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

September 2021, top cyber risk and compliance related local news stories and world events

Dear readers,

The Swiss National Cybersecurity Centre (NCSC) is the Confederation's competence centre for cybersecurity. It is the first contact point for businesses, public administrations, educational institutions, and the general public for cybersecurity related problems. It is also responsible for the coordinated implementation of the 2018–2022 national strategy for the protection of Switzerland against cyber-risks (NCS).

In September, the NCSC once again received a large number of reports. Many reports are about classified ad scams where the victim is supposed to pay an advance fee despite selling an item. The fraudsters go to considerable lengths to persuade the victims to hand over their credit card details.

The NCSC received a large number of reports about WhatsApp messages for an apparent Coop competition. Numerous examples of this approach have been observed in the past using different company names, including

Migros, Mediamarkt and Rolex. After answering a few very simple questions, the victims are supposed to guess which package contains a gift card. Of course, everybody wins a gift card.

However, to receive the gift card, people must first forward the link via WhatsApp to 20 contacts or 5 groups. In this way, the attackers ensure that the scam is spread without them having to do anything.

Finally, the victims are supposed to register and give their mobile phone numbers. What they overlook in their haste is the note telling them that, by registering, they are signing up to weekly mobile phone costs of CHF 10.

So, in fact, not only do they not receive a gift card, but they also subscribe to a regular charge on their mobile phone bill.

- Be skeptical about messages claiming that you have won something.
- Be particularly careful if you must give your credit card details or phone numbers in order to access free offers.
- Do not forward such messages.
- If you provided your phone number, please contact your mobile provider.

The NCSC also regularly receives reports of scam attempts involving classified ad platforms. We all know the method in which the seller is supposed to transfer money to the buyer or to an apparent intermediary company (for example, for shipping fees that are to be prepaid by the seller) before the buyer gives a benefit.

In a new variant, the apparent buyers now try to persuade the sellers to hand over their credit card details. The fraudsters go to some lengths by setting up official-looking parcel delivery webpages to make the story more believable.

In the recently reported cases, the victims received an email with an apparent link to a Swiss Post webpage, on which the transfer can be made, and the promised price can be accessed. The webpage, which appears

official and has both the Swiss Post logo and a similar internet address, contains not only the fictitious name of the beneficiary, but also a description and picture of the goods for sale.

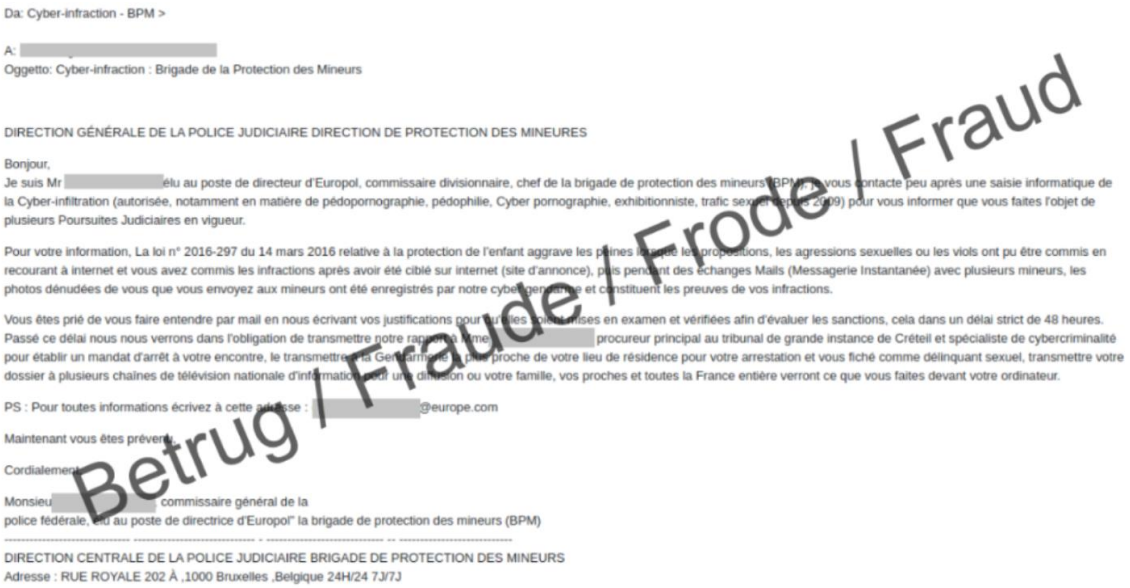
In other words, the attacker has set up a *personalized website for each seller!* This is of course all designed to dispel the victim's doubts and persuade them to click on the link.

If the victims click, they are diverted to a webpage asking them to enter their credit card details. The fraudsters' aim is to lull their victims into a false sense of security so that, in the second stage, they enter their credit card details without thinking about the fact that it makes no sense to do so to receive money.

For some time now, *fake threatening emails* have been circulating on the internet, claiming that recipients have allegedly been filmed visiting a pornographic websites. They threaten to publish the photo or video material if the ransom demanded is not paid by a certain deadline.

This is a bluff. The extortionists try their luck and send such emails in the hope that the recipients include people who recently visited pornographic websites.

Scammers are increasingly looking for new scenarios to make threats. For example, the NCSC noticed a sharp increase in emails in which the recipients are accused of having consumed child pornographic material. The recipients are asked to email a written statement of reasons to the sender within 72 hours. Most of the time, this then leads to the payment of a surety to avoid arrest.



Da: Cyber-infraction - BPM >

A: [redacted]
Oggetto: Cyber-infraction : Brigade de la Protection des Mineurs

DIRECTION GÉNÉRALE DE LA POLICE JUDICIAIRE DIRECTION DE PROTECTION DES MINEURS

Bonjour,
Je suis Mr [redacted] élu au poste de directeur d'Europol, commissaire divisionnaire, chef de la brigade de protection des mineurs (BPM) je vous contacte peu après une saisie informatique de la Cyber-infiltration (autorisée, notamment en matière de pédopornographie, pédophilie, Cyber pornographie, exhibitionniste, trafic sexuel [illegible]2009) pour vous informer que vous faites l'objet de plusieurs Poursuites Judiciaires en vigueur.

Pour votre information, La loi n° 2016-297 du 14 mars 2016 relative à la protection de l'enfant aggrave les peines lorsque les propositions, les agressions sexuelles ou les viols ont pu être commis en recourant à internet et vous avez commis les infractions après avoir été ciblé sur internet (site d'annonce), puis pendant des échanges Mails (Messagerie Instantanée) avec plusieurs mineurs, les photos dénudées de vous que vous envoyez aux mineurs ont été enregistrés par notre cyber gendarmerie et constituent les preuves de vos infractions.

Vous êtes prié de vous faire entendre par mail en nous écrivant vos justifications pour qu'elles soient mises en examen et vérifiées afin d'évaluer les sanctions, cela dans un délai strict de 48 heures. Passé ce délai nous nous verrons dans l'obligation de transmettre notre rapport à Mme [redacted] procureur principal au tribunal de grande instance de Créteil et spécialiste de cybercriminalité pour établir un mandat d'arrêt à votre encontre, le transmettre à la Gendarmerie la plus proche de votre lieu de résidence pour votre arrestation et vous fiché comme délinquant sexuel, transmettre votre dossier à plusieurs chaînes de télévision nationale d'information pour une diffusion ou votre famille, vos proches et toutes la France entière verront ce que vous faites devant votre ordinateur.

PS : Pour toutes informations écrivez à cette adresse : [redacted]@europe.com

Maintenant vous êtes prévenu.

Cordialement

Monsieur [redacted] commissaire général de la
police fédérale, élu au poste de directrice d'Europol" la brigade de protection des mineurs (BPM)

DIRECTION CENTRALE DE LA POLICE JUDICIAIRE BRIGADE DE PROTECTION DES MINEURS
Adresse : RUE ROYALE 202 À ,1000 Bruxelles ,Belgique 24H/24 7J/7J

Betrug / Fraude / Frode / Fraud

A supposedly official appearance is used to try to convince the victims that the emails are from the law enforcement authorities. In most cases, the logos and stamps of Europol, Interpol or the French police are used. However, the sender and documents are all bogus and private email addresses are in fact used to communicate with the victims.

In the past, the NCSC often received reports of supposed lawyers, notaries or even law enforcement agencies contacting victims following an investment scam – currently often involving cryptocurrencies – and promising to recover the lost money.

In September, an entire website offering such services was reported to the NCSC. The homepage has an advertisement to "get your money back if it was lost due to fraud". To do this, all that is required is the person's surname, first name and email address.

The name of the website "Kantonalberatung" suggests that it is an official cantonal office that supports victims of investment fraud. A quick look in the "Whois" directory for internet domains shows that the website was not registered until January 2021. There are also inconsistencies in the contact address: despite having its registered offices in Geneva and Jerusalem, the purported company has an Austrian telephone number. There is also no entry in the commercial register.

In these cases, after an initial free consultation, the victims are supposed to pay an advance "fee" in a second step. However, no guarantee is given that the money can be recovered. Here, the fraudsters take advantage of the victims' desperation and cheat them out of their money a second time.

In the past, the NCSC has warned about a fictitious hotel in Ticino that was looking for staff. If someone was interested in the position, the fraudsters demanded an advance payment of between EUR 300 and EUR 1,000 for a Swiss permit or for taking out health and accident insurance.

In September, the fraudsters have set up another fictitious hotel website. However, they have taken a few liberties with Swiss geography. The hotel is apparently located in "Montana" in the canton of Valais.

The photos show the hotel next to a large lake, whereas one would have expected to see the Valais Alps, since that region doesn't have a large lake.

More detailed research revealed that, in fact, the photos on the fake website were stolen from the websites of hotels on Lake Lucerne and in Boston.

The State Secretariat for Migration has published a corresponding warning:
https://www.sem.admin.ch/sem/en/home/sem/aktuell/betrug.html

In September, the NCSC received two reports on similar incidents, related to domain names which the original owner had closed down, but which had suddenly come back to life with the original content and domain.

The only discernible difference was that the resurrected websites were now advertising, more or less subtly, for online casinos which are forbidden in Switzerland.

This phenomenon is already well-known to the NCSC from previous cases. Often, the misappropriated websites have a small following, but one that is nonetheless interesting for the attackers. They exploit the ranking that the original websites have acquired in search engines.

If a relevant search term is entered, the attackers' newly resurrected website is displayed together with its content in the usual place, rather than the original site.

For the attackers, websites that display as the first result for a specific search term are most lucrative.

The attackers obtain the website's old content from web archiving services, which save earlier website versions and make them accessible – as we know, the internet never forgets. Both corporate and private websites are targeted, but those of clubs and local authorities, for example if they are no longer needed following a merger, are also popular targets.

In addition to the observed advertising for online casinos, the defunct domains are often also used to set up fraudulent web shops. Thus, it seems to be worthwhile for an attacker to pay the small fee to register a defunct website and then reactivate the site for their own aims, to obtain the corresponding search ranking.

Thank you Swiss National Cybersecurity Centre (NCSC), your contribution to cybersecurity in Switzerland is *very* important.

Supply chain refers to the ecosystem of processes, people, organizations, and distributors involved in the creation and delivery of a final solution or product.

In cybersecurity, the supply chain involves a wide range of resources (hardware and software), storage (cloud or local), distribution mechanisms (web applications, online stores), and management software.

We have a new paper from the European Network and Information Security Agency (ENISA) with title "*ENISA threat landscape for supply chain attacks*". According to the paper, supply chain attacks leverage the interconnectedness of the global markets.

When multiple customers rely on the same supplier, the consequences of a cyber-attack against this supplier are amplified, potentially resulting in a large-scale national or even cross-border impact.

For some products, such as software and executable code, the existence of a supply chain is opaque or even completely hidden to the end user.

End-user software depends, directly or indirectly, on software provided by the supplier. Such dependencies include packages, libraries, and modules — all of which are used pervasively to lower development costs and accelerate shipping times.

The better protected against cyber-attacks organizations become, the more the attention shifts to suppliers. The math is simple, suppliers are becoming the *weakest link* on the supply chain. At the same time, customers demand products that are more cybersecure but that remain at a low cost, two needs that it is not always possible to reconcile.

