March 2020, cyber risk and compliance in Switzerland

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

Dear readers,

The 24th of March 2020, the Reporting and Analysis Centre for Information Assurance (MELANI) released a paper responding to the increased use of *Remote Access* solutions.

According to the paper, the risks are increasing with the number of Remote Accesses into an organizations network. Attackers know about the current situation and may try to use different ways of getting access into an organization's network:

- Phishing attempts (be it the classical password harvesting or in case of 2 Factor Authentications the so-called Realtime Phishing),
- Attacks against passwords (Dictionary Attacks, Password Sprayings, Brute Forcing),
- Attacks against unpatched gateway systems,
- Malware attacks (often get undetected if no forced tunneling of all traffic is in place).

Risk management and operational security should quickly adapt to the changed attack surface due to the current situation and take appropriate countermeasures when risks are considered critically high.

MELANI does not recommend making complex changes in the current situation but rather to reduce the risk by increasing detection capabilities.

Using remote working solutions may lead to a large increase in bandwidth. It may not be sufficient to increase bandwidth if downstream devices cannot cope with the amount of traffic (e.g. Firewalls, Intrusion Prevention Systems, but also switches or servers).

If the usage of BYOD (bring your own device) increases due to the situation, ensure that you have basic guidelines for these devices, especially that data belonging to the organisation is stored securely (in an encrypted

container) so that it can be wiped efficiently after, especially when the employee wants to sell his/hers device.

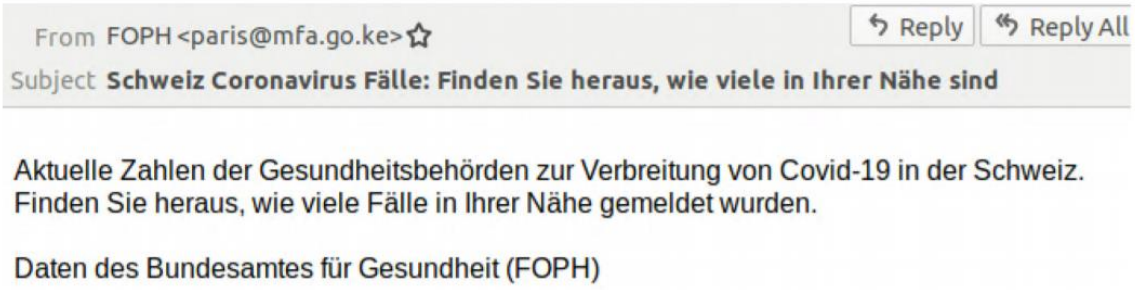
Data stored on an unencrypted SSD can only be wiped with additional effort (if at all).

You can find more at number 17 below.

The 14th of March 2020, the Reporting and Analysis Centre for Information Assurance (MELANI) made us aware of false emails purporting to be from the FOPH.

According to MELANI, since Friday lunchtime (13 March 2020), cybercriminals have been exploiting public anxiety related to the coronavirus.

They are attempting to spread malware using emails purporting to be from the FOPH. The Reporting and Analysis Centre for Information Assurance MELANI is therefore warning the public. Delete such emails immediately.



Using false emails and posts on the subject of the coronavirus, cybercriminals are currently attempting to infect computers and spread a malware entitled AgentTesla.

The emails appear to show the sender as being the Federal Office of Public Health (FOPH). MELANI is urgently calling on the public to ignore such emails, not to open any attachments, and on no account to click on any links they may contain.

The malware is installed by opening the attachment or by clicking on a link in the mail. This allows the attackers to gain remote access to the computer and obtain passwords.

If you clicked on an attachment or link in such an email, turn off the computer immediately. If possible, reset the computer or contact a specialist support service. Change all your passwords straight away.

MELANI is monitoring the situation and is in close contact with the relevant authorities.

Sigmund Freud believed that men are more *moral* than they think, and far more *immoral* than they can imagine.

According to *Friedrich Nietzsche,* there are *no moral* phenomena at all, but only a moral interpretation of phenomena.

Freud's or Nietzsche's approach would never restore investor confidence after a crisis. We definitely need clear and effective resolution regimes.

One of the cornerstones of a credible resolution regime is the requirement placed on financial institutions to have, at all times, adequate levels of own funds and specific types of liabilities to support resolution actions.

This requirement ensures that a resolution, necessary for the continuation of critical functions and/or to avoid adverse effects on the financial system, can be financed by reverting to shareholders and creditors of the institution, to minimise the impact of the institution's failure on the wider economy and the financial system, and avoid the use of public funds.

In the European Union (EU), the *Bank Recovery and Resolution Directive (BRRD)* introduced the concept of minimum requirement for own funds and eligible liabilities (MREL) to ensure that European banks have financial resources in sufficient quantity and quality to cover losses upon failure and restore the viability of the going-concern parts of the institution.

According to the report produced by the European Banking Authority (EBA), close to half of the relevant banks are already meeting their requirement, but 117 banks out of 222 exhibit an MREL shortfall reaching EUR 178 bn.

The MREL is one of the key requirements that make resolution credible. It ensures that banks have enough resources to allow resolution authorities to execute their preferred strategy in case of a bank's failure – usually a bail-in or a transfer to a healthy acquirer.

MREL along with effective resolution planning seek to ensure that no public money is required in case of bank's failure. This is critical to ensure that risks are effectively priced, that investors beyond shareholders effectively bear the cost of potential bank failures and that banks are not unduly incentivised to take risk (moral hazard).

Thomas Aquinas believed that a *theologian* considers sin mainly as an offence against God. A *moral* philosopher considers sin as an offence contrary to reasonableness. I know some bankers that consider resolution regimes as an offence contrary to reasonableness (and profitability), but now they have to comply.

Read more at number 6 below.

Cyber insurance is still evolving, as cyber risks change, and organizations still hide the full impact of breaches in order to avoid negative publicity.

This simply means that underwriters have *limited data* to determine the financial impact of attacks. When the risk of cyberattacks is not completely understood, how can they calculate the premium? Actuaries are the unsung heroes of the insurance industry.

After all, only an actuary can tell "*since the first time I saw you, my interest in you has compounded continuously"*.

I have just read an interesting presentation with title *"Cyber underwriting: Managing the risks of digital finance"*, by Fausto Parente, Executive Director of European Insurance and Occupational Pensions Authority (EIOPA) at the AFORE 4th Annual FinTech and Regulation Conference in Brussels. He said:

"In the old days, they used to say *knowledge is power*. Today, it's more likely to be *data is power*. In the world of insurance for example, products, policies and pricing are all *powered by data*."

He continued: "The increasing frequency of cyber attacks, coupled with stricter regulation regarding cyber security as well as continued technological developments are all expected to increase demand for cyber insurance in the near future.

First and foremost, we have seen that a *lack of data* is one of the biggest obstacles to a detailed understanding of the fundamental aspects of cyber risk and the provision of proper coverage.

It's understandable of course that companies are *reluctant* to share information on their security measures and their history of cyber incidents. The information is extremely sensitive, but it is also incredibly valuable to underwriters.

And this lack of quantitative information on incidents makes it difficult for insurers to *properly price* risk and estimate the liability of exposures. It also hampers cyber risk measurement and management for insurers."

Well, Fausto Parente hit the nail on the head.

Actuaries need data. When you tell them *"look at those white horses over there",* they will answer *"they're white on this side, anyway."* It will not be easy to give them accurate, complete and appropriate cyber risk data.

Read more at number 13 below. Welcome to the Top 10 list.

I have just read the Draft NISTIR (National Institute of Standards and Technology Interagency Report) 8276, Key Practices in Cyber Supply Chain Risk Management: Observations from Industry.

As we can read in the report, in today's highly connected world, all organizations rely on other organizations for critical products and services. However, today's world of globalization, while providing many benefits, has resulted in a world where organizations no longer fully control—and often do not have full visibility into—the supply ecosystems of the products that they make or the services that they deliver.

With more and more businesses becoming digital, producing digital products and services, and moving their workloads to the cloud, the impact of a cybersecurity event today is greater than ever before and could include personal data loss, significant financial losses, compromise of safety, and even loss of life.

Organizations can no longer protect themselves by simply securing their own infrastructures, since their electronic perimeter is no longer meaningful; threat actors intentionally target the suppliers of more cyber-mature organizations to take advantage of the weakest link.

There are 21 recommendations in this report. Some of them are:

- Know if your data and infrastructure are accessible to suppliers' sub-suppliers.

- Propagate security requirements to suppliers' sub-suppliers.

- Train key stakeholders in your organization and within the supplier's organization.

