Monday, February 26, 2024

Top 10 risk and compliance related news stories and world events that (for better or for worse) shaped the week's agenda, and what is next.

Heraclitus believed that there is nothing permanent except change.

Confucius has said that only the wisest and stupidest of men never change.

Changes are inherently risky. Fortunately, we have change management, where we acknowledge, anticipate, and manage risk. But what if we have "accelerated innovation"? This is accelerated change.

I have read carefully the *2024 Joint Cyber Defense Collaborative (JCDC) Priorities* from the Cybersecurity and Infrastructure Security Agency (CISA). This collaborative was established over two years ago to drive unified efforts across public and private partners, to achieve the most important cybersecurity outcomes. We read:

Anticipate Emerging Technology and Risks: Innovation can help to close off entire avenues of attack but may also create new cybersecurity risks. Our priorities in this focus area center on JCDC's work with the cybersecurity community to support accelerated innovation in cyber defense and reduce known and suspected risks posed by the deployment of emerging technologies.

Then, we read:

Decrease the risk posed by Artificial Intelligence (AI) to critical infrastructure. In alignment and coordination with CISA's Roadmap for Artificial Intelligence, JCDC will work to decrease the likelihood and impact of AI-related threats and vulnerabilities to critical infrastructure providers.

Lucius Annaeus Seneca, the stoic philosopher of Ancient Rome, was wrong. He has said: "Nothing is so wretched or foolish as to anticipate misfortunes. What madness is it to be expecting evil before it comes." Seneca would never pass a risk management exam.

I agree with CISA. We must anticipate emerging technology and risks and support accelerated innovation. Perhaps it is time for an Accelerated Change Management book. No, I am not going to write it.

Read more at number 1 below. Welcome to the Top 10 list.

Best regards,

George Lekatis
President of the IARCP
1200 G Street NW Suite 800,
Washington DC 20005, USA
Tel: (202) 449-9750
Email: lekatis@risk-compliance-association.com
Web: www.risk-compliance-association.com
HQ: 1220 N. Market Street Suite 804,
Wilmington DE 19801, USA
Tel: (302) 342-8828

Number 1 (Page 5)

2024 Joint Cyber Defense Collaborative (JCDC) Priorities

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

Number 2 (Page 8)

Consultation on Guidelines on preventing the abuse of funds and certain crypto-assets transfers for ML/TF (Travel rule Guidelines)

eba European Banking Authority

Number 3 (Page 10)

Tap, click and pay: how digital payments seize the day

Committee on Payments and Market Infrastructures | BIS

Number 4 (Page 12)

Proposed Insurance Circular Letter

NEW YORK STATE

Number 5 (Page 16)

Curiouser and Curiouser: Statement on Amendments to Form PF to Amend Reporting Requirements for All Filers and Large Hedge Fund Advisers

Number 6 (Page 20)

Joint Statement on Ivanti Connect Secure and Ivanti Policy Secure Vulnerabilities

enisa European Network and Information Security Agency

Number 7 (Page 23)

Enterprise Risk Mitigation Blueprint for Non-Intelligence Agencies

Number 8 (Page 27)

Piloting new ways of protecting Android users from financial fraud

Google Security Blog

Number 9 (Page 31)

DARPA's REMA Program to Add Mission Autonomy to Commercial Drones

From concept to contract in 70 business days: Companies collaborate to add capabilities for off-the-shelf drones to carry out predefined missions without need for operator connection

DARPA DEFENSE ADVANCED RESEARCH PROJECTS AGENCY

Number 10 (Page 33)

DOD Releases List of People's Republic of China (PRC) Military Companies in Accordance With Section 1260H of the National Defense Authorization Act for Fiscal Year 2021

U.S. Department of Defense

Number 1

2024 Joint Cyber Defense Collaborative (JCDC) Priorities

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

The Joint Cyber Defense Collaborative (JCDC) was established over two years ago to drive unified efforts across public and private partners to achieve our most important cybersecurity outcomes.

Each year, hundreds of JCDC partner organizations provide insight, expertise, and perspective to help identify our collective priorities for the coming year.

We are excited to introduce our 2024 Priorities.

Of course, these priorities are not CISA's alone; rather, they reflect shared goals across government, industry, and international partners that will enable cohesive planning and collaboration.

While these Priorities build on our 2023 Planning Agenda, they also represent a critical step in JCDC's maturation.

The 2023 JCDC Planning Agenda:
https://www.cisa.gov/topics/partnerships-and-collaboration/joint-cyber-defense-collaborative/2023-jcdc-planning-agenda

2023 JCDC Planning Agenda

The Joint Cyber Defense Collaborative (JCDC) is proud to announce its 2023 Planning Agenda—a major milestone in the collaborative's continued evolution and maturation. Economic prosperity, national defense, and public health and safety depend on interconnected digital technologies. Widespread security flaws and configuration missteps in these technologies create opportunities for malicious actors to steal information, destroy valuable data, and cut off access to critical goods and services. JCDC's planning agenda addresses these important and complex security challenges.

For the first time, we are aligning our priorities under three broad focus areas, which in turn will enable alignment of resources and strategic direction.

(1) Defend Against Advanced Persistent Threat (APT) Operations: Last year's ODNI Annual Threat Assessment makes clear the threat posed by malicious cyber actors, particularly those affiliated with the People's Republic of China (PRC).

