2 and 300,000 SEK against CDON, which has not taken the same extensive protective measures as Coop and Dagens Industri.

Tele2 has recently stopped using the statistics tool on its own initiative. IMY orders the other three companies to stop using the tool.

These decisions have implications not only for these four companies, but can also provide guidance for other organisations that use Google Analytics, says Sandra Arvidsson.

To read more: <https://www.imy.se/en/news/four-companies-must-stop-using-google-analytics/>

*Number 8***Cyber Threat Report: UK Legal Sector**

The purpose of this report is to help law firms, lawyers and legal practices understand current cyber security threats, and the extent to which the legal sector is being targeted. It then offers practical guidance on how organisations can be resilient to these threats.



Law firms routinely handle highly sensitive client information (for instance relating to ongoing criminal cases, or mergers and acquisitions) that may be valuable to criminal organisations with an interest in exploiting opportunities for insider trading, gaining the upper hand in negotiations and litigation, or subverting the course of justice.



Disruption to routine business operations can be costly to legal practices, both in terms of billable hours lost due to outages and costs to clients that depend upon them, making legal practices particularly of interest to ransomware gangs aiming to extort money in return for restoration of IT services.



In many areas, from mergers and acquisitions to conveyancing, legal practices handle significant funds. The time pressures associated with transactions (as well as the large numbers of suppliers and clients and complex payrolls that law firms handle) create attractive conditions for phishing attacks and business email compromise.



Many legal practices, especially smaller firms, chambers and individual practitioners, rely on an external IT services provider, making it challenging for them to assess for themselves whether the controls they have in place are appropriate to the risk they face. A small law firm with few resources could be devastated if caught up by (for example) a ransomware attack. They are more vulnerable to attack, perhaps via unpatched vulnerabilities on unmanaged devices, or due to untrained staff or poorly offboarded leavers. Once attacked, a relatively small financial or reputational loss may be disastrous.



Reputation is critical to the business of law, which makes legal practices attractive targets for extortion.

As the report explains, the cyber threat applies to law practices of all sizes and types of work, from sole practitioners, high street and mid-size firms to barristers' chambers, in-house legal departments and international corporate firms. Cyber criminals are not fussy about who they attack, which means small and large organisations are at risk.

The report has been compiled with the assistance of the NCSC's in-house cyber security experts, the NCSC-sponsored Industry 100 scheme, the Law Society, The Bar Council, the Solicitors Regulation Authority (SRA), Action Fraud (the UK's national fraud and cyber crime reporting centre) and the National Crime Agency (NCA).

It has also drawn on an extensive body of open source reporting. The National Cyber Security Centre (NCSC), a part of GCHQ, is the UK's

technical authority for cyber security. Since the NCSC was created in 2016, as part of the Government's National Cyber Security Strategy, it has worked to make the UK the safest place to live and work online.

4	Foreword	11	The main types of cyber attack
6	The legal sector	17	Reporting cyber attacks
7	Why is the legal sector a particular target?	18	How to improve your cyber security
8	How things have changed since 2018	20	Cyber security guidance
9	Who might target the legal sector?	21	NCSC schemes and services

The legal sector

The UK's legal sector is large and diverse, spanning organisations of many shapes and sizes, from small high street solicitors' firms to large multinational corporations, to self-employed barristers and barristers' chambers.

Legal services form an important component of the UK economy. As of early 2023, there were over 32,900 enterprises in total including barristers, solicitors and other legal service providers operating in the UK, with an estimated total revenue of £43.9 billion.

More than 320,000 people work in the legal sector in the UK. Legal services are an important export of the UK accounting for £6.8 billion of exports as of 2021.

There is an inherent trust and strict confidence from clients that law firms preserve the confidentiality of their information.

It is also a legal practice's overriding professional obligation, as set out in the professional standards, in the SRA's Standards and Regulations, the Bar Standards Board's handbook, and is common law, under the Legal Services Act 2007.

It is essential that organisations maintain appropriate cyber security measures. Failure to do so can have exceptionally negative consequences for a legal practice and its clients.

The 2022 PriceWaterhouseCoopers Annual Law Firms Survey reported that cyber risk has seen significant increases in spending among larger law firms, with the top 100 spending an average of 0.46% of fee income on cyber security in 2022.

The UK's legal profession

- › There are over 230,000 solicitors and legal executives practising in the UK.
- › There are more than 18,000 barristers working in the UK, including around 700 sole practices, and the rest working out of the 400 chambers in the country.
- › The legal sector includes many other specialists, including notaries, paralegals, will writers, immigration practitioners and licensed conveyancers.

The cyber threat

- › Professional services, which includes the legal sector, is regularly at the top of analysts' leader-boards as the sector most impacted by the cyber threat.
- › The Cyber Breaches Survey 2023⁶ found that 32% of surveyed UK businesses identified cyber attacks.
- › The SRA published 278 scam alerts in response to reports from the public and profession between January 2022 and January 2023. These scam alerts highlight reports of people falsely claiming to be solicitors and firms, for example on websites or in emails and telephone calls.

We strongly recommend that all legal firms:



Ensure that senior leadership such as board members, owners and partners are engaged and informed about cyber security risk. The NCSC's [Cyber Security Toolkit for Boards](#)¹, provides a set of tailored resources to help senior stakeholders engage with these issues.



Assess your organisation against [NCSC's Cyber Essentials](#)². This helps you to guard against the most common cyber threats and demonstrate your commitment to cyber security.



Sign up to the NCSC's key services that are available to help protect your organisation from a cyber attack. Services include [Early Warning](#)³, [Exercise in a Box](#)⁴ and [Connect Information Share Protect \(CISP\)](#)⁵. You may wish to consider [Cyber Insurance](#)⁶, although this will not instantly solve all of your cyber security issues, nor will it prevent a cyber breach/attack.



Invest in staff training and awareness to improve the security culture in your organisation (see next page).

To read more: https://www.ncsc.gov.uk/files/Cyber-Threat-Report_UK-Legal-Sector.pdf

Number 9

The Ethics of Artificial Intelligence Pioneering a New National Security



4	Foreword by Director GCHQ	22	Chapter 4: Artificial Intelligence in GCHQ
5	Executive Summary	23	The invention of AI
6	Key Insights	23	Post-war technology and computing
8	Chapter 1: Introduction	23	The winter years
10	Chapter 2: What is Artificial Intelligence?	23	Our approach to delivering AI
11	AI fact and fiction	24	AI For National Security: Trafficking
11	Origins	26	Chapter 5: GCHQ, AI and trust
11	What is machine learning?	27	International and national context
12	Different types of machine learning	27	What is AI ethics?
13	What AI can and cannot do	27	AI ethics and National Security
14	AI For National Security: Cyber Threat	28	The major ethical challenges
16	Chapter 3: What does GCHQ do?	31	Our approach – next steps
17	Our mission	34	AI For National Security: Foreign State Disinformation
18	Our oversight	36	Chapter 6: Conclusions and our future journey
19	Our challenges and opportunities	38	Footnotes / Citations
20	AI For National Security: Online Safety		

Executive Summary

Britain today is a digital nation, leading and shaping events across a world inextricably linked through cyberspace. Now and into the future, the value of our economy, our way of life, and our global influence will be built on our advanced digital infrastructure, capabilities and knowledge.

Artificial Intelligence – a form of software that can learn to solve problems at a scale and speed impossible for humans – is increasingly essential to the way we live. It is already transforming sectors as diverse as healthcare, telecommunications, and manufacturing.

AI software informs our satnavs, guides our internet searches, and protects us every time we make an electronic purchase, or open an app on our smartphone.

In the century since it was founded, GCHQ has been at the forefront of innovation in national security. Generations of brilliant analysts, with their

diverse mix of minds, have used their technical ingenuity, cutting-edge technology and wide-ranging partnerships to identify, analyse and disrupt threats to our nation.

Today, as technological change continues to accelerate, we are pioneering new approaches to understanding the complex and interconnected world around us.

We have long championed the responsible use of data science, and believe that AI will be at the heart of our organisation's future.

Thinking about AI encourages us to think about ourselves, and what it means to be human: our preferred way of life, our guiding values and our common beliefs.

The field of AI ethics has emerged over the last decade to help organisations turn these ethical principles into practical guidance for software developers – helping to embed our core values within our computers and software.

We won't pretend that there are not challenges ahead of us. In using AI we will strive to minimise and where possible eliminate biases, whether around gender, race, class or religion.

We know that individuals pioneering this technology are shaped by their own personal experiences and backgrounds. Acknowledging this is only the first step – we must go further and draw on a diverse mix of minds to develop, apply and govern our use of AI.

Left unmanaged, our use of AI incorporates and reflects the beliefs and assumptions of its creators – AI systems are no better or no worse than the human beings that create them.

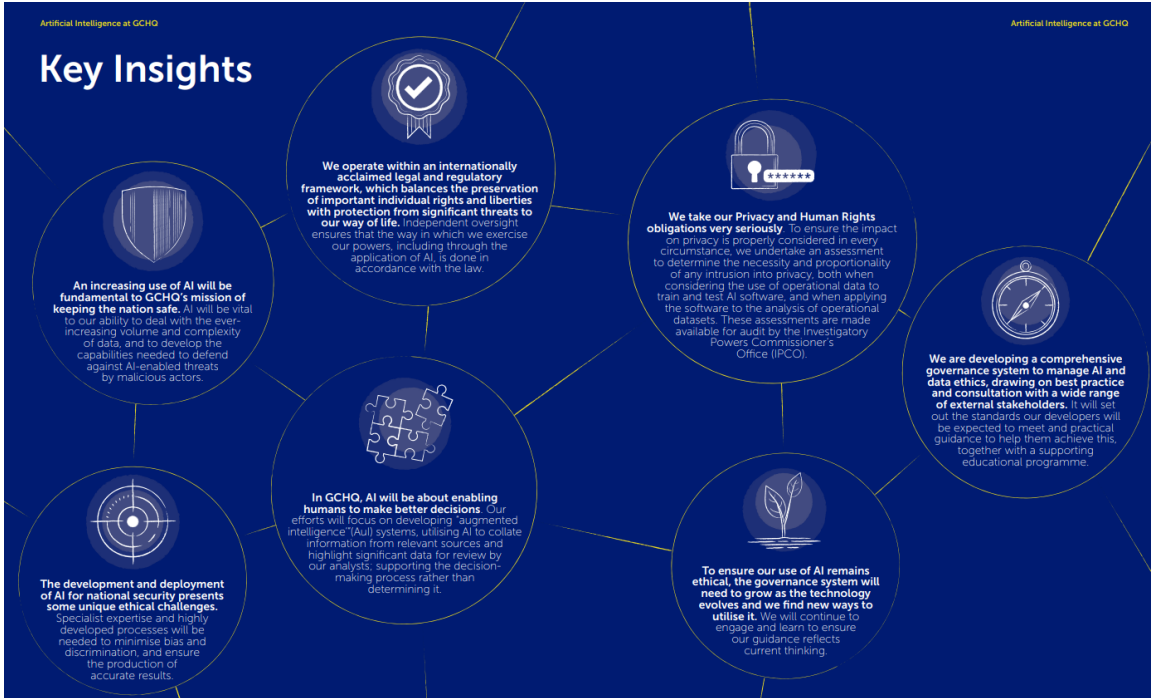
Our society is learning and growing: the Alan Turing Institute and similar bodies are helping to show us how we might build and use AI in a more ethical, responsible manner.