- Establish protocols for vulnerability disclosure and incident notification.

- Establish protocols for communications with external stakeholders during incidents.

- Train key stakeholders in your organization and within the supplier's organization.

The report defines Cyber Supply Chain Risk Management (C-SCRM) as a multidisciplinary approach to identify, assess, and mitigate cyber supply chain risks.

Read more at number 10 below.

Thomas A. Edison believed that the *doctor of the future* will give *no medicine* but will instruct his patient in the care of the human frame, in diet, and the cause and prevention of disease. I see that we live in this future (at least until we have a decent vaccine for Covid-19).

Coronaviruses are a large family of viruses that are known to cause illness ranging from the common cold to more severe diseases such as Middle East Respiratory Syndrome (MERS) and Severe Acute Respiratory Syndrome (SARS).

The novel coronavirus (COVID-19) that was identified in 2019 in Wuhan, China, has not been previously identified in humans. We must understand better which is the risk, and what we can do. The World Health Organization (WHO) had an excellent idea, to develop online training as a weapon to fight the new coronavirus.

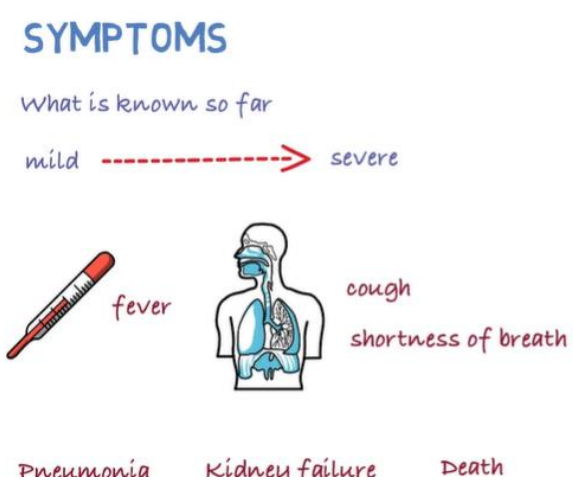
This course provides a general introduction to COVID-19 and emerging respiratory viruses and is intended for public health professionals, incident managers and personnel working for the United Nations, international organizations and NGOs.

The Cybersecurity and Infrastructure Security Agency (CISA) is working closely with partners to prepare for possible impacts of a COVID-19 outbreak in the United States.

COVID-19 containment and mitigation strategies will rely heavily on healthcare professionals and first responders detecting and notifying government officials of occurrences.

In the paper Risk Management for Novel Coronavirus (COVID-19), CISA facilitates communication, coordination, prioritization and information-sharing between the private sector and the government.

As the situation changes, the virus may affect essential operations for businesses and federal, state, local, tribal, and territorial (SLTT) government entities.



Read more at number 9 below.

Welcome to our monthly newsletter.

Best regards,

George Lekatis

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

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

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

Number 1 (Page 11)

Camouflage for the Digital Domain

NATO STRATCOM COE

Number 2 (Page 12)

Critical Infrastructure Protection, Additional Actions Needed to Identify Framework Adoption and Resulting Improvements

United States Government Accountability Office

GAO

Report to Congressional Committees

Number 3 (Page 16)

Robotrolling

Number 4 (Page 18)

Consumers urged to secure internet connected cameras

National Cyber Security Centre

Number 5 (Page 20)

Alert (AA20-049A)
Ransomware Impacting Pipeline Operations

Cybersecurity and Infrastructure Security Agency (CISA)

CISA
CYBER+INFRASTRUCTURE

Number 6 (Page 22)

EBA shows banks' progress in planning for failure but encourages them to issue eligible debt instruments

EBA EUROPEAN BANKING AUTHORITY

Number 7 (Page 24)

Helping to Protect the US 2020 Election

FACEBOOK

Number 8 (Page 26)

Rise in the number of Office 365 phishing scams

National Cyber Security Centre

Number 9 (Page 27)

CISA INSIGHTS
Risk Management for Novel Coronavirus (COVID-19)

CISA
CYBER+INFRASTRUCTURE

Number 10 (Page 34)

NIST Offers Strategies to Help Businesses Secure Their Cyber Supply Chains

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

Number 11 (Page 36)

Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

NIST Special Publication 800-171, Revision 2

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

Number 12 (Page 38)

Invisible Headlights

Harnessing ambient thermal emissions to enable passive 3D vision at night

DARPA
DEFENSE ADVANCED RESEARCH PROJECTS AGENCY

Number 13 (Page 40)

Cyber underwriting: Managing the risks of digital finance

Speech by Fausto Parente at the AFORE 4th Annual FinTech and Regulation Conference, Brussels.

Number 14 (Page 45)

New action to disrupt world's largest online criminal network

Tom Burt - Corporate Vice President, Customer Security & Trust

Microsoft

Number 15 (Page 48)

Cyberspace Solarium Commission (CSC)

A consensus on a strategic approach to defending the US in cyberspace against cyberattacks of significant consequences

Number 16 (Page 50)

The Mind in the Machine

Machine learning is a scientific revolution that is changing how science gets done.

Los Alamos National Laboratory
Delivering science and technology to protect our nation and promote world stability

Number 17 (Page 52)

Home Office: Securing Remote Access

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Finance FDF
National Cyber Security Centre NCSC

Number 1

Camouflage for the Digital Domain

NATO STRATCOM COE

Discoverability of geolocation

Protecting the geolocation of personnel, equipment, infrastructure, and installations of military units is crucial for mission success.

Today's digitalised society generates an abundance of open information that an adversary can exploit to obtain sensitive geolocation information.

While geolocation information is easily accessed using digital sources, it can also be provided directly by conflict participants and the general public via digital platforms.

Geolocation data allows an adversary to discover and adapt to the position and movements of forces, thus serving as a tactical, operational, or strategic force multiplier.

It also often enables or improves kinetic targeting and battle damage assessments. Geolocation data can also be useful information for enemy influence activities against friendly forces.

The paper:
https://www.stratcomcoe.org/camouflage-digital-domain

Number 2

Critical Infrastructure Protection, Additional Actions Needed to Identify Framework Adoption and Resulting Improvements

United States Government Accountability Office

Report to Congressional Committees

Abbreviations

ASPR - Assistant Secretary for Preparedness and Response
DHS - Department of Homeland Security
DOD - Department of Defense
DOT - Department of Transportation
EPA - Environmental Protection Agency
GSA - General Services Administration
HHS - Department of Health and Human Services
ISAC - Information Sharing and Analysis Center
ISO - International Organization for Standardization
IT - information technology
NIST - National Institute of Standards and Technology
SCC - Sector Coordinating Council
SSA - Sector Specific Agency

Conclusions

Most of the SSAs have not determined the level and type of framework adoption, as we previously recommended. Most of the sectors, however, had efforts underway to encourage and facilitate use of the framework. Even with this progress, implementation of our recommendations is essential to the success of protection efforts.

While selected organizations reported varying levels of improvements, the SSAs have not collected and reported sector-wide improvements as a result of framework use.

The SSAs and organizations identified impediments to collecting and reporting sector-wide improvements, including the lack of precise measurements of improvement, voluntary nature of the framework, and lack of a centralized information sharing mechanism.

However, NIST and DHS have initiatives to help address these impediments.

These included an information security measurement program, cybersecurity framework starter profile, information sharing

programs, self-assessment tools, and surveys to support SSAs in measuring and quantifying improvements in the protection of critical infrastructure as a result of using the framework.

However, NIST has yet to establish time frames for completing the information security measurement program and starter profile.

Moreover, the SSAs have yet to report on sector-wide improvements using the initiatives.

Until they do so, the critical infrastructure sectors may not fully understand the value of the framework to better protect their critical infrastructures from cyber threats.

Recommendations

We are making the following 10 recommendations to NIST and the nine sector-specific agencies.

The Director of NIST should establish time frames for completing NIST's initiatives, to include the information security measurement program and the cybersecurity framework starter profile, to enable the identification of sector-wide improvements from using the framework in the protection of critical infrastructure from cyber threats. (Recommendation 1).

The Secretary of Agriculture, in coordination with the Secretary of Health and Human Services, should take steps to consult with respective sector partner(s), such as the SCC, DHS, and NIST, as appropriate, to collect and report sector-wide improvements from use of the framework across its critical infrastructure sector using existing initiatives. (Recommendation 2).

The Secretary of Defense should take steps to consult with respective sector partner(s), such as the SCC, DHS, and NIST, as appropriate, to collect and report sector-wide improvements from use of the framework across its critical infrastructure sector using existing initiatives. (Recommendation 3).

