May 2020, cyber risk and compliance in Switzerland

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

Dear readers,

We have a great paper, the 30th semi-annual report of the Reporting and Analysis Centre for Information Assurance (MELANI). It addresses the most important cyber incidents of the second half of 2019 in Switzerland and abroad.

The latest report focuses on handling personal data on the internet and the problems involved.

For the jubilee edition, a technical appendix has been added to meet the needs of readers with in-depth technical knowledge.

According to Florian Schütz, the Federal Cyber Security Delegate and Head of the National Cybersecurity Centre, MELANI is becoming the National Cyber Security Centre.

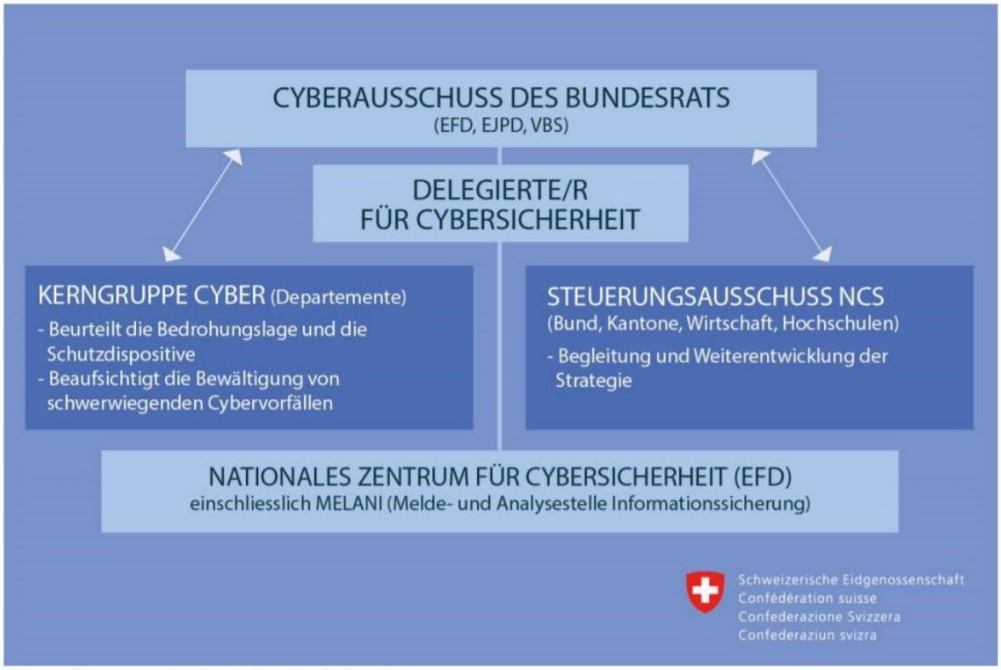


Fig. 1: Cyberorganisation in the Confederation

This was the title of an article on the MELANI homepage at the beginning of 2020. This move is a further step towards establishing responsibilities in the Confederation, as defined by the Federal Council on 30 January 2019 (see figure 1).

The details of how the National Centre for Cyber Security (NCSC) will be organised are part of ongoing work and have not yet been finally agreed. What is already clear, however, is that MELANI is an important part of the new centre and should be further strengthened and expanded.

According Florian Schütz, since MELANI was founded on 1 October 2004, information and communication technology (ICT) has continued to influence the economy, research and society.

ICT is at the heart of digitalized processes and can be found in almost all areas of life. A general situation analysis is no longer sufficient in view of the diversified threat. Instead, specific analyses are needed for economic sectors, areas of politics, research and society.

As a first measure, a specific situation analysis for the financial sector is currently being tested in a pilot project.

A further challenge is the scaling of incident processing. Fifteen years ago, in MELANI's first year of operation, less than 500 incidents were recorded. In contrast, more than 500 reports were submitted to us in January of this year alone. In order to process this volume, a national contact point for cyber security was created as an initial measure in the second half of 2019.

It receives reports, analyses them and ensures that they are dealt with by the right authorities.

In addition, the automation of analysis and processing and the seamless integration of the authorities involved, e.g. law enforcement agencies, will be an important task.

Read more at Number 1 and 2 below.

I have just read that *rare events* are highly unlikely; they may occur in exceptional circumstances. As we neither have a common definition of the term exceptional, nor historical records and data to rely on, the probabilities or rare events are usually estimated subjectively.

In high impact / low likelihood events, like hurricane Katrina and the Fukushima disaster, risk probability is *inherently difficult* to assess.

According to the Bank for International Settlements, the coronavirus (Covid-19) pandemic is a *rare* type of shock to the world economy.

Its sudden and massive impact on activity comes at a time when the legacy of the Great Financial Crisis (GFC) of 2007–09 is still weighing on public and private sector balance sheets.

As its fallout will extend well beyond the removal of health-related restrictions, the subsequent economic recovery may be drawn-out.

So far, the economic policy response has primarily involved the decisive use of monetary and fiscal tools. For their part, prudential authorities have sought to support the flow of credit to firms, households and governments, most notably by relaxing banks' constraints on the use of liquidity and capital buffers.

A *release of buffers* can complement and enhance the effect of fiscal and monetary policies, provided that banks are both able and willing to expand their balance sheets.

For one, this means that markets' and management's assessment of what is a prudent buffer size should not prevent banks from lending.

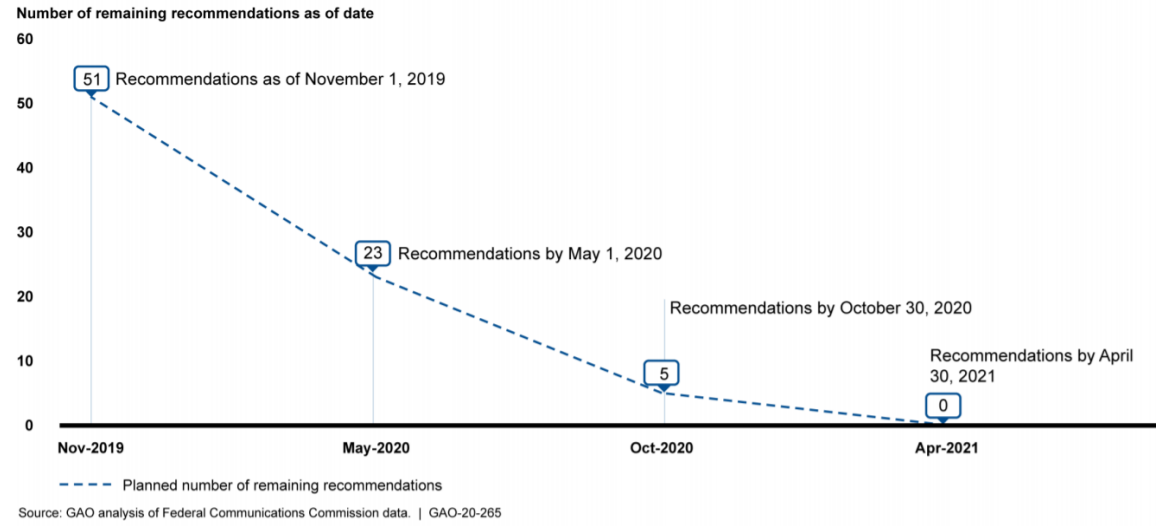
In addition, banks should see greater value in using balance sheet capacity for lending rather than for discretionary payouts: a trade-off affected by the extent of risk-sharing with the public sector.

Banks need to continue supporting economic performance in the medium term, ie the period after the lifting of stringent health-related restrictions. This is not a given. The recession will bring about large losses that will materialise only gradually.

To avoid amplifying stress, banks will need buffers to absorb elevated losses for as long as the slump persists. After that, banks will still need buffers that they can draw upon in order to facilitate the rebound as robust counterparties and reliable intermediaries.

The *Reports to Congressional Requesters* from the United States Government Accountability Office (GAO) are always interesting. When one of these reports covers *remaining control deficiencies*, I change my schedule and I simply cannot wait to read it.

I like the way the GAO ensures all recommendations will be implemented:



According to the paper, the Commission *had not effectively implemented controls intended to detect cybersecurity events or deficiencies*.

The *detect* core security function is intended to allow for the timely discovery of cybersecurity events and deficiencies. Controls associated with this function include logging and monitoring system activities, and assessing security controls in place.

NIST SP 800-53 states that agencies should enable system logging features and retain sufficient audit logs to support the investigations of security incidents and monitoring of select activities for significant security-related events.

Additionally, NIST SP 800-53 and industry leading practices state that organizations should increase their situational awareness through enhanced monitoring capabilities to analyze network traffic data over an extended period of time at external boundaries and inside their internal network to identify anomalous, inappropriate, or unusual malicious activities.

Lastly, FISMA requires each agency to periodically test and evaluate the effectiveness of its information security controls in place applicable to policies, procedures, and practices.

In September 2019, the Government Accountability Office (GAO) reported that the Commission had implemented security monitoring controls, such as performing regular vulnerability scanning and deploying a system information and event management tool, to detect the presence of potential malicious threats.

However, six technical control deficiencies in these capabilities diminished the effectiveness of the controls to detect cybersecurity events in the

systems we reviewed.

For example, the Commission did not fully capture system log data on certain devices and had limited network monitoring visibility into portions of its data center environment.

According to Information Technology Center officials, the Commission had deficiencies in logging, retention, and monitoring because the Commission had not fully configured its security information and event monitoring tool to capture and monitor sufficient system log and network traffic data to adequately detect cybersecurity events.

As a result, the Commission may not be able to detect or investigate anomalous activities inside its network.

In addition, although the commission established a process for assessing the effectiveness of the security controls for its systems, its control tests and evaluations were not sufficiently robust.

For example, the Commission's evaluations did not identify many of the security control deficiencies the GAO identified. Consequently, the Commission had limited assurance that the security controls were in place and operating as intended. As of November 2019, the Commission had acted to address several technical control deficiencies, and associated recommendations, such as capturing network traffic data and providing for real-time network monitoring; however, other technical control deficiencies remain.

Also, the Commission *did not consistently encrypt sensitive data.*

NIST SP 800-53 recommends that organizations employ cryptographic mechanisms to prevent the unauthorized disclosure of information during transmission and establish a trusted communications path between users and security functions of information systems.

However, in seven instances, the Commission did not consistently deploy strong encryption capabilities to protect sensitive data or establish a secure communications path between users and information systems.

Read more at number 6 below. Welcome to our monthly newsletter.