No longer can our cyber defense focus on espionage and data theft; we must now posture to protect our country and allies against destructive attacks designed to cause real-world harm.

Our priorities in this focus area center on JCDC's strategic and operational efforts to counter known and suspected APT attack campaigns targeting entities that support national critical functions.

- Discover and defend against malicious abuse by APT actors, particularly those backed by the PRC, on and against U.S.-based infrastructure.

- Prepare for major cyber incidents. CISA, through the JCDC, will finalize and publish the National Cyber Incident Response Plan (NCIRP), in close coordination with interagency and industry partners.

You may visit:
https://www.cisa.gov/sites/default/files/2023-10/NCIRP-2024-Fact-Sheet-508C.pdf

OVERVIEW

In 2016, the National Cyber Incident Response Plan (NCIRP) was published to provide a framework for significant cyber incident coordination. A lot has changed over the past eight years, including across the cyber threat landscape and the cyber defense ecosystem, and the NCIRP must evolve accordingly. As directed in the National Cybersecurity Strategy, the Cybersecurity and Infrastructure Security Agency (CISA) is leading the effort to update the NCIRP to provide a modern, agile, flexible framework to enable coherent and repeatable national incident response across the federal government, private sector, and other key partners.

WHAT IS THE NCIRP AND WHY WAS IT CREATED?

The NCIRP was developed in accordance with Presidential Policy Directive 41 (PPD-41) on U.S. Cyber Incident Coordination and describes how the federal government, private sector, and state, local, tribal, territorial (SLTT) government entities will organize to manage, respond to, and mitigate the consequences of significant cyber incidents. The NCIRP leverages principles from the National Preparedness System (NPS) to articulate how the nation responds to and recovers from significant cyber incidents. Alignment with the NPS also allows for significant cyber incident response to integrate with physical incident response in cases where cyber incidents may have physical impacts or vice versa.

(2) Raise the Cybersecurity Baseline: Too many successful intrusions are preventable, the result of inadequate investment in basic practices. Our priorities in this focus area center on JCDC's ability to organize and support efforts that raise the cybersecurity baseline of critical infrastructure entities.

- Help state and local election officials secure their networks and infrastructure against cyber threats as part of CISA's broader election security efforts.

- Measurably decrease the impact of ransomware on critical infrastructure.

- Make measurable progress toward a world where technology is Secure by Design. Even as we urgently work to help organizations implement the most effective cybersecurity measures, we know that scalable change requires a fundamental shift in how technology is designed, built, and maintained. We will continue to drive measurable commitments across the technology ecosystem that reduce the number of defective technology products by design and ensure that strong default settings are the norm.

(3) Anticipate Emerging Technology and Risks: Innovation can help to close off entire avenues of attack but may also create new cybersecurity risks. Our priorities in this focus area center on JCDC's work with the cybersecurity community to support accelerated innovation in cyber defense and reduce known and suspected risks posed by the deployment of emerging technologies.

- Decrease the risk posed by Artificial Intelligence (AI) to critical infrastructure. In alignment and coordination with CISA's Roadmap for Artificial Intelligence, JCDC will work to decrease the likelihood and impact of AI-related threats and vulnerabilities to critical infrastructure providers.

DHS Cybersecurity and Infrastructure Security Agency Releases Roadmap for Artificial Intelligence

Roadmap Will Guide CISA's Efforts to Manage the Risks and Harness the Opportunities Posed by Artificial Intelligence to Cybersecurity

Released: November 14, 2023

RELATED TOPICS: CYBERSECURITY BEST PRACTICES

For CISA's Roadmap for Artificial Intelligence, you may visit:
https://www.cisa.gov/news-events/news/dhs-cybersecurity-and-infrastructure-security-agency-releases-roadmap-artificial-intelligence

To read more:
https://www.cisa.gov/topics/partnerships-and-collaboration/joint-cyber-defense-collaborative/2024-jcdc-priorities

Number 2

Consultation on Guidelines on preventing the abuse of funds and certain crypto-assets transfers for ML/TF (Travel rule Guidelines)

The European Banking Authority (EBA) today launched a public consultation on new Guidelines on preventing the abuse of funds and certain crypto-assets transfers for money laundering and terrorist financing purposes.

These 'travel rule' Guidelines specify the steps that Payment Service Providers (PSPs), Intermediary PSPs (IPSPs), crypto-asset service providers (CASPs) and Intermediary CASPs (ICASPs) should take to detect missing or incomplete information that accompanies a transfer of funds or crypto-assets.

They also detail the procedures all these providers should put in place to manage a transfer of funds or a transfer of crypto-assets that lacks the required information.

These Guidelines aim at forging a common understanding to ensure the consistent application of EU law as well as a stronger anti-money laundering and countering the financing of terrorism (AML/CFT) regime.

The consultation runs until 26 February 2024.

The main objective of these Guidelines is to prevent the abuse of funds and crypto-assets transfers for terrorist financing and other financial crime purposes.

The Guidelines also ensure that relevant authorities can fully trace such transfers where this is necessary to prevent, detect or investigate money laundering and terrorist financing.

To achieve this, the EBA promotes the development of a common understanding by PSPs, IPSPs, CASPs and ICASPs and competent authorities across the EU, of what are the effective procedures to detect and manage the transfer of funds and crypto-assets lacking the required information on the payer/originator and the payee/beneficiary, and how they should be applied.