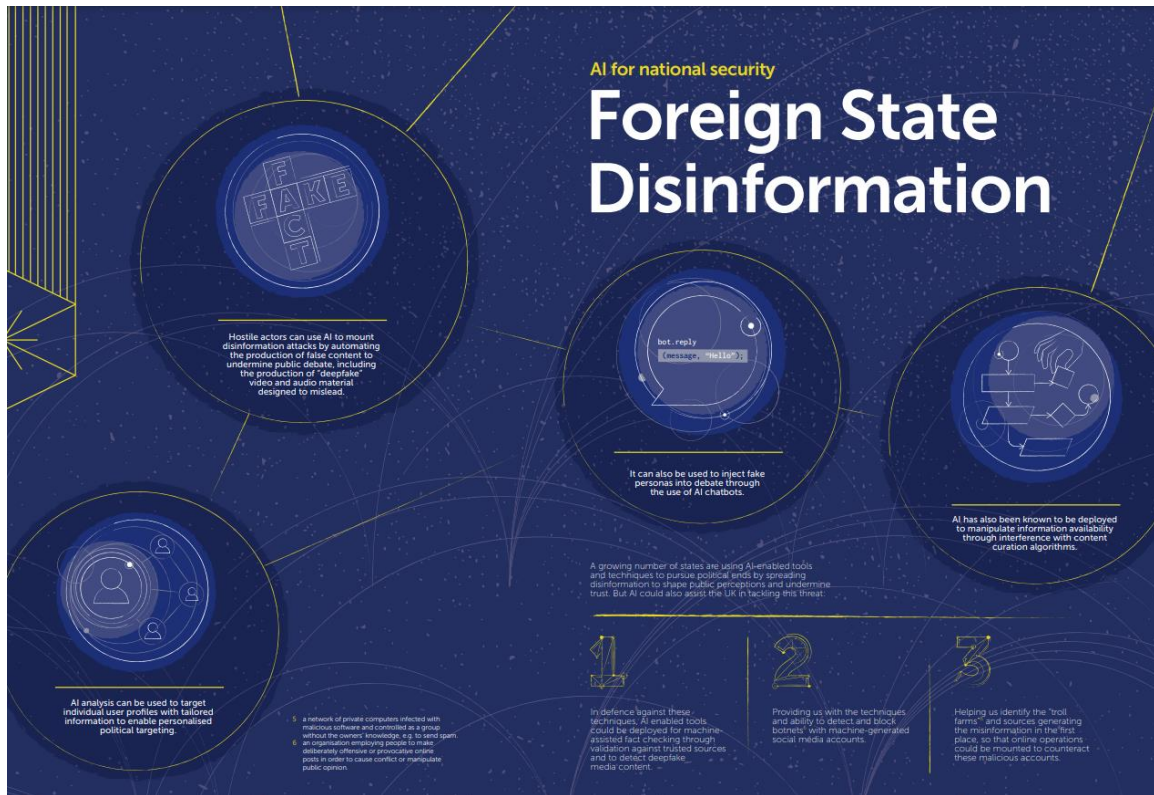
GCHQ is committed to creating and using AI in a way that supports fairness, empowerment, transparency and accountability – and to protecting the nation from AI-enabled security threats pursued by our adversaries. We believe that, by working together with our partners across Britain and beyond, we can deliver this vision.

This paper describes the digital Britain of today, and our values-led approach for the spaces where people, information and technology meet. It

lays out GCHQ's AI and Data Ethics Framework, and how we intend to use AI in our operations.

It forms part of our commitment to inclusion, debate and openness. The paper is the first step of a much longer journey: we'd like you to join us on it.





To read more: <https://www.gchq.gov.uk/files/GCHQAIPaper.pdf>

Number 10

DARPA Seeks a New Gold Standard in Cybersecurity

INGOTS aims to speed up identification and remediation of vulnerabilities using near-full automation



It's no secret that developers and cyberspace defenders must accurately understand risks within software and hardware to maintain a robust security posture.

Today, sophisticated cyberattacks link multiple vulnerabilities to bypass security measures and compromise critical, high-value devices.

Yet, often critical vulnerabilities go unfixed as resources are allocated to less significant issues.

That is because today's metrics fail to capture numerous nuanced factors that differentiate a harmless software flaw from a potent vulnerability.

Without accurate methods to measure the exploitability of a particular vulnerability, developers and defenders must rely on empirical evidence to assess its severity and prioritize it for remediation.

Such evidence requires time and costly resources and is often insufficient or incomplete, especially for vulnerabilities within complex systems.

DARPA's Intelligent Generation of Tools for Security (INGOTS) program aims to identify and fix high-severity, chainable vulnerabilities before attackers can exploit them.

INGOTS will pioneer new techniques driven by program analysis and artificial intelligence to measure vulnerabilities within modern, complex systems, such as web browsers and mobile operating systems.

"In an attack paradigm where exploitability depends on the emergent behavior of vulnerability combination, risk depends on understanding the complex relationships between neighboring vulnerabilities," said Perri Adams, INGOTS program manager in DARPA's Information Innovation Office.

"Rather than develop a fully automatic process, we want to create a computer-human pipeline that seamlessly allows human intervention in order to fix high-severity vulnerabilities before an attack."

Successful INGOTS research will improve software and hardware resiliency of pervasive commercial devices by rapidly identifying and prioritizing their most dangerous flaws.

INGOTS is a three-year program with two phases.

Phase 1 will focus on exploring, designing, developing, and demonstrating tools and techniques.

Phase 2 will focus on maturing and refining these tools and techniques and expanding their coverage across vulnerability and exploitation classes.

Each phase will have intermediate meetings, hackathons, and demonstrations and will end with an evaluation in collaboration with government partners.

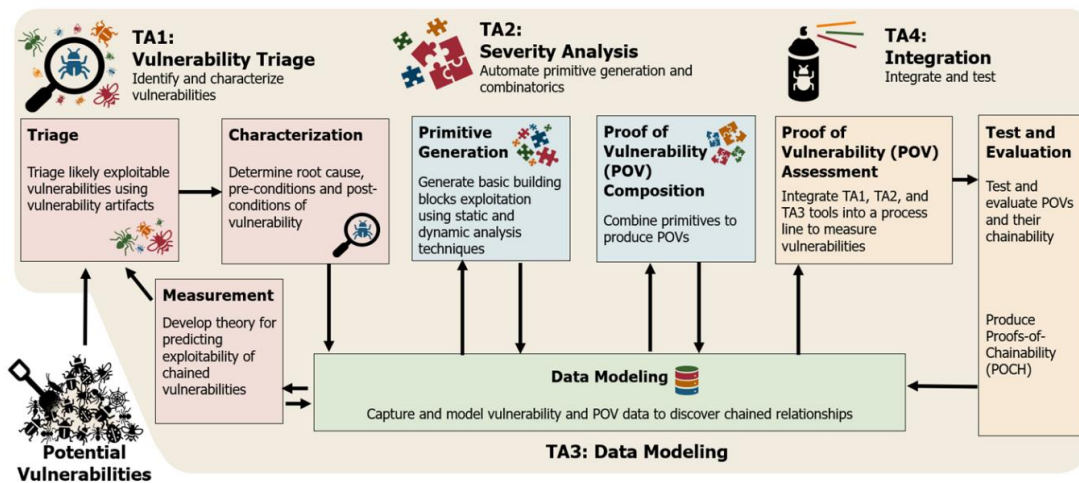


Figure 1: INGOTS Program Vision

To read more: <https://www.darpa.mil/news-events/2023-06-23>

Number 11

NIST ‘Toggle Switch’ Can Help Quantum Computers Cut Through the Noise

The novel device could lead to more versatile quantum processors with clearer outputs.



What good is a powerful computer if you can't read its output? Or readily reprogram it to do different jobs? People who design quantum computers face these challenges, and a new device may make them easier to solve.

The device, introduced by a team of scientists at the National Institute of Standards and Technology (NIST), includes two superconducting quantum bits, or qubits, which are a quantum computer's analogue to the logic bits in a classical computer's processing chip.

The heart of this new strategy relies on a “toggle switch” device that connects the qubits to a circuit called a “readout resonator” that can read the output of the qubits' calculations.

This toggle switch can be flipped into different states to adjust the strength of the connections between the qubits and the readout resonator. When toggled off, all three elements are isolated from each other.

When the switch is toggled on to connect the two qubits, they can interact and perform calculations. Once the calculations are complete, the toggle switch can connect either of the qubits and the readout resonator to retrieve the results.

Having a programmable toggle switch goes a long way toward reducing noise, a common problem in quantum computer circuits that makes it difficult for qubits to make calculations and show their results clearly.

“The goal is to keep the qubits happy so that they can calculate without distractions, while still being able to read them out when we want to,” said Ray Simmonds, a NIST physicist and one of the paper's authors.

“This device architecture helps protect the qubits and promises to improve our ability to make the high-fidelity measurements required to build quantum information processors out of qubits.”

The team, which also includes scientists from the University of Massachusetts Lowell, the University of Colorado Boulder and Raytheon BBN Technologies, describes its results in a paper published today in *Nature Physics*.

Quantum computers, which are still at a nascent stage of development, would harness the bizarre properties of quantum mechanics to do jobs that even our most powerful classical computers find intractable, such as aiding in the development of new drugs by performing sophisticated simulations of chemical interactions.

However, quantum computer designers still confront many problems. One of these is that quantum circuits are kicked around by external or even internal noise, which arises from defects in the materials used to make the computers. This noise is essentially random behavior that can create errors in qubit calculations.

Present-day qubits are inherently noisy by themselves, but that's not the only problem. Many quantum computer designs have what is called a static architecture, where each qubit in the processor is physically connected to its neighbors and to its readout resonator. The fabricated wiring that connects qubits together and to their readout can expose them to even more noise.

Such static architectures have another disadvantage: They cannot be reprogrammed easily. A static architecture's qubits could do a few related jobs, but for the computer to perform a wider range of tasks, it would need to swap in a different processor design with a different qubit organization or layout.

(Imagine changing the chip in your laptop every time you needed to use a different piece of software, and then consider that the chip needs to be kept a smidgen above absolute zero, and you get why this might prove inconvenient.)

The team's programmable toggle switch sidesteps both of these problems. First, it prevents circuit noise from creeping into the system through the readout resonator and prevents the qubits from having a conversation with each other when they are supposed to be quiet.

"This cuts down on a key source of noise in a quantum computer," Simmonds said.

Second, the opening and closing of the switches between elements are controlled with a train of microwave pulses sent from a distance, rather than through a static architecture's physical connections. Integrating more of these toggle switches could be the basis of a more easily programmable quantum computer. The microwave pulses can also set the order and sequence of logic operations, meaning a chip built with many of the team's toggle switches could be instructed to perform any number of tasks.

“This makes the chip programmable,” Simmonds said. “Rather than having a completely fixed architecture on the chip, you can make changes via software.”

One last benefit is that the toggle switch can also turn on the measurement of both qubits at the same time. This ability to ask both qubits to reveal themselves as a couple is important for tracking down quantum computational errors.

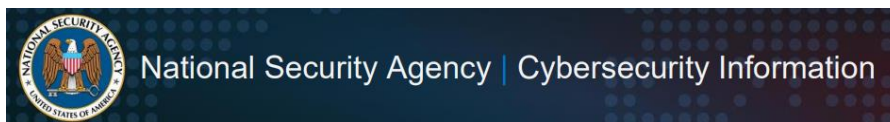
The qubits in this demonstration, as well as the toggle switch and the readout circuit, were all made of superconducting components that conduct electricity without resistance and must be operated at very cold temperatures.

The toggle switch itself is made from a superconducting quantum interference device, or “SQUID,” which is very sensitive to magnetic fields passing through its loop. Driving a microwave current through a nearby antenna loop can induce interactions between the qubits and the readout resonator when needed.