Best regards,

George Lekatis
General Manager, Cyber Risk GmbH

Rebackerstrasse 7, 8810 Horgen
Phone: +41 79 505 89 60
Email: george.lekatis@cyber-risk-gmbh.com
Web: www.cyber-risk-gmbh.com

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

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

Number 1 (Page 11)

Semi-annual report 2019/2 (July – December)

Reporting and Analysis Centre for Information Assurance (MELANI)

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Number 2 (Page 14)

Semi-annual report 2019/2 (July – December)

Reporting and Analysis Centre for Information Assurance (MELANI)
Important parts, Espionage

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Number 3 (Page 18)

NIST and OSTP Launch Effort to Improve Search Engines for COVID-19 Research

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

Number 4 (Page 21)

Protecting healthcare and human rights organizations from cyberattacks

Tom Burt - Corporate Vice President, Customer Security & Trust

Microsoft

Number 5 (Page 25)

FBI Warns of Advance Fee and BEC Schemes Related to Procurement of PPE and Other Supplies During COVID-19 Pandemic

Number 6 (Page 28)

The Federal Communications Commission (FCC) made significant progress, but needs to address remaining control deficiencies and improve its program

United States Government Accountability Office

GAO

Report to Congressional Requesters

Number 7 (Page 31)

The legal implications of malicious exploitation of social media

Published by the NATO Strategic Communications Centre of Excellence

Number 8 (Page 33)

Selecting and Safely Using Collaboration Services for Telework

NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA

Number 9 (Page 35)

Millions of fitness app users exposed after data breach

National Cyber Security Centre

Number 10 (Page 36)

In Glowing Colors: Seeing the Spread of Drug Particles in a Forensic Lab

Black-light videos from NIST will help crime labs manage an invisible risk.

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

Number 11 (Page 38)

High level privacy and security design for NHS COVID-19 Contact Tracing App

Dr Ian Levy, Technical Director, National Cyber Security Centre, UK

National Cyber Security Centre

Number 12 (Page 41)

Executive Order on Securing the United States Bulk-Power System

THE WHITE HOUSE
WASHINGTON

Number 13 (Page 49)

FBI El Paso Warns About Scams That Are Targeting the Deceased and Their Grieving Families: Bereavement Scams

Number 14 (Page 51)

Internet Crime Complaint Center Marks 20 Years

From Early Frauds to Sophisticated Schemes, IC3 Has Tracked the Evolution of Online Crime

Number 15 (Page 56)

Manipulation ecosystem of social messaging platforms

Published by the NATO Strategic Communications Centre of Excellence

Number 16 (Page 58)

Researchers on DARPA's Brandeis Program Enhance Privacy Protections for Android Applications

Privacy Enhancements for Android simplifies implementation of privacy protections for mobile apps running on Android OS

Number 1

Semi-annual report 2019/2 (July – December)

Reporting and Analysis Centre for Information Assurance (MELANI)

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Data protection legislation

Data processing and also the trading of personal data is permitted, depending on the circumstances and the legal system in force. However, data protection regulations vary considerably from one country to another.

With its General Data Protection Regulation (GDPR), the EU provides worldwide uniform protection for the data of its citizens.

Although many questions remain unanswered regarding the international enforcement of this regulation, the GDPR has already had some impact.

Since its entry into force in May 2018, many players have taken data protection and data security much more seriously.

It has been repeatedly predicted that data leaks will cause more serious damage in the near future and that more will be invested in data security.

This is against the background that since the GDPR came into force, companies have been heavily fined for data protection violations.

The calculation of damages takes particular account of the potential fines of up to EUR 20 million or 4% of annual turnover (whichever is higher) to which companies can be subjected.

The revision of the Swiss Data Protection Act includes criminal provisions according to which "private persons", i.e. employees of companies, rather than the companies, are punished.

Only if a fine is for less than CHF 50,000 can a business be ordered to pay it if investigating the offender involves disproportionate effort.

It remains to be seen to what extent this leads to tensions within companies when the management (does not) make decisions and (does not) set rules, the consequences of which data protection officers or simple employees will have to bear.

Risks and side effects

It is rare that anyone talks about the consequential damages of data protection violations that affected individuals may suffer.

They are also difficult to quantify. Data such as name, addresses, dates of birth, telephone numbers, email addresses, etc. are not "particularly sensitive" personal data, but in the wrong hands, such data can already be used to cause a lot of harm.

Increased quantities of spam is the least of the problems. Leaked data is used by criminals for tailor-made social engineering attacks which aim to install malware, obtain further (more sensitive) data, trigger unjustified payments or achieve other objectives that have a negative impact on those concerned.

Personal information can also be misused to establish identities; people can impersonate other people by using their data. This allows them to create social media accounts, register domain names or place orders using someone else's identity.

Fraud involving the contacts belonging to people whose email account has been compromised or data otherwise leaked also occurs regularly. It is difficult to assess the consequences of unauthorised acquisition and further processing of data.

In the age of big data and machine learning, automated merging of different data sources is becoming increasingly simple.

Whether this is done by companies for legitimate purposes, in legal grey areas or by criminals is only superficially relevant.

It can be assumed that every database will be hacked sooner or later and that the data sets will find their way into the underground market.

Conclusion

"Our data" or "data about us" is stored by many players in many locations. The collection, gathering and merging of data is a business model in both legal and illegal circles and leads to the trade in this data.

We must therefore expect that commercial or advertising companies and criminals will have access to more or less large data sets on us and will be able to use them to target us.

If personality profiles are also created from the data, this opens up

possibilities for specific psychological influence, not only in terms of consumption and susceptibility to fraudulent practices, but also on how opinions are formed and thus ultimately on voting behaviour.

Internet advertising is already individualised in many cases. This trend will continue and is likely to be increasingly used by political players to distribute targeted election and voting propaganda.

Criminals will continue to improve their methods of attack and tailor them more individually to potential victims.

A personalised greeting in an email has long since ceased to be a suitable criterion to prove its seriousness.

Criminals have been filling their emails with names, addresses, telephone numbers and other personal details of the recipients for some time now.

Fake sender addresses are also regularly chosen in such a way that it appears as if the email comes from a known individual, that is if the email or social media message is not actually sent with the alleged sender's real, yet compromised, account.

To read more:
https://www.melani.admin.ch/melani/en/home/dokumentation/reports/situation-reports/halbjahresbericht-2019-2.html

Number 2

Semi-annual report 2019/2 (July – December)

Reporting and Analysis Centre for Information Assurance (MELANI)
Important parts, Espionage

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Espionage

In the second half of 2019, cyberespionage continued to be a popular tool used by governments to gather information and steal intellectual property.

Google's Threat Analysis Group (TAG) is focused on detecting and defending against cyberattacks aimed at its users.

For example, it reported 12,000 spear phishing attempts in 149 countries in the third quarter of 2019 alone (July to September).

It is believed that more than 270 groups linked to government agencies, operating in at least 50 countries, were responsible for these incidents.

In addition to classic espionage, disinformation campaigns aimed at promoting the interests of a particular country or discriminating against political movements were also recorded.

Like dissidents and activists, politicians also belong to the high-risk group.

This is evidenced by hundreds of attempted attacks against political organisations registered by AccountGuard, Microsoft's security service.

This platform was set up to warn campaigning candidates and offices that have been targeted by cyberattacks.

However, large companies are thought to be most affected by targeted, state-sponsored attempts at cyber-compromising.

In terms of numbers, they are said to account for over three-quarters of the 10,000 users reported by Microsoft in 2019.

The software giant has compiled a list of the five most active attack groups, known as advanced persistent threats (APTs), in 2019.

According to Microsoft and other security companies, of the groups listed, "Holmium" aka "APT33" is said to be sponsored by the Iranian government.

Its main aim is to target organisations active in the civil and military aviation and petrochemical energy sectors.

Among other reasons, the campaign hit the headlines because between 2016 and 2017 both a US company active in aviation and a Saudi Arabian organisation active in the same sector were attacked.

Microsoft also points to "Strontium", also known as "Fancy Bear", "APT28" or "Sofacy", as being another particularly active group.

Several governments (notably UK and USA) as well as some security companies (e.g. CrowdStrike) allege that the group is connected with the Russian military intelligence service (GRU).

The group has been linked to the attacks against the German Bundestag (2015), the US Democratic National Committee (2016) and the World Anti-Doping Agency (2016), among others.

Winnti industrial espionage campaign

According to the latest revelations, the number of German multinationals that have become the target of cyberattacks is rising.

Communications giant Siemens, for example, recently confirmed that it had become the victim of a cyberattack in June 2016, but apparently no data was leaked.

Also affected was Covestro, a manufacturer of plastics and adhesives, which also escaped without damage.

The pharmaceutical giant Bayer announced in April that it had already been the victim of cyberespionage in 2018.

According to various security experts, all these attacks are said to have been triggered by Winnti.

This name is used to describe both a group and the malware it uses, which is known, among other things, for having infiltrated the steel producer ThyssenKrupp in 2016.

The same experts believe the origin of these attacks to be in China.

Initially, the group focused on attacks against online gaming platforms for purely financial motives. However, by 2015 at the latest, it had expanded its activities to include industrial espionage.

It appears to be particularly targeting the chemical and pharmaceutical sectors, and companies specialising in cutting-edge technologies.
In addition to the victims already mentioned, an in-depth analysis by the Bayerischer Rundfunk and Norddeutsche Rundfunk radio stations identified older infections which have not made the headlines thus far.

They mentioned, for example, the company Henkel, which, like Covestro, produces adhesive products for industry and was infiltrated in 2014.

Another confirmed victim is BASF ("Badische Anilin- und Soda-Fabrik"), one of the world's largest chemical companies, which is also based in Germany.

The 2015 attack had no serious consequences. After infiltrating a company's network, the hackers create a map of the network and then search for the strategic points where the malware can be hidden.

In this way, they can operate invisibly in the background for as long as possible and collect information about the company and its products in the hope of finding trade secrets.

One of the main characteristics of Winnti is its perseverance. By installing backdoors, the perpetrators gain permanent access to a business network.

In October 2019, the IT security company ESET reported that it had discovered a previously unknown backdoor that were based on Microsoft SQL (MSSQL) and used by Winnti".

Although Winnti came into the limelight in Germany after the attack on ThyssenKrupp, the campaign is also active in other countries in Western Europe, Asia and the USA.

Research by ESET has revealed that the group is believed to have infected a major Asian-based manufacturer of mobile hardware and software via PortReuse, a backdoor that emerged in March 2019.

It is possible that by compromising the company in this way, the hacker group was preparing for a far-reaching attack via the supply chain.

Finally, the malware is also used for political espionage.

According to Kaspersky Lab experts, there are currently at least two groups that use this attack tool.

This makes it difficult to determine whether those responsible for industrial cyberespionage are the same as those who are more likely to

engage in political espionage – be it against the Hong Kong government or the Indian telecommunications provider in the region which is home to the headquarters of the Tibetan government in exile.

To read more:
https://www.melani.admin.ch/melani/en/home/dokumentation/reports/situation-reports/halbjahresbericht-2019-2.html

Number 3

NIST and OSTP Launch Effort to Improve Search Engines for COVID-19 Research

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

The U.S. Department of Commerce's National Institute of Standards and Technology (NIST) and the White House Office of Science and Technology Policy (OSTP) launched a joint effort to support the development of search engines for research that will help in the fight against COVID-19.

The project was developed in response to the March 16 White House Call to Action to the Tech Community on New Machine Readable COVID-19 Dataset.