Read more at number 1 below.

Margaret Thatcher has said: "There are still people in my party who believe in *consensus politics*. I regard them as Quislings, as traitors... I mean it."

Although I do understand Margaret Thatcher's approach, I believe that *consensus* on a strategic approach to defending governments, organizations and companies in cyberspace is of paramount importance.

The Cyberspace Solarium Commission (CSC) was established in the John S. McCain National Defense Authorization Act for Fiscal Year 2019, to *"develop a consensus on a strategic approach to defending the United States in cyberspace against cyber-attacks of significant consequences."*

In January of 2021, the Cyberspace Solarium Commission released its *"Transition Book for the Incoming Biden Administration."* This document outlined *three areas* on which the new administration should focus in its first hundred days:

1. Establish the Office of the National Cyber Director;

2. Develop and promulgate a National Cyber Strategy; and

3. Improve the coherence and impact of existing government cybersecurity efforts and further strengthen partnerships with the private sector.

We read: "That those first hundred days have recently drawn to a close provides an opportunity both to evaluate whether the priority areas identified by the Commission have been addressed and to note where executive action in general is trending toward the implementation of Commission recommendations.

The context of the past several months, which have been fraught with repeated cyber incidents, becomes particularly pertinent as well.

The consequences of the SolarWinds compromise continue to unfold, even as major vulnerabilities are exploited in Microsoft Exchange Servers and as ransomware usage explodes, shutting down major critical infrastructure.

The administration should be commended for responding to these exigent circumstances—a monumental task—and progress in the response is evident in the May 12, 2021, executive order on improving the nation's cybersecurity.

While the demands of wrestling with these specific incidents have undoubtedly drawn time and attention away from other aspects of policy-making, they have also demonstrated the need for the coordination, coherence, and strategic guidance that improved policies could bring.

Efforts to address these three CSC 100-day priorities are under way to varying degrees, but only the first—establishing the Office of the National Cyber Director—is clearly on track to implementation, as is discussed at length below.

Meanwhile, a new national cyber strategy has not been released but is reportedly in process. The Interim National Security Strategic Guidance states that the administration "will elevate cybersecurity as an imperative across the government," and will encourage collaboration between the public and private sectors.

While the final result of the strategy development is not yet known, it is clear that its intent aligns with the Commission's priorities for executive action.

Beyond the priorities established in the Commission's transition book, early activity from the executive branch suggests progress on other CSC recommendations. One particular example is the February 2021 executive order on America's supply chains, which made major steps toward implementing the Commission's Recommendations 4.6 and 4.6.1, as well as the recommendations from the CSC white paper "Building a Trusted ICT Supply Chain."

The executive order initiated a series of reports that align with the first steps of the Commission's recommendations for developing an information communication technology supply chain strategy.

Similarly, the establishment of a cybersecurity working group involving the United States, Japan, India, and Australia, formed in March 2021, is a major step towards implementing the activities described in Commission Recommendation 2.1.1, which calls for international engagement to strengthen norms of responsible state behavior."

Read more at number 4 below.

I have just read the *Joint Committee Report on Risks and Vulnerabilities in the EU Financial System – September 2021,* from the European Supervisory Authorities. It is interesting to see how the insurance sector worries about the risks in the banking sector.

We read: "Vulnerabilities in the banking sector could spill over to insurers and Institutions for Occupational Retirement Provision (IORPs), as they are interconnected with the banking sector through investments in assets issued by banks.

At the end of 2020 on average approximately 13.7% (EUR 1,179 tn) of insurers' total investment is concentrated towards banks.

Over the course of last year insurers have reduced their exposure by approximately two percentage points.

It is smaller for the IORPs sector compared to the insurance sector, but its exposure towards the banking sector is also material; this holds especially for some specific countries.

At the end of 2020, on average ca. 12% (EUR 140 bn) of IORPs total investment is concentrated towards banks."

We also read: "The European corporate sector has been significantly hit by the pandemic, but the extraordinary monetary and fiscal stimulus has helped mitigate its impact. PGS loans have facilitated the flow of lending and have been supportive in particular for the SME sector.

PGS loans of a total volume of EUR 381bn in Q1 2021 nevertheless indirectly increase sovereign exposure and may contribute to an increase of the nexus between banks and the sovereign they are domiciled in.

Exposure to PGS loans is mostly concentrated to a few Member States only. In light of increasing levels of public debt in the pandemic, sovereign debt sustainability can have a direct impact on banks' balance sheets.

Total direct exposure of EU banks towards general governments was at over EUR 3.2 trillion in Q4 2020. 51% of total direct exposure was towards the home country (50% in Q2 2020).

Similarly, in the insurance and IORP sector the risk that certain countries are more affected by the pandemic amplifies the concentration risk, both of which also have significant home bias in their investments.

Looking through the bond portfolio, holdings of insurers and IORPs' bonds continue to show significant home bias, whereas home bias for corporate bonds, representing 30% (EUR 2,677 bn.) of insurers' portfolio, is lower compared to government bonds (EUR 2,748 bn. of total investments).

Furthermore, one third of the corporate bonds (EUR 824 bn.) are issued by banks, adding additional vulnerabilities to insurers' portfolios."

I read the paper, and I have spent a couple of hours thinking about the *concentration risk*. Excessive concentrations of credit have been key factors in banking crises and failures. Non-credit concentrations include:

- elevated *interest rate risk* due to maturity concentrations;
- *liquidity risk* due to funding concentrations;
- *operational risks* associated with concentrations of certain lines of business, such as mortgage servicing.

Before the 2008 financial crisis, concentrations of commercial real estate (CRE) loans, energy loans, leveraged financing loans, collateralized debt obligations, counterparty credit, loans to emerging market countries, loan

participations, and agricultural loans, played major roles in the failure or material weaknesses of a large number of banks.

Other credit concentrations, such as loans secured by first liens on residential real estate, have historically posed fewer problems. However, during the recession beginning in 2008, the banking industry experienced significant losses in these exposures when the national housing market suffered broad declines in home values.

Read more at Number 9 below.

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

Number 1 (Page 14)

ENISA threat landscape for supply chain attacks

Number 2 (Page 17)

NIST Study on Kids' Passwords Shows Gap Between Knowledge of Password Best Practices and Behavior

Number 3 (Page 20)

Attackers use Morse code, other encryption methods in evasive phishing campaign

Microsoft 365 Defender Threat Intelligence Team

Number 4 (Page 23)

2021 ANNUAL REPORT ON IMPLEMENTATION

Number 5 (Page 26)

Model Risk Management

Number 6 (Page 29)

Alert (AA21-243A) - Ransomware Awareness for Holidays and Weekends

Number 7 (Page 31)

NCSC and Federal Partners Kick Off "National Insider Threat Awareness Month"

This Year's Campaign Focuses on Insider Threat and Workplace Culture; Marks Nearly 10 Years since Executive Order Creating National Insider Threat Task Force

Number 8 (Page 35)

Organisations continue to face cyber security challenges with hybrid working patterns

Number 9 (Page 37)

Joint Committee Report on Risks and Vulnerabilities in the EU Financial System – September 2021

Number 10 (Page 41)

ESAs highlight risks in phasing out of crisis measures and call on financial institutions to adapt to increasing cyber risks

Number 11 (Page 43)

The "SecureSME Tool"

Number 12 (Page 46)

Forged in the Fires of 9/11: Partnerships, Challenges, and Lessons Learned 20 Years Later

Christopher Wray, Director, Federal Bureau of Investigation
International Association of Chiefs of Police Annual Conference

Number 13 (Page 55)

Robotrolling 2021/2

Number 14 (Page 58)

HOW DID THE NORDIC-BALTIC COUNTRIES HANDLE THE FIRST WAVE OF COVID-19?

A STRATEGIC COMMUNICATIONS ANALYSIS - Published by the NATO Strategic Communications Centre of Excellence

NATO STRATEGIC COMMUNICATIONS CENTRE OF EXCELLENCE

Number 15 (Page 62)

Enabling Military Systems to Adapt to the Unexpected

Program aims to provide physical systems with ability to adapt to unexpected events in real-time and effectively communicate system changes to human and AI operators

DARPA DEFENSE ADVANCED RESEARCH PROJECTS AGENCY

Number 1

ENISA threat landscape for supply chain attacks

Supply chain attacks have been a security concern for many years, but the community seems to have been facing a greater number of more organized attacks since early 2020.

It may be that, due to the more robust security protection that organizations have put in place, attackers successfully shifted towards suppliers.

They managed to have significant impacts in terms of the downtime of systems, monetary losses and reputational damages, to name but a few.

The importance of supply chains is attributed to the fact that successful attacks may impact a large amount number of customers who make use of the affected supplier.

Therefore, the cascading effects from a single attack may have a widely propagated impact.

This report aims at mapping and studying the supply chain attacks that were discovered from January 2020 to early July 2021.

Based on the trends and patterns observed, supply chain attacks increased in number and sophistication in the year 2020 and this trend is continuing in 2021, posing an increasing risk for organizations.

It is estimated that there will be four times more supply chain attacks in 2021 than in 2020.

With half of the attacks being attributed to Advanced Persistence Threat (APT) actors, their complexity and resources greatly exceed the more common nontargeted attacks, and, therefore, there is an increasing need for new protective methods that incorporate suppliers in order to guarantee that organizations remain secure.

This report presents the Agency's Threat Landscape concerning supply chain attacks, produced with the support of the Ad-Hoc Working Group on Cyber Threat Landscapes.

Table 1: Proposed taxonomy for supply chain attacks. It has four parts: (i) attack techniques used on the supplier, (ii) assets attacked in the supplier, (iii) attack techniques used on the customer, (iii) assets attacked in the customer.

SUPPLIER		CUSTOMER	
Attack Techniques Used to Compromise the Supply Chain	Supplier Assets Targeted by the Supply Chain Attack	Attack Techniques Used to Compromise the Customer	Customer Assets Targeted by the Supply Chain Attack
Malware Infection	Pre-existing Software	Trusted Relationship [T1199]	Data
Social Engineering	Software Libraries	Drive-by Compromise [T1189]	Personal Data
Brute-Force Attack	Code	Phishing [T1566]	Intellectual Property
Exploiting Software Vulnerability	Configurations	Malware Infection	Software
Exploiting Configuration Vulnerability	Data	Physical Attack or Modification	Processes
Open-Source Intelligence (OSINT)	Processes	Counterfeiting	Bandwidth
	Hardware		Financial
	People		People
	Supplier		

The main highlights of the report include the following:

- A taxonomy to classify supply chain attacks in order to better analyse them in a systematic manner and understand the way they manifest is described.

- 24 supply chain attacks were reported from January 2020 to early July 2021, and have been studied in this report.

- Around 50% of the attacks were attributed to well-known APT groups by the security community.

- Around 42% of the analysed attacks have not yet been attributed to a particular group.

- Around 62% of the attacks on customers took advantage of their trust in their supplier.

- In 62% of the cases, malware was the attack technique employed.

- When considering targeted assets, in 66% of the incidents attackers focused on the suppliers' code in order to further compromise targeted customers.

- Around 58% of the supply chain attacks aimed at gaining access to data (predominantly customer data, including personal data and intellectual property) and around 16% at gaining access to people.

- Not all attacks should be denoted as supply chain attacks, but due to their nature many of them are potential vectors for new supply chain attacks in the future.

- Organizations need to update their cybersecurity methodology with supply chain attacks in mind and to incorporate all their suppliers in their protection and security verification.

To read more: https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

Table 2: Attack techniques used to compromise the supplier in the chain. Each technique identifies how the attack happened, and not what was attacked. Several techniques may be used in the same attack.