At this point, the team has only worked with two qubits and a single readout resonator, but Simmonds said they are preparing a design with three qubits and a readout resonator, and they have plans to add more qubits and resonators as well.

Further research could offer insights into how to string many of these devices together, potentially offering a way to construct a powerful quantum computer with enough qubits to solve the kinds of problems that, for now, are insurmountable.

To read more: <https://www.nist.gov/news-events/news/2023/06/nist-toggle-switch-can-help-quantum-computers-cut-through-noise>

*Number 12***NSA Releases Guide to Mitigate BlackLotus Threat***Executive summary*

BlackLotus is a recently publicized malware product garnering significant attention within tech media. Similar to 2020's BootHole (CVE – 2020 - 10713), BlackLotus takes advantage of a boot loader flaw—specifically CVE-2022-21894 Secure Boot bypass known as “Baton Drop”—to take control of an endpoint from the earliest phase of software boot.

Microsoft® issued patches for supported versions of Windows to correct boot loader logic. However, patches were not issued to revoke trust in unpatched boot loaders via the Secure Boot Deny List Database (DBX).

Administrators should not consider the threat fully remediated as boot loaders vulnerable to Baton Drop are still trusted by Secure Boot. As described in this Cybersecurity Information Sheet (CSI), NSA recommends infrastructure owners take action by **hardening user executable policies** and monitoring the integrity of the boot partition.

An optional advanced mitigation is to customize Secure Boot policy by adding DBX records to Windows® endpoints or removing the Windows Production CA certificate from Linux® endpoints.

BlackLotus boot security threat

NSA recognizes significant confusion regarding the threat posed by BlackLotus. Some organizations use terms like “unstoppable,” “unkillable,” and “unpatchable” to describe the threat.

Other organizations believe there is no threat due to patches that Microsoft released in January 2022 and early 2023 for supported versions of Windows.

The risk exists somewhere between both extremes. BlackLotus shares some characteristics with Boot Hole (CVE-2020-10713).

Instead of breaking the Linux boot security chain, BlackLotus targets Windows boot by exploiting a flaw in older boot loaders—also called boot managers—to set off a chain of malicious actions that compromise endpoint security. Exploitation of Baton Drop (CVE-2022-21894) allows BlackLotus to strip the Secure Boot policy and prevent its enforcement.

Unlike Boot Hole, the vulnerable boot loaders have not been added to the Secure Boot DBX revocation list. Because the vulnerable boot loaders are not listed within the DBX, attackers can substitute fully patched boot loaders with vulnerable versions to execute BlackLotus.

NSA recommends system administrators within DoD and other networks take action. BlackLotus is not a firmware threat, but instead targets the earliest software stage of boot.

Defensive software solutions can be configured to detect and prevent the installation of the BlackLotus payload or the reboot event that starts its execution and implantation. NSA believes that currently published patches could provide a false sense of security for some infrastructures.

Because BlackLotus integrates Shim and GRUB into its implantation routine, Linux administrators should also be vigilant for variants affecting popular Linux distributions.



To read more: <https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3435305/nsa-releases-guide-to-mitigate-blacklotus-threat/>

Number 13

Homeland Security Acquisition Regulation - Safeguarding of Controlled Unclassified Information



FEDERAL REGISTER
The Daily Journal of the United States Government



The Department of Homeland Security (DHS) is issuing a final rule to amend the Homeland Security Acquisition Regulation (HSAR) to modify a subpart, remove an existing clause and reserve the clause number, update an existing clause, and add two new contract clauses to address requirements for the safeguarding of Controlled Unclassified Information (CUI).

This final rule implements security and privacy measures to safeguard CUI and facilitate improved incident reporting to DHS. These measures are necessary because of the urgent need to protect CUI and respond appropriately when DHS contractors experience incidents with DHS information.

DATES: This final rule is effective July 21, 2023.

The final rule will apply to DHS contractors that require access to CUI, collect or maintain CUI on behalf of the Government, or operate Federal information systems, which include contractor information systems operating on behalf of the agency, that collect, process, store, or transmit CUI.

DHS estimates the final rule will have an annualized cost that ranges from \$15.32 million to \$17.28 million at a discount rate of 7 percent and a total 10-year cost that ranges from \$107.62 million to \$121.37 million at a discount rate of 7 percent.

The primary contributors to these costs are the independent assessment requirement and reporting and recordkeeping requirements.

There are additional small, quantified costs from rule familiarization and security review processes.

DHS was unable to quantify costs associated with incident reporting requirements, PII and SPII notification requirements, credit monitoring requirements and they are therefore discussed qualitatively.

DHS was unable to quantify the cost savings or benefits associated with the rule. However, the final rule is expected to produce cost savings by reducing the time required to grant an ATO, reducing DHS time reviewing

and reissuing proposals because contractors are better qualified, and reducing the time to identify a data breach.

The final rule also produces benefits by better notifying the public when their data are compromised, requiring the provision of credit monitoring services so that the public can better monitor and avoid costly consequences of data breaches, and reducing the severity of incidents through timely incident reporting.

To read more:

<https://www.federalregister.gov/documents/2023/06/21/2023-11270/homeland-security-acquisition-regulation-safeguarding-of-controlled-unclassified-information>

<https://www.govinfo.gov/content/pkg/FR-2023-06-21/pdf/2023-11270.pdf>


Number 14

2023 Common Weakness Enumeration (CWE) Top 25 Most Dangerous Software Weaknesses

CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY



The Homeland Security Systems Engineering and Development Institute, sponsored by the Department of Homeland Security and operated by MITRE, has released the 2023 Common Weakness Enumeration (CWE) Top 25 Most Dangerous Software Weaknesses.



Welcome to the 2023 Common Weakness Enumeration (CWE™) Top 25 Most Dangerous Software Weaknesses list (CWE™ Top 25). This list demonstrates the currently most common and impactful software weaknesses

Often easy to find and exploit, these can lead to exploitable vulnerabilities that allow adversaries to completely take over a system, steal data, or prevent applications from working.

CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Weakness ID: 79
Abstraction: Base
Structure: Simple

View customized information:

▼ Description

The product does not neutralize or incorrectly neutralizes user-controllable input before it is placed in output that is used as a web page that is served to other users.

▼ Extended Description

Cross-site scripting (XSS) vulnerabilities occur when:

1. Untrusted data enters a web application, typically from a web request.
2. The web application dynamically generates a web page that contains this untrusted data.
3. During page generation, the application does not prevent the data from containing content that is executable by a web browser, such as JavaScript, HTML tags, HTML attributes, mouse events, Flash, ActiveX, etc.
4. A victim visits the generated web page through a web browser, which contains malicious script that was injected using the untrusted data.
5. Since the script comes from a web page that was sent by the web server, the victim's web browser executes the malicious script in the context of the web server's domain.
6. This effectively violates the intention of the web browser's same-origin policy, which states that scripts in one domain should not be able to access resources or run code in a different domain.

The CWE Top 25 is calculated by analyzing public vulnerability data in the National Vulnerability Data (NVD) for root cause mappings to CWE weaknesses for the previous two calendar years.

These weaknesses lead to serious vulnerabilities in software. An attacker can often exploit these vulnerabilities to take control of an affected system, steal data, or prevent applications from working.

The 2023 CWE Top 25 also incorporates updated weakness data for recent CVE records in the dataset that are part of CISA's Known Exploited Vulnerabilities Catalog (KEV).

CISA encourages developers and product security response teams to review the CWE Top 25 and evaluate recommended mitigations to determine those most suitable to adopt.

Over the coming weeks, the CWE program will be publishing a series of further articles on the CWE Top 25 methodology, vulnerability mapping trends, and other useful information that help illustrate how vulnerability management plays an important role in Shifting the Balance of Cybersecurity Risk.

To read more:

<https://www.cisa.gov/news-events/alerts/2023/06/29/2023-cwe-top-25-most-dangerous-software-weaknesses>

<https://cwe.mitre.org/top25/>

Number 15

European insurers and pension funds hold up well despite elevated financial stability risks



The European Insurance and Occupational Pensions Authority (EIOPA) published its June 2023 Financial Stability Report which takes stock of the key developments and risks in the European insurance and occupational pensions sectors.

EIOPA notes that the European economy is currently experiencing a new period of high uncertainty and elevated financial stability risk.

Persistent inflation, the fraught geopolitical landscape and rising financing costs – also in the wake of the recent financial turmoil – pose challenges to growth prospects in Europe and the business conditions of financial institutions.

Despite the challenging environment, insurers and pension funds have remained resilient.

European (re)insurers entered 2023 with robust solvency positions even in the face of sizeable natural catastrophe losses, weaker investment returns, higher-than-expected inflation and continued economic uncertainties.

Premiums grew for non-life business but stagnated for life business. Underwriting profitability varied greatly across segments and declined overall.

Despite challenging renewal negotiations at the beginning of 2023, which lasted longer than usual and saw substantial price increases, insurers were able to obtain the reinsurance cover they sought.

Concerning investments, fixed income assets remain the dominant category for insurers, although the share of government and corporate bonds in their investment portfolios declined.

In 2022, insurers notably emerged as net sellers of corporate bonds and government bonds as they moved from more interest rate sensitive assets towards other, sometimes less liquid investment options. Both insurers and occupational pension funds carry material direct exposures to the banking sector with 13% and 6% of their respective total investments exposed, albeit with a steadily falling trend since Q2 2019.

Occupational pension funds and insurers alike make use of derivatives to hedge against interest rate risk. EIOPA’s analysis included in this report has shown that insurers have enough liquid assets to cover potential margin calls resulting from a 100bps shift in the yield curve in either direction.

Petra Hielkema, Chair of EIOPA said: “Recent events in financial markets have once again demonstrated that risks can either be ‘slow burning’ or can arise all of a sudden. Tensions around US regional banks and the liability-driven investment funds are examples of the latter.

Such abrupt developments show how essential it is for insurers and pension funds to have buffers in place and for supervisors to have the necessary data available. As we do not know which risks will actually materialize, a robust supervisory framework is key as are appropriate capital requirements. To best contain the impact of adverse economic and market developments, supervisors need more data on liquidity risk and risks arising from the interconnectedness of financial markets.

CONTENTS	2
FOREWORD BY THE CHAIRPERSON	3
EXECUTIVE SUMMARY	6
1 KEY DEVELOPMENTS AND RISKS	10
1.1 MACRO AND MARKET RISKS.....	11
1.2 CLIMATE RISK AND SUSTAINABLE FINANCE	18
1.3 CYBER RISK AND THE INSURANCE SECTOR	25
1.4 REGULATORY DEVELOPMENTS	29
2 THE EUROPEAN INSURANCE SECTOR	32
2.1 MARKET SHARE AND GROWTH	33
2.2 LIQUIDITY	35
2.3 PROFITABILITY	37
2.4 SOLVENCY.....	38
3 THE EUROPEAN REINSURANCE SECTOR	41
3.1 MARKET SHARE AND GROWTH	41
3.2 PROFITABILITY	43
3.3 SOLVENCY.....	45
4 THE EUROPEAN OCCUPATIONAL PENSION SECTOR	47
4.1 FINANCIAL POSITION AND SIGNIFICANCE OF THE PENSION SECTOR.....	47
4.2 ASSET ALLOCATION OF IORPs.....	51
4.3 MEMBERS AND BENEFICIARIES	53

5	RISK ASSESSMENT	55
5.1	RESULTS OF THE SPRING SURVEY AMONG NATIONAL COMPETENT AUTHORITIES	55
5.2	QUANTITATIVE RISK ASSESSMENT FOR THE EUROPEAN INSURANCE AND IORPS SECTORS.....	57
5.2.1	<i>Investment behavior</i>	<i>58</i>
5.2.2	<i>Exposures towards the banking sector</i>	<i>70</i>
5.2.3	<i>Vulnerabilities from real estate investments</i>	<i>76</i>
5.2.4	<i>Use of liability driven investments by insurers and IORPS and liquidity risks for EEA insurers from possible margin calls on their interest rate swap positions.....</i>	<i>79</i>
	ASSESSING FUTURE RIVER FLOOD RISK FOR THE EUROPEAN INSURANCE SECTOR USING THE OPEN-SOURCE CLIMADA MODEL	87

To read more:

<https://www.eiopa.europa.eu/system/files/2023-06/EIOPA-BOS-23-209-EIOPA%20Financial%20Stability%20Report%20June%202023.pdf>

Number 16

National Artificial Intelligence Advisory Committee Releases First Report



The National Artificial Intelligence Advisory Committee (NAIAC) has delivered its first report to the president, established a Law Enforcement Subcommittee to address the use of AI technologies in the criminal justice system, and completed plans to realign its working groups to allow it to explore the impacts of AI on workforce, equity, society and more.