Consultation process

Comments to the consultation paper can be sent by clicking on the "send your comments" button on the EBA's consultation page. The deadline for the submission of comments is 26 February 2024.

The EBA will hold a virtual public hearing on the consultation paper on 17 January 2024 from 14:00 to 16:00 Paris time. The EBA invites interested stakeholders to register using this link by 3 January 2023 at 16:00 CET. The dial-in details will be communicated to those who have registered for the meeting.

All contributions received will be published following the end of the consultation, unless requested otherwise.

Legal basis, background

In July 2021 the European Commission issued a legislative package with four proposals to reform the EU's legal and institutional AML/CFT framework. It included a proposal for a recast of Regulation (EU) 2015/847, now published in the Official Journal of the European Union since June 2023 as Regulation (EU) 2023/1113.

The recast brings the EU's legal framework in line with the Financial Action Task Force (FATF)'s standards by extending the obligation to include information about the originator and beneficiary to CASPs – the so-called "travel rule".

It also amends Directive (EU) 2015/849 to subject CASPs, which are authorized in accordance with the Regulation (EU) 2023/1114 to the same AML/CFT requirements and AML/CFT supervision as credit and financial institutions.

Article 36 (first and second subparagraphs) of Regulation (EU) 2023/1113 and Article 19a(2) of Directive (EU) 2015/849 mandate the EBA to issue guidelines to competent authorities, PSPs and CASPs on:

(a) the measures those providers should take to comply with certain articles of Regulation (EU) 2023/1113;

(b) the technical aspects of the application of this Regulation to direct debits; and

© the measures, including the criteria and means for identification and verification of the identity of the originator or beneficiary of a transfer made to or from a self-hosted address.

The EBA is proposing to deliver this mandate by repealing the 2017 Joint European supervisory authorities (ESAs)'s Guidelines under Article 25 of Regulation (EU) 2015/847 on the measures payment service providers should take to detect missing or incomplete information on the payer or the payee, and the procedures they should put in place to manage a transfer of funds lacking the required information (JC/GL/2017/16) and replace them with new Guidelines.

Responses

Responses to the consultations can be sent to the EBA. All contributions received will be published after the consultation closes, unless requested otherwise.

Deadline for submitting responses: 26/02/2024 at 23:59

To read more:
https://www.eba.europa.eu/publications-and-media/events/consultation-guidelines-preventing-abuse-funds-and-certain-crypto

Number 3

Tap, click and pay: how digital payments seize the day

Committee on Payments and Market Infrastructures | BIS

Highlights

- The use of digital payment methods continues to increase, particularly for small amounts. In tandem, cash withdrawals and the number of small-denomination banknotes in circulation have declined.
- Fast payments reached new heights and are a prominent driver of the digitalisation of countries' payment ecosystems.
- Even so, consumers continue to use cash to pay at home and abroad: both cross-border card and e-money payments and cross-border cash withdrawals increased sharply in 2022.

Introduction

It is nearly impossible to imagine a world without digital payments. Due to technological innovations and increased demand for convenience, speed, and safety, payments by cashless payment methods, such as card, e-money and credit transfers, have been on the rise for many years.

These trends accelerated over the Covid-19 pandemic and their growth has steadily continued since. One exciting development, in particular, is the rapid and widespread growth of fast payments.

This CPMI Brief highlights key payment trends as observed in the 2022 Red Book statistics. These statistics were collected in the second half of 2022 from member jurisdictions of the Bank for International Settlements (BIS) Committee on Payments and Market Infrastructures (CPMI) and are available at the BIS Data Portal.

The year 2022 was marked by high and rising inflation and increasing policy rates. The year 2022 was also when global travel soared as the remaining Covid-19 restrictions were lifted. These factors may have impacted global payment habits.

The trends summarised in this CPMI Brief shed light on the use of payment methods and are helpful for understanding factors driving the uptake of payment innovations.

In addition, the statistics provide some insight into the demand for cross-border payments – a priority for G20 leaders who have committed to addressing the long-standing challenges of high costs, low speed and insufficient access and transparency.

Box 1

Red Book statistics are now available in the BIS Data Portal

Red Book statistics

The Red Book statistics are annual statistics on payments and financial market infrastructures (FMIs) in the CPMI member jurisdictions.① The data are collected in a standardised and harmonised way, based on the Red Book Methodology published in 2017. The Red Book statistics contain data on:

- retail payment services and instruments, currency in circulation and related macroeconomic indicators. These include statistics on banknotes and coins in circulation, institutions offering payment services to end users, supply of cards and terminals, use of cashless payments, cash withdrawals and deposits. The data also contain qualitative information on card schemes and cover general macroeconomic statistics, which can be used to relate the size of a jurisdiction's payment industry to the size of its economic activity.
- financial market infrastructures and their critical service providers. These include quantitative and qualitative information on payment systems, central securities depositories and central counterparties, such as the number of participants and their overall settlement and clearing activity.