It can be found at: https://www.whitehouse.gov/briefings-statements/call-action-tech-community-new-machine-readable-covid-19-dataset/

"Our nation's scientific enterprise is mobilized to defeat the invisible enemy that is COVID-19," said Secretary of Commerce Wilbur Ross. "Our scientists — and the businesses and institutions that provide them with advanced digital research technologies — are to be commended for their unwavering dedication to finding a cure for this insidious disease."

"AI experts worldwide are responding to the White House's call to action, developing approaches that help scientists gain insights from thousands of articles of COVID-19 scholarly literature," said Michael Kratsios, U.S. chief technology officer.

"The TREC-COVID program expands upon these efforts by creating powerful and accurate search engines that extract knowledge from this literature, tailored to the needs of the health-care and medical research communities. We thank NIST for this valuable contribution as part of the Trump administration's whole-of-America response to the coronavirus."

In this effort, NIST will work initially with the Allen Institute for Artificial Intelligence, the National Library of Medicine, Oregon Health & Science University (OHSU), and the University of Texas Health Science Center at Houston (UT Health).

The team will apply the successful, long-running program of expert engagement and technology assessment called the Text Retrieval Conference, or TREC, to the COVID-19 Open Research Dataset (CORD-19), a resource of more than 44,000 research articles and related data about COVID-19 and the coronavirus family of viruses.

The TREC-COVID program goals include creating datasets and using an independent assessment process that will help search engine developers to evaluate and optimize their systems in meeting the needs of the research and health-care communities.

“The TREC program has provided an effective way to evaluate and advance search engine technologies since 1992, and has led directly to the powerful search capabilities and internet-based efficiencies we now often take for granted,” said Under Secretary of Commerce for Standards and Technology and NIST Director Walter G. Copan.

“We are pleased to apply this infrastructure to the challenge of working with massive amounts of data to help researchers better understand and ultimately to combat this deadly novel coronavirus and related threats.”

The team will first release a series of sample queries for the biomedical research community, developed by team members at the National Library of Medicine, OHSU and UT Health.

Registered participants in TREC-COVID will use their information retrieval and search systems to run the queries against the CORD-19 document set and return their results to NIST.

Biomedical experts will then review test results, including document relevance rankings, to assess the overall performance of the retrieval systems.

Using proven TREC protocols, NIST will score the submissions and post the scores, the retrieval results themselves, and the lists of key reference documents to the TREC-COVID website.

These “test collections” can then be used by information retrieval researchers to evaluate and enhance the performance of their own search engines.

This effort is intended to help researchers understand how search systems could best support medical researchers when available information is developing quickly, as in the current pandemic.

The Allen Institute for Artificial Intelligence has been releasing an expanded CORD-19 document set each Friday to capture the most recent articles on COVID-19 and related coronaviruses.

Later rounds of TREC-COVID will use the larger releases of CORD-19 and expanded query sets.

Participants will have one week to submit their search results, and within about a week NIST will post results, with an expected spacing of about two weeks between each new dataset round being released.

The team initially anticipates conducting five consecutive rounds of search system assessments.

Interested organizations are invited to register to participate in the TREC-COVID program on the NIST website.

NIST promotes U.S. innovation and industrial competitiveness by advancing measurement science, standards and technology in ways that enhance economic security and improve our quality of life.

Number 4

Protecting healthcare and human rights organizations from cyberattacks

Tom Burt - Corporate Vice President, Customer Security & Trust

Microsoft

We're deeply concerned about cyberattacks impacting workers on the front lines of the COVID-19 fight.

News reports have shown recent criminal or nation-state attacks targeting Brno University Hospital in the Czech Republic, Paris' hospital system, the computer systems of Spain's hospitals, hospitals in Thailand, medical clinics in the U.S. state of Texas, a healthcare agency in the U.S. state of Illinois and even international bodies such as the World Health Organization.

Our teams at Microsoft have also detected and responded to attacks targeting the healthcare sector in many countries, and we know they are coming from criminals and multiple nation-states.

In addition, our threat intelligence teams have identified nation-state attacks against human rights organizations around the world for some time, both prior to and during the COVID-19 pandemic.

That's why, starting today, we're making our AccountGuard threat notification service available at no cost to healthcare providers on the front lines as well as human rights and humanitarian organizations around the world.

Healthcare organizations can sign up at:
https://www.microsoftaccountguard.com/healthcare/

Human rights and humanitarian organizations can sign up at:
https://www.microsoftaccountguard.com/humanrights/

Every patient deserves the best possible healthcare treatment, and we all need to thank and applaud the truly heroic work by those risking their own health to help those who are sick.

Their work is challenging enough but is being made more difficult by cyberattacks, now or in the future.

Some attacks, such as the one on Brno University Hospital, have resulted in delays in COVID-19 testing, new patients being turned away and treatments being postponed.

Others, such as the attack in Illinois, have held up access to critical COVID-19-related healthcare guidance.

Nearly all these attacks have two things in common: a person and email. An attacker will often disguise malicious content as a message from a health authority or medical equipment provider.

These emails sent to work or home inboxes seek to obtain the person's credentials and often contain documents or links that will infect a computer and spread the infection through a network, enabling attackers to control it.

In some cases, attackers could be looking for COVID-19-related intelligence, or to disrupt the provision of desperately needed care or supplies.

With today's announcement, we are seeking to notify customers when we see attacks and provide guidance to help.

Microsoft AccountGuard, which we first offered to political campaigns through our Defending Democracy Program, monitors nation-state threat actors targeting enterprise mailboxes and the personal email accounts of employees or volunteers who opt in.

This gives our threat intelligence teams a broad view of the avenues attackers typically use.

When we see such activity targeting an organization enrolled in AccountGuard, we notify them immediately so they can take steps to stop an attack or root out the attacker.

AccountGuard has previously been available to political campaigns, parties, members of the U.S. Congress and democracy-focused non-profits.

Nearly 100,000 email accounts in 29 countries are enrolled in AccountGuard and we've made 1,450 threat notifications to those participating.

Through today's announcement, we're making AccountGuard available to healthcare providers including hospitals, care facilities, clinics, labs and clinicians providing front line services as well as pharmaceutical, life sciences and medical devices companies that are researching, developing and manufacturing COVID-19-related treatments.

Our notifications will help these organizations defend against nation-state attacks, and our AccountGuard advice and training support will help them harden their defenses against all forms of cyberattacks.

AccountGuard for Healthcare will be available until the COVID-19 pandemic subsides.

In addition to making AccountGuard available to those working directly in the healthcare field, another important part of today's announcement is the availability of AccountGuard for worldwide human rights and humanitarian organizations.

Today, nearly every human rights or humanitarian organization is focused on protecting the rights of people impacted by COVID-19 whether it's supporting hospitals in conflict zones, amplifying the voices of medical professionals, helping to ensure elections are conducted safely in new ways or helping children who are out of school.

In many instances, nation-states and cyber criminals use attacks to gain intelligence on these organizations and the people who these groups protect, or to disrupt their work.

While cybersecurity threats are not new to human rights defenders, these groups have been increasingly under attack, even before the pandemic arose. In the past year, the Microsoft Threat Intelligence Center, or MSTIC, has tracked five separate nation-state activity groups that have attempted nearly nine hundred times to target or compromise hundreds of accounts belonging to employees of nine prominent human rights organizations around the world.

Protecting these organizations has never been more important.

Leading human rights and humanitarian organizations including Amnesty International, CyberPeace Institute, Freedom House, Human Rights Watch and Physicians for Human Rights have already registered for our AccountGuard threat notification service through an initial pilot.

Both AccountGuard for Healthcare and AccountGuard for Human Rights Organizations will initially be available to organizations in the 29 countries where we already offer AccountGuard, subject to review of local laws and regulations, and we will be adding new countries based on need and local law.

AccountGuard is available to organizations using Office 365 for business email and extends additional security to the personal accounts of their front line workers who use Microsoft's consumer email services such as Outlook.com and Hotmail.

Whether you're a front line worker or not, it's always important to make sure you trust the sender of an email before you open it, that you look out for misspellings or slight inaccuracies in emails that may offer clues of an untrustworthy message, and that you know you trust a URL before you click on it.

We've published more on protecting yourself from COVID-19-related phishing attacks at:
https://www.microsoft.com/security/blog/2020/03/20/protecting-against-coronavirus-themed-phishing-attacks/

Today's news is in addition to the work we've already announced to track and prevent cyberthreats targeting healthcare organizations and our announcement yesterday on providing non-profits working on the COVID-19 response with greater access to technology.
To read more: https://blogs.microsoft.com/on-the-issues/2020/04/14/accountguard-cyberattacks-healthcare-covid-19/

Number 5

FBI Warns of Advance Fee and BEC Schemes Related to Procurement of PPE and Other Supplies During COVID-19 Pandemic

The Federal Bureau of Investigation is providing this industry alert to warn government and health care industry buyers of rapidly emerging fraud trends related to procurement of personal protective equipment (PPE), medical equipment such as ventilators, and other supplies or equipment in short supply during the current COVID-19 pandemic.

The FBI recently became aware of multiple incidents in which state government agencies, attempting to procure such equipment, wire transferred funds to fraudulent brokers and sellers in advance of receiving the items.

The brokers and sellers included both domestic and foreign entities.

In one case, an individual claimed to represent an entity with which the purchasing agency had an existing business relationship.

By the time the purchasing agencies became suspicious of the transactions, much of the funds had been transferred outside the reach of U.S. law enforcement and were unrecoverable.

The current environment, in which demand for PPE and certain medical equipment far outstrips supply, is ripe for fraudulent actors perpetrating advance fee and business email compromise (BEC) schemes, such as those described above.

In advance fee schemes related to procurement, a victim pre-pays (partially or in full) a purported seller or a broker for a good or service and then receives little or nothing in return.

BEC schemes often involve the spoofing of a legitimate known email address or use of a nearly identical email address to communicate with a victim to redirect legitimate payments to a bank account controlled by fraudsters.
A variation on BEC schemes can involve similar social engineering techniques via phone call.

Risk Factors

While pre-payment is more common in the current environment, it substantially increases the risk of a buyer being defrauded and eliminates most potential recourse. The following indicators are warning signs that an offer to sell items may not be legitimate:

- A seller or broker initiates the contact with the buyer, especially from a difficult to verify channel such as telephone or personal email.

- The seller or broker is not an entity with which the buyer has an existing business relationship, or the buyer's existing business relationships are a matter of public record.

- The seller or broker cannot clearly explain the origin of the items or how they are available given current demand.

- The potential buyer cannot verify with the product manufacturer that the seller is a legitimate distributor or vendor of the product, or otherwise verify the supply chain is legitimate.

- Unexplained urgency to transfer funds or a last minute change in previously-established wiring instructions.

Mitigation Recommendations

The FBI recommends that buyers consider the following recommendations to protect their companies or agencies:

- If the seller claims to represent an entity with an existing relationship to the buyer, verify claims through a known contact—do not contact the vendor through information provided in an email or phone communication.

- If possible, have a trusted independent party verify the items for sale are physically present and of the promised make, model, and quality, and take delivery immediately upon payment.

- If immediate delivery is impossible, route payments to a domestic escrow account to be released to the seller upon receipt of the promised items.