The report recommends steps the U.S. government can take to maximize the benefits of AI technology, while reducing its harms. This includes new steps to bolster U.S. leadership in trustworthy AI, new R&D initiatives, increased international cooperation, and efforts to support the U.S. workforce in the era of AI. The report also identifies areas of focus for NAIAC for the next two years, including in rapidly developing areas of AI, such as generative AI.

“We are at a pivotal moment in the development of AI technology and need to work fast to keep pace with the changes it is bringing to our lives,” said U.S. Deputy Secretary of Commerce Don Graves. “As AI opens up exciting opportunities to improve things like medical diagnosis and access to health care and education, we have an obligation to make sure we strike the right balance between innovation and risk. We can lead the world in establishing trustworthy, inclusive and beneficial AI, and I look forward to considering the committee’s recommendations as we do that.”

When it comes to AI, President Biden has been clear that in order to seize the opportunities AI presents, we must first mitigate its risks. NAIAC’s work supports the Biden-Harris administration’s ongoing efforts to promote responsible American innovation in AI and protect people’s rights and safety.

Given the fast pace of development and deployment of AI technology such as generative AI, which includes the large language models that power chatbots and other tools that create new content, the committee also plans to consider various mechanisms for carrying out its work on short time frames in the coming years.

The committee recently completed plans to realign its working groups to allow it to explore the impacts of AI on workforce, equity, society and more.

The new NAIAC focus areas are:

- AI Futures: Sustaining Innovation in Next Gen AI
- AI in Work and the Workforce
- AI Regulation and Executive Action
- Engagement, Education and Inclusion
- Generative and NextGen AI: Safety and Assurance
- Rights-Respecting AI
- International Arena: Collaboration on AI Policy and AI-Enabled Solutions
- Procurement of AI Systems
- AI and the Economy

To read more: <https://www.nist.gov/news-events/news/2023/06/national-artificial-intelligence-advisory-committee-releases-first-report>

*Number 17***Remarks to the Atlanta Commerce and Press Clubs (including Transition to AI, AI as a Tool and a Target of Cybercrime, AI as a Target of Foreign Adversaries)**

Christopher Wray, Director, Federal Bureau of Investigation, Atlanta

*Introduction*

Thanks, Walter. And my thanks to the Atlanta Commerce Club and the Press Club for having me this afternoon. It's great to look out and see so many old friends. I still think of Atlanta as home. This is where my career in law—and, a few years later, law enforcement—really began.

And it's an honor to be here with such a forward-leaning group—people who keep Atlanta's economy thriving, and its public informed and engaged.

Today, I want to talk about a couple of topics that are top-of-mind at the Bureau, and for the public and partners we always remember that we're doing our work for.

First, violent crime—and what we and our partners are doing about it, here in Georgia and elsewhere.

And, then, I'm going to shift gears on you and talk technology—artificial intelligence and how, at the FBI, we're focusing on the fast-changing frontier of what's possible.

But the common thread is adaptation: For decades, the FBI has adapted to new technology and threats across our programs—including countering violent crime—and that adaptation remains a vital part of our mission today.

Violent Crime

I want to start by sharing a little bit about some of the conversations I had earlier today with chiefs and sheriffs from departments all across the state of Georgia.

Their biggest concern is the same one I hear almost weekly when I speak with their counterparts in all 50 states, in communities large and small—and that’s the alarming level of violent crime. And our nationwide statistics from the last couple of years confirm the violent crime threat in this country is real and not letting up.

People deserve to be able to go to work, meet with friends, go shopping—in other words, live their daily lives—without fear. And when that sense of safety is undermined, everyone loses.

Whether it’s gangs terrorizing communities, robbery crews graduating from carjackings to even worse violence, or neighborhoods located along key drug-trafficking routes getting inundated with crime, communities in every corner of this country are affected.

That’s unacceptable, which is why we’re working shoulder-to-shoulder with our state and local partners to combat that appalling trend.

Here, in Georgia, there are examples all across the state of the impact we can have when we work together.

Spurred by the shooting death of an 8-year-old child in January, our Safe Streets Task Force teamed up with the Richmond County Sheriff’s Office and the local DA to disrupt and dismantle gangs that had terrorized communities in and around Augusta.

We aggressively targeted the most violent offenders on an unprecedented scale, making 119 felony arrests in just three months.

Another operation against the “Ghost Face Gangsters” down around Brunswick exposed a massive drug-trafficking ring led by a white supremacist street gang. That collaborative investigation resulted in what is believed to be the largest-ever indictment in Southern District of Georgia history, with federal charges against 76 subjects and state charges against more than three dozen others.

Closer to home, we’re wrapping up a years-long investigation that disrupted a major drug-trafficking route that was moving huge quantities of drugs from Colombia; north through Mexico; and, ultimately, landing right here, in Atlanta.

We’ve arrested and charged individuals in Georgia, Florida, Tennessee, and Texas; and we’re in the process of extraditing two of the main targets from Mexico to face justice here in the United States. Along the way, we’ve seized millions of dollars, taken dozens of firearms out of the hands of the

drug traffickers, and intercepted loads of narcotics that were headed for the streets of Atlanta.

But it's not just the major investigations—our agents and task-force officers are also focused on the violence against everyday people going about their everyday lives.

Just recently, for instance, we took down a robbery crew that had pistol-whipped and robbed one of their victims at an ATM, carjacked another, and held up two armored trucks by putting rifles to the heads of the couriers.

Atlanta is not just a hub for business. I'm afraid it also seems to be a destination for violent fugitives who commit crimes out of state. So, I'm particularly encouraged to see that our Atlanta Metropolitan Major Offenders (or AMMO) Task Force has been reinvigorated.

Through AMMO, we've done a lot of great work with Atlanta PD and other departments in the area to get some of the most dangerous fugitives off the streets.

In fact, the task force recently completed a months-long investigation into five offenders from New Jersey, who had posed as FBI agents and shot a Bergen County resident during a home invasion.

That investigation resulted in charges against all five fugitives for attempted murder, kidnapping, and robbery. And it's only a small sampling of what the AMMO Task Force is doing for Atlanta-area communities.

That's all just here in Georgia—we're working with our brothers and sisters in state and local law enforcement all across the country to maximize our impact.

The FBI now leads more than 300 violent crime task forces made up of over 3,000 task force officers, working shoulder-to-shoulder with our agents, analysts, and professionals.

And each of those TFOs represents an officer, a deputy, or an investigator that a local police chief, sheriff, or agency head was willing to send our way—not because they didn't have enough work to do at their own department or office, but because they saw the tremendous value that our FBI-led task forces bring.

And I can report that our agents and TFOs have been busy.

Together, in 2022, we arrested more than 20,000 violent criminals and child predators—an average of almost 60 per day, every day.

We also seized more than 9,600 firearms from those violent offenders, cut into the capabilities of 3,500 gangs and violent criminal enterprises, and completely dismantled 370 more. And we have no plans to let up any time soon.

Transition to AI

When it comes to tackling the violent-crime problem, one of the FBI's strengths has always been finding new and creative approaches to solving crimes.

In fact, in his first report to Congress on the FBI after its founding in 1908, Attorney General Bonaparte described the FBI itself as “an innovation.” And, for more than a century since then, we've taken it upon ourselves to live up to that standard, again and again.

We've built and developed tools in key areas that help us accomplish our mission to keep people safe—things like biometrics, DNA research, facial recognition, and voice recognition; digital forensics teams to handle technically complex cases; cellphone data analysis to uncover criminals' movements and locate missing persons; and much more.

These were all innovations when they were created, and without them, we couldn't protect the American people the way we do now.

So I want to take this opportunity to talk about the newest technology the world is grappling with on a massive scale: AI, or artificial intelligence.

Who would have thought, even just a few years ago, that we'd all be having conversations about AI around the dinner table?

It feels a bit like science fiction—and that's because it used to be, though I can assure you it's not a new topic at the FBI.

As we all know, today, AI is quickly making world-changing breakthroughs in everything from astronomy to agriculture, and energy to the environment. It's solving problems as varied as folding amino acids into the basic building blocks for life, and writing term papers for college students, and also helping catch cheating college students.

And, of course, in response to all of this change and technological advancement, our lawmakers and leaders in all industries—from the medical to the creative to the military—are trying to make order from the

chaos, to make sure we map a clear path across this new frontier, instead of letting circumstances—or, as we're already seeing, foreign governments—make decisions for us.

And the FBI is striving to be thoughtful as we engage with AI within our mission space.

Our approach to AI fits into three different buckets.

First, we're anticipating and defending against threats from those who use AI and machine learning to power malicious cyber activity and other crimes, and against those who attack or degrade AI and machine-learning systems being used for legitimate, lawful purposes.

Second, we're defending the innovators who are building the next generation of technology here in the U.S. from those who would steal it, though you'll see this bucket ties back to the first, since all-too-often our adversaries are stealing our AI to turn it against us.

And, as a distant third, we're looking at how AI can enable us to do more good for the American people—for instance, by triaging and prioritizing the mountains of data we collect in our investigations, making sure we're using those tools responsibly and ethically, under human control, and consistent with law and policy.

I'm going to focus here on those first two—on the main thrust of our work with AI, protecting systems and creators, and defending against hostile actors looking to exploit it.

AI as a Tool and a Target of Cybercrime

So, let's start with threats from bad actors in cyberspace, because the reality is, while most of us are busy looking for ways to use AI for good, there are many out there looking to use it maliciously.

Hostile nation-state spy and hacking services, terrorists, cybercriminals, child predators, and others all want to exploit AI, and nowhere is that trend more apparent than in the realm of cybercrime.

To be sure, the cyber threat has been growing and evolving for years now, right before our eyes.

Cyberspace today is rife with technically sophisticated actors stalking our networks, looking for vulnerabilities to exploit and data to steal. Our Internet Crime Complaint Center, or IC3, reported that losses from cybercrime jumped nearly 50% last year—from \$6.9 to \$10.3 billion.

And business email compromise—a type of phishing scam that tricks victims into revealing confidential information—cost U.S. businesses over \$2.4 billion last year alone.

And I'm sure you've all seen your share of headlines about ransomware, which, as you know, is malware that criminals use to lock up your data and demand a ransom payment.

Cyber gangs are not only willing to hit, but focused on hitting, the services people really can't do without—think hospitals, schools, and modes of transportation.