The Secretary of Energy should take steps to consult with respective sector partner(s), such as the SCC, DHS, and NIST, as appropriate, to collect and report sector-wide improvements from use of the framework across its critical infrastructure sector using existing initiatives. (Recommendation 4).

The Administrator of the Environmental Protection Agency should take steps to consult with respective sector partner(s), such as the SCC, DHS,

and NIST, as appropriate, to collect and report sector-wide improvements from use of the framework across its critical infrastructure sector using existing initiatives. (Recommendation 5).

The Administrator of the General Services Administration, in coordination with the Secretary of Homeland Security, should take steps to consult with respective sector partner(s), such as the Coordinating Council and NIST, as appropriate, to collect and report sector-wide improvements from use of the framework across its critical infrastructure sector using existing initiatives. (Recommendation 6).

Figure 1: Critical Infrastructure Sectors and Related Sector-Specific Agencies

Source: GAO analysis of Presidential Policy Directive-21 and Critical Infrastructure Protection GAO-18-211; Art Explosion (clip art). | GAO-20-299

The Secretary of Health and Human Services, in coordination with the Secretary of Agriculture, should take steps to consult with respective sector partner(s), such as the SCC, DHS, and NIST, as appropriate, to collect and report sector-wide improvements from use of the framework across its critical infrastructure sector using existing initiatives. (Recommendation 7).

The Secretary of Homeland Security should take steps to consult with

respective sector partner(s), such as the SCC and NIST, as appropriate, to collect and report sector-wide improvements from use of the framework across its critical infrastructure sectors using existing initiatives. (Recommendation 8).

The Secretary of Transportation, in coordination with the Secretary of Homeland Security, should take steps to consult with respective sector partner(s) such as the SCC and NIST, as appropriate, to collect and report sector-wide improvements from use of the framework across its critical infrastructure sector using existing initiatives. (Recommendation 9).

The Secretary of the Treasury should take steps to consult with respective sector partner(s), such as the SCC, DHS, and NIST, as appropriate, to collect and report sector-wide improvements from use of the framework across its critical infrastructure sector using existing initiatives. (Recommendation 10).

The report:
https://www.gao.gov/assets/710/704808.pdf

Number 3

Robotrolling

In authentic English- and Russian-language conversations on Twitter about the NATO presence in Poland and the Baltic States peaked on 4 and 5 December, respectively, coinciding with the 2019 NATO Leaders' Meeting in London.

Robotic accounts focused heavily on the meeting this quarter, particularly on English-language Twitter, which saw roughly 3 times the usual level of bot activity.

On VK, an anomalous increase in activity from anonymous human - controlled accounts coincided with the meeting.

Due to the contentious atmosphere surrounding the meeting in London, a considerable increase in the proportion of posts generated by bots was observed on English-language Twitter this quarter.

At the same time, Russian-language bot activity on Twitter decreased to the lowest level observed thus far.

In this issue of Robotrolling, we dig deeply into a sample of political pages amassed by a COE report on commercial social media manipulation in order to identify patterns in inauthentic activity on Facebook.

We demonstrate that the 2019 elections in Ukraine were the primary focus of actors willing to pay for inflated social media engagement.

Our analysis also reveals several shared traits among political manipulators on Facebook and provides a network visualisation that shows the connections between them.

As a new year of Robotrolling begins, we review trends observed in VK groups over the past 18 months.

A steady reduction in the proportion of content shared in communities dedicated to the so-called Novorossia region and the Donbass coincides with inauthentic content increasingly being posted in community spaces such as private groups or pages.

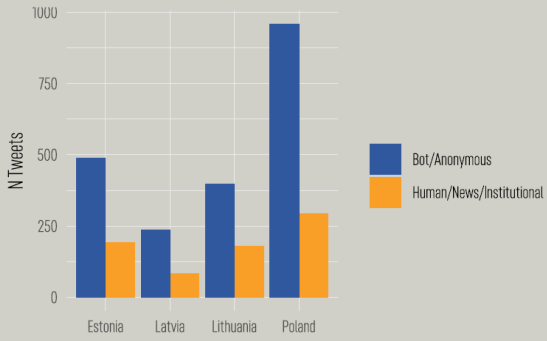


Figure 2: Total number of tweets mentioning NATO and Estonia, Latvia, Lithuania, or Poland, by account type.

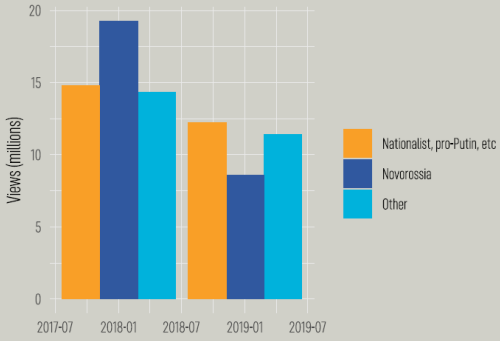


Figure 3: Views of content about NATO in the Baltics and Poland, posted to community spaces on VK and subdivided by community cluster.

Figure 4: Timeline of VK and Twitter mentions.

To read more: https://www.stratcomcoe.org/publications

Number 4

Consumers urged to secure internet connected cameras

This week, with the support from Which? (https://www.which.co.uk/news/2020/03/consumers-urged-to-secure-internet-connected-cameras-in-the-home/), we published new consumer advice and guidance on how to secure internet connected cameras in the home (https://www.ncsc.gov.uk/guidance/smart-security-cameras-using-them-safely-in-your-home).

We're all becoming more reliant on 'smart' technology, and things like connected security cameras and baby monitors help make our lives easier. However, insecure default settings can leave devices vulnerable to cyber criminals.

In rare cases, live feeds or images from smart cameras can be accessed by unauthorised users and that's why we outlined three steps people can take to make their devices safer:

- If your camera comes with a default password, change it to a secure one – connecting three random words which you'll remember is a good way to do this.

  You can usually change your password using the app you use to manage the device.

- Keep your camera secure by regularly updating security software. Not only does this keep your devices secure, but often adds new features and other improvements.

- If you do not use the feature that lets you remotely access the camera from the internet, it is recommended you disable it.

The NCSC is supporting the Department for Digital, Culture, Media & Sport (DCMS) in the development of future UK legislation, which will ensure consumer smart devices sold in the UK adhere to three rigorous security requirements.

These are:

1. Device passwords must be unique and not resettable to any universal factory setting,

2. Manufacturers must provide a public point of contact so anyone can report a vulnerability,

3. Manufacturers & retailers must state the minimum length of time for which the device will receive security updates.

More information at: https://www.ncsc.gov.uk/guidance/smart-security-cameras-using-them-safely-in-your-home

Number 5

Alert (AA20-049A)
Ransomware Impacting Pipeline Operations

Cybersecurity and Infrastructure Security Agency (CISA)

The Cybersecurity and Infrastructure Security Agency (CISA) encourages asset owner operators across all critical infrastructure sectors to review the below threat actor techniques and ensure the corresponding mitigations are applied.

CISA responded to a cyberattack affecting control and communication assets on the operational technology (OT) network of a natural gas compression facility.

A cyber threat actor used a Spear phishing Link [https://attack.mitre.org/techniques/T1192/] to obtain initial access to the organization's information technology (IT) network before pivoting to its OT network.

The threat actor then deployed commodity ransomware to Encrypt Data for Impact on both networks. Specific assets experiencing a Loss of Availability on the OT network included human machine interfaces (HMIs), data historians, and polling servers.

Impacted assets were no longer able to read and aggregate real-time operational data reported from low-level OT devices, resulting in a partial Loss of View for human operators.

The attack did not impact any programmable logic controllers (PLCs) and at no point did the victim lose control of operations.

Although the victim's emergency response plan did not specifically consider cyberattacks, the decision was made to implement a deliberate and controlled shutdown to operations.

This lasted approximately two days, resulting in a Loss of Productivity and Revenue, after which normal operations resumed. CISA is providing this Alert to help administrators and network defenders protect their organizations against this and similar ransomware attacks.

Network and Assets

- The victim failed to implement robust segmentation between the IT and OT networks, which allowed the adversary to traverse the IT-OT boundary and disable assets on both networks.

- The threat actor used commodity ransomware to compromise Windows-based assets on both the IT and OT networks. Assets impacted on the organization's OT network included HMIs, data historians, and polling servers.

- Because the attack was limited to Windows-based systems, PLCs responsible for directly reading and manipulating physical processes at the facility were not impacted.

- The victim was able to obtain replacement equipment and load last-known-good configurations to facilitate the recovery process.