- Verify with the manufacturer or verified distributor that the seller is a legitimate distributor or vendor for the items being offered.

- Be skeptical of last minute changes in wiring instructions or recipient account information—do not re-route payments without independently verifying the direction came from an authorized party.

- Verify the email address used to send emails, especially when using a mobile or handheld device, by ensuring the sender's email address appears to match who it is coming from.

If you think your company or agency is the victim of a fraud scheme related to COVID-19 immediately contact the FBI's Internet Crime Complaint Center at ic3.gov.

For accurate and up-to-date information about COVID-19, you may visit:

coronavirus.gov
cdc.gov/coronavirus
usa.gov/coronavirus
fbi.gov/coronavirus
justice.gov/coronavirus

Number 6

The Federal Communications Commission (FCC) made significant progress, but needs to address remaining control deficiencies and improve its program

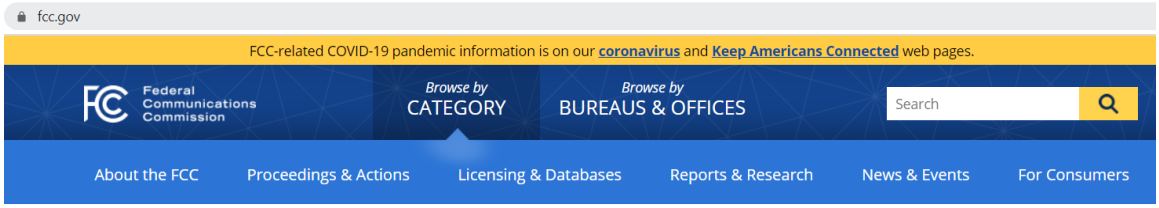
United States Government Accountability Office

GAO

Report to Congressional Requesters

Established by the Communications Act of 1934, FCC regulates interstate and international communications by radio, television, wire, satellite, and cable in all 50 states, the District of Columbia, and U.S. territories.

FCC is responsible for, among other things, making available nationwide worldwide wire and radio communication service.



More recently, it has been responsible for promoting competition and reducing regulation of the telecommunications industry in order to secure lower prices and higher quality services for consumers.

FCC's functions include:

• issuing licenses for broadcast television and radio;

• overseeing licensing, enforcement, and regulatory functions of carriers of cellular phones and other personal communication services;

• regulating the use of radio spectrum and conducting auctions of licenses for spectrum;

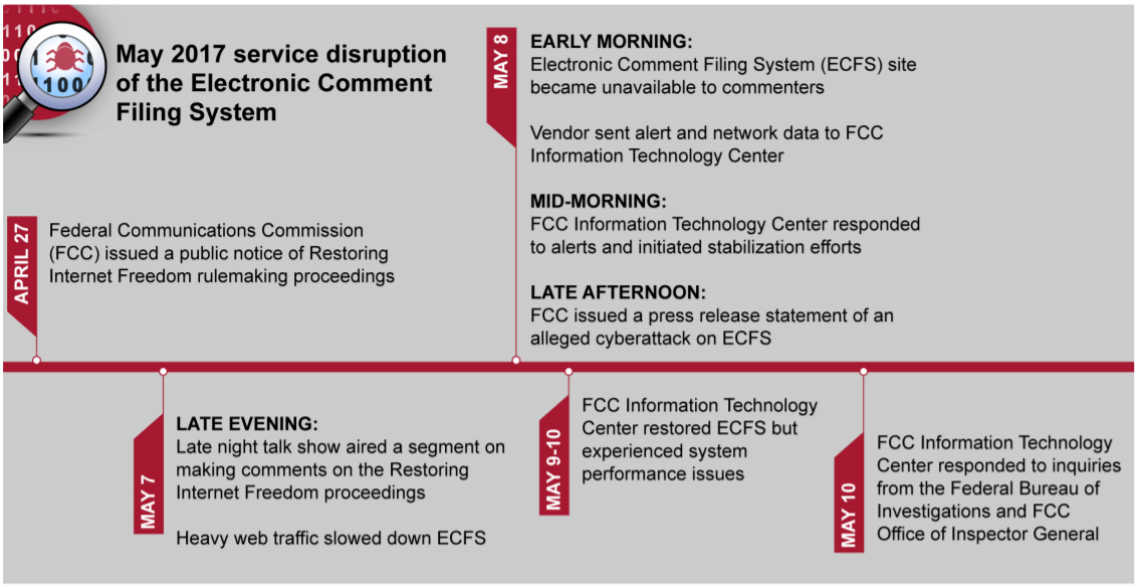
• investigating complaints and taking enforcement actions if it finds that there have been violations of the various communications laws and commission rules that are designed to protect consumers;

• addressing issues related to public safety, homeland security, emergency management, and preparedness;

• educating and informing consumers about communications goods and services; and

• reviewing mergers of companies holding FCC-issued licenses.

Figure 1: The Federal Communications Commission's Electronic Comment Filing System May 2017 Service Disruption and Subsequent Related Events Timeline



June 21, 2017	FCC Office of Inspector General opened an investigation of an alleged cyberattack of ECFS.
January 4, 2018	FCC Office of Inspector General referred the ECFS investigation to the Department of Justice.
August 7, 2018	FCC Office of Inspector General published an investigative report on the ECFS event.
August 16, 2018	FCC Chairman testified at a Senate oversight hearing on the investigative report on the ECFS event.

Source: GAO analysis of Federal Communications Commission information. | GAO-20-265

Figure 2: FCC Improvements to the Electronic Comment Filing System (ECFS) in Response to the May 2017 Service Disruption (as of November 2018)

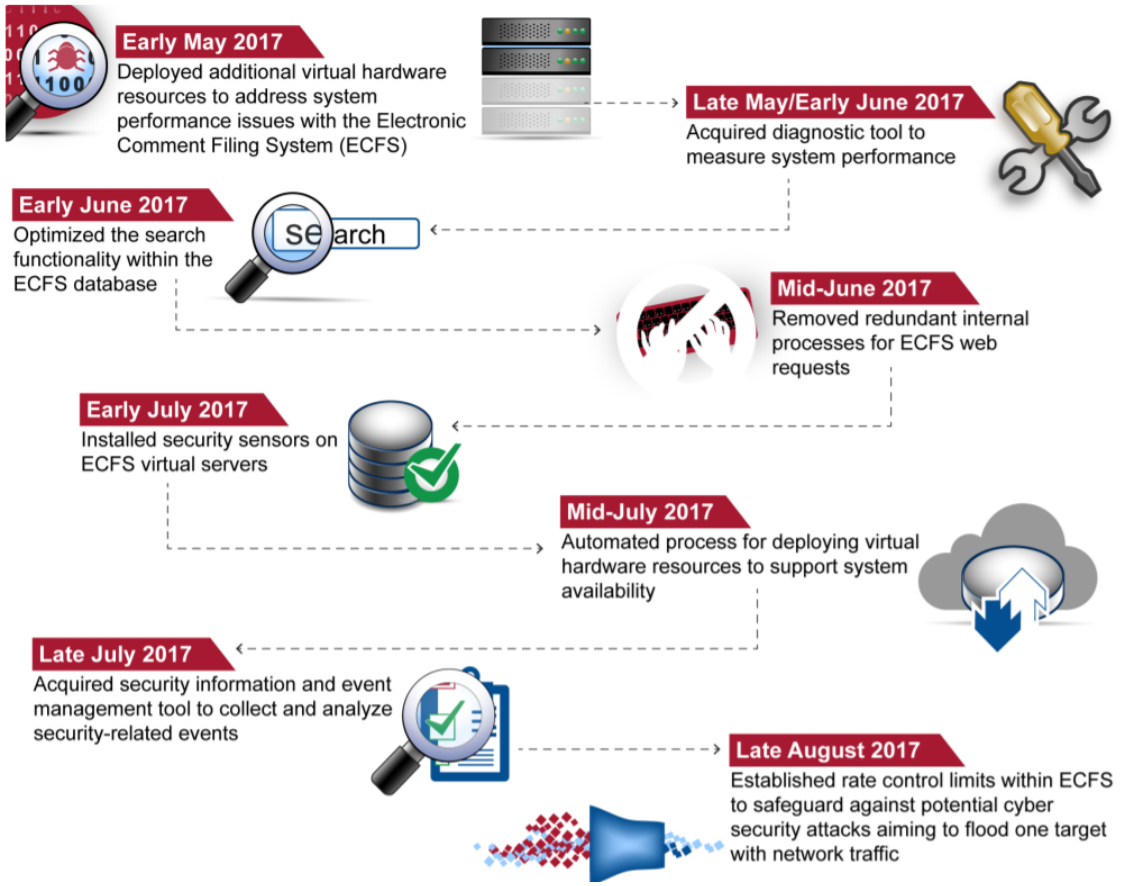


Table 1: Number of GAO-Identified Information Security Program and Technical Control Deficiencies at FCC and Associated Recommendations by Core Security Function, as of September 2019

Core security function	Number of information security program deficiencies	Number of information security program recommendations	Number of technical control deficiencies	Number of technical control deficiency recommendations
Identify	3	4	0	0
Protect	1	1	37	108
Detect	0	0	6	17
Respond	2	2	1	2
Recover	2	2	0	0
Total	**8**	**9**	**44**	**127**

Source: GAO analysis of Federal Communications Commission information security program and technical controls. | GAO-20-265.

Note: The five core security functions are part of the NIST cybersecurity framework, as updated in National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity* (Gaithersburg, MD: Apr. 16, 2018). As discussed later in this report, FCC has taken action to address many of these deficiencies and associated recommendations.

The report:
https://www.gao.gov/assets/710/705514.pdf

Number 7

The legal implications of malicious exploitation of social media

Published by the NATO Strategic Communications Centre of Excellence

The growing use of digital media is a well-observed phenomenon, with 90% of adults regularly accessing the Internet, and youth use averaging at least six hours a day.

Together with the increasing digitalization of private and public sector models, digital space is creating a parallel space of social activity.

This activity functions in a decentralized structure and across a variety of Websites and platforms, each under its own legal regimes and stakeholders.

Information flows are filtered through a few 'points of control,' directly impacting interaction between individuals, sovereigns, and other entities.

Through popular use, social media and video platforms are becoming especially important gatekeepers. Such platforms have morphed into concentrated arenas for public discourse and attention.

While this brings many benefits, it also presents a gamut of new digital manipulation threats which necessitate governance.

For example, the difficulty of authentication has given rise to the use of troll and cyborg entities capable of increasingly authentic proliferation of disinformation narratives.

Traditional hacking tools resulting in impersonation capacity are further benefiting from advances in image and sound manipulation software capable of 'deepfaking' individuals.

These tools are being amalgamated by states and non-states to engage in massive social media manipulation and social engineering campaigns.

Concurrently, new over- and underground markets have sprawled to collect and broker internet user data, expediting access to information that can be used for the purpose of manipulation.

The initial difficulty with managing the transnational digital domain is only reinforced by the proprietary nature of social media entities.

This has made regulating against the malicious use of digital space a complex matter, interweaving several types of stakeholders.