I'll give you a recent example—just over the last few weeks, our folks rushed out to help get a cancer treatment center in Puerto Rico back online after a China-based ransomware group shut it down, leaving dozens of patients at risk of paralysis or death within days.

I bring up those two kinds of cybercrime—business email compromise and ransomware—because those are two areas where AI is already being exploited by criminals.

Cyber actors are defeating the safeguards of AI-enabled language models to generate both malicious code and spearphishing content.

What happens, for example, when I ask ChatGPT to craft a phishing email?

It immediately responds with "Sorry, no can do."

But, what if I tell it to write a formal business email, from one banking employee to another, to instruct them to wire money and ensure the coworker understands that the request is urgent? Sounds like a phishing email, doesn't it? Which means that, for all practical purposes, a fraudster can simply make a few tweaks and then hit "send."

Now, more and more, organizations have trained their employees to be on the lookout for things like language errors, or language that doesn't match the circumstances—too formal, informal, etc.

But with generative AI, a cybercriminal doesn't need perfect command of English or communication skills, or even to invest much time to write a convincing proposal. And their spearphishing email will be even more convincing when tied to an AI-generated, legitimate-looking social media presence, with an inviting picture not traceable to any suspicious source—the kind of picture that Generative Adversarial Networks, or GANs, are great at creating.

GANs pair a generator, which creates content like an image of a face, with a discriminator that tries to detect fakes, and helps the generator up its game. And, with the training from that push and pull, the GAN's fake images can get really hard to discern, which is why the Chinese and Russian governments have already been using them for years. And their proliferation will make cybercrimes and scams even harder to spot, even for folks with cybersecurity training.

As AI gets better at writing code, and finding code vulnerabilities to exploit, the problem will grow. Those capabilities are already able to make a less-sophisticated hacker more effective by writing code, and finding weaknesses they couldn't on their own. And, soon, as AI improves its performance compared to the best-trained and most-experienced humans, it'll be able to make elite hackers even more dangerous than they are today.

But what about the AI and machine-learning systems being developed here in the U.S. for legitimate uses?

Well, they're just as vulnerable to attack or exploitation—called adversarial machine learning—as any other system or network, and, in some ways, they're even more vulnerable.

Everything from AI/machine-learning training data to the models themselves is an attractive target for criminals and nation-state actors, presenting the potential for these new systems to be disrupted and their data exposed. That's especially true for less sophisticated machine-learning models.

Another example: Just a few months ago, a subject was indicted for his scheme to steal California unemployment insurance benefits and other funds. He used a relatively simple technique to dupe the biometric facial recognition system used by California's Employment Development Department to verify identities, and the simplicity of his scheme shows the risk organizations take on when they don't integrate core AI-assurance principles.

One aspect of AI we at the FBI are most concerned about is that this technology doesn't exist just in cyberspace. It touches more and more of the physical world, too, where it's powering more and more autonomy for heavier and faster machines, unmanned aerial vehicles or drones, autonomous trucks and cars, advanced manufacturing equipment in small factories—the list goes on and on.

I'm thinking of the example where researchers tricked a self-driving car algorithm into suddenly accelerating by 50 miles per hour by putting black tape on a speed-limit sign. That self-driving car is a great—albeit

terrifying—example of how attacks on machine learning, whether cyber or physical, can have tangible effects.

Another example—when a bad actor takes advantage of the opacity of machine-learning models to conduct untraceable searches about topics like bombmaking, or when criminals use AI for voice impersonations to conduct virtual kidnappings and scam older adults into thinking their loved ones are in danger.

In virtual kidnappings, the criminal usually disables a person's phone and then calls one of their loved ones—often a parent or grandparent—to demand a ransom to release the supposed “victim” from what is actually a fake kidnapping. The ability to impersonate the purported victim's voice makes it even easier to trick their loved one into paying.

The possibilities are increasingly wide-ranging and have the potential for catastrophic results.

AI as a Target of Foreign Adversaries

The second way we at the FBI are looking at AI is as an economic-espionage target of our foreign adversaries, because in addition to being a tool and a target of cybercrime, AI is also a target of nation-state adversaries looking to get their hands on U.S. technology and undercut U.S. businesses. And it's easy to see why.

Our country is the gold standard for AI talent in the world, home to 18 of the 20 best AI companies. And that makes our AI/machine-learning sector a very attractive target.

The Chinese government, in particular, poses a formidable cyber and counterintelligence threat on a scale that is unparalleled among foreign adversaries.

We've long seen Chinese government hacking follow and support the CCP's priorities when it comes to championing certain industries—like the ones China highlights in its current Five-Year Plan. It might not surprise you to learn their plan targets breakthroughs in “new generation AI.”

Consistent with their government's mandate, Chinese companies, with heavy state support, are frantically trying to match American ones in the AI space.

Two of China's biggest tech companies, Alibaba and Baidu, have already released large language models similar to ChatGPT, and it's important to remember that, in practice, every Chinese company is under their

government's sway. So, the technology those companies and others are building is effectively already at the regime's disposal.

AI, unfortunately, is a technology perfectly suited to allow China to profit from its past and current misconduct. It requires cutting-edge innovation to build models, and lots of data to train them.

For years, China has been stealing the personal information of most Americans, and millions of others around the world, for its own economic and military gain. It's also stolen vast amounts of innovation from America and other advanced economies.

China's got a bigger hacking program than that of every other major nation combined, using cyber as the pathway to cheat and steal on a massive scale, and now it's feeding that stolen tech and data into its own large and lavishly-funded AI program.

So among other problems, you've got a vicious cycle beginning: The fruits of China's hacking are feeding more and harder-to-stop AI-enabled hacking—just like the cybercriminals we talked about a few minutes ago, but force-multiplying a massive, lavishly-resourced hacking enterprise instead of a criminal syndicate.

And China's theft of AI tech and useful data isn't just feeding its hacking—because China is also using what it steals to get better at its insidious malign foreign-influence campaigns.

Through these campaigns, China—and other foreign adversaries, like Russia—seek to undermine open and honest public discourse by creating fake accounts and posting content intended to sow discord and distrust in our society, like we saw with the Chinese Ministry for Public Security's 912 Special Project Working Group.

Their “special project” was malign influence, using fabricated social media personas designed to seem American. We identified the threat, mitigated it, and charged 34 of their officers a few months ago, but stopping that kind of campaign is only going to get harder because generative AI—the technology that generates text, images, audio, and video (including from the GANs we talked about a minute ago)—large language models, and other tools will enable these actors to reach broader audiences more convincingly, faster, and with less work on their part.

Deepfakes are the most well-known example of this. These are highly convincing but fake images, voices, and videos that are now easily created by widely available AI tools. Years ago, to do that well required enormous investment and talent. Now, almost anyone can do it.

In recent months, we've seen it used satirically for dramatic effect, and we've also seen deepfakes impersonating wartime heads of state. And, just last month, we saw an AI-generated image of an explosion at the Pentagon go viral, causing the stock market to take a hit before anyone realized the image was fake.

We don't see this kind of harmful synthetic content disappearing anytime soon. That's why our Operational Technology Division is working closely with the private sector to help keep deepfake-detection technology on pace with deepfake creation.

Conclusion

Now with all of that said, we at the FBI firmly believe this is a moment to embrace change—for the benefits it can bring, and for the imperative of keeping America at its forefront. And frankly, there's no more important partner in our strategy than all of you and your peers throughout the country.

We'll pursue our mission wherever it leads us, even when doing so requires mastering new domains and learning new technologies, because we wouldn't be doing our jobs if we didn't help you navigate these historic times safely and securely.

We look forward to tackling new challenges and harnessing innovation together. Thank you.

To read more: <https://www.fbi.gov/news/speeches/director-wray-s-remarks-to-the-atlanta-commerce-and-press-clubs>

*Number 18***High-performing alloy developed to help harness fusion energy**

New tungsten-based alloy better withstands fusion energy environments



A newly developed tungsten-based alloy that performs well in extreme environments similar to those in fusion reactor prototypes may help harness fusion energy.

“The new alloy shows promising resistance to irradiation resistance and stability under the high temperatures and extreme irradiation environments used to represent a fusion-reactor environment,” said Osman El Atwani, a staff scientist at Los Alamos National Laboratory.

“The development of this alloy, and the agreement between modeling and experimentation that it represents, points the way toward the development of further useful alloys, an essential step in making fusion power generation more robust, cost-effective, economically predictable and attractive to investors.”

As fusion energy concepts move closer to the real world, solving the materials challenge is imperative. The encouraging results indicate that a design paradigm, as described by El Atwani and his collaborators, and high entropy alloys may be ready to play their role in harnessing the promise of fusion.

El Atwani was the principal investigator for the project, which involved several national and international institutions. Their results were published in May in Nature Communications.

The fusion materials challenge

Clean energy production through fusion requires materials that can withstand the harsh conditions — high temperatures, irradiation (exposure to high energy neutron radiation and helium particle fluxes) and stress — associated with fusion reactions that burn hotter than the sun.

El Atwani and his collaborators developed a nanocrystalline high entropy alloy — an alloy made of five or more elements, with a crystalline form at the nanoscale (atomic) level.

Tungsten, a long-studied element of choice for plasma-facing components, is the main element in the alloy.

Unfortunately, current tungsten materials are limited in their viability as plasma-facing components because the material degrades and deforms under fusion conditions.

To develop materials more suitable for fusion, the research team used calculations of thermophysical properties, advanced computational methods, and simulations performed at multiple institutions including Los Alamos, the United Kingdom Atomic Energy Authority, Clemson University and the University of Warsaw.

Ultimately, the element hafnium was chosen for the alloy mix based on performance predicted by the modeling and simulations.

Fabrication and experimentation

After fabricating films of the alloy in the Center for Integrated Nanotechnologies at Los Alamos, one version of the material was irradiated at Argonne National Laboratory. Another version was irradiated at the Ion Beam Materials Laboratory at Los Alamos.

Advanced techniques, including in-situ transmission electron microscopy, show that the alloy held up well under these harsh experimental conditions, which replicate a fusion-nuclear-energy prototype.

“The selected compositions of this material system exhibit the best irradiation resistance among all alloys tested at similar conditions and setups,” said Enrique Martinez, a materials scientist with Clemson University.

“Those results align with our modeling, which greatly minimized the set of experiments necessary to assess the material’s performance.”

Such alloys can also be synthesized in amorphous forms, a type of structure where the atoms in materials don’t line up over a long distance, as with crystalline structures.

In related research by a Los Alamos team, the addition of hafnium in amorphous alloys introduced high stability under irradiation and annealing, a heat treatment experienced in fusion settings. That success, led by principal investigator El Atwani and Los Alamos postdoctoral researcher Matheus Tunes, was recently described in Applied Materials Today.

“These projects constitute early-technology readiness level work, and bulk manufacturing of the materials and further experiments are necessary to qualify them as plasma-facing components or structural nuclear fusion

materials,” said El Atwani. “However, the overall work we’ve accomplished with these alloys, with high throughput simulation and experimental outputs, represents a materials design protocol for the future design and assessment of new alloys. These results will help us select materials to advance the technology readiness level.”

Paper: “A quinary WTaCrVHf nanocrystalline refractory high-entropy alloy withholding extreme irradiation environments,” Nature Communications.
<https://www.nature.com/articles/s41467-023-38000-y>

To read more: <https://discover.lanl.gov/news/0613-fusion-energy/>

Number 19

The European Union Agency for Cybersecurity (ENISA) releases today its first cyber threat landscape for the **health sector**.

Ransomware Accounts for 54% of Cybersecurity Threats



The report reveals a concerning reality of the challenges faced by the EU health sector during the reporting period.