ATTACK TECHNIQUES USED TO COMPROMISE A SUPPLY CHAIN	
Malware Infection	e.g. spyware used to steal credentials from employees.
Social Engineering	e.g. phishing, fake applications, typo-squatting, Wi-Fi impersonation, convincing the supplier to do something.
Brute-Force Attack	e.g. guessing an SSH password, guessing a web login.
Exploiting Software Vulnerability	e.g. SQL injection or buffer overflow exploit in an application.
Exploiting Configuration Vulnerability	e.g. taking advantage of a configuration problem.
Physical Attack or Modification	e.g. modify hardware, physical intrusion.
Open-Source Intelligence (OSINT)	e.g. search online for credentials, API keys, usernames.
Counterfeiting	e.g. imitation of USB with malicious purposes.

Number 2

NIST Study on Kids' Passwords Shows Gap Between Knowledge of Password Best Practices and Behavior

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

When it comes to passwords, the challenges are endless. We must create multiple passwords to manage our many online accounts, from email to shopping sites and social media profiles.

We have to safely keep track of these many passwords and ensure they're strong enough to reduce the risk of cyberattacks.

All of these reasons emphasize why education and training are so important for strengthening passwords and protecting personal accounts.

The problem isn't limited to just adults. Children may seem more technologically savvy because they've grown up in the digital space, but they still face the same cybersecurity threats.

So, to shed light on what kids understand about passwords and their behavior in creating and using them, researchers at the National Institute of Standards and Technology (NIST) conducted a study that surveyed kids from third to 12th grade.

The study found that children are learning best practices, such as memorizing passwords, but are demonstrating a gap between their knowledge of good password practices and their behavior.

The NIST researchers present their findings today at a virtual cybersecurity conference called USENIX Security Symposium 2021.

According to recent data from the Pew Research Center, more than one-third of parents with a child younger than 12 say their child began interacting with a smartphone before the age of 5, and 67% of parents say their child uses or interacts with a tablet computer. You may visit: https://www.pewresearch.org/internet/2020/07/28/childrens-engagement-with-digital-devices-screen-time/

"Younger children rely on parents a lot. Their first passwords were either given to them at school or by a parent to open their phone or tablet. So, what kind of guidance can we provide?" said NIST researcher Yee-Yin Choong.

The researchers surveyed more than 1,500 kids from ages 8 to 18 who attended schools across the South, Midwest and Eastern regions of the U.S. Teachers administered two versions of the survey, one for third to fifth graders and the other for sixth to 12th graders. Each survey featured the same questions but had different age-appropriate language.

On the plus side, results from the study showed that kids are learning best practices on passwords, such as limiting their writing of passwords on paper, keeping their passwords private, and logging out after online sessions. They're also not burdened with a lot of passwords as adults are, with kids on average reporting they have two passwords for school and two to four for home.

The passwords that kids created often consisted of concepts reflecting the current state of their lives. Passwords referenced sports, video games, names, animals, movies, titles (such as "princess"), numbers and colors. Examples included "yellow," "doggysafesecure" and "PrincessFrog248."

Password strength increased from elementary to high school students. Examples of stronger passwords among middle and high school students included "dancingdinosaursavrwhoop164" and "Aiken_bacon@28."

But despite the evidence that kids are learning best practices, they also demonstrated bad password habits. They tended to reuse passwords, a habit that increased in frequency from elementary to high school students, and shared their passwords with their friends. "For adolescents, an important part of building friendships is building trust, which is shown with sharing secrets. Their perspective is that sharing passwords is not risky behavior," said Choong.

The study also shed light onto what kids thought about passwords. The survey asked, "Why do people need passwords?" The answers were different for younger and older kids. Elementary students said safety was the primary reason, while for middle and high school students, privacy became more a more dominant answer.

Another notable finding was that younger kids relied on family support for creating and maintaining their passwords at home. This suggests that families play a central role in establishing best practices and that parents affect kids' behavior with passwords.

Not many studies have been performed on kids and cybersecurity, said Choong, which is why this work could be significant in helping researchers understand more about kids' password use.

"This was a very carefully designed study. We had to think carefully about the methodology," said Choong. Researchers contacted the principal of each school first to gain school support for the research, she said. They also worked with the teachers in getting parental consent and administering the surveys.

In future work, the NIST researchers will move outside the scope of passwords to investigate children's and parents' perceptions of online security, privacy and risky behaviors.

"The end goal of this research is to better support children and provide recommendations that can be used to provide guidance to them, parents and educators. Overall, the focus is on providing guidelines and best practices so that they can stay safe and secure online while enjoying the benefits of the internet," said Choong.

Number 3

Attackers use Morse code, other encryption methods in evasive phishing campaign

Microsoft 365 Defender Threat Intelligence Team

Microsoft

Cybercriminals attempt to change tactics as fast as security and protection technologies do. During our year-long investigation of a targeted, invoice-themed XLS.HTML phishing campaign, attackers changed obfuscation and encryption mechanisms every 37 days on average, demonstrating high motivation and skill to constantly evade detection and keep the credential theft operation running.

This phishing campaign exemplifies the modern email threat: sophisticated, evasive, and relentlessly evolving.

The HTML attachment is divided into several segments, including the JavaScript files used to steal passwords, which are then encoded using various mechanisms.

These attackers moved from using plaintext HTML code to employing multiple encoding techniques, including old and unusual encryption methods like Morse code, to hide these attack segments.

Some of these code segments are not even present in the attachment itself. Instead, they reside in various open directories and are called by encoded scripts.

In effect, the attachment is comparable to a jigsaw puzzle: on their own, the individual segments of the HMTL file may appear harmless at the code level and may thus slip past conventional security solutions. Only when these segments are put together and properly decoded does the malicious intent show.

This campaign's primary goal is to harvest usernames, passwords, and—in its more recent iteration—other information like IP address and location, which attackers use as the initial entry point for later infiltration attempts.

As we previously noted, the campaign components include information about the targets, such as their email address and company logo. Such details enhance a campaign's social engineering lure and suggest that a prior reconnaissance of a target recipient occurs.

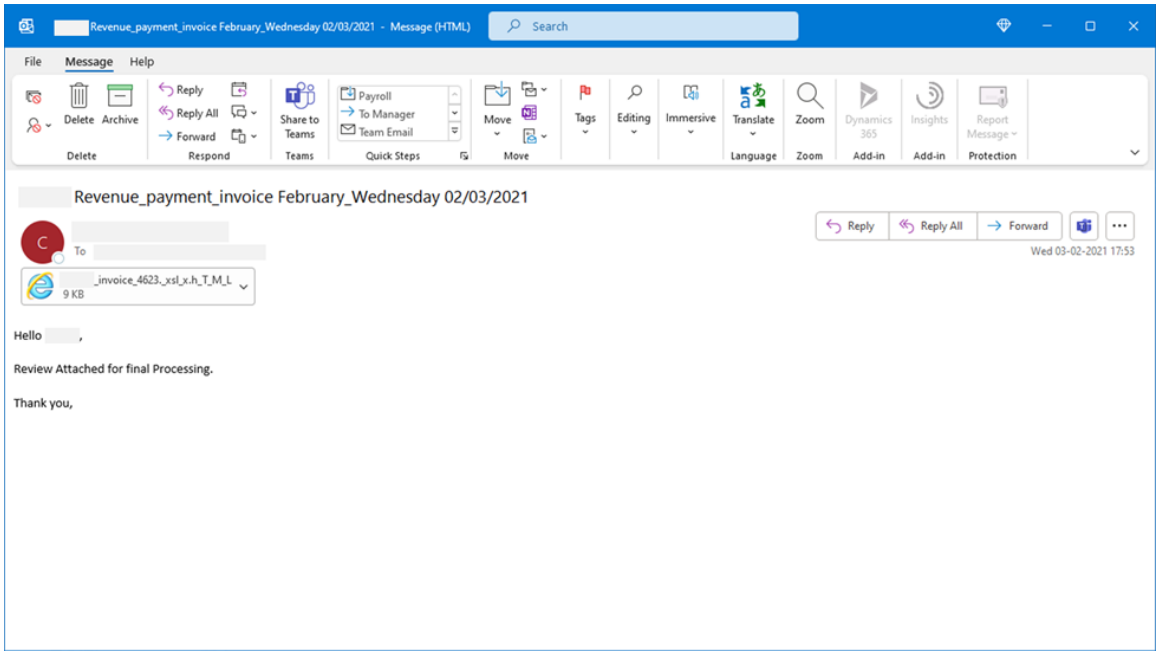
Email-based attacks continue to make novel attempts to bypass email security solutions. In the case of this phishing campaign, these attempts

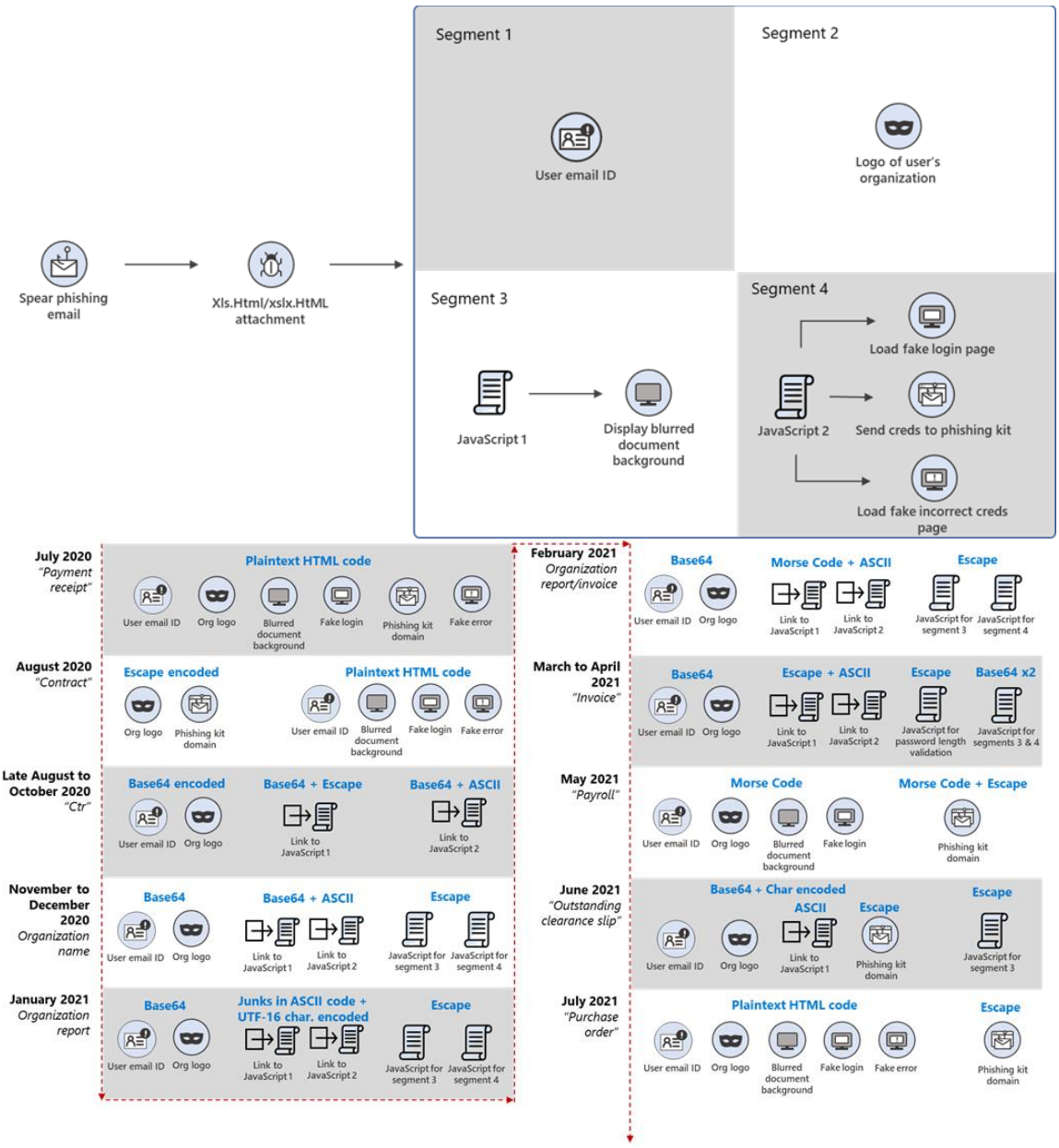
include using multilayer obfuscation and encryption mechanisms for known existing file types, such as JavaScript. Multilayer obfuscation in HTML can likewise evade browser security solutions.