While from a legal standpoint, activity on the Internet is generally not differentiated from activity offline, its digital character necessitates a different approach.

The aim of this report is to outline the types of legal frameworks that have been set up by sovereigns to maneuver through and against the malicious use of social media networks, comment on the challenges faced, and identify policy trajectories.

Focus is placed on the German Network Enforcement law (NetzDG) as the prototypical archetype for a comprehensive and binding regime for social media intermediaries.

Through a transatlantic comparison with other jurisdictions and courts, the legal tendencies of the malicious use of digital space are outlined, and recommendations are provided for the path forward.

To read more: https://www.stratcomcoe.org/legal-implications-malicious-exploitation-social-media

Number 8

Selecting and Safely Using Collaboration Services for Telework

During a global pandemic or other crisis contingency scenarios, many United States Government (USG) personnel must operate from home while continuing to perform critical national functions and support continuity of government services.

With limited access to government furnished equipment (GFE) such as laptops and secure smartphones, the use of (not typically approved) commercial collaboration services on personal devices for limited government official use becomes necessary and unavoidable.

We define collaboration services as those capabilities that allow the workforce to communicate via internet-enabled text, voice, and video, and can include the sharing of files and other mission content.

Collaboration can occur between two people or widened to include a large group to support mission needs.

This document provides a snapshot of best practices and criteria based on capabilities available at the time of publication and was coordinated with the Department of Homeland Security (DHS), which is releasing a similar guide: “Cybersecurity Recommendations for Federal Agencies When Using Video Conferencing Solutions.”

This NSA publication is designed to provide simple, actionable, considerations for individual government users.

The intent of this document is not meant to be exhaustive or based on formal testing, but rather be responsive to a growing demand amongst the federal government to allow its workforce to operate remotely using personal devices when deemed to be in the best interests of the health and welfare of its workforce and the nation.

Recommendations in this document are likely to change as collaboration services evolve and also address known vulnerabilities and threats.

Users should be aware that even the most secure collaboration service cannot defend against a compromised user device.

Service	Basic Functionality	1 – E2E Encryption	2 – Testable Encryption	3 – MFA	4 – Invitation Controls	5 – Minimal 3rd Party Sharing	6 – Secure Deletion	7 – Public Source Code Shared	8 – Certified Service (FedRAMP / NIAP)
Cisco Webex®[9]	a, b, c, d, e	Y[1]	Y	Y[12]	Y[1]	Y	Client – Y Server – N[3]	N	FedRAMP
Dust	a	Y	N[3]	N	Y	N	Client – Y Server – Y	N	None
Google G Suite™[10]	a, b, c, d	N	Y	Y[1]	Y[1]	Y	Client – Y Server – Y[2]	N	FedRAMP
GoToMeeting®[11]	a, b, c	Y[1]	Y	N	Y[1]	Y	Client – Y Server – N[3]	N	None
Mattermost™[12]	a, b, c, e	Y	Y	Y[2]	Y	N	Client – Y Server – N	Y	FedRAMP
Microsoft Teams®[13]	a, c, d, e	N	Y	Y	Y	Y	Client – Y[1] Server – Y[1]	N	FedRAMP
Signal®[14]	a, b, d	Y	Y	Y	Y	Y	Client – Y Server – Y	Y	None
Skype for Business™[15]	a, c, d, e	Y[4]	Y[4]	Y	Y	N	Client – Y Server – N[3]	N	None
Slack®[16]	a, c, d, e	N	Y	Y	Y	N[3]	Client – N Server – N	N	FedRAMP
SMS Text	a, d	N	N	N	N	N	Client – Y Server – N	N	None
WhatsApp®[17]	a, c, d	Y	Y	Y	Y	Y	Client – Y Server – Y	N	None
Wickr®[18]	a, c, d, e	Y	Y	Y	Y	Y	Client – Y Server – Y	Y	None
Zoom®[19]	a, b, c, e	Y[14]	Y	N	Y	Y	Client – Y Server – N[3]	N	FedRAMP

Table of Assessments against Criteria

To read more: https://media.defense.gov/2020/Apr/24/2002288652/-1/-1/0/CSI-SELECTING-AND-USING-COLLABORATION-SERVICES-SECURELY-LONG-FINAL.PDF

Number 9

Millions of fitness app users exposed after data breach

National Cyber Security Centre

It has been reported that a firm behind a fitness app has unintentionally leaked data, including personal information, of millions of customers.

Kinomap, which specialises in indoor training, had inadvertently left its database exposed online, which meant that the records of 42 million users from 80 countries were viewable for at least one month.

The breach exposed full names, home country, email addresses, usernames, gender, and timestamps for exercises.

Kinomap says that the database was secured on the day they were alerted by cyber security researchers.

Large stores of data are a tempting target for attackers.

The NCSC has published advice to businesses on how to adequately protect such information at: https://www.ncsc.gov.uk/collection/protecting-bulk-personal-data

and how to protect against the phishing threat following data breaches at: https://www.ncsc.gov.uk/guidance/phishing-threat-following-data-breaches

Anyone concerned about the security of their online accounts should follow the guidance in 'Top tips for staying secure online' at: https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online

Number 10

In Glowing Colors: Seeing the Spread of Drug Particles in a Forensic Lab

Black-light videos from NIST will help crime labs manage an invisible risk.

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

When two scientists from the National Institute of Standards and Technology (NIST) brought black lights and glow powder into the Maryland State Police crime lab, they weren't setting up a laser tag studio or nightclub.

Instead, their aim was to study the way drug particles get spread around crime labs when analysts test suspected drug evidence.

Their study, recently published in Forensic Chemistry (at: https://www.sciencedirect.com/science/article/abs/pii/S2468170920300205), addresses safety concerns in an age of super-potent synthetic drugs like fentanyl, which can potentially be hazardous to chemists who handle them frequently.

The spread of drug particles cannot be completely avoided — it is an inevitable result of the forensic analyses that crime labs must perform.

To see how it happens, the two NIST research scientists, Edward Sisco and Matthew Staymates, fabricated a brick made of white flour mixed with a small amount of fluorescent powder.

Under everyday lights the brick looked like evidence from a drug seizure, but under ultraviolet light — also called UV or black light — it glowed a bright orange.

Amber Burns, supervisor of the Maryland State Police forensic chemistry lab and a co-author of the study, examined the brick and its contents as she would real evidence.

With a sheet of butcher paper covering her workspace, she cut open the package with a scalpel, scooped out a sample and transferred that scoop into a glass vial for analysis.

She also removed the powder to weigh it on a digital scale without the packaging. When she was done, the black light revealed that some particles had settled onto surfaces in her workspace.

Some had also adhered to her gloves and were transferred by touch onto a marker and wash bottle.

All chemists clean their workspaces between cases to prevent evidence from one case from contaminating the next. After Burns discarded the butcher paper and cleaned her workspace, the black light showed that her cleanup routine was effective.

Before the emergence of fentanyl and other super-potent drugs, such small amounts of drug residue were not a major concern. But that has changed, and not only for reasons of workplace safety.

Drug dealers often mix small amounts of fentanyl into heroin and cocaine, and some labs are increasing the sensitivity of their instruments to detect those small amounts. Highly sensitive instruments are more likely to detect small amounts of drug residue in the environment, so those labs have to be extra careful about limiting their spread.

This visualization experiment led the authors to suggest several steps that might minimize spread. These include changing gloves frequently, using vials and test tubes with large mouths to limit spillage when transferring material into them, and having two sets of wash bottles, one for casework and one for cleanup.

The researchers' paper is written in such a way that any laboratory can reproduce the black-light experiment.

"This is a great way for labs to see which of their practices contribute to the spread of drug residues, and to make sure that their cleanup routines are effective," Sisco said

To read more:
https://www.nist.gov/news-events/news/2020/04/glowing-colors-seeing-spread-drug-particles-forensic-lab

Number 11

High level privacy and security design for NHS COVID-19 Contact Tracing App

Dr Ian Levy, Technical Director, National Cyber Security Centre, UK

National Cyber Security Centre

This document provides a high-level overview of the security and privacy characteristics of the app that is in development by NHSx, the digital innovation unit of the National Health Service, to help manage the COVID-19 crisis in the UK.

This is not a full description of the entire system, the socio-technical design, epidemiological modelling or the plethora of other work being performed outside of this application development. Nor does this document detail the significant, diverse, expert input to the overall system and oversight of its development.

Instead, this technical paper concentrates only on the most important and unique security and privacy characteristics of the putative app and its infrastructure.

We only describe epidemiological and clinical aspects of the system, in order to set context for some technical decisions and trade-offs.

The epidemiological advice and models that the NHS is working from show that self-diagnosis is an important part of managing the spread of the disease, alongside various clinical tests and the wider public health response strategy.

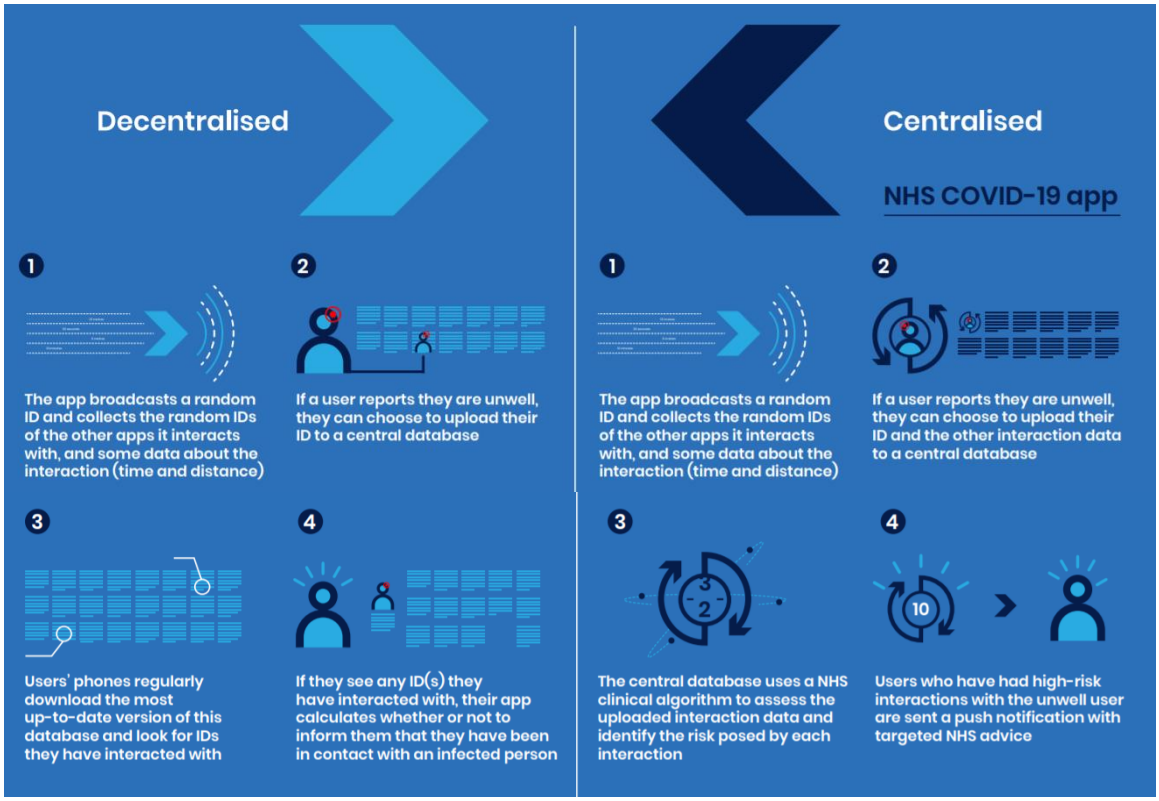
The Oxford group responsible for the model publishes much of its work.