- All OT assets directly impacted by the attack were limited to a single geographic facility.

To read more: https://www.us-cert.gov/ncas/alerts/aa20-049a

Number 6

EBA shows banks' progress in planning for failure but encourages them to issue eligible debt instruments

- Close to half of the relevant banks are already meeting their requirement yet the EBA Report estimates that 117 banks out of 222 exhibit an MREL shortfall reaching EUR 178 bn

- Weighted average MREL requirements range between 26.5% and 19%

- Bank should take advantage of positive market condition to close MREL shortfalls

The European Banking Authority (EBA) published its first quantitative Report on minimum requirements for own funds and eligible liabilities (MREL) under a new methodology. The report shows that authorities have made strong progress in agreeing resolution strategies and setting related MREL requirements but it also notes that banks need to issue MREL eligible debt to close their shortfall.

222 European banks representing 80% of total assets are covered by a resolution strategy other than liquidation. This is reflective of the fact that authorities have progressed since the introduction of BRRD in 2014 and the fact that the majority of European banking assets are held by large and complex banking groups for which liquidation is not deemed appropriate.

On a weighted average basis, MREL requirements in the EU range between 26.5% of risk-weighted assets (RWAs) for the global systemically important institutions (G-SIIs) – the largest and most complex banks – and 19% of RWAs for the banks with total assets below EUR 1 billion that are neither G-SIIs nor other systemically important institutions (O-SIIs).

Overall, MREL levels are reflective of banks' going-concern requirements; in the case of transfer strategies, MREL levels also reflect the scaling down of MREL based on the transfer perimeter.

105 banks out of 222 sample already meet their requirement while the rest reported an estimated MREL shortfall of EUR178bn. While this is significant, it is worth noting that 65 of those banks with shortfalls also report instruments totaling EUR67bn that are close in nature to MREL but not eligible.

This shows that some banks already have a sophisticated investor base, likely to invest in long-term unsecured debt such as MREL eligible instruments.

In the light of these shortfalls, the EBA encourages European resolution groups to take advantage of the current positive market conditions to issue and build up resources.

As pointed out in the recent EBA risk assessment report, despite continued volatility, spreads for all market instrument have been on a downward trend for most of 2019, with spreads between secured and unsecured as well as between senior and subordinated instruments narrowing.

Note

The Report is based on data provided by resolution authorities and covers the actual population of banks covered by an MREL decision, the actual level of this requirement and the level of resources effectively eligible in the relevant jurisdictions.

The Report will be updated annually. You may visit: https://eba.europa.eu/eba-shows-banks%E2%80%99-progress-planning-failure-encourages-them-issue-eligible-debt-instruments

Number 7

Helping to Protect the US 2020 Election

FACEBOOK

This overview provides a look at Facebook's comprehensive efforts over the past three years to help protect the democratic process ahead of the 2020 US elections.

We know that elections have changed, and so has Facebook.

We've worked to develop a comprehensive strategy to close previous vulnerabilities while addressing new and emerging threats.

And we've developed smarter tools, greater transparency, and stronger partnerships to help us do just that.

We have more than 35,000 people dedicated to safety and security issues, with about 40 teams contributing to our work on elections.

We block millions of fake accounts each day so they can't spread misinformation.

We continue to improve our coordination and cooperation with law enforcement, including DNI, DHS, FBI, as well as other federal officials, state election officials, and technology companies, to support better information sharing and threat detection in service of public safety.

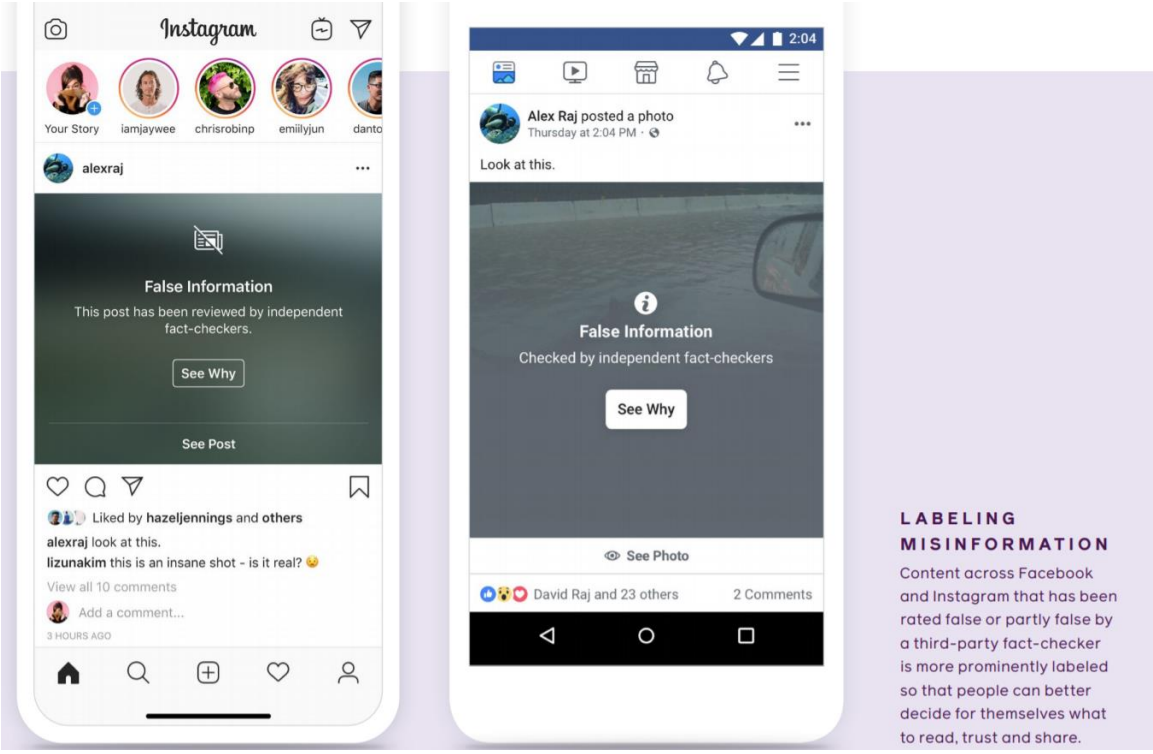
And we've set a new standard for transparency in Pages and political ads so people can see who is behind them.

In 2016, we were on the lookout for traditional cyber threats like hacking and stealing information.

What happened was a much different kind of attack, meant to sow social discord around divisive political issues.

We've learned lessons from 2016 and while we have seen threats evolve, we're working hard to stay ahead of those efforts so it's harder to use our platform for election interference.

We know that security is never finished and we can't do this alone— that's why we continue to work with policymakers and experts to make sure we are constantly improving.



The report: https://about.fb.com/wp-content/uploads/2020/02/Helping-to-Protect-the-US-2020-Elections.pdf

Number 8

Rise in the number of Office 365 phishing scams

Cyber security researchers have uncovered an increase in the number of low-quality phishing scams that aim to trick users into revealing their credentials.

According to a new report from Cofense, there has been a surge in scam attempts using illegitimate and badly created Office 365 credentials update forms. The report: https://cofense.com/phishers-using-google-forms-bypass-popular-email-gateways/

Potential victims receive an email claiming to be from their organisation's IT team that tells them their account will expire unless they click the link and update their details.

Cofense note that the criminals behind the scam went to great lengths to appear legitimate. The phishing email originates from a compromised company email account, which allows the scam to bypass basic email security checks.

However, the forms that potential victims are directed to are often littered with grammatical and spelling mistakes.

Phishers use a wide variety of techniques to try and scam users into revealing sensitive data about themselves or the businesses they work for. The NCSC has published guidance on how the public and organisations can defend themselves against such attacks.

The NCSC has also published advice on securely configuring Office 365 to protect against the rise in credential stealing attacks at: https://www.ncsc.gov.uk/blog-post/securing-office-365-with-better-configuration

Number 9

CISA INSIGHTS
Risk Management for Novel Coronavirus (COVID-19)

The Threat and How to Think About It

This product is for executives to help them think through physical, supply chain, and cybersecurity issues that may arise from the spread of Novel Coronavirus, or COVID-19.