To defend organizations against this campaign and similar threats, Microsoft Defender for Office 365 uses multiple layers of dynamic protection technologies backed by security expert monitoring of email campaigns.

Rich email threat data from Defender for Office 365 informs Microsoft 365 Defender, which provides coordinated defense against follow-on attacks that use credentials stolen through phishing.

Microsoft 365 Defender does this by correlating threat data from email, endpoints, identities, and cloud apps to provide cross-domain defense.

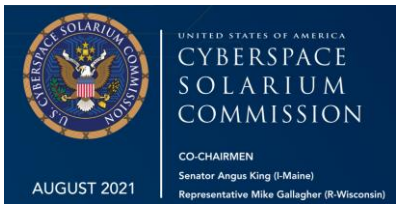




To read more:
https://www.microsoft.com/security/blog/2021/08/12/attackers-use-morse-code-other-encryption-methods-in-evasive-phishing-campaign/

Number 4

2021 ANNUAL REPORT ON IMPLEMENTATION



The digital connectivity that has brought economic growth, technological dominance, and an improved quality of life to nearly every American has also created a strategic dilemma.

The United States now operates in a cyber landscape that requires a level of data security, resilience, and trustworthiness that neither the U.S. government nor the private sector alone is currently equipped to provide.

Moreover, shortfalls in agility, technical expertise, and unity of effort, both within the U.S. government and between the public and private sectors, are growing.

For more than 20 years, nation-states and non-state actors have leveraged cyberspace to subvert American power, American security, and the American way of life.

The perpetrators of these cyberattacks exploited weaknesses in both systems and strategy and assessed that their forays damaged the United States without triggering any significant retaliation.

American restraint was met with unchecked predation.

The U.S. Cyberspace Solarium Commission (CSC) was established in the John S. McCain National Defense Authorization Act for Fiscal Year 2019 to address these challenges and "develop a consensus on a strategic approach to defending the United States in cyberspace against cyber attacks of significant consequences."

To meet its mandate, the CSC produced a final report, published in March 2020, outlining a strategic approach and 82 recommendations for the U.S. government.

In developing the final report, task forces met with more than 300 stakeholders from industry; academia; federal, state, and local governments; international organizations; and think tanks, and they

stress-tested their recommendations through a series of red team reviews and a scenario-based Solarium event.

Following the Solarium event, the Commissioners assessed each strategy and its supporting policy recommendations, providing formal feedback.

The staff tabulated this feedback and used the insights and guidance to further refine the recommendations.

In the months following the launch of the final report, Commissioners and staff produced legislative proposals (where appropriate) to support its recommendations, and worked with relevant committees in the House and Senate to implement many of the Commission's original recommendations.

In addition, the Commission issued four white papers with new and updated recommendations: they addressed lessons on cybersecurity from the pandemic, details on the national cyber director recommendation, a framework for a cybersecurity workforce development strategy, and proposals on how to secure America's information and communications technology (ICT) supply chains.

A fifth white paper, published in January 2021, highlighted specific priorities for the incoming Biden-Harris administration.

Many of the Commission's key recommendations have been enacted in legislation, but there is still more work to be done to meet the urgent challenges facing our nation, and much can be achieved through coordinated and thoughtful executive action.

This assessment is intended to review the implementation of the recommendations made by the Commission over the course of the previous year. The recommendations themselves are discussed in more detail in the Commission's final report and accompanying white papers.

The report:
https://drive.google.com/file/d/19V7Yfc5fvEE6dGIoU_7bidLRf5OvV2__/view

IMPLEMENTATION STATUS	
	Implemented: Legislation has been passed, an executive order issued, or other definitive action taken.
	Nearing Implementation: The recommendation is included in legislation or an executive order that has a clear path to approval, or it is partially implemented in law/policy.
	On Track/Partial Implementation: The recommendation is being considered for a legislative vehicle, an executive order or other policy is being considered, or there are measurable/reported signs of progress.
	Progress Limited/Delayed: The recommendation has not been rejected, but it is not in a legislative vehicle and there are no known policy actions under way.
	Significant Barriers to Implementation: These recommendations are not expected to move in the immediate future but are ready to be taken up if future crises spur action.

Number 5

Model Risk Management

Office of the Comptroller of the Currency

The Office of the Comptroller of the Currency's (OCC) Comptroller's Handbook booklet, "Model Risk Management," is prepared for use by OCC examiners in connection with their examination and supervision of national banks, federal savings associations, and federal branches and agencies of foreign banking organizations (collectively, banks).

Each bank is different and may present specific issues. Accordingly, examiners should apply the information in this booklet consistent with each bank's individual circumstances.

This booklet aligns with the principles laid out in the "Supervisory Guidance on Model Risk Management" conveyed by OCC Bulletin 2011-12, "Sound Practices for Model Risk Management: Supervisory Guidance on Model Risk Management" (MRM Supervisory Guidance).

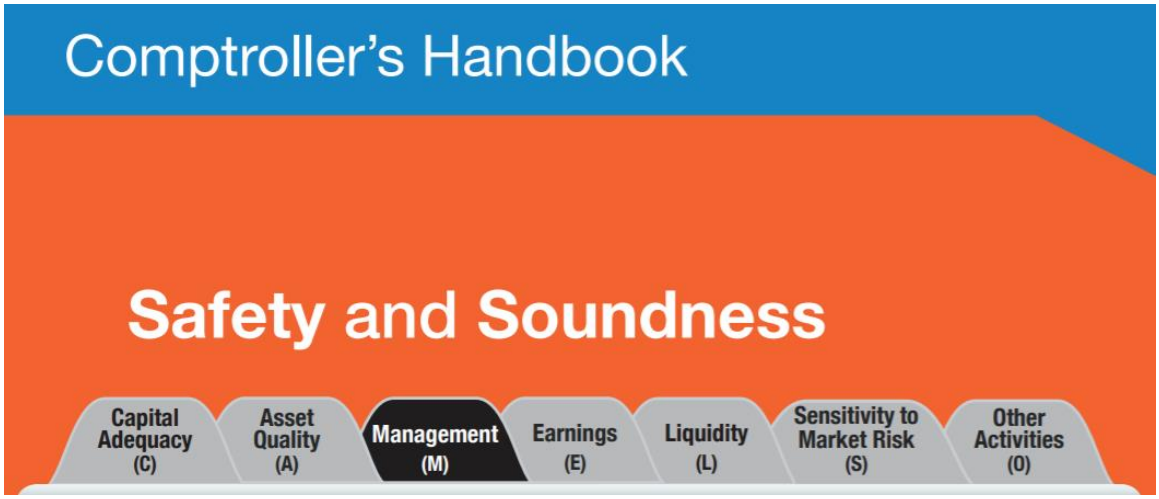
This booklet:

• is designed to guide examiners in performing consistent, high-quality model risk management examinations.

• presents the concepts and general principles of model risk management.

• informs and educates examiners about sound model risk management practices that should be assessed during an examination.

• provides information needed to plan and coordinate examinations on model risk management, identify deficient practices, and conduct appropriate follow-up.



You may visit: https://www.occ.treas.gov/publications-and-resources/publications/comptrollers-handbook/files/model-risk-management/index-model-risk-management.html

Number 6

Alert (AA21-243A) - Ransomware Awareness for Holidays and Weekends

The Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) have observed an increase in highly impactful ransomware attacks occurring on holidays and weekends—when offices are normally closed—in the United States, as recently as the Fourth of July holiday in 2021.

The FBI and CISA do not currently have any specific threat reporting indicating a cyberattack will occur over the upcoming Labor Day holiday.

However, the FBI and CISA are sharing the below information to provide awareness to be especially diligent in your network defense practices in the run up to holidays and weekends, based on recent actor tactics, techniques, and procedures (TTPs) and cyberattacks over holidays and weekends during the past few months.

The FBI and CISA encourage all entities to examine their current cybersecurity posture and implement the recommended best practices and mitigations to manage the risk posed by all cyber threats, including ransomware.

Threat Overview

Recent Holiday Targeting

Cyber actors have conducted increasingly impactful attacks against U.S. entities on or around holiday weekends over the last several months. The FBI and CISA do not currently have specific information regarding cyber threats coinciding with upcoming holidays and weekends.

Cyber criminals, however, may view holidays and weekends—especially holiday weekends—as attractive timeframes in which to target potential victims, including small and large businesses.

In some cases, this tactic provides a head start for malicious actors conducting network exploitation and follow-on propagation of ransomware, as network defenders and IT support of victim organizations are at limited capacity for an extended time.

- In May 2021, leading into Mother's Day weekend, malicious cyber actors deployed DarkSide ransomware against the IT network of a U.S.-based critical infrastructure entity in the Energy Sector, resulting in a week-long suspension of operations. After DarkSide actors gained access to the victim's network, they deployed ransomware to encrypt victim data and—as a secondary form of extortion—exfiltrated the data before threatening to publish it to further pressure victims into paying the ransom demand.

- In May 2021, over the Memorial Day weekend, a critical infrastructure entity in the Food and Agricultural Sector suffered a Sodinokibi/REvil ransomware attack affecting U.S. and Australian meat production facilities, resulting in a complete production stoppage.

- In July 2021, during the Fourth of July holiday weekend, Sodinokibi/REvil ransomware actors attacked a U.S.-based critical infrastructure entity in the IT Sector and implementations of their remote monitoring and management tool, affecting hundreds of organizations—including multiple managed service providers and their customers.

You may visit: https://us-cert.cisa.gov/sites/default/files/publications/AA21-243A-Ransomware_Awareness_for_Holidays_and_Weekends.pdf

Number 7

NCSC and Federal Partners Kick Off "National Insider Threat Awareness Month"

This Year's Campaign Focuses on Insider Threat and Workplace Culture; Marks Nearly 10 Years since Executive Order Creating National Insider Threat Task Force

The National Counterintelligence and Security Center (NCSC), the National Insider Threat Task Force (NITTF), the Office of the Under Secretary of Defense Intelligence and Security, the Defense Counterintelligence and Security Agency, and the Department of Homeland Security today launched the third-annual "National Insider Threat Awareness Month" (NITAM).

NITAM is an annual, month-long campaign during September to educate government and industry about the risks posed by insider threats and the role of insider threat programs.

Federal insider threat programs are composed of multi-disciplinary teams that address insider threats while protecting privacy and civil liberties of the workforce; maximizing organizational trust and ensuring positive work cultures that foster diversity and inclusion.

The NITAM campaign seeks to encourage employees in government and the private sector to recognize behaviors of concern and report them so early intervention can occur, leading to positive outcomes for at-risk individuals and reduced risks to organizations.

To learn more about the campaign and resources available to organizations, visit the NITAM 2021 website. You may visit: https://www.cdse.edu/itawareness/index.html

All organizations are vulnerable to insider threats. An insider threat is anyone with authorized access who uses that access to wittingly or unwittingly harm an organization or its resources.

Most insider threats exhibit risky behavior prior to committing negative workplace events. If identified early, many insider threats can be mitigated before harm occurs.

"The risks to government and industry from insider threats are severe. These threats can take many forms, whether it's a federal employee coopted by a foreign adversary to steal sensitive information or a corporate employee clicking on a spear-phishing link that infects their company's networks," said NCSC Acting Director Michael Orlando.

"Through this campaign, we hope to bring much-needed attention to insider threats and help organizations and their employees prevent and mitigate these issues early on."

This year's campaign focuses on insider threat and workplace culture. Organizations with positive and inclusive work cultures that foster trust between employees and leadership have more engaged and loyal employees and are better positioned to reduce insider threats.

Studies have demonstrated that disengaged workers have higher absenteeism, more accidents, and more errors, and that organizations with low employee engagement suffer from lower productivity, lower profitability, and lower job growth – all conditions that can contribute to insider threats.