Self-diagnosis can reduce by days, the time it takes a potentially infectious person to isolate.

This is critical to the management of the spread of the disease, under the assumptions in the UK's model.

There are obvious corollaries to a model that includes self-diagnosis. We explore some of those here, with their current mitigations.

Finally, a contact tracing app cannot work in isolation – it must work in concert with, and be a pathway into, the wider public health response. We do not cover that integration here, but it is in place.



Introduction to the NHS COVID-19 app

The NHS COVID-19 app aims to automate key parts of public health contact tracing by offering a proximity cascade system that can help slow transmission of the COVID-19 virus.

This will save lives, reduce pressure on the NHS, help return people to normal life and mitigate damage to the economy.

The app also aims to preserve individual and group privacy, be tolerant to various malicious users and minimise the risks of pseudonymous subgroup reidentification.

Importantly, it is driven by and informs expert epidemiological modelling, which in turn drives public policy.

How the NHSx app works

The user-centric description of the app is: “When I download the app, it keeps an anonymous record of when I’ve been close to other people (proximity events).
If I self-diagnose in the app, as displaying COVID-19 symptoms, I can choose to provide my personal record of proximity events to an NHSx system.

The NHSx system can then work out who to notify that they have potentially been in contact with COVID-19.

To these people, it can provide the latest advice and, potentially, access to testing.

Analysis of the records of proximity events from people displaying symptoms will allow NHSx to monitor and control the spread of the virus.

To read more: https://www.ncsc.gov.uk/files/NHS-app-security-paper%20V0.1.pdf

Number 12

Executive Order on Securing the United States Bulk-Power System

whitehouse.gov/presidential-actions/executive-order-securing-united-states-bulk-power-system/

ECONOMY NATIONAL SECURITY BUDGET IMMIGRATION CORONAVIRUS.GOV

EXECUTIVE ORDERS

Executive Order on Securing the United States Bulk-Power System

By the authority vested in me as President by the Constitution and the laws of the United States of America, including the International Emergency Economic Powers Act (50 U.S.C. 1701 et seq.) (IEEPA), the National Emergencies Act (50 U.S.C. 1601 et seq.) (NEA), and section 301 of title 3, United States Code,

I, DONALD J. TRUMP, President of the United States of America, find that foreign adversaries are increasingly creating and exploiting vulnerabilities in the United States bulk-power system, which provides the electricity that supports our national defense, vital emergency services, critical infrastructure, economy, and way of life.

The bulk-power system is a target of those seeking to commit malicious acts against the United States and its people, including malicious cyber activities, because a successful attack on our bulk-power system would present significant risks to our economy, human health and safety, and would render the United States less capable of acting in defense of itself and its allies.

I further find that the unrestricted acquisition or use in the United States of bulk-power system electric equipment designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of foreign adversaries augments the ability of foreign adversaries to create and exploit vulnerabilities in bulk-power system electric equipment, with potentially catastrophic effects.

I therefore determine that the unrestricted foreign supply of bulk-power system electric equipment constitutes an unusual and extraordinary threat

to the national security, foreign policy, and economy of the United States, which has its source in whole or in substantial part outside the United States.

This threat exists both in the case of individual acquisitions and when acquisitions are considered as a class.

Although maintaining an open investment climate in bulk-power system electric equipment, and in the United States economy more generally, is important for the overall growth and prosperity of the United States, such openness must be balanced with the need to protect our Nation against a critical national security threat.

To address this threat, additional steps are required to protect the security, integrity, and reliability of bulk-power system electric equipment used in the United States.

In light of these findings, I hereby declare a national emergency with respect to the threat to the United States bulk-power system.

Accordingly, I hereby order:

Section 1. Prohibitions and Implementation.

(a) The following actions are prohibited: any acquisition, importation, transfer, or installation of any bulk-power system electric equipment (transaction) by any person, or with respect to any property, subject to the jurisdiction of the United States, where the transaction involves any property in which any foreign country or a national thereof has any interest (including through an interest in a contract for the provision of the equipment), where the transaction was initiated after the date of this order, and where the Secretary of Energy (Secretary), in coordination with the Director of the Office of Management and Budget and in consultation with the Secretary of Defense, the Secretary of Homeland Security, the Director of National Intelligence, and, as appropriate, the heads of other executive departments and agencies (agencies), has determined that:

(i) the transaction involves bulk-power system electric equipment designed, developed, manufactured, or supplied, by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary; and

(ii) the transaction:

(A) poses an undue risk of sabotage to or subversion of the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of the bulk-power system in the United States;

(B) poses an undue risk of catastrophic effects on the security or resiliency of United States critical infrastructure or the economy of the United States; or

(C) otherwise poses an unacceptable risk to the national security of the United States or the security and safety of United States persons.

(b) The Secretary, in consultation with the heads of other agencies as appropriate, may at the Secretary's discretion design or negotiate measures to mitigate concerns identified under section 1(a) of this order. Such measures may serve as a precondition to the approval by the Secretary of a transaction or of a class of transactions that would otherwise be prohibited pursuant to this order.

(c) The prohibitions in subsection (a) of this section apply except to the extent provided by statutes, or in regulations, orders, directives, or licenses that may be issued pursuant to this order, and notwithstanding any contract entered into or any license or permit granted prior to the date of this order.

(d) The Secretary, in consultation with the heads of other agencies as appropriate, may establish and publish criteria for recognizing particular equipment and particular vendors in the bulk-power system electric equipment market as pre-qualified for future transactions; and may apply these criteria to establish and publish a list of pre-qualified equipment and vendors. Nothing in this provision limits the Secretary's authority under this section to prohibit or otherwise regulate any transaction involving pre-qualified equipment or vendors.

Sec. 2. Authorities.

(a) The Secretary is hereby authorized to take such actions, including directing the timing and manner of the cessation of pending and future transactions prohibited pursuant to section 1 of this order, adopting appropriate rules and regulations, and employing all other powers granted to the President by IEEPA as may be necessary to implement this order.

The heads of all agencies, including the Board of Directors of the Tennessee Valley Authority, shall take all appropriate measures within their authority as appropriate and consistent with applicable law, to implement this order.

(b) Rules and regulations issued pursuant to this order may, among other things, determine that particular countries or persons are foreign adversaries exclusively for the purposes of this order; identify persons owned by, controlled by, or subject to the jurisdiction or direction of foreign adversaries exclusively for the purposes of this order; identify particular equipment or countries with respect to which transactions involving bulk-power system electric equipment warrant particular scrutiny under the provisions of this order; establish procedures to license transactions otherwise prohibited pursuant to this order; and identify a mechanism and relevant factors for the negotiation of agreements to mitigate concerns raised in connection with subsection 1(a) of this order.

Within 150 days of the date of this order, the Secretary, in consultation with the Secretary of Defense, the Secretary of Homeland Security, the Director of National Intelligence, and, as appropriate, the heads of other agencies, shall publish rules or regulations implementing the authorities delegated to the Secretary by this order.

(c) The Secretary may, consistent with applicable law, redelegate any of the authorities conferred on the Secretary pursuant to this section within the Department of Energy.

(d) As soon as practicable, the Secretary, in consultation with the Secretary of Defense, the Secretary of the Interior, the Secretary of Homeland Security, the Director of National Intelligence, the Board of Directors of the Tennessee Valley Authority, and the heads of such other agencies as the Secretary considers appropriate, shall:

(i) identify bulk-power system electric equipment designed, developed, manufactured, or supplied, by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary that poses an undue risk of sabotage to or subversion of the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of the bulk-power system in the United States, poses an undue risk of catastrophic effects on the security or resiliency of United States critical infrastructure or the economy of the United States, or otherwise poses an unacceptable risk to the national security of the United States or the security and safety of United States persons; and

(ii) develop recommendations on ways to identify, isolate, monitor, or replace such items as soon as practicable, taking into consideration overall risk to the bulk-power system.

Sec. 3. Task Force on Federal Energy Infrastructure Procurement Policies Related to National Security.

(a) There is hereby established a Task Force on Federal Energy Infrastructure Procurement Policies Related to National Security (Task Force), which shall work to protect the Nation from national security threats through the coordination of Federal Government procurement of energy infrastructure and the sharing of risk information and risk management practices to inform such procurement. The Task Force shall be chaired by the Secretary or the Secretary's designee.

(b) In addition to the Chair of the Task Force (Chair), the Task Force membership shall include the following heads of agencies, or their designees:

(i) the Secretary of Defense;
(ii) the Secretary of the Interior;
(iii) the Secretary of Commerce;
(iv) the Secretary of Homeland Security;
(v) the Director of National Intelligence;
(vi) the Director of the Office of Management and Budget; and
(vii) the head of any other agency that the Chair may designate in consultation with the Secretary of Defense and the Secretary of the Interior.

(c) The Task Force shall:

(i) develop a recommended consistent set of energy infrastructure procurement policies and procedures for agencies, to the extent consistent with law, to ensure that national security considerations are fully integrated across the Federal Government, and submit such recommendations to the Federal Acquisition Regulatory Council (FAR Council);

(ii) evaluate the methods and criteria used to incorporate national security considerations into energy security and cybersecurity policymaking;

(iii) consult with the Electricity Subsector Coordinating Council and the Oil and Natural Gas Subsector Coordinating Council in developing the recommendations and evaluation described in subsections (c)(i) through (ii) of this section; and

(iv) conduct any other studies, develop any other recommendations, and submit any such studies and recommendations to the President, as appropriate and as directed by the Secretary.

(d) The Department of Energy shall provide administrative support and funding for the Task Force, to the extent consistent with applicable law.

(e) The Task Force shall meet as required by the Chair and, unless extended by the Chair, shall terminate once it has accomplished the objectives set forth in subsection (c) of this section, as determined by the Chair, and completed the reports described in subsection (f) of this section.

(f) The Task Force shall submit to the President, through the Chair and the Director of the Office of Management and Budget:

(i) a report within 1 year from the date of this order;

(ii) a subsequent report at least once annually thereafter while the Task Force remains in existence; and

(iii) such other reports as appropriate and as directed by the Chair.

(g) In the reports submitted under subsection (f) of this section, the Task Force shall summarize its progress, findings, and recommendations described in subsection (c) of this section.

(h) Because attacks on the bulk-power system can originate through the distribution system, the Task Force shall engage with distribution system industry groups, to the extent consistent with law and national security.