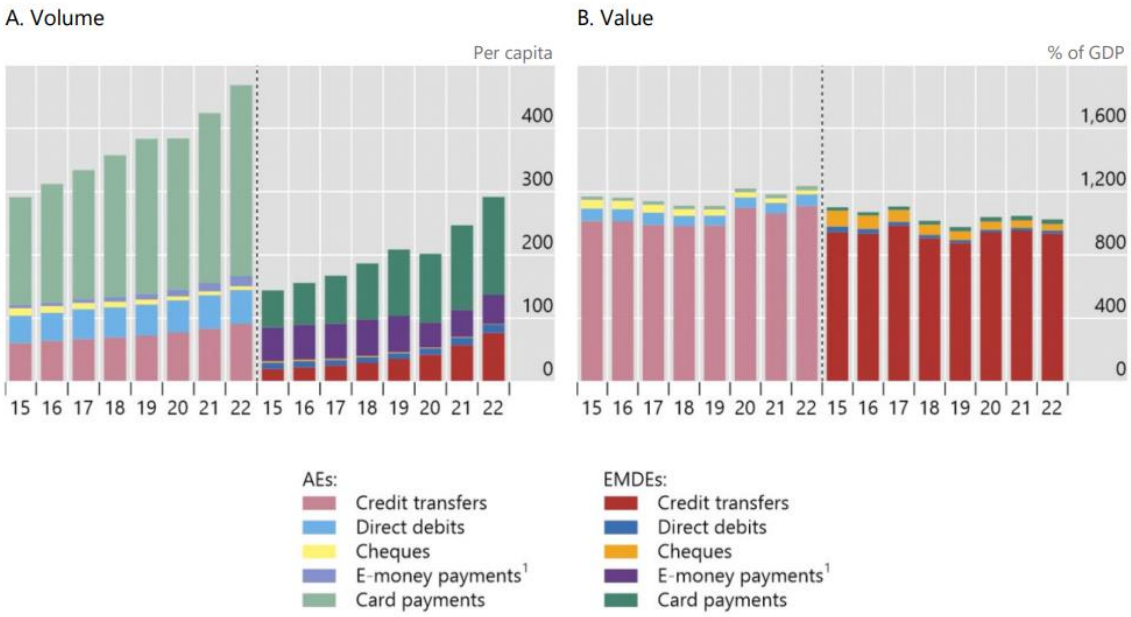
BIS Data Portal

As of December 2023, the Red Book statistics can be accessed through the BIS Data Portal. The BIS Data Portal, launched in November 2023, is the new one-stop platform for all BIS statistics. It features a variety of new tools to easily navigate and access data, metadata, dashboards and tables to gain quick insights into the BIS statistics and to export them into multiple formats. The BIS Data Portal contains global and jurisdiction-specific data – not only on payments and financial market infrastructures, but also on international banking, credit and debt securities, property prices, consumer price indexes, exchange rates and more.②

① For the list of all CPMI jurisdictions please refer to the CPMI website.
② For more on the BIS Data Portal, watch the introductory video: https://www.youtube.com/watch?v=s40w3_xeoVA.

Cashless payments continued to grow in AEs and EMDEs

Graph 1



[1] The distinction between card and e-money payments is not available for CA, CN, GB, MX, SA and ZA. For these countries, e-money payments might be included in card payments.

Sources: CPMI Red Book statistics; authors' calculations.

To read more:
https://www.bis.org/statistics/payment_stats/commentary2402.pdf

Number 4

Proposed Insurance Circular Letter

TO: All Insurers Authorized to Write Insurance in New York State, Licensed Fraternal Benefit Societies, and the New York State Insurance Fund

RE: Use of Artificial Intelligence Systems and External Consumer Data and Information Sources in Insurance Underwriting and Pricing

I. Purpose and Background

The New York State Department of Financial Services ("Department") is committed to innovation and the responsible use of technology to improve financial access and contribute to the safety and stability of insurance markets. The Department expects that insurers use of emerging technologies such as artificial intelligence will be conducted in a manner that complies with all applicable federal and state laws, rules, and regulations.

The use of external consumer data and information sources ("ECDIS") and artificial intelligence systems ("AIS") can both benefit insurers and consumers alike by simplifying and expediting insurance underwriting and pricing processes, and potentially result in more accurate underwriting and pricing of insurance.

At the same time, ECDIS may reflect systemic biases and its use can reinforce and exacerbate inequality. This raises significant concerns about the potential for unfair adverse effects or discriminatory decision-making. ECDIS may also have variable accuracy and reliability and may come from entities that are not subject to regulatory oversight and consumer protections.

Furthermore, the self-learning behavior of AIS increases the risks of inaccurate, arbitrary, capricious, or unfairly discriminatory outcomes that may disproportionately affect vulnerable communities and individuals or otherwise undermine the insurance marketplace in New York.

Therefore, it is critical that insurers who utilize such technologies establish a proper governance and risk management framework to mitigate the potential harm to consumers and comply with all relevant legal obligations.

The purpose of this circular letter ("Circular Letter") is to identify DFS's expectations that all insurers authorized to write insurance in New York State, licensed fraternal benefit societies, and the New York State Insurance Fund (collectively, "insurers") develop and manage their use of ECDIS, artificial intelligence systems, and other predictive models in underwriting and pricing insurance policies and annuity contracts.

For purposes of this Circular Letter, AIS means any machine-based system designed to perform functions normally associated with human intelligence, such as reasoning, learning, and self-improvement, that is used – in whole or in part – to supplement traditional medical, property or casualty underwriting or pricing, as a proxy for traditional medical, property or casualty underwriting or pricing, or to establish "lifestyle indicators" that may contribute to an underwriting or pricing assessment of an applicant for insurance coverage.