Tomorrow, insider threat practitioners from across the U.S. government and industry will participate in the 2021 Insider Threat Virtual Conference, sponsored by the Department of Defense. You may visit: https://cdse-events.acms.com/content/connect/c1/7/en/events/event/shared/33897197/event_landing.html?sco-id=33880313&_charset_=utf-8

The conference features senior level speakers and panelists who will present on the current state of federal and industry insider threat programs; the importance of and strategies for developing positive organizational culture and sub-culture in combating the insider threat; and resources for training and professionalization of the insider threat practitioner community.

Recent examples underscore the damage that can be caused by insider threats:

- In July 2021, a 20-year-old sailor who had failed in his attempt at becoming a Navy SEAL was charged with deliberately setting fire to the USS Bonhomme Richard, an 800-foot Navy amphibious assault ship. The USS Bonhomme Richard went up in flames on July 12, 2020, burning for several days while docked in San Diego and causing some 60 people to be treated for injuries. The Navy later decided against repairing the vessel after determining it would cost an estimated $3

billion and take more than five years. The Navy officially decommissioned the USS Bonhomme Richard this year.

- In April 2021, a Ph.D. chemist who had worked at Coca-Cola and Eastman Chemicals was convicted of conspiracy to steal trade secrets, economic espionage, and wire fraud. According to court documents, the chemist stole trade secrets that cost some $120 million to develop in order to help a new company in China that had received millions of dollars in grants from the Chinese government. The chemist sought to benefit not only the Chinese company, but also the Chinese government and Communist Party.

The launch of this year's campaign marks nearly a decade since an October 2011 Executive Order that required all federal agencies with access to classified information to have their own insider threat prevention programs and directed the creation of the NITTF under the leadership of the Attorney General and the Director of National Intelligence.

NITTF is currently housed at NCSC. Since its inception, the NITTF has worked with federal agencies to build programs that deter, detect, and mitigate insider threats.

NITTF and NCSC coordinate insider threat training and awareness; liaison and assistance; governance and advocacy; and research and analysis for stakeholders in the public and private sector to reduce the risk of insider threats to public health and safety, economic security, and national security.

In recent years, NCSC and NITTF have expanded their outreach to help private sector entities address insider threats.

In March 2021, NCSC published Insider Threat Mitigation for U.S. Critical Infrastructure Entities: Guidelines from an Intelligence Perspective, and in July 2021, NCSC and the Department of Defense's Center for Development of Security Excellence (CDSE) collaborated to publish Insider Risk Implementation Guide for the Food and Agriculture Sector.

You may visit:
https://www.dni.gov/files/NCSC/documents/nittf/20210319-Insider-Threat-Mitigation-for-US-Critical-Infrastru-March-2021updated-5Apr21b.pdf

https://www.dni.gov/files/NCSC/documents/nittf/Insider_Risk_Implementation_Guide_for_Food_and_Agriculture20210708.pdf

Insider Risk Mitigation Programs
Food and Agriculture Sector Implementation Guide

Number 8

Organisations continue to face cyber security challenges with hybrid working patterns

National Cyber Security Centre

Coronavirus caused many organisations to move to home working at a greater speed and scale than many had foreseen or prepared for.

As organisations look to make hybrid working patterns a permanent option for staff the cyber security challenges brought by home working continue.

A recent survey from Palo Alto Networks looked at the impact of working from home decisions. You may visit: https://start.paloaltonetworks.com/state-of-hybrid-workforce-security-2021

44% stated that while money was spent improving remote access to corporate networks it was not matched by investment in cyber security. Meanwhile 21% said little had changed in their existing network architecture or security.

The NCSC issued guidance on preparing for home working and using video conferencing tools (availability of good communications was one of the tools cited that helped reduce security incidents). You may visit: https://www.ncsc.gov.uk/guidance/home-working

Further guidance on cloud security and device security is also available from the NCSC.

You may visit: https://www.ncsc.gov.uk/collection/cloud-security

National Cyber Security Centre

Home working:
Managing the cyber risks

Working from home is not new to many of us, but the coronavirus (COVID 19) means organisations are using home working on a greater scale, and for longer periods. This page will help organisations introducing (or scaling up) home working. It also provides advice on spotting COVID-19 scam emails.

Cyber criminals are preying on fears of COVID-19 and sending scam emails. These may claim to have a cure for the virus, offer a financial reward, or might encourage you to donate. If clicked, you're sent to a dodgy website which could download viruses onto your device, or steal your passwords.

Don't click on any such links. For genuine information about the virus, please use trusted resources such as the **Public Health England** or **NHS** websites.

If you' ve already clicked, don't panic:

- open your antivirus software and run a full scan, following any instructions
- if you've been tricked into providing your password, you should change your passwords on all your other accounts
- if you're using a work device, contact your IT department and let them know
- if you have lost money, you need to report it as a crime to Action Fraud (you can do this by visiting **www.actionfraud.police.uk**)

© Crown Copyright 2020

1. Setting up user accounts & accesses

Set strong passwords for user accounts; use NCSC guidance on passwords and review your password policy. Implement two-factor authentication (2FA) where available.

2. Preparing for home working

Think about whether you need **new** services, or to just **extend** existing services so teams can still collaborate. NCSC guidance on implementing Software as a Service (SaaS) can help you choose and roll out a range of popular services. In addition:

- **Consider producing 'How do I?' guides for new services so that your help desk staff aren't overwhelmed with requests for help.**
- **Devices are more likely to be stolen (or lost) when home working. Ensure devices encrypt data whilst at rest. Most modern devices have encryption built in, but may need to be turned on and configured.**
- **Use mobile device management (MDM) software to set up devices with a standard configuration in case the device needs to be remotely locked, or have data erased from it.**
- **Make sure staff know how to report any problems, or raise support calls. This is especially important for security issues.**
- **Staff feeling more exposed to cyber threats when home working should work through the NCSC's Top Tips for Staff e-learning package.**

3. Controlling access to corporate systems

Virtual Private Networks (VPNs) allow home workers to securely access your organisation's IT resources (such as email). If you've not used one before, refer to the NCSC's VPN Guidance, which covers everything from choosing a VPN to the advice you give to staff.

If you already use a VPN, make sure it's fully patched. You may need extra licenses, capacity or bandwidth if you're supporting more home workers.

4. Helping staff to look after devices

Whether using their own device or the organisation's, ensure staff understand the risks of using them outside the office. When not in use, staff should keep devices somewhere safe.

Make sure they know what to do (and who to call) if devices are lost or stolen. Encourage users to report any losses as soon as they can.

Ensure staff understand how to keep software and devices up-to-date, and that they apply updates promptly.

5. Using removable media safely

USB drives may contain sensitive data, are easily lost, and can introduce malware into your systems. To reduce the likelihood of infection you can:

- disable removable media using MDM settings
- use antivirus tools where appropriate
- only permit the use of sanctioned products
- protect data at rest (encrypt) on removable media
- encourage alternative means of file transfer (such as online tools).

www.ncsc.gov.uk @NCSC National Cyber Security Centre @cyberhq

Number 9

Joint Committee Report on Risks and Vulnerabilities in the EU Financial System – September 2021

After over a year since the COVID-19 pandemic started, the financial sector has largely proved resilient in the face of its severe economic impact.

A range of fiscal, monetary and prudential response measures as well as the availability of capital buffers have been essential in dampening the impact of the crisis.

As the recovery begins, the appropriate phasing out of exceptional crisis measures plays a key role.

Despite the positive outlook, the expectations for economic recovery remain uncertain and uneven across member states. Vulnerabilities in the financial sector are increasing, not least because of side effects of the crisis measures, such as increasing debt levels and upward pressure on asset prices.

Also, expectations of inflation- and yield growth, as well as increased investor risk-taking and financial interconnectedness issues, might put additional pressure on the financial system.

Next to economic vulnerabilities, the financial sector is also increasingly exposed to cyber risk and informationand communication technology (ICT) related vulnerabilities.

Financial institutions have to rapidly adapt their technical infrastructure in response to the pandemic, and the crisis has acted as a catalyst for digital transformation more generally.

The reliance of the financial system on technology and the scope for cyber vulnerabilities have further increased.

The financial sector has been hit by cyber-attacks more often than other sectors, while across the digital economy cyber-criminals are developing new techniques to exploit vulnerabilities.

In light of the above-mentioned risks and uncertainties, the Joint Committee advises the ESAs, national competent authorities, financial institutions and market participants to take the following policy actions:

1. Financial institutions and supervisors should continue to be prepared for a possible deterioration of asset quality in the financial sector, notwithstanding the improved economic outlook.

In light of persisting risks and high uncertainties, supervisors should continue to closely monitor asset quality and provisioning in the banking sector, in particular of assets under support schemes. This includes identifying possible practices of under-provisioning.

Such monitoring is an important prerequisite when coordinating the unwinding of the various support measures.

2. As the economic environment gradually improves, the focus should in particular shift to allow a proper recognition of the consequences of the pandemic on banks' lending books, and that banks adequately manage the transition towards the recovery phase.

Banks may need to withstand possibly increasing credit risk losses, as a consequence of expiring payment moratoria and other public support measures, while maintaining adequate lending volumes.

Banks and borrowers experiencing financial difficulties should proactively work together to find appropriate solutions for their specific circumstances.

That should include not only financial restructuring, but also a timely recognition of credit losses. Other financial institutions, including investment funds, should monitor their investments in corporate bonds and into private lending.

3. Disorderly increases in yields and sudden reversals of risk premia should be closely monitored in terms of their impacts for financial institutions as well as for investors.

On the investor side, rising valuations across asset classes, massive price swings in crypto assets, and event-driven risks (such as GameStop, Archegos, Greensill) observed in 1Q21 amid elevated trading volumes raise questions about increased risk-taking behaviour and possible market exuberance.

Rising yields could result in higher funding costs for banks and increase default risks for corporates via higher borrowing costs.

Supervisors, policy makers and financial institutions should also continue to develop further actions to accommodate a "low-for-long" real

interest rate environment and risks its entails against the background of rising in inflation. This includes addressing overcapacities in the financial sector.

4. Policymakers, regulators, financial institutions and supervisors can start reflecting on lessons learnt from the COVID-19 crisis. While the EU economy is still subject to high risks, some lessons learnt have, for example, already been reflected in EIOPA's advice on the Solvency II review.

EIOPA recommends in its opinion that supervisors should have additional powers, including a macroprudential toolkit to tackle systemic risk, such as restrictions on distributions of dividends to preserve insurers' financial position in periods of extremely adverse developments.

In the banking sector, the crisis has underlined the need to advance the Banking Union, and to achieve its potential additional benefits of cross-border financial flows, private risk sharing, and exploiting economies of scale in a larger market.

The ongoing crisis also highlighted the critical importance of coordinated approaches among national competent authorities.

5. Financial institutions and supervisors should continue to carefully manage their ICT and cyber risks. They should ensure that appropriate technologies and adequate control frameworks are in place to address threats to information security and business continuity, including risks stemming from increasingly sophisticated cyber-attacks.

It will be important for EU financial institutions to achieve a high common level of digital operational resilience, and to swiftly put in place an EU-wide common framework for digital operational resilience.

An important aspect of digital operational resilience is proper management of risks around ICT outsourcing, including chain outsourcing. Additionally, there is increasingly a need for financial institutions to carry out resilience testing in proportion to the risks faced and in a consistent manner.

To read more: https://www.eiopa.europa.eu/sites/default/files/joint-committee/jc-2021-45-joint-committee-autumn-2021-report-on-risks-and-vulnerabilities.pdf?fbclid=IwAR1kJP7I_WF41wzeot_GQAb1P2NbcLB1AnucPdb2eNeuV4167HJVzRBlRZk

JOINT COMMITTEE REPORT ON

RISKS AND VULNERABILITIES IN THE EU FINANCIAL SYSTEM

SEPTEMBER 2021

Number 10

ESAs highlight risks in phasing out of crisis measures and call on financial institutions to adapt to increasing cyber risks

The three European Supervisory Authorities (EBA, EIOPA and ESMA - ESAs) issued their second joint risk assessment report for 2021. The report highlights the increasing vulnerabilities across the financial sector, the rise seen in terms of cyber risk and the materialisation of event-driven risks.

As the recovery begins, the appropriate phasing out of exceptional crisis measures plays a key role. Despite the positive outlook, the expectations for economic recovery remain uncertain and uneven across member states.