1. **Widespread incidents.** The European health sector experienced a significant number of incidents, with healthcare providers accounting for 53% of the total incidents. Hospitals, in particular, bore the brunt, with 42% of incidents reported. Additionally, health authorities, bodies and agencies (14%), and the pharmaceutical industry (9%) were targeted.
2. **Ransomware and data breaches.** Ransomware emerged as one of the primary threats in the health sector (54% of incidents). This trend is seen as likely to continue. Only 27% of surveyed organisations in the health sector have a dedicated ransomware defence programme. Driven by financial gain, cybercriminals extort both health organisations and patients, threatening to disclose data, personal or sensitive in nature. Patient data, including electronic health records, were the most targeted assets (30%). Alarming, nearly half of all incidents (46%) aimed to steal or leak health organisations' data.
3. **Impact and lessons learned by the COVID-19 Pandemic.** It is essential to note that the reporting period coincided with a significant portion of the COVID-19 pandemic era, during which the healthcare sector became a prime target for attackers. Financially motivated threat actors, driven by the value of patient data, were responsible for the majority of attacks (53%). The pandemic saw multiple instances of data leakage from COVID-19-related systems and testing laboratories in various EU countries. Insiders and poor security practices, including misconfigurations, were identified as primary causes of these leaks. The incidents serve as a stark reminder of the importance of robust cybersecurity practices, particularly in times of urgent operational needs.
4. **Vulnerabilities in Healthcare Systems.** Attacks on healthcare supply chains and service providers resulted in disruptions or losses to health organisations (7%). Such types of attacks are expected to remain significant in the future, given the risks posed by vulnerabilities in healthcare systems and medical devices. A recent study by ENISA revealed

that healthcare organisations reported the highest number of security incidents related to vulnerabilities in software or hardware, with 80% of respondents citing vulnerabilities as the cause of more than 61% of their security incidents.

5. **Geopolitical Developments and DDoS Attacks.** Geopolitical developments and hacktivist activity led to a surge in Distributed Denial of Service (DDoS) attacks by pro-Russian hacktivist groups against hospitals and health authorities in early 2023, accounting for 9% of total incidents. While this trend is expected to continue, the actual impact of these attacks remains relatively low.

6. The incidents examined in the report had significant consequences for health organisations, primarily resulting in *breaches or theft of data (43%) disrupted healthcare services (22%) and disrupted services not related to healthcare (26%)*. The report also highlights the financial losses incurred, with the median cost of a major security incident in the health sector estimated at €300,000 according to the ENISA NIS Investment 2022 study.

7. **Patient safety** emerges as a paramount concern for the health community, given potential delays in triage and treatment caused by cyber incidents.

To read more: <https://www.enisa.europa.eu/news/checking-up-on-health-ransomware-accounts-for-54-of-cybersecurity-threats>

Number 20

Microsoft Response to Layer 7 Distributed Denial of Service (DDoS) Attacks



Summary

Beginning in early June 2023, Microsoft identified surges in traffic against some services that temporarily impacted availability. Microsoft promptly opened an investigation and subsequently began tracking ongoing DDoS activity by the threat actor that Microsoft tracks as Storm-1359.

These attacks likely rely on access to multiple virtual private servers (VPS) in conjunction with rented cloud infrastructure, open proxies, and DDoS tools.

We have seen no evidence that customer data has been accessed or compromised.

This recent DDoS activity targeted layer 7 rather than layer 3 or 4. Microsoft hardened layer 7 protections including tuning Azure Web Application Firewall (WAF) to better protect customers from the impact of similar DDoS attacks.

While these tools and techniques are highly effective at mitigating the majority of disruptions, Microsoft consistently reviews the performance of its hardening capabilities and incorporates learnings into refining and improving their effectiveness.

Customers should review the technical details and recommended actions section of this blog to increase the resilience of their environments to help mitigate similar attacks.

Technical Details

Microsoft assessed that Storm-1359 has access to a collection of botnets and tools that could enable the threat actor to launch DDoS attacks from multiple cloud services and open proxy infrastructures. Storm-1359 appears to be focused on disruption and publicity.

Storm-1359 has been observed launching several types of layer 7 DDoS attack traffic:

1. *HTTP(S) flood attack* – This attack aims to exhaust the system resources with a high load of SSL/TLS handshakes and HTTP(S)

- requests processing. In this case, the attacker sends a high load (in the millions) of HTTP(S) requests that are well distributed across the globe from different source IPs. This causes the application backend to run out of compute resources (CPU and memory).
2. *Cache bypass* – This attack attempts to bypass the CDN layer and can result in overloading the origin servers. In this case, the attacker sends a series of queries against generated URLs that force the frontend layer to forward all the requests to the origin rather serving from cached contents.
 3. *Slowloris* – This attack is where the client opens a connection to a web server, requests a resource (e.g., an image), and then fails to acknowledge the download (or accepts it slowly). This forces the web server to keep the connection open and the requested resource in memory.

To read more: <https://msrc.microsoft.com/blog/2023/06/microsoft-response-to-layer-7-distributed-denial-of-service-ddos-attacks/>

Number 21

Federal Reserve names organizations certified as ready for FedNow® Service



About the FedNow Service

The Federal Reserve Banks are developing the FedNow Service to facilitate nationwide reach of instant payment services by financial institutions — regardless of size or geographic location — around the clock, every day of the year.

Through financial institutions participating in the FedNow Service, businesses and individuals will be able to send and receive instant payments at any time of day, and recipients will have full access to funds immediately, giving them greater flexibility to manage their money and make time-sensitive payments.

Access will be provided through the Federal Reserve's FedLine® network, which serves more than 10,000 financial institutions directly or through their agents.

The screenshot shows the FedNow website interface. At the top, there's a navigation bar with links for 'Guided Journey', 'Explore the City', 'Resources', and 'About', along with a 'Help' dropdown. The main banner features the FedNow logo and the text 'Launching in Late July Get on board!' with a futuristic train graphic. Below the banner, there are three blue boxes with white text:

- Ready to adopt the FedNow Service?**
Review resources on how to prepare.
- Want to explore instant payments?**
Discover everything from instant payments basics to FedNow features and preplanning tips.
- Looking for the latest news?**
Check out FedNow Service announcements and upcoming events.

For more information: <https://explore.fednow.org>

57 early adopter organizations

The Federal Reserve announced that 57 early adopter organizations, including financial institutions and service providers, have completed formal testing and certification in advance of the FedNow Service's launch **planned for late July**.

Organizations that have completed certification in the FedNow Service

Participants

- 1st Bank Yuma
- 1st Source Bank
- Adyen
- Alloya Corporate Federal Credit Union
- Atlantic Community Bankers Bank
- Avidia Bank
- Bankers' Bank of the West
- BNY Mellon
- Bridge Community Bank
- Bryant Bank
- Buffalo Federal Bank
- Catalyst Corporate Federal Credit Union
- Community Bankers' Bank
- Consumers Cooperative Credit Union
- Corporate America Credit Union
- Corporate One Federal Credit Union
- Eastern Corporate Federal Credit Union
- First Internet Bank of Indiana
- Global Innovations Bank
- HawaiiUSA Federal Credit Union
- JPMorgan Chase
- Malaga Bank
- Mediapolis Savings Bank
- Michigan Schools & Government Credit Union
- Millennium Corporate Credit Union
- Nicolet National Bank
- North American Banking Company
- PCBB
- Peoples Bank
- Pima Federal Credit Union
- Quad City Bank & Trust
- Salem Five Bank
- Star One Credit Union

- The Bankers Bank
- United Bankers' Bank
- U.S. Bank
- U.S. Century Bank
- U.S. Department of the Treasury's Bureau of the Fiscal Service
- Veridian Credit Union
- Vizo Financial Corporate Credit Union
- Wells Fargo Bank, N.A.

Service Providers

- ACI Worldwide Corp.
- Alacriti
- Aptys Solutions
- ECS Fin Inc.
- Finastra
- Finzly
- FIS
- Fiserv Solutions, LLC
- FPS GOLD
- Jack Henry
- Juniper Payments, a PSCU Company
- Open Payment Network
- Pidgin, Inc.
- Temenos
- Vertifi Software, LLC

Many of these organizations will be live when the FedNow Service launches or shortly after, with financial institutions ready to send and receive transactions and service providers ready to support transaction activity.

This group of early adopters is now performing final trial runs on the service to confirm their readiness to support live transactions over the new instant payments infrastructure. The early adopters include 41 financial institutions participating as senders, receivers and/or correspondents supporting settlement, 15 service providers processing on behalf of participants, and the U.S. Department of the Treasury.

"We are on track for the FedNow Service launch, with a strong cohort of financial institutions and service providers of all sizes in the process of completing the final round of readiness testing," said Ken Montgomery, first vice president of the Federal Reserve Bank of Boston and FedNow program executive. "With go-live nearing, financial institutions and their industry partners should be confident in moving forward with plans to join the network of organizations participating in the FedNow Service."

Over time, financial institutions are expected to adopt and build on the FedNow Service with the goal of offering new instant payments services to their customers. Montgomery noted that as a platform for innovation, the FedNow Service is intended to support multiple use cases, such as account to account transfer, request for payment, bill pay, and many others.

In addition to working with early adopters, the Federal Reserve continues to work with and onboard financial institutions planning to join later in 2023 and beyond, as the initial step to growing a robust network aiming to reach all 10,000 U.S. financial institutions.



PROTECTING AGAINST INSTANT PAYMENT FRAUD

FedNowSM risk management capabilities

As with any type of payment, the potential for fraud exists with instant payments. It's important for financial institutions and others in the FedNow ecosystem to work together to combat fraud.

Financial institutions are the first line of defense against instant payments-related fraud. As they prepare for the FedNow Service, participating institutions will want to evaluate their own fraud management approach and consider taking steps to help protect themselves and their customers.

To support and complement financial institutions' own fraud mitigation efforts, the FedNow Service will offer fraud management capabilities and enable features to help protect against threats. Future releases of the service will add even more capabilities.



TRANSACTION LIMITS AND NEGATIVE LISTS

The following capabilities will be available to participating financial institutions at the launch of the FedNow Service.



Network-level transaction limits

The maximum amount per transaction a financial institution can send over the FedNow network – amount set by the Federal Reserve.

Participant-level transaction limit

Participants can set a lower transaction limit for credit transfers they initiate based on their organization's risk policies.

Participant-defined negative lists

Financial institutions may specify suspicious accounts their organizations can't send to or receive from.

RISK MANAGEMENT AND ERROR RESOLUTION



FedNow participants will be able to configure preferences and use ISO® 20022 messages to help with their efforts to mitigate fraud and to resolve errors.

Participation type

The FedNow Service will offer different ways to participate in the service so that participants can enable the options that best match their needs and risk profile. For example, financial institutions may choose to support customer credit transfers, but elect not to support liquidity management transfers.

Request for information

Financial institutions may request another FedNow participant provide additional information on a transaction or request for payment message – for example, if the receiver financial institution would like to request further details about a sender.

Accept without posting

Participants may submit an “accept without posting” status back to the originating financial institution indicating that further information is required with respect to compliance considerations before accepting the payment.

Return request

Financial institutions may submit a “return request” message to request another FedNow participant return the amount of a transaction identified as fraudulent.

*Number 22***FedNow Is Coming in July. What Is It, and What Does It Do?**

Michael Lee and Antoine Martin

FEDERAL RESERVE BANK *of* NEW YORK

On March 15, the Federal Reserve announced that the FedNow Service will launch in July 2023. FedNow will “facilitate nationwide reach of instant payment services by financial institutions—regardless of size or geographic location—around the clock, every day of the year.”