For purposes of this Circular Letter, ECDIS includes data or information used – in whole or in part – to supplement traditional medical, property or casualty underwriting or pricing, as a proxy for traditional medical, property or casualty underwriting or pricing, or to establish "lifestyle indicators" that may contribute to an underwriting or pricing assessment of an applicant for insurance coverage.

For the purposes of this Circular Letter, ECDIS does not include an MIB Group, Inc. member information exchange service, a motor vehicle report, or a criminal history search. An insurer conducting a criminal history search for insurance underwriting and pricing purposes must comply with Executive Law § 296(16). See e.g., Insurance Circular Letter No. 13 (2022).

An insurer may deploy ECDIS and AIS in a variety of ways throughout the underwriting and pricing process. The Department recognizes there is no one-size-fits-all approach to managing data and decisioning systems.

Therefore, insurers should take an approach to developing and managing their use of ECDIS and AIS that is reasonable and appropriate to each insurer's business model and the overall complexity and materiality of the risks inherent in using ECDIS and AIS.

This Circular Letter is not intended to provide an exhaustive list of potential issues that could arise from the use of ECDIS or AIS and is not intended to suggest that an insurer's due diligence in assessing ECDIS or AIS should be limited to the concerns enumerated below.

This Circular Letter also is not intended to address phases of the insurance product lifecycle other than underwriting and pricing.
The Department may audit and examine an insurer's use of ECDIS and AIS, including within the scope of regular or targeted examinations pursuant to New York Insurance Law ("Insurance Law") § 309, or a request for special report pursuant to Insurance Law § 308.

II. Fairness Principles

An insurer should not use ECDIS or AIS for underwriting or pricing purposes unless the insurer can establish that the data source or model, as applicable, does not use and is not based in any way on any class protected pursuant to Insurance Law Article 26. Moreover, an insurer should not use ECDIS or AIS for underwriting or pricing purposes if such use would result in or permit any unfair discrimination or otherwise violate the Insurance Law or any regulations promulgated thereunder.

A. Data Actuarial Validity

As with any other variables employed in underwriting and pricing, insurers should be able to demonstrate that the ECDIS are supported by generally accepted actuarial standards of practice and are based on actual or reasonably anticipated experience, including, but not limited to, statistical studies, predictive modeling, and risk assessments.

The underlying analyses should demonstrate a clear, empirical, statistically significant, rational, and not unfairly discriminatory relationship between the variables used and the relevant risk of the insured.

Insurers must be able to demonstrate that the ECDIS employed for underwriting and pricing are not prohibited by the Insurance Law or regulations promulgated thereunder and should be able to demonstrate that they do not serve as a proxy for any protected classes that may result in unfair or unlawful discrimination.

B. Unfair and Unlawful Discrimination

State and federal law prohibits insurers from unlawfully discriminating against certain protected classes of individuals and from engaging in unfair discrimination, including the ability of insurers to underwrite based on certain criteria.

An insurer should not use ECDIS or AIS in underwriting or pricing unless the insurer has determined that the ECDIS or AIS does not collect or use criteria that would constitute unfair or unlawful discrimination or an unfair trade practice.

When using ECDIS or AIS as part of their insurance business, insurers are responsible for complying with these anti-discrimination laws irrespective of whether they themselves are collecting data and directly underwriting consumers, or relying on ECDIS or AIS of external vendors that are intended to be partial or full substitutes for direct underwriting or pricing.

An insurer may not use ECDIS or AIS to collect or use information that the insurer would otherwise be prohibited from collecting or using directly.

An insurer may not rely solely on a vendor's claim of non-discrimination or a proprietary third-party process to determine compliance with anti-discrimination laws. The responsibility to comply with anti-discrimination laws remains with the insurer at all times.

An insurer should not use ECDIS or AIS in underwriting or pricing unless the insurer can establish through a comprehensive assessment that the underwriting or pricing guidelines are not unfairly or unlawfully discriminatory in violation of the Insurance Law. A comprehensive assessment of whether an underwriting or pricing guideline derived from ECDIS or AIS unfairly discriminates between similarly situated individuals or unlawfully discriminates against a protected class should, at a minimum, include the following steps:

- assessing whether the use of ECDIS or AIS produces disproportionate adverse effects in underwriting and/or pricing on similarly situated insureds, or insureds of a protected class. If there is no prima facie showing of a disproportionate adverse effect, then the insurer may conclude its evaluation.

- if there is prima facie showing of such a disproportionate adverse effect, further assessing whether there is a legitimate, lawful, and fair explanation or rationale for the differential effect on similarly situated insureds. If no legitimate, lawful, and fair explanation or rationale can account for the differential effect on similarly situated insureds, the insurer should modify its use of such ECDIS or AIS and evaluate the modified use of ECDIS or AIS.

- if a legitimate, lawful, and fair explanation or rationale can account for the differential effect, further conducting and appropriately documenting a search and analysis for a less discriminatory alternative variable(s) or methodology that would reasonably meet the insurer's legitimate business needs. If a less discriminatory alternative exists, the insurer should modify its use of ECDIS or AIS accordingly.

To read more:
https://www.dfs.ny.gov/industry_guidance/circular_letters/cl2024_nn_proposed

Number 5

Curiouser and Curiouser: Statement on Amendments to Form PF to Amend Reporting Requirements for All Filers and Large Hedge Fund Advisers

I write to dissent from the latest unwarranted expansion of Form PF. These revisions stem from the Commission's unbridled curiosity rather than from a legitimate regulatory objective.