Vulnerabilities in the financial sector are increasing, not least because of side effects of the crisis measures, such as increasing debt levels and upward pressure on asset prices.

Expectations of inflation- and yield growth, as well as increased investor risk-taking and financial interconnectedness issues, might put additional pressure on the financial system.

The financial sector is also increasingly exposed to cyber risk. The financial sector has been hit by cyber-attacks more often than other sectors, while across the digital economy, cyber-criminals are developing new techniques to exploit vulnerabilities.

Financial institutions will have to rapidly adapt their technical infrastructure in response to the pandemic, and the crisis has acted as a catalyst for digital transformation more generally.

Finally, the materialisation of event-driven risks (such as GameStop, Archegos, Greensill), as well as rising prices and volumes traded on crypto-assets, raise questions about increased risk-taking behaviour and possible market exuberance.

Concerns about the sustainability of current market valuations remain, and current trends need to show resilience over an extended period of time for a more positive risk assessment.

In light of the above-mentioned risks and uncertainties, the ESAs advise national competent authorities, financial institutions and market participants to take the following policy actions:

- financial institutions and supervisors should continue to be prepared for a possible deterioration of asset quality in the financial sector, notwithstanding the improved economic outlook;

- as the economic environment gradually improves, the focus should shift to allow a proper assessment of the consequences of the pandemic on banks' lending books, and banks should adequately manage the transition towards the recovery phase;

- disorderly increases in yields and sudden reversals of risk premia should be closely monitored in terms of their impacts for financial institutions as well as for investors;

- financial institutions and supervisors should continue to carefully manage their ICT and cyber risks.

The ESAs also consider that policymakers, regulators, financial institutions and supervisors can start reflecting on lessons learnt from the COVID-19 crisis.

To read more:
https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Reports/2021/1019147/JC%202021%2045%20-%20Joint%20Committee%20Autumn%202021%20Report%20on%20Risks%20and%20Vulnerabilities.pdf

Number II

The "SecureSME Tool"

The European Union Agency for Cybersecurity (ENISA) announces the creation of the "SecureSME Tool". A practical and user-friendly tool facilitating SMEs to navigate to ENISA's tips, guidelines and recommendation.

According to the European Commission's data, small and medium-sized enterprises (SMEs) constitute 99% of all businesses in the EU and employ around 100 million people.

In order to overcome the challenges imposed by the COVID-19 pandemic many SMEs applied new business continuity measures and turned to new technologies such as adopting to cloud services, upgrading their internet services, improving their websites, and enabling staff to work remotely.

Although SMEs have turned to new technologies, they often fail to raise the level of their security, mainly due to the lack of funding and cybersecurity guidelines.

The European Union Agency for Cybersecurity is providing continuous support to SMEs.

In doing so the "SecureSME" Tool has been created as a means to raise awareness and help SMEs become digitally secure.

The "SecureSME" tool is a one-stop shop for European SMEs, which provides related cybersecurity recommendations, guidelines and tips in a simplistic and user friendly manner.

The goal of the tool is to support those businesses in securing their ICT services and infrastructure from cyberattacks and ensure business continuity.

The tool will be presented and become directly accessible to the public on the 8th September 2021, within the framework of the International Cybersecurity Forum (FIC 2021) in Lille, France.

ENISA is an active participant to the fair dedicated to public and private cybersecurity operators, by running an awareness campaign dedicated to SMEs.

What is the "SecureSME" Tool?

Cybersecurity doesn't necessarily have to be costly for SMEs to implement and maintain. There are several measures that can be implemented, without having to invest a large amount.

ENISA's ''SecureSME Tool'' is a dedicated platform designed to support small and medium size businesses in their efforts to become digitally secure. This is achieved through the provision of practical and concise cyber tips and guidelines on how to secure ICT infrastructure.

The "SecureSME" tool presents the following main sections of particular interest to SMEs:

- Cyber tips that include instructions on how to:

Protect Employees
Enhance Processes
Strengthen technical measures
Overcome Covid19 issues

- Videos

- Guidelines in relation to SME cybersecurity published by ENISA and Member States' National Authorities

- EU H2020 related projects

Background

"SecureSME" tool comes as the next step following the publication of the "Cybersecurity for SMEs" report by ENISA last June. The report provides SMEs with advice on how to successfully cope with cybersecurity challenges, particularly those resulting from the COVID-19 pandemic.

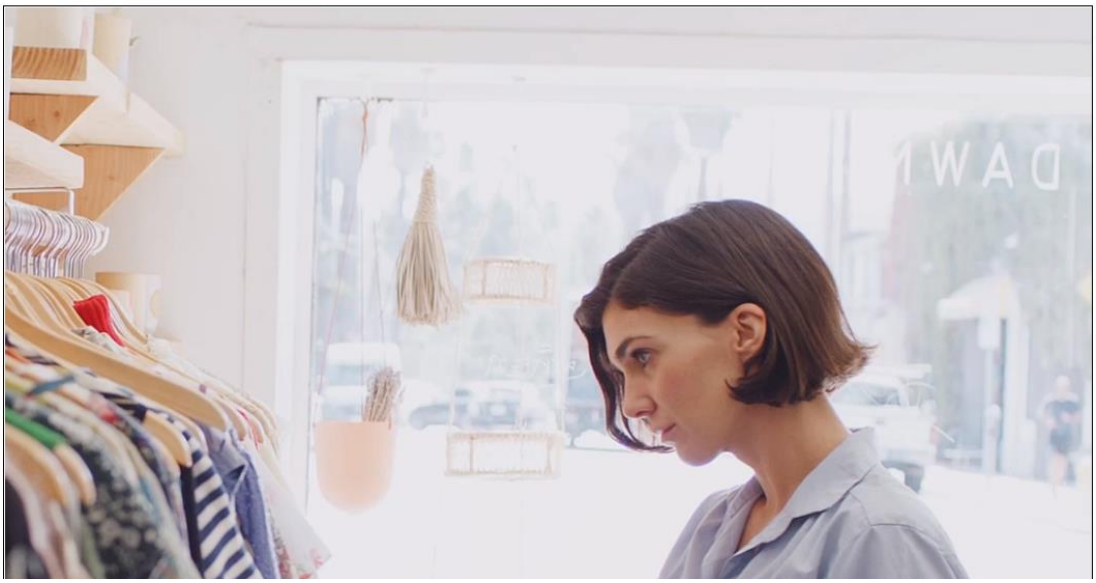
In addition to the report, ENISA also published a short cybersecurity guide in the form of a leaflet: "12 steps to securing your business", which provides SMEs with practical high-level actions to better secure their systems and hence their businesses.

To read more: https://www.enisa.europa.eu/news/enisa-news/new-tool-is-another-step-towards-securing-the-digital-future-of-smes

https://www.enisa.europa.eu/securesme#/

Cybersecurity for SMEs - 12 steps to securing your business

Small and Medium-sized enterprises are facing major cybersecurity challenges. In a time of increased remote work and growing cyber threats, low security budget and lack of cyber-skills can seriously impact their competitiveness.



Discover all Cyber Tips

Protect Employees

Enhance processes

Strengthen technical measures

Overcome COVID19 issues

Number 12

Forged in the Fires of 9/11: Partnerships, Challenges, and Lessons Learned 20 Years Later

Christopher Wray, Director, Federal Bureau of Investigation
International Association of Chiefs of Police Annual Conference

Thank you for the introduction, Cynthia, and thank you for inviting me to speak to IACP once again. Obviously, our hearts go out to everyone affected by Hurricane Ida—especially our colleagues in law enforcement and emergency response. And I'm grateful to everyone at IACP for pivoting so quickly and making it possible for us to meet virtually.

In our line of work, confronting and adapting to the unexpected is part of the job. Never was that more true than 20 years ago today—September 11, 2001 was one of the darkest days our nation has ever faced.

Just this morning I was in New York for the memorial ceremony, where family and friends read aloud the names of the nearly 3,000 innocent lives lost that day. Among them were more than 400 first responders—including more than 70 law enforcement officers.

The FBI lost two of our own that day: Special Agent Lenny Hatton and former Special Agent John O'Neill. That day, Lenny and John and hundreds more heroic men and women did what first responders always do: They put others before themselves and did whatever it took to rescue people and save lives.

On this solemn anniversary, we resolve once more to "never forget": to never forget the lives we lost on 9/11, to never forget the colleagues we've lost to 9/11-related illnesses since then, and to never forget the incredible bravery and sacrifices of our police, firefighters, and emergency personnel.

But there's one more thing I know you'll agree we should never forget—the spirit of unity and shared purpose that brought our nation together on September 12 and in the weeks and months that followed.

We in law enforcement and intelligence also felt that incredible spirit of solidarity in those days after 9/11. We'd always known that partnerships were important in our profession—but after that day, we realized they were something we couldn't function without. To prevent more 9/11s, we knew we had to build even stronger partnerships, work together even more closely, and share information even more seamlessly.

We've spent the last 20 years doing just that, together. And the changes we've made and the hard work we've done over those two decades have helped keep our country safe. That's something we should all be proud of.

Still, we can never rest on our laurels, because the threats keep shifting, and the challenges keep coming. So this afternoon, I want to talk to you about some of those challenges—and why the deeper partnerships we forged in the fires of 9/11 are so critical to confronting the threats we're up against today.

Lessons Learned

Twenty years ago, 9/11 forced those of us in law enforcement and intelligence to take a hard look at ourselves. At the FBI, we asked ourselves—what did we miss? What could we have done better to stop the attack before it happened?

Because of that terrible day, the Bureau transformed itself in ways that have made us stronger and better—and our country safer. And we couldn't have done it without your help.

We became an intelligence-driven, national security and law enforcement organization—one that collects, uses, and shares intelligence in everything we do. We developed new capabilities to combat the terrorist threat. And we changed our focus from investigating terrorist plots and attacks after the fact, to stopping them before they occur.

We built more integral partnerships with our law enforcement and intelligence community colleagues—starting by expanding and strengthening our task forces. They've grown, in fact, thrived in collaboration with hundreds of your departments nationwide, as we continue the critical work of protecting our country in a post-9/11 world. And in field office after field office, I see and hear how seamlessly our task force officers and agents work together.

Time and time again, when we've disrupted would-be terrorists before they strike; those cases have been driven by your frontline observations and your eagerness to share that reporting. That's why our partnerships remain paramount in the fight against terrorism. And that includes our

partnerships with community leaders, which we've also worked hard to improve since 9/11.

September 11 also taught us painful yet crucial lessons about the need to avoid complacency, and the need to keep innovating—because, as 19 hijackers armed with nothing more than box cutters showed us, the bad guys never stop innovating.

All these years later, the FBI still feels the ripple effects of the evolution in how we tackle our work. And not just in counterterrorism. We've applied the lessons we learned from 9/11 to every FBI program and every investigation, in every community we serve.

Current Terrorism Threat Picture

Of course, even as we all evolved in how we combat terrorism, the terrorist threat itself evolved as well.

Two decades after 9/11, we still face threats from al Qaeda and other foreign terrorist groups that want to carry out large-scale attacks here in the United States and around the world.

Some of those groups, like ISIS, use social media both to spread propaganda and to recruit and inspire followers to attack wherever they can, in whatever way they can. We also continue to track state-associated groups, like Iran's Islamic Revolutionary Guard Corps, that pose threats both at home and abroad.

But we also know that today's terror threat is different from what it was 20 years ago.

Today, the greatest terrorist threat we face in the U.S. is from lone actors. These include not only homegrown violent extremists, who take inspiration from foreign terror groups and ideologies, but also domestic violent extremists—especially racially or ethnically motivated violent extremists, and anti-government or anti-authority violent extremists.

Far too often, we're seeing people resort to violence to advance their ideological, political, or social goals. That's why, throughout the last year, the FBI has significantly surged resources to our increasing number of domestic terrorism investigations.

Bottom line: 20 years after 9/11, preventing terrorist attacks remains the FBI's top priority—now and for the foreseeable future.