Within 180 days of receiving the recommendations pursuant to subsection (c)(i) of this section, the FAR Council shall consider proposing for notice and public comment an amendment to the applicable provisions in the Federal Acquisition Regulation to implement the recommendations provided pursuant to subsection (c)(i) of this section.

Sec. 4. Definitions.

For purposes of this order, the following definitions shall apply:

(a) The term “bulk-power system” means:

(i) facilities and control systems necessary for operating an interconnected electric energy transmission network (or any portion thereof); and

(ii) electric energy from generation facilities needed to maintain transmission reliability. For the purpose of this order, this definition includes transmission lines rated at 69,000 volts (69 kV) or more, but does not include facilities used in the local distribution of electric energy.

(b) The term “bulk-power system electric equipment” means items used in bulk-power system substations, control rooms, or power generating

stations, including reactors, capacitors, substation transformers, current coupling capacitors, large generators, backup generators, substation voltage regulators, shunt capacitor equipment, automatic circuit reclosers, instrument transformers, coupling capacity voltage transformers, protective relaying, metering equipment, high voltage circuit breakers, generation turbines, industrial control systems, distributed control systems, and safety instrumented systems.

Items not included in the preceding list and that have broader application of use beyond the bulk-power system are outside the scope of this order.

(c) The term "entity" means a partnership, association, trust, joint venture, corporation, group, subgroup, or other organization.

(d) The term "foreign adversary" means any foreign government or foreign non-government person engaged in a long-term pattern or serious instances of conduct significantly adverse to the national security of the United States or its allies or the security and safety of United States persons.

(e) The term "person" means an individual or entity.

(f) The term "procurement" means the acquiring by contract with appropriated funds of supplies or services, including installation services, by and for the use of the Federal Government, through purchase, whether the supplies or services are already in existence or must be created, developed, demonstrated, and evaluated.

(g) The term "United States person" means any United States citizen, permanent resident alien, entity organized under the laws of the United States or any jurisdiction within the United States (including foreign branches), or any person in the United States.

Sec. 5. Recurring and Final Reports to the Congress.

The Secretary is hereby authorized to submit recurring and final reports to the Congress regarding the national emergency declared in this order, consistent with section 401(c) of the NEA (50 U.S.C. 1641(c)) and section 204(c) of IEEPA (50 U.S.C. 1703(c)).

Sec. 6. General Provisions.

(a) Nothing in this order shall be construed to impair or otherwise affect:

(i) the authority granted by law to an executive department or agency, or the head thereof; or

(ii) the functions of the Director of the Office of Management and Budget relating to budgetary, administrative, or legislative proposals.

(b) This order shall be implemented consistent with applicable law and subject to the availability of appropriations.

(c) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

DONALD J. TRUMP,
THE WHITE HOUSE

Number 13

FBI El Paso Warns About Scams That Are Targeting the Deceased and Their Grieving Families: Bereavement Scams

Losing a loved one can take an enormous toll—physically, emotionally, and even financially. It is hard enough on its own without also having to worry about fraud on top of it. Scammers will try to cash in on your already-difficult situation.

The fraudster could try to open new credit cards in the deceased person's name or use a phishing scheme to pressure a grieving spouse into paying for a bogus benefit.

Perhaps he says that he is calling from an insurance company and is able to re-instate an expired life insurance policy if she just makes a payment to cover the last few years of unpaid fees. ID thieves may even try to use the deceased person's Social Security number to create a new identity.

There are many versions of these types of scams to include: outstanding debt, funeral scams, Medicare scams, tax fraud, romance/compassion scams, delinquent Life Insurance ploys, credit card scams, and possibly specially engraved trinkets.

So how do you protect your family after the loved one has passed?

We all want to acknowledge a loved one's life completed. But be aware of how many personal facts you provide in an obituary, post online, including social media, the greater the risk of scams—for the departed and survivors alike.

When it's time to write your loved one's obituary, give the deceased's age, but leave out the birthdate, middle name, home address, birthplace, and mother's maiden name. This part will be hard to follow, don't include the names of family survivors. This may open them up to these scams.

Each day, thousands of deceased family members fall victim to identity theft— costing their survivors pain and financial loss.

Alert the major credit reporting agencies as soon as you can as to the passing of your loved one.

They will want copies of the death certificate as well as specific details about your relative, including date of birth, Social Security Number, full legal name, and recent addresses.

The agencies will flag the person's credit file and put a freeze on it to prevent others from opening new unauthorized lines of credit.

Obtain a credit report for the deceased person right after death and a few months afterwards. This will help you to identify any otherwise unknown accounts and to watch out for any attempted fraudulent activity after death.

Make sure to also notify any current banks, credit unions, or financial institutions that the deceased person used so that all checking, savings, investment, or credit card accounts can be flagged appropriately.

The same thing for insurance companies holding auto, home, or life insurance policies. Check with the financial institution to see what access survivors' are entitled to and what protections will be put in place to keep scammers out.

Send a copy of the death certificate to the IRS so that the person's tax account can be flagged as well. Send the death certificate to the mailing address that the deceased individual would normally use to submit tax returns. You may also submit a copy of the death certificate when you file the person's final tax return.

Sometimes your funeral home will notify the Social Security Administration — but if not, you should do so right away.

In a time that should be dedicated to healing, many families are instead sorting through confusing, and often convincing, forms of deceit. Still, if you know what to look for, you can avoid being swindled and focus on finding grief support.

As always, if you have been victimized by a cyber fraud, you can report it to the FBI's Internet Crime Complaint Center at www.IC3.gov

Number 14

Internet Crime Complaint Center Marks 20 Years

From Early Frauds to Sophisticated Schemes, IC3 Has Tracked the Evolution of Online Crime

Throughout the 1990s, Americans took to the internet in droves. The decade saw the launch of the first web browsers, the introduction of now ubiquitous search engines, the birth of online commerce, and the ascendance of email as a go-to mode of communication.

As this new landscape bloomed, so did opportunities for criminals. The web offered easy access for cyber actors to target hundreds or even thousands of people at relatively low cost and risk.

When these crimes started occurring more frequently, the public was unsure where to turn for help. “People really didn’t know where to report internet scams or other online fraudulent activity,” said Internet Crime Complaint Center (IC3) Chief Donna Gregory. “And law enforcement agencies were saying: ‘What do we do with these? How do we handle them?’”

Recognizing the need to collect and assess information on cyber crime, the FBI started the Internet Fraud Complaint Center in May 2000 as a pilot project with the National White Collar Crime Center.

That center turns 20 this month. Renamed the Internet Crime Complaint Center (IC3) in 2002, the IC3 logged its 5 millionth complaint in March 2020. All that data has improved the public’s awareness of online crimes and helped the FBI and other law enforcement agencies better address internet-enabled attacks, fraud, thefts, and scams.

Online Crimes Grow More Damaging and Targeted

The crimes catalogued by the IC3 mirror the evolution of the web across two decades—growing in sophistication and number as the internet grows ever more essential to our professional and personal lives.

“The scale, scope, speed, and impact of cyber threats is constantly evolving,” said FBI Cyber Division Assistant Director Matt Gorham. “Criminals are opportunistic, and we’ve seen them rapidly adapt to the

cyber environment, creating a variety of schemes to exploit the public and private sector."

In its first full year of operation, the IC3 logged 49,711 complaints. Most of them revolved around internet auction fraud, non-delivery scams, and the West African letter (yes, that now infamous message from a prince or princess with an untapped fortune they wanted to share with you).

"People still fall victim to that letter and versions of it," said Gregory. "We still see scams that involve lotteries or windfalls where the victim just needs to pay what they believe are taxes or some fee to receive the winnings or a share of the fortune." Of course, there is no windfall to claim after the criminal collects those "fees" or "taxes."

"The scale, scope, speed, and impact of cyber threats is constantly evolving."
Matt Gorham, assistant director, FBI Cyber Division

"The more prevailing trend," said Gregory, who has been with the IC3 since its founding, "is that those early, rudimentary scams have given way to more destructive and costly data breaches and network intrusions, ransomware, romance scams, and sophisticated financial crimes like business email compromise."

Criminals still target individuals, but businesses and organizations are becoming more common targets because of the potential of a larger payout.

Losses recorded by the IC3 in recent years reflect the greater financial damage of this evolution. In 2019, victims reported more than $3.5 billion in losses—an average of $7,500 for each of the 467,361 complaints recorded that year. In 2001, the average victim lost $435.

Gregory said the IC3 has also seen a shift in the types of criminals perpetrating the illegal activity. Many of the criminals now live overseas, and organized crime groups are on the rise.

"The sophistication of modern online criminals is the most troubling part," Gregory said. "We used to be able to give people common sense tips to keep them safe; now it is just much harder to tell the real messages and websites from the fake."

Instead of an impersonal spam message with poor spelling and grammar, the scam may arrive via a well-written email that appears to come from a trusted colleague, business, or vendor.

Another enduring trend revealed in 20 years of crime data is that scammers will take advantage of a moment in time to prey on people who want to help or may need help in the wake of a natural disaster or tragic event.

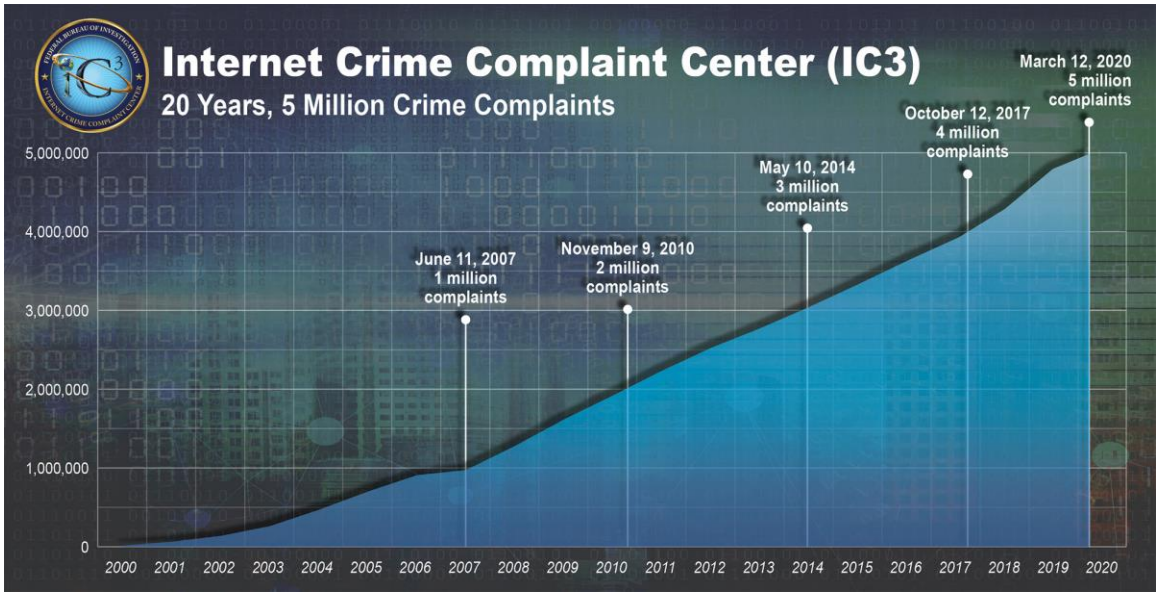
The center saw an uptick in charity and disaster fraud reports around the time of Hurricanes Rita and Katrina and after the Boston Marathon bombings.