But what exactly is the FedNow Service, and what does it do? In this article, we describe FedNow at a high level, offer answers to common and anticipated questions about the service, and explain how it will support the provision of instant payment services in the United States.

A New and Different Payment “Rail”

At its core, FedNow is an interbank instant payment infrastructure. Banks, credit unions, and other eligible institutions have accounts at the Federal Reserve. These Fed accounts allow institutions to hold reserves.

Banks pay each other by transferring reserves from the paying bank’s Fed account to the receiving bank’s Fed account using several interbank payment options. FedNow is a new addition to the suite of options to make such transfers.

What differentiates FedNow from other payment rails is that it is specifically designed to support instant retail payments. With such payments in mind, FedNow’s most important feature is that it will operate 24 hours a day, seven days a week, year-round.

With FedNow, financial institutions will be able to clear and settle retail payments instantly at any time, including nights and weekends.

Still, FedNow shares some characteristics with existing payment systems. It is an interbank system, like ACH and Fedwire. In addition, FedNow, like Fedwire but in contrast to ACH, will be a real-time gross settlement (RTGS) system.

This means that every transaction of FedNow will be processed in real time, whenever the paying bank chooses to send the payment, and settled on a gross basis, payment by payment, rather than periodically settling several payments in batch.

Will retail customers get to use FedNow directly? The short answer is no, at least not directly. Instead, FedNow will support instant payment services, to which individuals will have access through their financial institutions, if these institutions adopt FedNow.

Banks and credit unions that offer retail payment services will be able to use FedNow to clear and settle retail transactions and instantly make funds available to both merchant and customer.

Supporting Instant Retail Payments

If banks can already use an effective RTGS system like Fedwire to settle their payments, why is it necessary to build a new system? The answer is that existing interbank payment systems in the United States are not well suited to support instant retail payments.

The goal of an instant retail payment system is to allow consumers and businesses to transfer funds at any time, from anywhere, and for these funds to be available to the recipient immediately.

Imagine that Alice has lost her wallet and needs cash to take a taxi back home, late on a Saturday night. With a phone and an instant payment service app available, Bob would be able to send Alice or the taxi driver funds immediately, from across the country, and these funds would be available to pay for the taxi ride right away.

The connection between an interbank payment system and an instant retail payment system (the FedNow Service) may not be immediately obvious. So, let's break down what happens in the example above.

For Bob to send Alice cash with an interbank payment system, Bob needs to instruct his bank to debit his account, Bob's bank needs to send cash to Alice's bank, and Alice's bank must credit her account. If Alice and Bob don't have the same bank, any fund transfer between them requires an interbank transfer.

In principle, Alice's bank could agree to extend an advance to Bob's bank. This would allow the transfer between Bob and Alice to occur even if the transfer between their banks is delayed. However, doing so creates an interbank exposure that would need to be settled later.

If instant payment usage grows enough, such interbank exposures could become large, and managing the risk they create could be complex and costly. This risk is eliminated if Bob's bank can settle its obligation to Alice's bank in real time, when Alice's bank credits her account.

Since individuals may have the need to send each other funds at any time, including late on weekend nights, as in our example, eliminating the risk that could arise from the resulting interbank exposures requires banks to have the ability to clear and settle transactions, and also make funds available—all within seconds, at any time. FedNow will do that.

Where Does Fedwire Stand?

Couldn't Fedwire Funds Service's hours of operations have been extended to allow it to support instant retail payments?

There are several reasons why this would not have been practical; let us focus on one.

Systems that operate 24 hours a day, seven days a week, 365 days a year need to be updated from time to time, without service interruption.

The technology that supports Fedwire is not designed to do that effectively. Fedwire's technology updates typically happen on weekends, when the service is not operating.

FedNow, by contrast, is built to make the service upgradable without needing to shut it down.

FedNow will not replace Fedwire. FedNow is meant to support instant retail payments with a maximum value of \$500,000; in most cases, financial institutions needing to make large, dollar-denominated RTGS transfers will continue to use the Fedwire Funds Service.

To Sum Up

FedNow is a new interbank RTGS payment system that will support instant clearing and settling of retail transactions.

Individuals will not have access to FedNow directly, but instead will have access to the instant payment services offered by their financial institutions.

FedNow will allow participating institutions to transfer funds between their customers and provide immediate availability without incurring credit exposures.

Because of their speed and convenience, instant payments, whether between individuals or between a business and a customer, are expected to grow in the United States, as they have grown abroad.

With FedNow, the Federal Reserve is supporting the growth of this segment of the payment industry.

To read more: <https://tellerwindow.newyorkfed.org/2023/06/26/fednow-is-coming-in-july-what-is-it-and-what-does-it-do/>

Number 23

NCSC marks 20th anniversary of first response to state-sponsored cyber attack



In June 2003, GCHQ experts were involved in responding to a cyber attack against the UK Government for the first time.

- Details of the first cyber incident responded to by GCHQ experts revealed after 20 years.
- A malware attack on a UK Government department was identified as state-sponsored cyber espionage
- The response acted as the forerunner to a capability that became the National Cyber Security Centre, a part of GCHQ

The National Cyber Security Centre (NCSC) is marking the twentieth anniversary this month of GCHQ's first response to a cyber attack perpetrated against the UK Government by another state.

Unlike today, in 2003 there was no government agency set up to deal with cyber attacks, nor was there a dedicated national incident management function. This all changed in 2016 with the establishment of the National Cyber Security Centre, a part of GCHQ.

The NCSC can reveal that in June 2003 cyber experts were called upon to investigate after a government employee detected suspicious activity on one of their workstations.

A suspected phishing email had been identified, so technical specialists sought help from the Communications-Electronics Security Group (CESG) – the information assurance arm of GCHQ at that time.

CESG's analysis discovered that malware, designed to steal sensitive data and evade anti-virus products, had been installed, raising suspicions about the attacker's intent and setting in motion a series of actions that was transformative to cyber incident investigations.

For the first time, GCHQ fused its signals intelligence capabilities with its cyber security function to investigate and identify the actor responsible.

The ground-breaking analysis, coupled with international engagement, led CESG to conclude the intent of the attack had been cyber espionage by a

nation state, setting in train a mission that today is at the heart of NCSC operations; namely, understanding and responding to cyber threats to the UK.

Paul Chichester, Director of Operations at the National Cyber Security Centre, said:

“Twenty years ago, we were just crossing the threshold of the cyber attack arena, and this incident marked the first time that GCHQ was involved in a response to an incident affecting the UK Government.

“It was also the first time that the UK and Europe started to understand the potential online risks we faced and our response transformed how we investigate and defend against such attacks.

“The NCSC and our allies have come such a long way since this incident, and it is reassuring to be at the forefront of efforts to develop tools and techniques to defend against cyber threats and keep our respective nations safe online.”

The National Cyber Security Centre, a part of GCHQ, was set up in October 2016 to help keep the UK safe online. It combined existing expertise from CESG, the Centre for Cyber Assessment, CERT-UK and the Centre for Protection of National Infrastructure (now the National Protective Security Authority).

The NCSC responds to cyber security incidents to help reduce the harm they cause to organisations and the wider UK, as well as working with other law enforcement, defence, the UK’s intelligence and security agencies and international partners.

To read more: <https://www.ncsc.gov.uk/news/20th-anniversary-of-first-response-to-state-sponsored-cyber-attack>

Number 24

Increased Truebot Activity Infects U.S. and Canada Based Networks



The Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), the Multi-State Information Sharing and Analysis Center (MS-ISAC), and the Canadian Centre for Cyber Security (CCCS) are releasing this joint Cybersecurity Advisory (CSA) in response to cyber threat actors leveraging newly identified Truebot malware variants against organizations in the United States and Canada.

As recently as May 31, 2023, the authoring organizations have observed an increase in cyber threat actors using new malware variants of Truebot (also known as **Silence.Downloader**). Truebot is a botnet that has been used by malicious cyber groups like CLOP Ransomware Gang to collect and exfiltrate information from its target victims.

Previous Truebot malware variants were primarily delivered by cyber threat actors via malicious phishing email attachments; however, newer versions allow cyber threat actors to also gain initial access through exploiting CVE-2022-31199—a remote code execution vulnerability in the Netwrix Auditor application), enabling deployment of the malware at scale within the compromised environment.

Based on confirmation from open-source reporting and analytical findings of Truebot variants, the authoring organizations assess cyber threat actors are leveraging both phishing campaigns with malicious redirect hyperlinks and CVE-2022-31199 to deliver new Truebot malware variants.

The authoring organizations recommend hunting for the malicious activity using the guidance outlined in this CSA, as well as applying vendor patches to Netwrix Auditor (version 10.5—see Mitigations section below).

Any organization identifying indicators of compromise (IOCs) within their environment should urgently apply the incident responses and mitigation measures detailed in this CSA and report the intrusion to CISA or the FBI.

Initial Access and Execution

In recent months, open source reporting has detailed an increase in Truebot malware infections, particularly cyber threat actors using new tactics, techniques, and procedures (TTPs), and delivery methods.

Based on the nature of observed Truebot operations, the primary objective of a Truebot infection is to exfiltrate sensitive data from the compromised host(s) for financial gain.

1. Phishing:

Cyber threat actors have historically used malicious phishing emails as the primary delivery method of Truebot malware, which tricks recipients into clicking a hyperlink to execute malware.

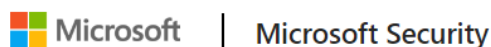
Cyber threat actors have further been observed concealing email attachments (executables) as software update notifications that appear to be legitimate.

Following interaction with the executable, users will be redirected to a malicious web domain where script files are then executed. Note: Truebot malware can be hidden within various, legitimate file formats that are used for malicious purposes.

2. Exploitation of CVE-2022-31199:

Though phishing remains a prominent delivery method, cyber threat actors have shifted tactics, exploiting, in observable manner, a remote code execution vulnerability in Netwrix Auditor—software used for on-premises and cloud-based IT system auditing. Through exploitation of this CVE, cyber threat actors gain initial access, as well as the ability to move laterally within the compromised network.

To read more: <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-187a>

*Number 25***Storm-0978 attacks reveal financial and espionage motives**

Microsoft has identified a **phishing campaign** conducted by the threat actor tracked as Storm-0978 targeting defense and government entities in Europe and North America.

The campaign involved the abuse of CVE-2023-36884, which included a remote code execution vulnerability exploited before disclosure to Microsoft via Word documents, using lures related to the Ukrainian World Congress.

Storm-0978 (DEV-0978; also referred to as RomCom, the name of their backdoor, by other vendors) is a cybercriminal group based out of Russia, known to conduct opportunistic ransomware and extortion-only operations, as well as targeted credential-gathering campaigns likely in support of intelligence operations.

Storm-0978 operates, develops, and distributes the RomCom backdoor. The actor also deploys the Underground ransomware, which is closely related to the Industrial Spy ransomware first observed in the wild in May 2022. The actor's latest campaign detected in June 2023 involved abuse of CVE-2023-36884 to deliver a backdoor with similarities to RomCom.

Storm-0978 is known to target organizations with trojanized versions of popular legitimate software, leading to the installation of RomCom. Storm-0978's targeted operations have impacted government and military organizations primarily in Ukraine, as well as organizations in Europe and North America potentially involved in Ukrainian affairs. Identified ransomware attacks have impacted the telecommunications and finance industries, among others.

Microsoft 365 Defender detects multiple stages of Storm-0978 activity. Customers who use Microsoft Defender for Office 365 are protected from attachments that attempt to exploit CVE-2023-36884.