Violent Crime Surge

But even as we counter the terrorism threat, we're staying laser focused on violent crime in our cities and communities. Mass shootings, gun violence, homicides, and aggravated assaults are all occurring at an appalling rate across the country, along with an uptick in reported hate crimes.

Today's violent crime situation is hellishly challenging—and for the Americans caught in the crosshairs of this surge in violent crime, it's just plain hell.

Like in Louisville, where homicides went up 92% in 2020—and are on pace this year to eclipse that, with more than 20 of those murder victims innocent children. Or in Dallas, or Milwaukee, where aggravated assaults are up—with Milwaukee, in particular, on track to surpass their 2020 rates for homicides, shootings, and carjackings, all by the end of this year.

Meanwhile, gangs in places like Memphis, Louisville, Chicago, and Oklahoma City are establishing narcotics pipelines to traffic heroin and other drugs throughout the Midwest and South. And in Phoenix, local gangs are working with transnational organized crime groups, helping them traffic people, drugs, and firearms throughout the Southwest.

Everyone listening to me knows all too well that the violent crime surge in our country is real and growing. It's taking the lives of too many innocent people, tearing apart too many communities, and denying too many Americans their basic right to feel safe in their own homes and neighborhoods.

Now I realize I'm preaching to the choir—because we all know that at all levels of government, our most fundamental duty is to safeguard people's right to live without fear of violence.

To meet this duty, we in the FBI know we've got to stand in lockstep with our law enforcement partners, now more than ever. And I can assure you we're using all of our tools and working strategically with our partners to face the violent crime surge head-on.

FBI Resources to Tackle Violent Crime

Across the country, we're determined to tackle violent crime together through our FBI Violent Crime, Safe Streets, and Safe Trails task forces. Just last year, our Safe Streets Task Forces made more than 6,000 arrests, seized more than 4,000 guns, and dismantled 80 violent gangs across the country.
To build on those task force efforts, in the coming months, the FBI will deploy new rapid response teams to some of the places hardest hit by the increased violence.

We'll be sending agents and intelligence analysts, surging resources and leveraging the intelligence we gather from violent crime investigations to help crack down on violent gangs and disrupt multi-state criminal enterprises.

As we confront the massive rise in violent crime, at the FBI it's all hands on deck—with every part of the Bureau, not just our violent crime task forces, sharing intelligence and resources to help our state, local, and tribal partners.

The FBI Lab is providing forensic analysis and testimony, shooting incident reconstruction, and support for searches of the 20 million DNA profiles in our National DNA Database.

The FBI-led National Gang Intelligence Center is supporting investigations with timely information on gang migration and criminal activity.

Our CJIS Division is working 24/7 to provide crucial data through systems like NCIC, NICS, and Next Generation Identification.

Our Critical Incident Response Group is deploying command post operations, tactical response, crisis negotiation, and behavioral analysis.

And our Victim Services Division is standing by to provide operational and victim support in crisis and mass-casualty events.

In all these ways and scores more, you can count on the entire FBI to stand shoulder-to-shoulder with you in the fight against violent crime.

The recent violent crime surge is a big challenge for all of us, and the way we'll meet it is with the same intelligence-driven, partnership-grounded approach that we've used successfully against the terrorist threat since 9/11.

Threats to Law Enforcement

Unfortunately, it's not just dangerous out there for the people we protect and serve; it's also dangerous for our officers, agents, and deputies. I want to sound the alarm again about another kind of emergency—one that threatens the very people Americans rely on to keep them safe.

Over the past year, we've seen a surge of violence against the law enforcement community. In just the first eight months of this year, 50 law enforcement officers have been feloniously killed on the job in our country—that's more than in all of 2020. Let me say that again, there have

been 50 officers murdered this year while doing their job to keep their communities safe.

I know some of you are all too familiar with the pain of losing your own in the line of duty. We are, too. Earlier this year two of our special agents, Laura Schwartzenberger and Dan Alfin, were shot and killed while serving a search warrant in Florida. And in July, one of our longtime task force officers, Detective Greg Ferency of the Terre Haute, Indiana, Police Department, was shot and killed in an ambush right outside one of our offices. Three of our own, murdered in just a few months.

As I never tire of telling people, it takes an incredibly special person to put his or her life on the line for a total stranger, day after day. When I started this job a little over four years ago, I made a point to know when any officer is murdered in the line of duty, so I can call the chief or sheriff of that department to offer the FBI's condolences and support.

Since August 2017, I've made more than 200 of those calls.

Enough is enough. As a country, we cannot blind ourselves to the sacrifices that law enforcement officers make every day. All of us—their law enforcement colleagues and the citizens they died protecting—owe these dedicated public servants a debt of gratitude.

Mental Health

Given all we're up against, it's no wonder that many of your officers feel beleaguered, underappreciated, and under siege. Which is why I want to turn to an issue that's sometimes hard to discuss, but vital to address—and that's the mental health and well-being of our people.

Our officers and agents offer a lot of the best humanity has to offer. Courage. Selflessness. Honor. But to do their jobs, they have to confront the worst that humanity has to offer.

That kind of ongoing stress and pressure is a lot of weight to carry, day after day. It's likely one of the reasons suicides have become an epidemic in law enforcement—and hardly any agency is immune. Last year, there were 174 officer suicides in our country.

We need to figure out exactly what's going on. That's why the FBI's Uniform Crime Reporting program is establishing a new data collection effort to better understand and prevent suicides among current and former law enforcement officers. Agencies can submit information about their officers who have attempted or died by suicide—and getting that information from all of you and the rest of our partners is essential.

Because when it launches next year, UCR's collection will include data on the circumstance and events before each suicide and attempt. The results—that intelligence—will be crucial to understanding the problem and finding solutions before it is too late.

But even more importantly, just as we do in every other battle, we need to draw on our partnerships. In this case, that means being the best possible partner to colleagues who are hurting and getting rid of the stigma that stops folks from seeking help.

These aren't 9-to-5 jobs with 9-to-5 pressures. So we need to tell our people it's okay to not be okay. It's okay to admit that—because that's not a sign of weakness, it's a sign of real strength. And we shouldn't wait. Taking care of ourselves and one another should be an all-the-time thing, not just something we think about when things become unbearable.

We want all our people around for the long haul—the country needs them around for the long haul—so let's make sure we're getting them the help they need, and let them know we're going to stand beside them, every step of the way.

Our Work: The Right Thing in the Right Way

Since becoming FBI Director, I've tried to drive home the importance of always doing the right thing, in the right way. The 20th anniversary of 9/11 is a fitting reminder of why that's so important.

9/11 showed us just how much is on the line in our work, how we're always just one attack away from a tragedy will change people's lives forever. Millions of people we'll never know are counting on us to do our jobs well—to get it right.

After 9/11, appreciation for law enforcement and our fellow first responders was near-universal. Folks understood that our work was about doing the right thing, and they recognized the nobility of our mission. A rising generation saw that, and as a result, scores of young people chose to pursue public service, including in law enforcement.

Twenty years later, we have fewer and fewer people who either worked for us during 9/11 or joined our ranks because of 9/11. It sounds hard to believe, but we now have agents and analysts joining the FBI who were only in elementary school when the 9/11 attacks happened—and in a few years we'll be hiring folks who weren't even alive on that fateful day.

So we need to make a special effort to ensure that September 11 and its lessons don't become some historical footnote—especially in the current

environment, when the negativity surrounding law enforcement has made recruiting tough for so many departments.

There's no question that law enforcement remains a noble profession. And I truly believe that—although sometimes it may not seem like it—folks still recognize and appreciate the sacrifices our people make.

As a new generation enters our ranks, it falls on those of us who lived through the post-9/11 transformation of our work to show them why it's so crucial to do things the right way. That takes a lot when your work is as hard and consequential as ours is—from precision and rigor, to uncompromising integrity, to following the facts wherever they lead, no matter who likes it. It also means setting aside concerns about who gets credit, and focusing on impact.

We've all seen firsthand how the shift away from turf battles and stove-piping, to sharing intelligence and strengthening our partnerships, gets results that keep people safer. And now the young men and women in our departments, who listen to and learn from us, don't know any other way than that post-9/11 shoulder-to-shoulder approach.

That's how it should be. That's how it needs to be. 9/11 should always remind us that we can't go back to the old ways. Because when we work in the right way, together—when we combine our unique capabilities and authorities, our strengths and assets—we're so much stronger than when we do the job alone.

Conclusion

I began today by recalling the solidarity and spirit of September 12, and the enduring resilience of this country and of our law enforcement family. There's perhaps no better symbol of that resilience than the Survivor Tree, which stands as part of the 9/11 Memorial in New York City.

A month after the terrorist attacks, recovery workers discovered a Callery pear tree buried in the rubble of the Twin Towers. It was badly damaged, its roots snapped, and its branches broken and burned. The tree was dug up from the ruins and placed in the care of the New York City Department of Parks and Recreation. They replanted it in a park in the Bronx, where it wasn't expected to survive.

But over the years, that pear tree recovered. It was returned to the 9/11 Memorial back in 2010. Today, smooth limbs extend from the tree's gnarled stumps, clearly showing the line between the tree's past and present—before 9/11 and after. It stands at the memorial as a living reminder of our country's enduring spirit and resilience.

Like that tree, our law enforcement family has its own clear line in our history—before 9/11 and after. We learned hard lessons from that terrible day. And we've experienced our own rebirth—one that has helped us to better protect all the people who are counting on us.

Thank you all for your leadership, and your partnership with the FBI. And thanks for listening to me today.

Number 13

Robotrolling 2021/2

In this edition of Robotrolling we track the most significant increase in inauthentic Russian-language social media activity we have observed since we began in 2017.

While the level of bot activity remains much lower than four years ago, the uptick is concerning.

The increased activity coincided with the spring and summer military exercise season, and the period running up to the Russian Federation's Zapad exercises, scheduled for September 2021.

While fake activity increased in the Russian-language space, we observed no increase in English-language activity, either from bots or from human-controlled accounts.

In this edition of Robotrolling, we introduce the *Global Database of Events Location and Tone (GDELT)*.

This database of news articles helps map how the conversation about NATO in Poland and the Baltics is covered by news media, and serves as a contrast to the environment observed on Twitter and VK.

This contrast reveals that in April 2021—as Russian troops mobilized along the Ukrainian border—inauthentic Russian accounts were also disproportionately active online.

We round off the issue with a discussion of how AI can help us better understand the global news environment in near-realtime, based on conversations with StratCom COE expert Gundars Bergmanis-Korāts and GDELT-founder Kalev Leetaru.

In this edition of Robotrolling, we continue to track manipulation on social media platforms about the NATO presence in Poland, Estonia, Latvia, and Lithuania.
Our analysis focuses on the activities of automated accounts (bots) and coordinated anonymous human accounts.

With this—our seventeenth—issue we are making a change to publishing the report biannually, with six-month reporting windows.

The period currently under consideration in this spring/summer issue is 1 February to 31 July 2021.

This window is compared and contrasted with the previous six months, 1 August 2020 to 31 January 2021.

In the Russian-language information space automated activity has increased markedly in the previous six months.

Currently, 36% of tweets come from automated accounts, constituting a 50% increase compared to the previous period.

English-language automated activity has also increased, but from a much lower comparative baseline.

Not only was bot messaging more widespread, but we also note a divergence in Russian- and English-language messaging volumes: the number of English messages (excluding retweets) about the NATO presence was unchanged at 11 200; Russian-language messages increased by 40% to 7 200.

On VK, the total messaging volume increased from 43 000 to 58 000 — a 35% increase.

Simultaneously, the percentage of automated Russian-language accounts increased on Twitter from 16% to 19% and on VK from 14% to 16%.

Automated activity on VK this quarter mirrored our findings for Twitter.

The proportion of bot activity increased along with message volume.

On VK, 56% of messages were posted in groups, an increase from 51% in the previous period.

The increased bot levels for spring and summer 2021 are a statistical outlier.

Since starting our observations in 2017 the overall trend has been for gradually declining levels of automated activity on Twitter, thanks to the company's efforts to clean up the platform.

The trend has stalled and may now even have reversed.

This change in trajectory coincides with the run-up to the Russian military's Zapad exercises to take place in September 2021.