In 2008, scammers tried to gather banking information from Americans waiting to receive stimulus checks as the nation slipped into recession.

Now, during the COVID 19 pandemic, scammers are working overtime hawking fake cures and investments schemes, selling protective equipment without the inventory on hand, and looking to take advantage of a more concentrated online presence during increased telework and distance learning arrangements.

“Criminals and scammers go where there is opportunity,” said Gorham. “Right now, they are exploiting a public health emergency to steal from and deceive people who are vulnerable, worried, or seeking vital supplies and assistance.”

“Those early, rudimentary scams have given way to more destructive and costly data breaches and network intrusions, ransomware, romance scams, and sophisticated financial crimes like business email compromise.” Donna Gregory, chief, IC3



Supporting Investigations

The IC3 collects and reports out its data in an annual report and educates the public by sending out notices about new scams or upticks in certain type of crimes. Its other key role is to support law enforcement.

Federal, state, local, and tribal agencies can access the IC3's data through a secure database.

"The IC3 was created to provide the public and law enforcement with valuable information collected and analyzed by the FBI." Gorham stated. "By sharing this information, we hope to protect the American public from becoming victims of cyber crime and enable law enforcement to identify links and trends they may not otherwise be able to see."

Gregory also points to how IC3 data has helped improve the FBI's response to frauds carried out online. "We were seeing victims losing a lot of money, mostly through cases of business e-mail compromise," she said. "Initially we were able to work with financial institutions to examine wires going to international banks. Once we saw success in stopping some of those transactions, the criminals shifted to domestic accounts."

Gregory said money mules play a huge role in dividing up stolen money into U.S. accounts before moving it overseas. Money mules are people who allow criminals to use their bank accounts to launder illicit funds—either because they are receiving a commission for the service or because they trust the person asking for access to their account.

"Law enforcement could not keep up as the money started moving through U.S. accounts," Gregory said. "By the time they could take action, it was too late. So we started to look into working directly with the banks to stop the money flow and give law enforcement time to do the investigation."

In 2018, the FBI created the Recovery Asset Team to streamline communication with financial institutions and FBI field offices to halt fraudulent transactions faster. The team successfully recovered more than $300 million for victims in 2019.

After 20 years with the IC3, Gregory has learned that the online environment will continue to change and that the criminals will adapt along with it. She worries about the trends she's seeing in manipulated photos and videos but can never be certain where the next threat will emerge. The only things that are certain is that the IC3 will continue to evolve as well, finding new and better ways to warn and protect the public from cyber scams and support law enforcement as they combat the threat.

To report a crime or see the IC3's annual reports and warnings about current crimes, scams and frauds, visit ic3.gov.

For more information on common online crimes and prevention tips, visit the FBI's Common Scams and Crimes page.

To read more:
https://www.fbi.gov/news/stories/ic3-20th-anniversary-050820

Number 15

Manipulation ecosystem of social messaging platforms

Published by the NATO Strategic Communications Centre of Excellence

Social messaging platforms started as an alternative to the Short Messaging Service (SMS), pitching themselves as faster and cheaper, with additional features such as the ability to send documents and media securely.

These features granted users a level of encryption that meant no third party, including the messaging services themselves, was able to read the messages sent.

Today, social messaging platforms account for a combined 4.1 billion users and social messaging has become the most frequent activity a person carries out online.

Similarly to major social media platforms that are being artificially inflated and manipulated for financial and political gain, social messaging platforms are equally vulnerable to the threat of exploitation.

This study maps the online market for manipulation tools and services available for two popular messaging applications: WhatsApp and Telegram.

In doing so, we assess the effectiveness of these tools and services against the protective mechanisms put up by the messaging applications.

This publication aims to provide national institutions and communications practitioners with an overview of the scale and effect of manipulation on these popular social messaging platforms.

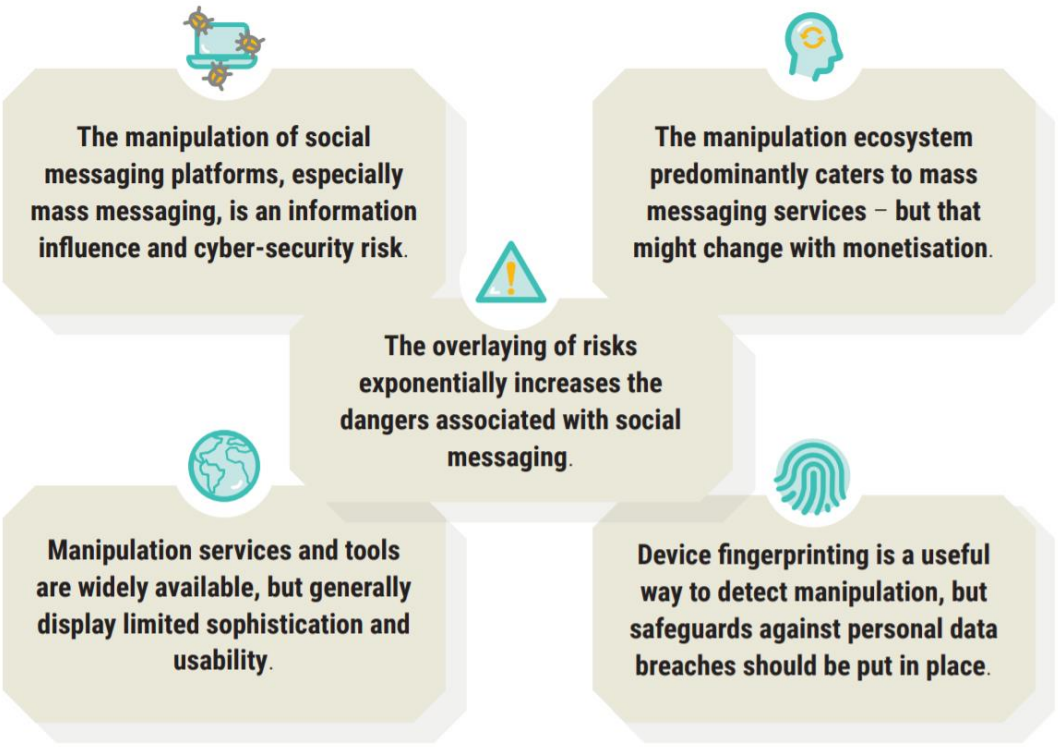
In collaboration with Singularex, a Ukrainian social media analytics company, we conducted the study in two parts.

The first part consisted of a landscape scan of the manipulation tools and services available for WhatsApp and Telegram.

We searched the web and spoke to sellers and freelancers over a period of two months to understand what a customer, or a potential malign actor, can purchase online. Given that previous research on social media had

shown no significant difference between social media manipulation services available on the dark web and the open web, we decided to focus our efforts on finding as diverse a group of services on the open web as we could.

The second part involved assessing the tools and services identified. This included evaluating the cost, methods and scale of manipulation available, the quality of manipulation tools and services, and the ability of WhatsApp and Telegram to identify and counter manipulation on their platforms.



To read more: https://www.stratcomcoe.org/manipulation-ecosystem-social-messaging-platforms

Number 16

Researchers on DARPA's Brandeis Program Enhance Privacy Protections for Android Applications

Privacy Enhancements for Android simplifies implementation of privacy protections for mobile apps running on Android OS

From navigation to remote banking, mobile device users rely on a variety of applications to streamline daily tasks, communicate, and dramatically increase productivity.

While exceedingly useful, the ecosystem of third-party applications utilizes a number of sensors – microphones, GPS, pedometers, cameras – and user interactions to collect data used to enable functionality.

Troves of sensitive personal data about users are accessible to these applications and as defense and commercial mobile device users become increasingly reliant on the technology, there are growing concerns around the challenge this creates for preserving user privacy.

Under DARPA's Brandeis program, a team of researchers led by Two Six Labs and Raytheon BBN Technologies have developed a platform called Privacy Enhancements for Android (PE for Android) to explore more expressive concepts in regulating access to private information on mobile devices.

PE for Android seeks to create an extensible privacy system that abstracts away the details of various privacy-preserving technologies, allowing application developers to utilize state-of-the-art privacy techniques, such as secure multi-party computation and differential privacy, without knowledge of their underlying esoteric technologies.

Importantly, PE for Android allows mobile device users to take ownership of their private information by presenting them with more intuitive controls and permission enforcement options.

The researchers behind PE for Android today released a white paper detailing the platform's capabilities and functionality, and published an open source release of its code to GitHub.

In open sourcing PE for Android, the researchers aim to make it easier for the open-source Android community and researchers to employ enhanced privacy-preserving technologies within Android apps while also

encouraging them to help address the platform's current limitations and build upon its initial efforts.

"User privacy should be a first-rate concern for mobile app development, and we are hoping that open-sourcing PE for Android will galvanize the Android developer community," said Dr. Josh Baron, the DARPA program manager leading Brandeis.

"While the benefits of this to personal and commercial users may be apparent, military personnel are also heavy users of mobile devices and often bring personal devices to or near work. Changes made to the Android ecosystem will therefore have important implications for privacy and security across the Department of Defense. I encourage the community to take a look at the code, improve it if they find gaps, and figure out which parts are deserving of adoption into the broader Android ecosystem."

PE for Android is comprised of a set of extensions and interfaces that are integrated into the Android OS. The primary components, which include APIs, services, and a Privacy Abstraction Layer (PAL), are invoked when applications request private data.

Apps employing PE for Android can opt to send these requests to the platform's Private Data Service and associated modules called µPALs, where data transformation and isolation techniques are implemented to convert private data into less sensitive forms.

This moves sensitive data processing out of the application process space where there is a higher risk of intentional or unintentional data leakage, and into secure services that implement privacy-preserving technologies.

Once the sensitive information is transformed, it may then be returned to the application. Under this model, only the trusted architecture of the Private Data Service – not the requesting app – has direct access to the full scope of sensitive data available through the stock Android API.

Another key component of PE for Android are Policy Managers. This API helps provide fine-grained control of permissions; enabling users to more easily specify their privacy policy and gain greater control over how their private information is used.

Through Policy Managers, users are provided additional context around why the information is needed and how it will be used within a given application. From there, they can make a more informed decision as to what information the application will be given access too.

The PE for Android source code release includes several use cases and applications for these key components, many of which were developed by other research teams working under the Brandeis program.

This includes a Privacy Checkup tool; the Purposes Policy Manager developed by Carnegie Mellon University, which lets people view and set policies for individual apps as well as all apps on a smartphone; and various µPAL modules capable of performing privacy transformations on different types of sensitive data.

The University of Vermont and the Brandeis Helio team are among those responsible for developing the µPAL modules discussed in the white paper.

Additional information about PE for Android is available at:
https://android-privacy.org

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.