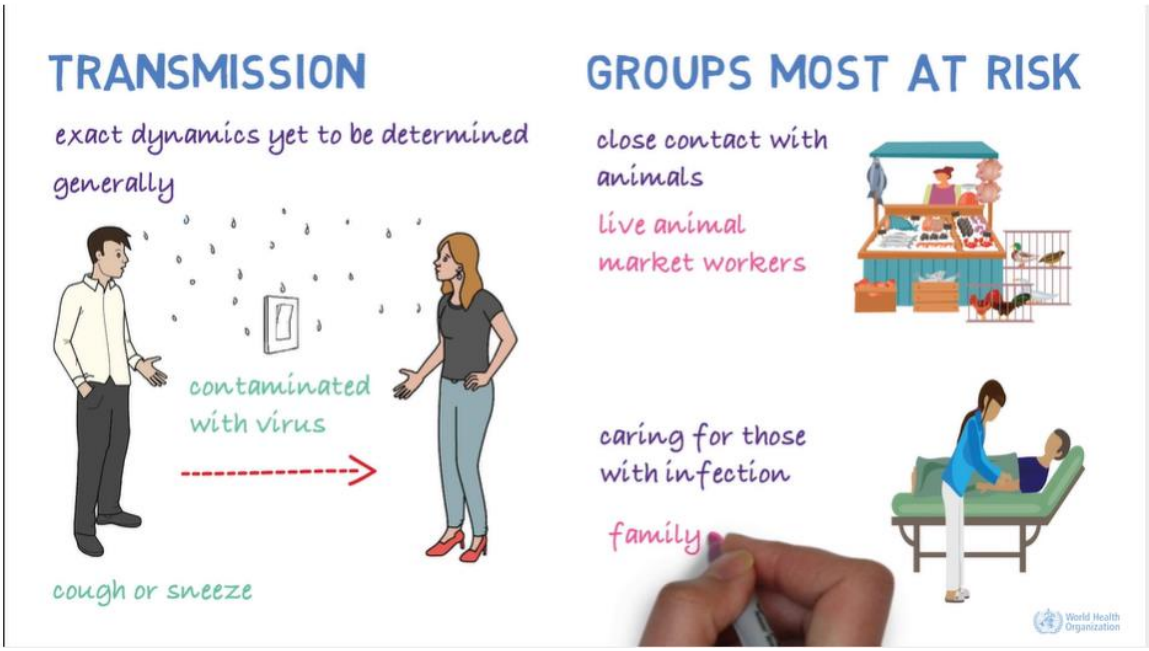
According to the U.S. Centers for Disease Control and Prevention (CDC), COVID-19 has been detected in locations around the world, including multiple areas throughout the U.S. This is a rapidly evolving situation and for more information, visit the CDC's COVID-19 Situation Summary.

To read more:
https://www.cisa.gov/sites/default/files/publications/20_0306_cisa_insights_risk_management_for_novel_coronavirus_0.pdf

https://www.cdc.gov/coronavirus/2019-ncov/summary.html

Online training as a weapon to fight the new coronavirus

The learning team of the WHO Health Emergencies Programme worked with technical experts to quickly develop and publish the online course – you may visit: https://openwho.org/courses/introduction-to-ncov



Approximately 3000 new users have registered for the training every day since its launch, demonstrating the high level of interest in the virus among health professionals and the general public.

In addition, more than 200 000 people have viewed the introductory video to the course on YouTube.

The high engagement levels emerged as the international community launched a US$675 million preparedness and response plan to fight further spread of the new coronavirus and protect states with weaker health systems.

The free learning resource is available to anyone interested in novel coronavirus on WHO's open learning platform for emergencies, OpenWHO.org.

The platform was established 3 years ago with emergencies such as nCoV in mind, in which WHO would need to reach millions of people across the globe with real-time, accessible learning materials.

The online training – entitled “Emerging respiratory viruses, including nCoV: methods for detection, prevention, response and control” – is currently being produced in all official UN languages and Portuguese.

“Our job is to work with technical health experts to package knowledge using adult learning principles, quickly so that it is most useful to health workers and our staff,” said Heini Utunen, who manages OpenWHO for the WHO Health Emergencies Programme (WHE).

“Our online platform – OpenWHO – is already accessed by users from every country on earth, providing more than 60 courses in 21 languages. Delivering trainings in the local language of responders is really important, especially in an emergency”.

WHE has been investing in learning and training to strengthen preparedness and real-time response to health emergencies.

The programme developed its first-ever learning strategy in 2018 and has a small dedicated Learning and Capacity Development Unit that allows WHE to develop trainings quickly and get know-how to those who most need it at the front line.

Interim Guidance for Businesses and Employers

This interim guidance is based on what is currently known about the coronavirus disease 2019 (COVID-19). The Centers for Disease Control and Prevention (CDC) will update this interim guidance as needed and as additional information becomes available.

The following interim guidance may help prevent workplace exposures to acute respiratory illnesses, including COVID-19, in non-healthcare settings. The guidance also provides planning considerations if there are more widespread, community outbreaks of COVID-19.

Recommended strategies for employers to use now:

1. Actively encourage sick employees to stay home:

- Employees who have symptoms of acute respiratory illness are recommended to stay home and not come to work until they are free of fever (100.4° F [37.8° C] or greater using an oral thermometer), signs of a fever, and any other symptoms for at least 24 hours, without the use of fever-reducing or other symptom-altering medicines (e.g. cough suppressants). Employees should notify their supervisor and stay home if they are sick.

- Ensure that your sick leave policies are flexible and consistent with public health guidance and that employees are aware of these policies.

- Talk with companies that provide your business with contract or temporary employees about the importance of sick employees staying home and encourage them to develop non-punitive leave policies.

- Do not require a healthcare provider's note for employees who are sick with acute respiratory illness to validate their illness or to return to work, as healthcare provider offices and medical facilities may be extremely busy and not able to provide such documentation in a timely way.

- Employers should maintain flexible policies that permit employees to stay home to care for a sick family member. Employers should be aware that more employees may need to stay at home to care for sick children or other sick family members than is usual.

2. Separate sick employees:

CDC recommends that employees who appear to have acute respiratory illness symptoms (i.e. cough, shortness of breath) upon arrival to work or become sick during the day should be separated from other employees and be sent home immediately. Sick employees should cover their noses and mouths with a tissue when coughing or sneezing (or an elbow or shoulder if no tissue is available).

3. Emphasize staying home when sick, respiratory etiquette and hand hygiene by all employees:

- Place posters that encourage staying home when sick, cough and sneeze etiquette, and hand hygiene at the entrance to your workplace and in other workplace areas where they are likely to be seen.

- Provide tissues and no-touch disposal receptacles for use by employees.

- Instruct employees to clean their hands often with an alcohol-based hand sanitizer that contains at least 60-95% alcohol, or wash their hands with soap and water for at least 20 seconds. Soap and water should be used preferentially if hands are visibly dirty.

- Provide soap and water and alcohol-based hand rubs in the workplace. Ensure that adequate supplies are maintained. Place hand rubs in multiple locations or in conference rooms to encourage hand hygiene.

- Visit the coughing and sneezing etiquette and clean hands webpage for more information.

4. Perform routine environmental cleaning:

- Routinely clean all frequently touched surfaces in the workplace, such as workstations, countertops, and doorknobs. Use the cleaning agents that are usually used in these areas and follow the directions on the label.

- No additional disinfection beyond routine cleaning is recommended at this time.

- Provide disposable wipes so that commonly used surfaces (for example, doorknobs, keyboards, remote controls, desks) can be wiped down by employees before each use.

5. Advise employees before traveling to take certain steps:

- Check the CDC's Traveler's Health Notices for the latest guidance and recommendations for each country to which you will travel. Specific travel information for travelers going to and returning from China, and information for aircrew, can be found at on the CDC website.

- Advise employees to check themselves for symptoms of acute respiratory illness before starting travel and notify their supervisor and stay home if they are sick.

- Ensure employees who become sick while traveling or on temporary assignment understand that they should notify their supervisor and should promptly call a healthcare provider for advice if needed.

- If outside the United States, sick employees should follow your company's policy for obtaining medical care or contact a healthcare provider or overseas medical assistance company to assist them with finding an appropriate healthcare provider in that country. A U.S. consular officer can help locate healthcare services. However, U.S. embassies, consulates, and military facilities do not have the legal authority, capability, and resources to evacuate or give medicines, vaccines, or medical care to private U.S. citizens overseas.

6. Additional Measures in Response to Currently Occurring Sporadic Importations of the COVID-19:

- Employees who are well but who have a sick family member at home with COVID-19 should notify their supervisor and refer to CDC guidance for how to conduct a risk assessment of their potential exposure.

- If an employee is confirmed to have COVID-19, employers should inform fellow employees of their possible exposure to COVID-19 in the workplace but maintain confidentiality as required by the Americans with Disabilities Act (ADA). Employees exposed to a co-worker with confirmed COVID-19 should refer to CDC guidance for how to conduct a risk assessment of their potential exposure.