In 2010, Congress established the Financial Stability Oversight Council ("FSOC") and charged it with, among other things, "identify[ing] risks to the financial stability of the United States."

Congress directed the Securities and Exchange Commission ("SEC" or "Commission") and the Commodity Futures Trading Commission ("CFTC") (collectively, "Commissions") to provide some of the information FSOC would need to fulfill its duties, and so in 2011 Form PF was born.

At its inception, the Commissions acknowledged that, while Form PF data could be used for their own regulatory purposes, Form PF's primary function was "to collect information . . . to assist FSOC in its monitoring obligations."

Since that time, however, respect for Form PF's primary purpose has given way to curiosity. We pair as co-equal FSOC's use of Form PF data to "monitor and assess systemic risk" with our own desire "to collect additional data and make data more useful for the Commissions' use in their respective regulatory programs."

Relying on both these purposes, we are expanding dramatically the information Form PF collects.

In the Form's early days, we were comfortable with its limitations. We stated clearly, for instance, that "[w]e have not sought to design a form that would provide FSOC in all cases with all the information it may need to make a determination that a particular entity should be designated for supervision by the [Federal Reserve Board]."

We recognized that the cost of demanding more information from all fund advisers would outweigh the benefits. Our sensibilities have changed in the intervening thirteen years, and Form PF is being amended to accommodate them.

Despite this attitudinal shift, we continue to provide occasional lip service to the idea that these amendments have been made largely in pursuit of improving the

identification and monitoring of systemic risk. As one commenter correctly highlighted, however, neither we nor the CFTC "describe[s] the types of activities that may give rise to systemic risk, nor do [we] describe how the proposed reporting requirements are specifically tailored to identify and effectively monitor these activities."

Form PF has not-so-subtly morphed into an all-purpose means to gather information from the private market under the seemingly limitless rubric of systemic risk. Through strained logic, we manage to transform one-off reports describing the idiosyncrasies of individual private funds into harbingers of market-wide contagion.

Our apparent inability to articulate a rationale for compelling more data has in no way blunted our craving for it—in fact, it appears to have stoked it. Absent any discernible limiting features, we have seemingly decided that all gaps are created equal and filling them provides its own justification. Even a partial list of the additional data we will now collect with these revisions is dizzying.

As one commenter put it, "the Commissions appear to believe that monitoring for systemic risk and protecting investors may only be conducted by having access to every piece of fund-related data." A systemic risk regulator does not need to know everything about every entity.

Boundless curiosity is wonderful in a small child; it is a less attractive trait in regulatory agencies. As diligent regulators we should want to know why market disturbances occur, or even prevent them if we can do so without exceeding our statutory mandates. But we chase a white whale if we believe we are but one discrete piece of information away from being able to prevent the next Flash Crash or Global Financial Crisis.

We insist, for instance, that each component fund in a master-feeder arrangement be reported separately. We ignored commenters who pointed out that disaggregation makes little sense in light of how private funds manage risk and that the information submitted will be of little use to the Commission.

We dismiss these concerns by stating that this fund-level data "allows for a clearer understanding of the reporting fund's structure, including its portfolio liquidity."

And besides, we say, "the disaggregated data can still be aggregated by FSOC and the Commissions if necessary to understand and assess the risk of the fund."

The Commissions similarly reject a commonsense request for an exception to allow disregarded feeder funds to invest a de minimis amount in something other than a single master fund, U.S. treasury bills, or cash and cash equivalents.

Even a ten percent exception could cloud "our understanding of these funds and the risks they may pose."

We likewise said no to calls to carve out certain private funds from the definition of hedge fund—such as private funds that can short or use leverage, but do not

engage in those activities for a specified period of time. Allowing carveouts from the definition, we determined, among other problems, would mean that we "would not receive important reporting on these activities which may contribute to systemic risk, particularly in the event of a fund that has the ability to engage in borrowing or short selling activities."

We do not have the better argument here. We have failed to explain why we must collect a small, unrepresentative component of the whole in order to fulfill Form PF's purpose.

Systemic risk involves the forest—trying to monitor the state of every individual tree at every given moment in time is a distraction and trades off the mistaken belief that we have the capacity to draw meaning from limitless amounts of discrete and often disparate information. Unbridled curiosity seems to be driving this decision rather than demonstrated need.

In our never-satisfied hunger for more particularized information, we too casually ignore concerns about cost, utility, and data protection. Form PF contains highly proprietary information. Unless we need it, we should not collect it. The leakage of such confidential business information could have serious competitive repercussions.

What we put forward as streamlining of Form PF's data gathering effort—say the drop-down menus to assist a filer in identifying its investment strategy, or the introduction of sub-asset classes—commenters rightly see as costly fact-gathering endeavors of little value that create an increasingly tempting target for cyberthieves.

Our curiosity could have serious consequences—"an intrusive path into the proprietary workings of fund managers under the guise of regulatory 'need to know'."

Ensuring that the data we collect are used only for their intended regulatory purposes is a very weighty responsibility—so weighty that it ought to have us thinking twice about collecting data that is not needed for systemic risk assessment.

Moreover, as one commenter suggests, perhaps we should ensure that we have fully used the information we already receive before adding to private funds' reporting burden. Given that the last amendments are less than a year old, private funds might justifiably be feeling Form PF fatigue.