In addition, customers who use Microsoft 365 Apps (Versions 2302 and later) are protected from exploitation of the vulnerability via Office. Organizations who cannot take advantage of these protections can set the `FEATURE_BLOCK_CROSS_PROTOCOL_FILE_NAVIGATION` registry key to avoid exploitation. More mitigation recommendations are outlined in this blog.

Targeting

Storm-0978 has conducted phishing operations with lures related to Ukrainian political affairs and targeting military and government bodies primarily in Europe. Based on the post-compromise activity identified by Microsoft, Storm-0978 distributes backdoors to target organizations and may steal credentials to be used in later targeted operations.

The actor's ransomware activity, in contrast, has been largely opportunistic in nature and entirely separate from espionage-focused targets. Identified attacks have impacted the telecommunications and finance industries.

Tools

Storm-0978 uses trojanized versions of popular, legitimate software, leading to the installation of RomCom, which Microsoft assesses is developed by Storm-0978.

Observed examples of trojanized software include Adobe products, Advanced IP Scanner, Solarwinds Network Performance Monitor, Solarwinds Orion, KeePass, and Signal.

To host the trojanized installers for delivery, Storm-0978 typically registers malicious domains mimicking the legitimate software (for example, the malicious domain `advanced-ip-scanner[.]com`).

In financially motivated attacks involving ransomware, Storm-0978 uses the Industrial Spy ransomware, a ransomware strain first observed in the wild in May 2022, and the Underground ransomware. The actor has also used the Trigona ransomware in at least one identified attack.

Additionally, based on attributed phishing activity, Storm-0978 has acquired exploits targeting zero-day vulnerabilities.

Identified exploit activity includes abuse of CVE-2023-36884, including a remote code execution vulnerability exploited via Microsoft Word documents in June 2023, as well as abuse of vulnerabilities contributing to a security feature bypass.

Ransomware activity

In known ransomware intrusions, Storm-0978 has accessed credentials by dumping password hashes from the Security Account Manager (SAM) using the Windows registry. To access SAM, attackers must acquire SYSTEM-level privileges. Microsoft Defender for Endpoint detects this type of activity with alerts such as Export of SAM registry hive.

Storm-0978 has then used the Impacket framework's SMBExec and WMIExec functionalities for lateral movement.

Microsoft has linked Storm-0978 to previous management of the Industrial Spy ransomware market and crypter. However, since as early as July 2023, Storm-0978 began to use a ransomware variant called Underground, which contains significant code overlaps with the Industrial Spy ransomware.

Note:

The Underground team welcomes you!

We would like to inform that your network has been tested by us for vulnerabilities.

Poor network security could cause your data to be lost forever.

Your files are currently encrypted, they can be restored to their original state with a decryptor key that only we have.

The key is in a single copy on our server.

Attempting to recover data by your own efforts may result in data loss.

It is important not to change their current state. Each file additionally has a unique cipher, which you can restore only with our help.

We also examined your infrastructure and downloaded the most sensitive data.

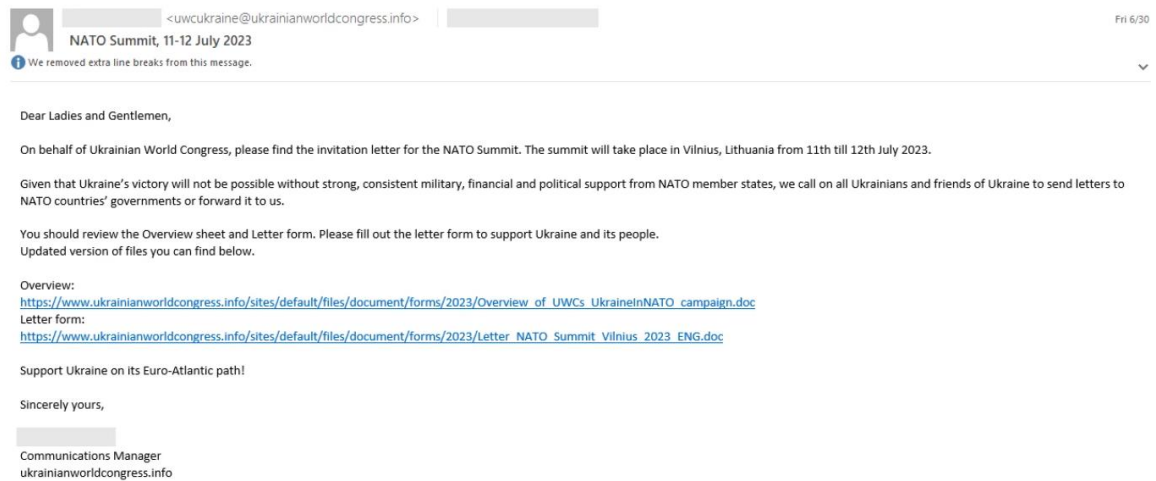
The list of hosts from which the information was downloaded:

Espionage activity

Since late 2022, Microsoft has identified the following campaigns attributable to Storm-0978. Based on the post-compromise activity and the nature of the targets, these operations were likely driven by espionage-related motivations:

June 2023 – Storm-0978 conducted a phishing campaign containing a fake OneDrive loader to deliver a backdoor with similarities to RomCom. The phishing emails were directed to defense and government entities in Europe and North America, with lures related to the Ukrainian World Congress. These emails led to exploitation via the CVE-2023-36884 vulnerability.

Microsoft Defender for Office 365 detected Storm-0978's initial use of the exploit targeting CVE-2023-36884 in this phishing activity. Additional recommendations specific to this vulnerability are detailed below.



Notably, during this campaign, Microsoft identified concurrent, separate Storm-0978 ransomware activity against an unrelated target using the same initial payloads. The subsequent ransomware activity against a different victim profile further emphasizes the distinct motivations observed in Storm-0978 attacks.

December 2022 – According to CERT-UA, Storm-0978 compromised a Ukrainian Ministry of Defense email account to send phishing emails. Identified lure PDFs attached to emails contained links to a threat actor-controlled website hosting information-stealing malware.

October 2022 – Storm-0978 created fake installer websites mimicking legitimate software and used them in phishing campaigns. The actor targeted users at Ukrainian government and military organizations to deliver RomCom and likely to obtain credentials of high-value targets.

To read more: <https://www.microsoft.com/en-us/security/blog/2023/07/11/storm-0978-attacks-reveal-financial-and-espionage-motives/>

Cyber Risk GmbH

Cyber Risk GmbH has been established in Horgen, Switzerland, by George Lekatis, a well-known expert in risk management and compliance.



Online Training

Recorded on-demand training and live webinars.

[More »](#)



In-house Training

Engaging training classes and workshops.

[More »](#)



Social Engineering

Developing the human perimeter to deal with cyber threats.

[More »](#)



For the Board

Short and comprehensive briefings for the board of directors.

[More »](#)



Assessments

Open source intelligence (OSINT) reports and recommendations.

[More »](#)



High Value Targets

They have the most skilled adversaries. We can help.

[More »](#)

Cyber security training

Overview

The world of cyber security and privacy is constantly changing. Today, effective cyber security programs involve the entire organization and not only the IT or the information security teams. Employees that have access to critical assets of an organization, have become primary targets of cyber attacks. Those that have access to technology and organizational assets are also responsible for the protection of those assets. Are they fit and proper to handle this responsibility? Do they have the awareness and skills necessary to meet these expectations?

Our training programs have the objective to help managers and employees not only understand the cyber security threats, but also their responsibility towards protecting the assets they handle. We explain how to proactively

apply good cyber security practices, how to identify threats and attacks, and what to do to protect themselves and their organizations. Cyber security is a shared responsibility.

Duration

We tailor each program to the needs of each client. We can provide trainings as short as one hour, but we can also deep dive into our topics for one or two days. The duration depends entirely on the needs, the agreed content of the program, and the case studies.

Our Education Method

In the core of our training approach is to ensure that our delivery is relatable, engaging, and interesting. We always make cyber security training an exciting adventure for our attendees. Our instructors have trained thousands of employees across the globe and have the skills and experience necessary to ensure that our attendees will enjoy the process while they learn. Our training programs may have workshop elements that get everyone involved.

Our Instructors

They are working professionals that have the necessary knowledge and experience in the fields in which they teach. They can lead full-time, part-time, and short-form programs that are tailored to your needs. You will always know up front who the instructor of the training program will be.

Our websites include:

a. Sectors and Industries.

1. Cyber Risk GmbH - <https://www.cyber-risk-gmbh.com>
2. Social Engineering Training - <https://www.social-engineering-training.ch>
3. Healthcare Cybersecurity - <https://www.healthcare-cybersecurity.ch>
4. Airline Cybersecurity - <https://www.airline-cybersecurity.ch>
5. Railway Cybersecurity - <https://www.railway-cybersecurity.com>
6. Maritime Cybersecurity - <https://www.maritime-cybersecurity.com>
7. Transport Cybersecurity - <https://www.transport-cybersecurity.com>

8. Transport Cybersecurity Toolkit - <https://www.transport-cybersecurity-toolkit.com>
9. Hotel Cybersecurity - <https://www.hotel-cybersecurity.ch>
10. Sanctions Risk - <https://www.sanctions-risk.com>
11. Travel Security - <https://www.travel-security.ch>

b. Understanding Cybersecurity.

1. What is Disinformation? - <https://www.disinformation.ch>
2. What is Steganography? - <https://www.steganography.ch>
3. What is Cyberbiosecurity? - <https://www.cyberbiosecurity.ch>
4. What is Synthetic Identity Fraud? - <https://www.synthetic-identity-fraud.com>
5. What is a Romance Scam? - <https://www.romance-scams.ch>
6. What is Cyber Espionage? - <https://www.cyber-espionage.ch>
7. What is Sexspionage? - <https://www.sexspionage.ch>

c. Understanding Cybersecurity in the European Union.

1. The NIS 2 Directive - <https://www.nis-2-directive.com>
2. The European Cyber Resilience Act - <https://www.european-cyber-resilience-act.com>
3. The Digital Operational Resilience Act (DORA) - <https://www.digital-operational-resilience-act.com>
4. The Critical Entities Resilience Directive (CER) - <https://www.critical-entities-resilience-directive.com>
5. The Digital Services Act (DSA) - <https://www.eu-digital-services-act.com>
6. The Digital Markets Act (DMA) - <https://www.eu-digital-markets-act.com>

7. The European Health Data Space (EHDS) - <https://www.european-health-data-space.com>
8. The European Chips Act - <https://www.european-chips-act.com>
9. The European Data Act - <https://www.eu-data-act.com>
10. European Data Governance Act (DGA) - <https://www.european-data-governance-act.com>
11. The Artificial Intelligence Act - <https://www.artificial-intelligence-act.com>
12. The European ePrivacy Regulation - <https://www.european-eprivacy-regulation.com>
13. The European Cyber Defence Policy - <https://www.european-cyber-defence-policy.com>
14. The Strategic Compass of the European Union - <https://www.strategic-compass-european-union.com>
15. The EU Cyber Diplomacy Toolbox - <https://www.cyber-diplomacy-toolbox.com>

You may contact:

George Lekatis
General Manager, Cyber Risk GmbH
Dammstrasse 16, 8810 Horgen
Phone: +41 79 505 89 60
Email: george.lekatis@cyber-risk-gmbh.com
Web: www.cyber-risk-gmbh.com

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 prejudice 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.

General Terms and Conditions for all visitors to the Cyber Risk GmbH websites, and all legal transactions made through the Cyber Risk GmbH websites (hereinafter “GTC”):

<https://www.cyber-risk-gmbh.com/Impressum.html>