The severity of illness or how many people will fall ill from COVID-19 is unknown at this time. If there is evidence of a COVID-19 outbreak in the U.S., employers should plan to be able to respond in a flexible way to varying levels of severity and be prepared to refine their business response plans as needed.

For the general American public, such as workers in non-healthcare settings and where it is unlikely that work tasks create an increased risk of

exposures to COVID-19, the immediate health risk from COVID-19 is considered low.

The CDC and its partners will continue to monitor national and international data on the severity of illness caused by COVID-19, will disseminate the results of these ongoing surveillance assessments, and will make additional recommendations as needed.

To read more: https://www.cdc.gov/coronavirus/2019-ncov/community/guidance-business-response.html

Number 10

NIST Offers Strategies to Help Businesses Secure Their Cyber Supply Chains

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

Reducing the cybersecurity risk to one of the most vulnerable aspects of commerce — global supply chains — is the goal of a new publication by the National Institute of Standards and Technology (NIST), whose computer security experts have distilled a set of effective risk management techniques into a draft guidebook for businesses. NIST is seeking public comment on the draft for the next 30 days.

Key Practices in Cyber Supply Chain Risk Management (Draft NISTIR 8276 - https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8276-draft.pdf) provides a set of strategies to help businesses address the cybersecurity issues posed by modern information and communications technology products, which are commonly built using components and services supplied by third-party organizations.

The composed nature of these devices and systems makes them difficult to secure effectively against malware and other threats, placing manufacturers, service providers and end users at risk.

“The seed of the problem is that everything is interconnected nowadays,” said NIST’s Jon Boyens, one of the draft report’s authors. “Products are very sophisticated, and with our globalized economy, companies often outsource the tasks of developing components and code to other companies, involving multiple tiers of suppliers.”

Vulnerabilities in the cyber supply chain — really a complex network of connections rather than a single strand — involve not only microchips and their internal code, but also the support software for a device and the other companies that have access to its components.

Put them all together, and it can be a daunting task to anticipate every systemic weakness that an adversary might exploit.

Many recent cyber breaches have been linked to supply chain risks. A recent high-profile attack from the second half of 2018, Operation ShadowHammer, is estimated to have affected up to a million users. A 2013 attack by the Dragonfly group targeted companies with industrial control systems, such as those distributing energy within the U.S. This attack infected companies in critical industries with malware. Symantec’s

2019 Internet Security Threat Report found supply chain attacks increased by 78 percent in 2018.

The NIST report is a high-level document intended to be easily understood and applied in managing these risks. Its core is a 27-page section outlining eight key practices that have proved to be useful, from establishing a formal risk management program to collaborating closely with key suppliers.

Each key practice is accompanied by a set of recommendations, and because each organization will have its own specific needs, the authors also include guidance on how to apply these recommendations.

Acknowledging that companies in different economic sectors might manage supply chain risk differently, the authors also offer a set of 24 case studies in risk management that feature a variety of businesses ranging from aerospace and IT manufacturers to consumer goods companies. These case studies, along with a summary of the findings, are available at NIST's Cyber Supply Chain Risk Management Key Practices page.

"Many companies share the same suppliers, but their overall supply chains are still very different," Boyens said. "To supplement our report you can look for the case studies that are relevant to your industry."

The April 2018 update to the NIST Cybersecurity Framework added a new section about supply chain risk management, and the new report cross-references the framework so that organizations can use both sets of NIST guidance together, Boyens said.

Public comments on Draft NISTIR 8276 can be submitted until March 4, 2020, to scrm-nist@nist.gov, and NIST will consider them before releasing a final version, planned for Spring 2020.

Number 11

Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

NIST Special Publication 800-171, Revision 2

The protection of Controlled Unclassified Information (CUI) resident in nonfederal systems and organizations is of paramount importance to federal agencies and can directly impact the ability of the federal government to successfully conduct its essential missions and functions.

This publication provides agencies with recommended security requirements for protecting the confidentiality of CUI when the information is resident in nonfederal systems and organizations; when the nonfederal organization is not collecting or maintaining information on behalf of a federal agency or using or operating a system on behalf of an agency; and where there are no specific safeguarding requirements for protecting the confidentiality of CUI prescribed by the authorizing law, regulation, or governmentwide policy for the CUI category listed in the CUI Registry.

The requirements apply to all components of nonfederal systems and organizations that process, store, and/or transmit CUI, or that provide protection for such components.

The security requirements are intended for use by federal agencies in contractual vehicles or other agreements established between those agencies and nonfederal organizations.

TABLE 1: SECURITY REQUIREMENT FAMILIES

FAMILY	FAMILY
Access Control	Media Protection
Awareness and Training	Personnel Security
Audit and Accountability	Physical Protection
Configuration Management	Risk Assessment
Identification and Authentication	Security Assessment
Incident Response	System and Communications Protection
Maintenance	System and Information Integrity

The purpose of this publication is to provide federal agencies with recommended security requirements for protecting the confidentiality of CUI:

(1) when the CUI is resident in a nonfederal system and organization;

(2) when the nonfederal organization is not collecting or maintaining information on behalf of a federal agency or using or operating a system on behalf of an agency; and

(3) where there are no specific safeguarding requirements for protecting the confidentiality of CUI prescribed by the authorizing law, regulation, or governmentwide policy for the CUI category listed in the CUI Registry.

The requirements apply only to components of nonfederal systems that process, store, or transmit CUI, or that provide security protection for such components.

The requirements are intended for use by federal agencies in appropriate contractual vehicles or other agreements established between those agencies and nonfederal organizations. In CUI guidance and the CUI Federal Acquisition Regulation (FAR), the CUI Executive Agent will address determining compliance with security requirements.

To read more:
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf

Number 12

Invisible Headlights

Harnessing ambient thermal emissions to enable passive 3D vision at night

DEFENSE ADVANCED RESEARCH PROJECTS AGENCY

Autonomous and semi-autonomous systems need active illumination to navigate at night or underground. Switching on visible headlights or some other emitting system like lidar, however, has a significant drawback: It allows adversaries to detect a vehicle's presence, in some cases from long distances away.

To eliminate this vulnerability, DARPA announced the Invisible Headlights program. The fundamental research effort seeks to discover and quantify information contained in ambient thermal emissions in a wide variety of environments and to create new passive 3D sensors and algorithms to exploit that information.

"We're aiming to make completely passive navigation in pitch dark conditions possible," said Joe Altepeter, program manager in DARPA's Defense Sciences Office. "In the depths of a cave or in the dark of a moonless, starless night with dense fog, current autonomous systems can't make sense of the environment without radiating some signal—whether it's a laser pulse, radar or visible light beam—all of which we want to avoid. If it involves emitting a signal, it's not invisible for the sake of this program."

Since everything—animate and inanimate—gives off some thermal energy, the goal is to discover what information can be captured from even an extremely small amount of thermal radiation and then develop novel algorithms and passive sensors to transform that information into a 3D scene for navigation.

The program includes three phases:

1) Discovery – to determine if thermal emissions contain sufficient information to enable autonomous driving at night or underground;

2) Optimization – to refine models, experimental designs, and ensure system feasibility for achieving 3D vision at both low speeds (<25 mph) and high speeds (>25 mph); and

3) Advanced Prototypes – to build and test passive demonstration systems that compete with active sensors.

“If we’re successful, the capability of Invisible Headlights could extend the environments and types of missions in which autonomous assets can operate – at night, underground, in the arctic, and in fog,” Altepeter said. “The fundamental understanding of what information is available in ambient thermal emissions could lead to advances in other areas, such as chemical sensing, multispectral vision systems, and other applications that exploit infrared light.”

A Proposers Day is scheduled for March 16, 2020, in Arlington, Virginia. A webcast will also be available for those participating online. For in-person and webcast registration details visit: https://go.usa.gov/xddrT

A Broad Agency Announcement solicitation is anticipated in the coming weeks to post on https://beta.sam.gov/

Number 13

Cyber underwriting: Managing the risks of digital finance

Speech by Fausto Parente at the AFORE 4th Annual FinTech and Regulation Conference, Brussels.

Introduction

Thank you for inviting me to today's conference. It's always so interesting to hear about the different aspects of FinTech and the pace of innovation. I'm also pleased to be here with the Chairs from my fellow supervisory authorities. Digital finance and FinTech are areas that we all follow closely.

We've heard a lot today about the vast potential of FinTech and how it is changing the lives of business and people.