The final rule does incorporate some commenter suggestions to reduce the costs and burdens and duplication associated with some of the proposal's features, which could indicate that the notice and comment process has worked as designed. Far from it.

The Commissions dismissed far too many comments calling for revisions or relief, but more troubling, countless numbers of similar pleas likely were never submitted. By my count, we acknowledge that the Commissions received no

comment on an element of the proposal more than 40 times in this release. Overburdened commenters are forced to pick and choose among hundreds of questions posed in this and other releases. They concentrate their limited time and strained resources on those matters they believe will be particularly disruptive.

With so many questions going unaddressed, we cannot be confident that we have a clear understanding of what the true costs of these amendments will be, let alone whether they are justified. For these reasons and others, I cannot support this rule.

Commenters are not alone in being overburdened. I am grateful to the hardworking staff of the Securities and Exchange Commission and the CFTC. Form amendments can be particularly challenging, especially with respect to a joint form such as this one and without the benefit of comment on many sections of the proposal. I commend the staffs of both agencies for their diligence and professionalism.

To read more:
https://www.sec.gov/news/statement/peirce-statement-amendments-form-pf-amend-reporting-reqs-020823

Number 6

Joint Statement on Ivanti Connect Secure and Ivanti Policy Secure Vulnerabilities

The European Commission, ENISA, the EU Agency for Cybersecurity, CERT-EU, Europol and the network of the EU national computer security incident response teams (CSIRTs network), have been closely following the active exploitation of vulnerabilities in the Ivanti Connect Secure and Ivanti Policy Secure Gateway products, commercial virtual private network (VPN) solutions previously known as Pulse Connect Secure.

Following the initial disclosure of two vulnerabilities at the beginning of January, two additional vulnerabilities were disclosed on 31 January 2024, which impact all supported versions of Ivanti Connect Secure and Ivanti Policy Secure Gateway products and make it possible for attackers to run commands on the system. Broader exploitation of the initially disclosed vulnerabilities had been observed already as early as mid-January.

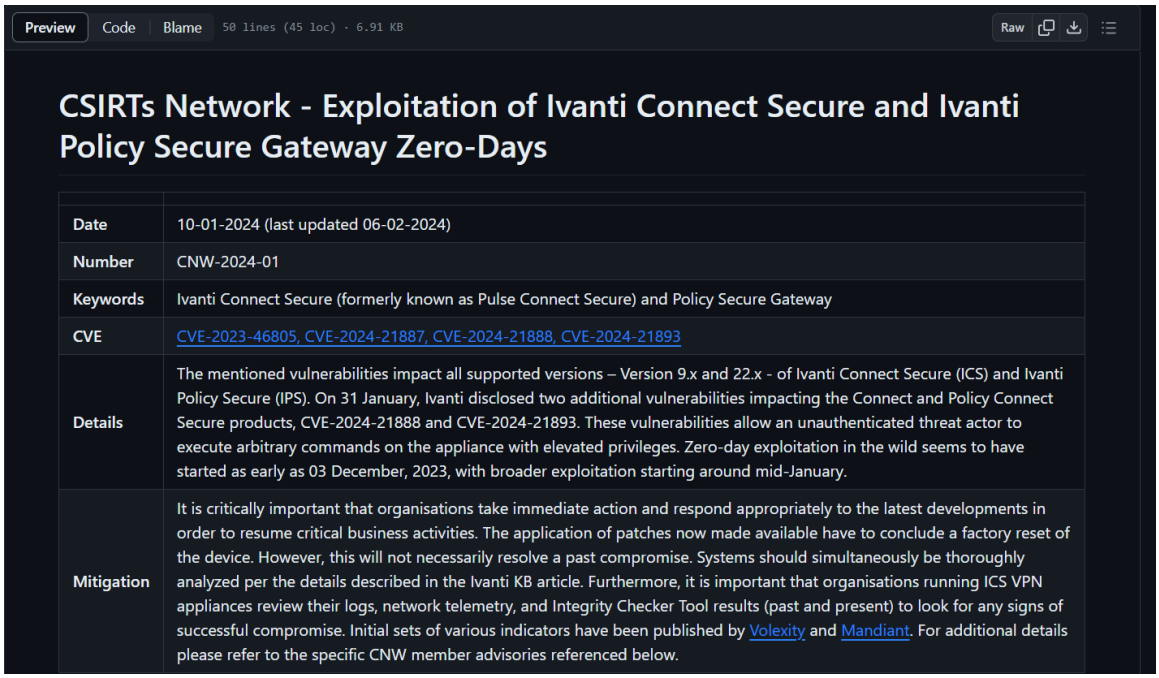
As this is a developing situation, we strongly recommend all organisations to regularly check the guidance provided by the CSIRTs Network members and CERT-EU for the latest assessment and advice.

For detailed instructions on how to complete the advised factory reset, organisations may also follow the detailed vendor instructions.

It is crucial for organisations to respond appropriately to the latest developments in order to resume their critical business activities.

The latest advisories published by CSIRTs Network members can be found in their relevant official communication channels.