As ever, social media companies should not rest on their laurels thinking the battle against bots has been won.

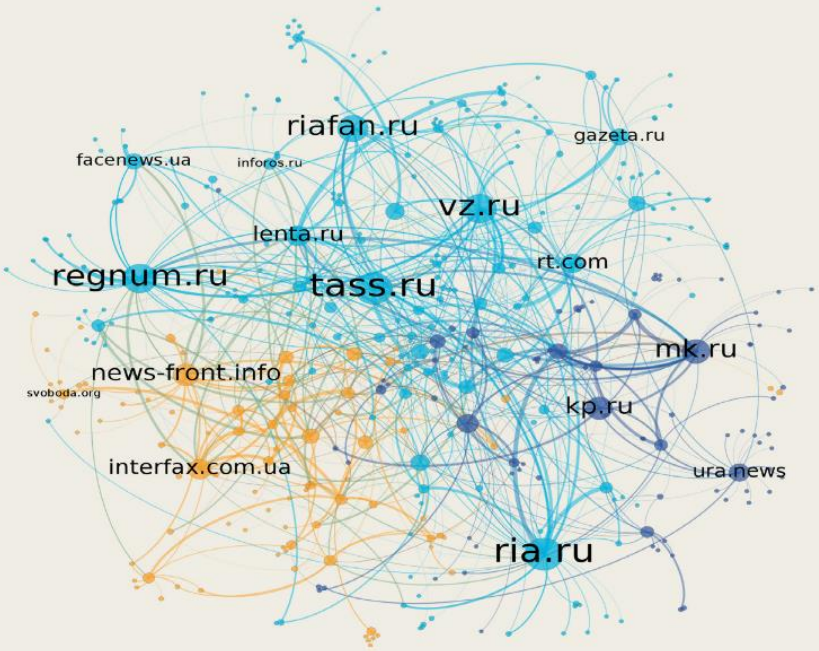


Figure 5: Russian-language news outlets, connected by similarity scores for articles mentioning NATO (July 2021).

To read more: https://stratcomcoe.org/publications/robotrolling-20212/214

Number 14

HOW DID THE NORDIC-BALTIC COUNTRIES HANDLE THE FIRST WAVE OF COVID-19?

A STRATEGIC COMMUNICATIONS ANALYSIS - Published by the NATO Strategic Communications Centre of Excellence

What is this project?

When the Covid-19 virus struck Europe in 2020 with the full force of a pandemic, eight countries allied in the Nordic-Baltic region immediately faced a challenge to their hard-won partnership.

For three decades Denmark, Estonia, Finland, Iceland, Latvia, Lithuania, Norway, and Sweden had been building a common purpose.

How would that friendship respond to the greatest health scare in a hundred years?

This report aims to answer this question by looking at developments in the Nordic-Baltic Eight (NB8) through a Strategic Communications lens.

Why a Strategic Communications lens?

To understand fully the pandemic that gripped these eight partner states is to paint a picture that goes beyond the number of human lives lost or the rise in unemployment, fall in national economic growth, and assumption of state debt so punitive to their taxpayers.

Any complete picture would also tell the story of how governments chose to speak to their electorates, and how civil society would respond to unprecedented measures imposed in peace time: curbing individual freedoms, it may be assumed, would elicit a consequent questioning of trust between government and governed.

All states communicate strategically. But that is not to say they engage in Strategic Communications. Which is understood as the shifting and shaping of significant discourses in societies.

It aspires to change the way people think and behave; in other words, to achieve a strategic effect. Inevitably, such an ambitious task requires separating out diverse audiences and honing particular approaches to appeal to those audiences' attitudes and grievances.

In trying to achieve a strategic effect – inshort, change – the strategic dimension of the term Strategic Communications sees strategy as focused on the long term; more specifically, its proponents play the long game.

However, the NB8 members in early 2020 would find themselves facing a national crisis on a scale they had not experienced since the Second World War.

Uneven levels of preparedness, despite repeated warnings from global health officials that dated back to the early years of this century, would suddenly demand governments act in ways for which their populations had not yet been prepared.

By the time the scale of the pandemic had been recognised by scientists and politicians, governments could be excused for having resorted to short term reactions expressed through crisis communications.

The latter, however necessary, live in constant tension with long term communications.

The aim, after all in Strategic Communications, is to ensure consistency and coherence between the demands of today and the ambitions of tomorrow.

How did the NB8 fare? The answer is not simple, especially when faced with the conundrum brought about by the Covid-19 pandemic.

From the outset, it was clear that the pandemic was as much political, economic, and social in its effect as it was bio-medical in its nature.

Governments across the world have since faced hard choices in balancing these threats against the well-being of their citizens while retaining friendly relations and long-term objectives in international politics.

The Nordic governments started from a strong position. The Nordic countries (Denmark, Finland, Iceland, Norway, Sweden) make up the world'seleventh largest economy.

Their populations show high levels of trust in government structures and law enforcement, and demonstrate a high degree of confidence in their partner states.

The same cannot be said of the Baltic countries. By comparison, trust in government is low and their economies are less prosperous.

Consequently, the Nordic countries spend above the European average on healthcare, whereas the Baltic countries allocate significantly less.

This context would influence the decisions of governments and the subsequent debate.

The Baltic countries would find themselves trapped between trying to maintain their under-funded health systems throughout stricter lock-downs, while at the same time fearing for the consequences for their economies.

Disinformation in the Baltics

From the beginning of the pandemic, the Baltic countries were concerned with the potential spread of disinformation, particularly emanating from the Kremlin.

Although the concern with disinformation was apparent in all Nordic-Baltic countries, Estonia, Latvia and Lithuania were particularly wary.

Since the restoration of Baltic independence, the Kremlin has worked to shape public opinion and politics in the Baltic countries by driving wedges between ethnic groups, sowing distrust in media outlets and governments, and undermining NATO and the EU.

Historical experience and large Russian-speaking minorities who consume Russian language media make Baltic governments particularly cautious.

Understandably perhaps, since investigative reports show Russian government officials, media outlets, proxy news sites, and social media accounts to have engaged in coordinated campaigns to spread disinformation on Covid-19 and Western-manufactured vaccines.

At a meeting in June 2020, the Presidents of Latvia and Estonia discussed how to manage the pandemic and remarked that the levels of disinformation had increased significantly, posing a threat to their societies.

In a recent meeting between the Foreign Ministers of the Baltic countries and the UK, the lack of resilience shared by democratic societies against Covid-19 related disinformation was raised as a major concern.

It was proposed that transatlantic partners pursue joint solutions to the threat posed by disinformation operations.

Baltic countries have been strong advocates for EU-level regulation to fight disinformation.

At the same time, Latvia has initiated a resolution since adopted by the United Nations in March 2021 to fight the spread of disinformation and misinformation, particularly in the context of the continuing pandemic.

Faced with the Covid-19 crisis, populations around the world have become more vulnerable. They face fear at the level of the individual, and instability at the community level.

Fear hinders rational judgement, rendering society more susceptible to disinformation and talk of conspiracies.

As research shows, emotionally packaged stigmas – unjustified disapproval of something or someone shared by a group – exert a particularly strong effect on people.

Consequently, it was perhaps to be anticipated that Moscow would leverage the stigma it has been creating and attaching to NATO and its Enhanced Forward Presence in the Baltics.

The pandemic has provided a new storyline for the Russian government to discredit NATO and its forces.

To read more: https://stratcomcoe.org/pdfjs/?file=/cuploads/pfiles/Nato-Covid19-Nordic-Baltic-d6933.pdf?zoom=page-fit

Number 15

Enabling Military Systems to Adapt to the Unexpected

Program aims to provide physical systems with ability to adapt to unexpected events in real-time and effectively communicate system changes to human and AI operators

Many complex, cyber-physical military systems are designed to last for decades but their expected functionality and capabilities will likely evolve over time, prompting a need for modifications and adaptation.

High Mobility Multipurpose Wheeled Vehicles (HMMWV), for example, had a design life of 15 years, but are now undergoing modernization to extend the average age of the fleet to 37+ years.

At design time, these systems are built to handle a range of expected operating environments and parameters.

Adapting them is currently done in an improvisational manner – often involving custom-tailored aftermarket remedies, which are not always commonly available, require a skilled technician to install, and can take months or even years to procure.

Further, as they evolve and are placed outside of their original design envelop these systems can fail unexpectedly or become unintentionally dangerous.

“Today, we start with exquisitely built control systems but then someone needs to add something or make a modification – all of which results in changes to the safe operating limits,” said DARPA program manager John-Francis Mergen. “These changes are done in a way that wasn’t anticipated – or more likely couldn’t have been anticipated – by the original designers. Knowing that military systems will undoubtedly need to be altered, we need greater adaptability.”

In response, DARPA developed the Learning Introspective Control (LINC) program. The program aims to develop machine learning (ML)-based introspection technologies that enable systems to adapt their control laws as they encounter uncertainty or unexpected events.

The program also seeks to develop technologies to communicate these changes to a human or AI operator while retaining operator confidence and ensuring continuity of operations.

"When a system 'wakes up' in a different space, it needs to be able to realize there are things it can't do anymore or new things it can, and 'learn' how to adapt to its new operating reality," noted Mergen. "With LINC, we want to provide physical systems with the ability to figure out what is still feasible, alert the operator, and then help them operate in that new space."

Developing LINC technologies will require addressing a specific set of challenges related to learning control and communicating situational awareness to the operator.

Current state of the art (SOTA) ML approaches are not robust to unknown or unstructured parameter uncertainty, owing largely to the bounds set on their operation at design time as well as their reliance on fixed assumptions about their operating model.

Further, complex systems – like drone swarms – are unable to rapidly converge on a common solution.

When damage occurs to a single drone, the swarm is unable to uniformly adapt, potentially resulting in a failed operator or unsafe operating conditions.

LINC's first research area will seek to overcome existing limitations in learning models and ML techniques that currently hamper system adaptation.

The program will explore how to provide a system with the ability to sense change and then reconstitute control using only onboard sensors and actuators.

LINC aims to develop new control regimes that detect and characterize changes in the system's operations in real-time, rapidly find solutions for reconstituting control under these changing conditions, and then calculate operating limits to identify a safe operating envelope.

"The idea is that you have a plethora of indigenous sensors on the system, and you can use these to determine and define a new set of control laws. With those new laws, you can then calibrate the system," said Mergen.

Another challenge area LINC seeks to address is around operator communications.

Today, operators are not often provided with sufficient explanations or guidance around a system's behavior or it's situation-specific operating limits.

Existing cues to operators about system dynamics don't always provide options, making it difficult for an operator to appropriately trust the information its receiving.

Further, interpreting current system diagnostics displays, which are not always intuitive, creates additional cognitive load for human operators.

This further erodes operator trust and can lead to misunderstanding, confusion, and incorrect actions.

A second research area will focus on improving how situational awareness and guidance are shared with the operator. This area will explore ways of translating and effectively communicating the operational information generated by the dynamic model developed under the first research area.

The resulting technologies must be able to provide the operator – whether human or AI – with updates on the operating status of the system as well as cues for safe actions. Further, they must be able to help retain operator trust by providing optionality and explainability around what's happening "under the hood."

A third research area will focus on testing and evaluating the resulting technologies. LINC expects to use demonstration platforms that will evolve in sophistication and complexity throughout the life of the program – starting with a realistic physical model and progressing to a military-relevant system in the program's final phase.

Interested proposers will have an opportunity to learn more about the Learning Introspective Control (LINC) program during a Proposers Day, which will be held on August 26, 2021, from 9:00 AM to 2:00 PM (ET) both at the DARPA Conference Center, located at 675 N. Randolph Street, Arlington, Virginia, 22203, and virtually through Zoom. Advance registration is required to attend. To learn more: https://sam.gov/opp/69db6bff225344f481f229edc1e2b97a/view

The LINC Broad Agency Announcement is forthcoming and will be published on the System for Award Management (SAM) website at https://beta.sam.gov/

Disclaimer

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

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

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

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

This information:

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

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

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

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

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

- is in no way constitutive of interpretative;

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

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

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

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