The digitalisation of finance is dependent on many things, but the core drivers are technology and data. Data is valuable, especially the type of data held by financial institutions. And technology is vulnerable.

And that leaves companies and people open to the risks of cybercrime.

Earlier this morning we heard about the need for operational resilience and the importance of cyber security. The threat of cyber attacks are a serious risk to business. Ask any CEO what keeps him up at night, and cyber attacks and data theft are likely to be high on the list of answers.

So today, I would like to talk to you about two things: the importance of respecting data, and the importance of protecting the people through cyber insurance.

Data is power

Let me start with a few words on the importance of how we treat data.

In the old days, they used to say, 'knowledge is power'. Today, it's more likely to be 'data is power'.

In the world of insurance for example, products, policies and pricing are all powered by data.

This is what makes it so valuable: with data an insurance company is able to offer the consumer just what they need and hopefully at just the right price. It should be a win-win for provider and policyholder.

And more choice and lower costs are what makes consumers so ready to share their data.

But what happens when data is not used ethically? When people find themselves excluded from insurance? Or when the holders of the data do not act responsibly?

At EIOPA, we believe that data needs to be respected. It must be used fairly and organisations holding data must act responsibly.

Because of this, last year we set up a consultative expert group on digital ethics in insurance to help us develop principles of digital responsibility in insurance.

We want these principles to have European values at their core while at the same time recognising the important role that insurance plays in our economy and also in our society.

So we are not reinventing the wheel. Nor are we ignoring the work on artificial intelligence being done by the European Commission and other bodies. Instead we want to operationalise best practice for the insurance sector.

In particular we are paying attention to:

- Fairness and non-discrimination – including data biases and the fairness around the use of price optimisation practices;

- Transparency and explainability – being clear on how data is used and any trade-offs with accuracy;

- Governance – touching on accountability, security and resilience. Security of data is perhaps the most important thing here.

Because cyber attacks and data thefts cost.

They leave companies liable for fines of millions of euro. On top of that, there is the cost to a company's reputation, which is harder to quantify and very difficult – sometimes impossible – to earn back.

So cyber resilience is essential for any organisation and an effective cyber insurance market is a core component of a sound cyber resilience framework.

The cyber insurance market today

A sound cyber insurance market is an enabler of the digital economy.

From raising awareness of the risks and losses that can result from cyber attacks to facilitating responses and recovery, a well-developed cyber insurance market can play a valuable role in risk management.

And the European cyber insurance market is growing rapidly.

This is in part due to the overall increase in written contracts offered by insurers, and also because of the growing number of insurers providing cyber insurance.

And we expect the market to continue to grow.

The increasing frequency of cyber attacks, coupled with stricter regulation regarding cyber security as well as continued technological developments are all expected to increase demand for cyber insurance in the near future.

It's also likely that as businesses make their own investigations and investment into cyber security, they will become more aware of the growing need for insurance cover against cyber attacks.

Cyber underwriting to build European resilience

We need to work together to strengthen cyber resilience and create a strong cyber insurance market.

At EIOPA we have been studying the evolution of cyber insurance in Europe for some years now, including regular dialogue with insurance companies, and we have just published our cyber underwriting strategy.

Our strategy outlines the areas that we see need strengthening and sets out our approach and proposed actions.

First and foremost, we have seen that a lack of data is one of the biggest obstacles to a detailed understanding of the fundamental aspects of cyber risk and the provision of proper coverage.

It's understandable of course that companies are reluctant to share information on their security measures and their history of cyber incidents.

The information is extremely sensitive but it is also incredibly valuable to underwriters.

And this lack of quantitative information on incidents makes it difficult for insurers to properly price risk and estimate the liability of exposures. It also hampers cyber risk measurement and management for insurers.

Therefore, we believe that we need to develop at European level a standardised cyber incident reporting framework that enables the sharing of aggregated data, anonymised to protect sensitive information, so that insurers and reinsurers can develop adequate pricing and risk management models.

To do this, we will engage with different bodies, including national authorities, the EBA and ESMA, as well as ENISA to explore and promote the development of a harmonised cyber incident reporting taxonomy so that we can put the data to work to underpin cyber underwriting modelling.

We also believe that there needs to be a common understanding of contractual definitions. Policyholders and insurers must share the same understanding of contract terms. Clear and transparent cyber coverage is essential from a consumer protection perspective. This is just as important for big companies as it is for individuals.

At European level, EIOPA will work other EU institutions can help to accelerate and promote engagement between industry and consumer associations which, in the long run, will help to maintain consumer confidence and avoid the potential for disputes.

As a supervisor, we are also working closely with national supervisors to ensure that appropriate underwriting standards are in place and that national supervisors have the capacity to supervise these. Technology changes, the nature of cyber attacks change, supervisors must be able to keep pace with these changes.

Continuing European cooperation

Cyber attacks are complex. They are dangerous. And they are ever more sophisticated.

Because of this, cyber risk is seen as a potentially systemic risk for the financial system and the real economy.

So we need a common approach to mitigate this risk.
And this involves continuing to work together to find shared solutions.
Because a shared approach will mean a more effective approach.

And so in addition to working with national supervisors to foster a common approach to supervision, we will also continue our very valuable dialogue with industry, consumer associations and other stakeholders to raise awareness of cyber security and insurance issues.

And at European level, we will continue our close cooperation, not only with the EBA and ESMA, but also with other EU bodies, so that we can strengthen Europe's over all resilience to cyber attacks.

In conclusion

Let me say in conclusion that it is no surprise that cyber security and cyber risks are a top concern not only for the financial sector, but for all industry and, indeed, for all people.

The digital era, and digital finance in particular, has brought us many benefits. But if too many people suffer because they are not better protected, we will quickly lose faith not only in the company that caused the suffering but also in technology itself.

This should not happen.

Let's work together to make sure that the risks resulting from digitalisation are considered and managed appropriately, including through an appropriate cyber insurance framework, so that digital finance continues to work for the people.

Ladies and gentlemen, thank you very much.

Number 14

New action to disrupt world's largest online criminal network

Tom Burt - Corporate Vice President, Customer Security & Trust

Microsoft and partners across 35 countries took coordinated legal and technical steps to disrupt one of the world's most prolific botnets, called Necurs, which has infected more than nine million computers globally.

This disruption is the result of eight years of tracking and planning and will help ensure the criminals behind this network are no longer able to use key elements of its infrastructure to execute cyberattacks.

A botnet is a network of computers that a cybercriminal has infected with malicious software, or malware.

Once infected, criminals can control those computers remotely and use them to commit crimes.

Microsoft's Digital Crimes Unit, BitSight and others in the security community first observed the Necurs botnet in 2012 and have seen it distribute several forms of malware, including the GameOver Zeus banking trojan.

The Necurs botnet is one of the largest networks in the spam email threat ecosystem, with victims in nearly every country in the world. During a 58-day period in our investigation, for example, we observed that one Necurs-infected computer sent a total of 3.8 million spam emails to over 40.6 million potential victims.

Necurs is believed to be operated by criminals based in Russia and has also been used for a wide range of crimes including pump-and-dump stock scams, fake pharmaceutical spam email and "Russian dating" scams.

It has also been used to attack other computers on the internet, steal credentials for online accounts, and steal people's personal information and confidential data.

Interestingly, it seems the criminals behind Necurs sell or rent access to the infected computer devices to other cybercriminals as part of a botnet-for-hire service.

Necurs is also known for distributing financially targeted malware and ransomware, cryptomining, and even has a DDoS (distributed denial of

service) capability that has not yet been activated but could be at any moment.

On Thursday, March 5, the U.S. District Court for the Eastern District of New York issued an order enabling Microsoft to take control of U.S.-based infrastructure Necurs uses to distribute malware and infect victim computers.

With this legal action and through a collaborative effort involving public-private partnerships around the globe, Microsoft is leading activities that will prevent the criminals behind Necurs from registering new domains to execute attacks in the future.

This was accomplished by analyzing a technique used by Necurs to systematically generate new domains through an algorithm. We were then able to accurately predict over six million unique domains that would be created in the next 25 months.

Microsoft reported these domains to their respective registries in countries around the world so the websites can be blocked and thus prevented from becoming part of the Necurs infrastructure.

By taking control of existing websites and inhibiting the ability to register new ones, we have significantly disrupted the botnet.

Microsoft is also taking the additional step of partnering with Internet Service Providers (ISPs) and others around the world to rid their customers' computers of malware associated with the Necurs botnet.

This remediation effort is global in scale and involves collaboration with partners in industry, government and law enforcement via the Microsoft Cyber Threat Intelligence Program (CTIP).

Through CTIP, Microsoft provides law enforcement, government Computer Emergency Response Teams (CERTs), ISPs and government agencies responsible for the enforcement of cyber laws and the protection of critical infrastructure with better insights into criminal cyber infrastructure located within their jurisdiction, as well as a view of compromised computers and victims impacted by such criminal infrastructure.

For this disruption, we are working with ISPs, domain registries, government CERTs and law enforcement in Mexico, Colombia, Taiwan, India, Japan, France, Spain, Poland and Romania, among others.

Each of us has a critical role to play in protecting customers and keeping the internet safe.

To make sure your computer is free of malware, you may visit: https://docs.microsoft.com/en-us/windows/security/threat-protection/intelligence/safety-scanner-download

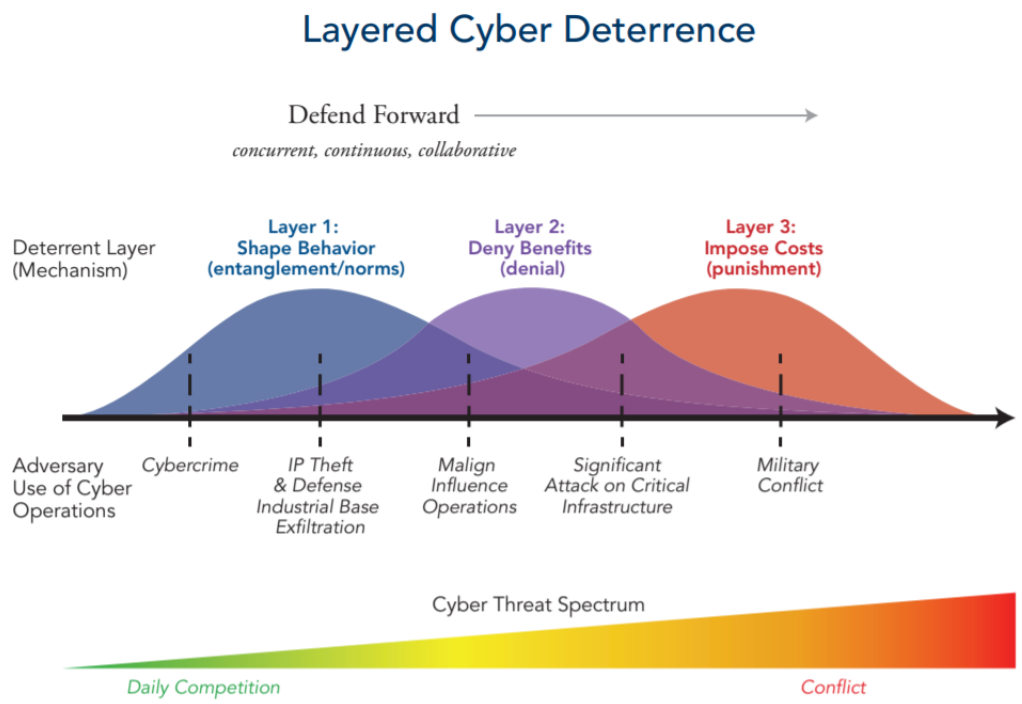
Number 15

Cyberspace Solarium Commission (CSC)

A consensus on a strategic approach to defending the US in cyberspace against cyberattacks of significant consequences

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

The finished report was presented to the public on March 11, 2020.



The Cyberspace Solarium Commission's proposes a strategy of layered cyber deterrence. The report consists of over 80 recommendations to implement the strategy.

These recommendations are organized into 6 pillars:

1. Reform the U.S. Government's Structure and Organization for Cyberspace.
2. Strengthen Norms and Non-Military Tools.
3. Promote National Resilience.
4. Reshape the Cyber Ecosystem.
5. Operationalize Cybersecurity Collaboration with the Private Sector.
6. Preserve and Employ the Military Instrument of National Power.

To read more:
https://drive.google.com/file/d/1ryMCIL_dZ30QyjFqFkkf10MxIXJGT4yv/view

Cyberspace Solarium Commission
@CyberSolarium
"@SenAngusKing and @RepGallagher: 'We are doing a 9/11 report to prevent a 9/11 in the future.'… It's Sept. 10 in cyberspace. Congress united to create the commission. Now it needs to enact the laws." –

Number 16

The Mind in the Machine

Machine learning is a scientific revolution that is changing how science gets done.

Los Alamos National Laboratory
Delivering science and technology to protect our nation and promote world stability

We are not talking about robots (though it would be cool if we were). Sentient humanoid automatons, whether benevolent or malevolent, walking and talking amongst us, are still science fiction.

But some things that used to be impossible are now science fact, like computers that can tell if two disparate images are actually showing the same thing or that can predict if and when a supercomputer will crash.

Los Alamos has always excelled at data science, and the data-science techniques known collectively as machine learning are now taking data analysis to the next level.

Through machine learning, or ML, scientists are exploring new ways of answering old questions, and, in some instances for the first time, they are actually getting some answers.

Machine learning is a natural product of increased computational power. The questions aren't necessarily new, and the math isn't necessarily new. But the machines are, and what scientists are doing with them certainly is.

Enabled by major advances in computer hardware and software, and by the massive amounts of data newly available, tech entities from social media companies to national laboratories are using and developing ML.

But while social media and computer companies are mostly working on problems like targeted marketing, virtual assistants, and self-driving cars, Los Alamos scientists are working on mission-critical science problems like nuclear nonproliferation, global security, and ensuring the safety, efficacy, and reliability of the country's nuclear arsenal.

The level of performance required for the Laboratory is more stringent owing to the knowledge. The broad body of physics expertise that exists at the Laboratory, when married to ML, makes new approaches to national security possible.

Scientists at the Laboratory are using and developing ML in a plethora of ways. Some are going after answers to age-old questions, some are asking

brand new questions, and some are pioneering new ways of doing and thinking about ML itself.

By no means comprehensive, this article provides several examples of machine learning being done at Los Alamos.

What it is and what it isn't

ML is not synonymous with artificial intelligence (AI).

General AI refers to learning and reasoning by machines without the intervention of humans, and most scientists agree that we aren't there yet.

ML is a specialized subset of AI, wherein a human still writes the code, but the output of the code depends on data—usually vast amounts of it—that is also chosen and fed to the computer by a human. And the computer usually needs to be told, by a human, whether or not it is doing the right thing with the data.

To read more: https://www.lanl.gov/discover/publications/1663/2020-january/_assets/docs/1663-35-MindInTheMachine.pdf

Number 17

Home Office: Securing Remote Access

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Finance FDF
National Cyber Security Centre NCSC

Malware / Phishing mitigations

• Always use a second factor for authenticating your users. The best choice is either a Cryptostick / Smartcard or a hardware-based OTP (one time password) token such as RSA, also MobileID is a possibility. If this is not feasible, software based OTP tokens such as Google Authenticator work pretty well.

• Enforce good passwords and remind the users not to reuse passwords for other services and to avoid any sequences in the passwords (e.g. xyz2018, xyz2019, xyz2020).

• Monitor your log of the remote access devices files closely for any anomaly (e.g. IP addresses from outside Switzerland if most of your staff is working from Switzerland, IP addresses originating from TOR nodes, VPNs or generally from networks of hosting providers).

• Use a forced tunneling for all devices in order to secure communication and to ensure visibility on connections towards the Internet, but keep in mind that this increases bandwidth requirements significantly.

• Inform the users about the dangers of working at home and provide them with contact information in case they see anything suspicious.

• Make plans for forensic readiness, especially if you allow users to access company resources from their own device.

• Ensure that all your Remote Access devices are patched and have a plan to quickly roll-out emergency patches in case of a critical vulnerability.

• Ensure that remote devices can be patched without being physically on site, preferably during night time and respecting the available bandwidth.

• Ensure that the home user is not "inter-connecting" his home network with your company network.

• Plan for remote restaging / replacing of infected devices, e.g. via a dedicated dls/fiber line

Apart from these rather specific recommendations, we would like to remind you of the protection measures against targeted ransomware attacks that we have described lately:

https://www.govcert.ch/blog/severe-ransomware-attacks-against-swiss-smes

https://www.melani.admin.ch/melani/de/home/dokumentation/newsletter/sicherheitsrisiko-durch-ransomware.html

https://www.govcert.ch/blog/severe-ransomware-attacks-against-swiss-smes/assets/blocked-filetypes.txt

To read the paper:
https://www.melani.admin.ch/melani/en/home/dokumentation/checklists-and-instructions/fernzugriff.html

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.