Organisations may also refer to guidance given by CERT-EU. ENISA maintains an advisory collection under:
https://github.com/enisaeu/CNW/blob/main/advisories/2024/Multiple-Vulns-Ivanti-Secure-Gateways.md



Preview | Code | Blame | 50 lines (45 loc) · 6.91 KB | Raw

CSIRTs Network - Exploitation of Ivanti Connect Secure and Ivanti Policy Secure Gateway Zero-Days

Date	10-01-2024 (last updated 06-02-2024)
Number	CNW-2024-01
Keywords	Ivanti Connect Secure (formerly known as Pulse Connect Secure) and Policy Secure Gateway
CVE	CVE-2023-46805, CVE-2024-21887, CVE-2024-21888, CVE-2024-21893
Details	The mentioned vulnerabilities impact all supported versions – Version 9.x and 22.x - of Ivanti Connect Secure (ICS) and Ivanti Policy Secure (IPS). On 31 January, Ivanti disclosed two additional vulnerabilities impacting the Connect and Policy Connect Secure products, CVE-2024-21888 and CVE-2024-21893. These vulnerabilities allow an unauthenticated threat actor to execute arbitrary commands on the appliance with elevated privileges. Zero-day exploitation in the wild seems to have started as early as 03 December, 2023, with broader exploitation starting around mid-January.
Mitigation	It is critically important that organisations take immediate action and respond appropriately to the latest developments in order to resume critical business activities. The application of patches now made available have to conclude a factory reset of the device. However, this will not necessarily resolve a past compromise. Systems should simultaneously be thoroughly analyzed per the details described in the Ivanti KB article. Furthermore, it is important that organisations running ICS VPN appliances review their logs, network telemetry, and Integrity Checker Tool results (past and present) to look for any signs of successful compromise. Initial sets of various indicators have been published by Volexity and Mandiant. For additional details please refer to the specific CNW member advisories referenced below.

ENISA and all relevant EU actors will continue to monitor this threat to contribute to the overall situational awareness at the Union level.

EU Policy

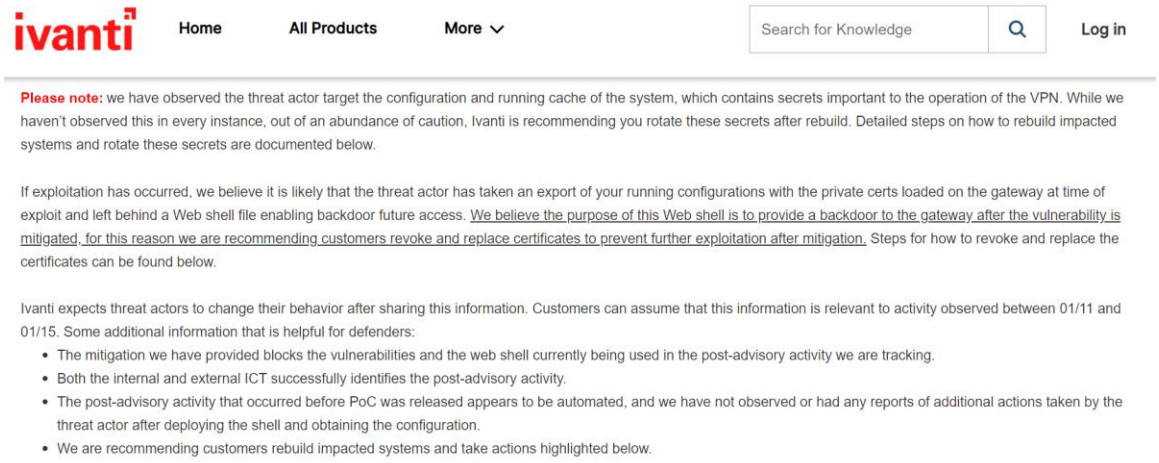
Organisations should be further aware that the EU Cyber Resilience Act (CRA), once in force, will require manufacturers of hardware and software products, including VPN solutions, to follow security-by-design principles throughout the lifecycle of such products.

This includes the remediation of vulnerabilities without delay.

Given their criticality, VPN solutions will be subject to strict conformity assessment requirements.

Resources for mitigate actions

Ivanti recovery instructions:
https://forums.ivanti.com/s/article/Recovery-Steps-Related-to-CVE-2023-46805-and-CVE-2024-21887?language=en_US



To read more: https://www.enisa.europa.eu/news/joint-statement-on-ivanti

Number 7

Enterprise Risk Mitigation Blueprint for Non-Intelligence Agencies

Protect Your Organization from the Foreign Intelligence Threat - Enterprise Risk Mitigation Blueprint

Preamble

Nothing in this document shall be construed as authorization for any organization to conduct activities not otherwise authorized under statutes, executive order, or other applicable law, policy, or regulation nor does this document obviate an organization's responsibility to conduct activities that are otherwise mandated, directed, or recommended for execution under the same.

Threats are not limited to only cyber, insider, foreign intelligence and/or criminal activities.

Introduction

Today's global threat environment is more diverse and dynamic than ever. The 2023 Annual Threat Assessment of the U.S. Intelligence Community (IC) identified a growing number of foreign intelligence entities (FIE), state actors, and non-state actors targeting the United States Government (USG) and the private sector. The Assessment: https://www.dni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf

They are no longer interested just in obtaining classified U.S. secrets, but are also collecting sensitive unclassified information from most government agencies and virtually every sector of our economy.

Personal data, trade secrets, intellectual property, technology, and research and development are being aggressively targeted by adversaries who have the capability, patience, and resources to obtain them.

To achieve their objectives, FIEs are employing a wide range of illegal techniques including insider threats, cyber penetrations, supply chain attacks, and blended operations that combine some or all of these methods.

They are also using a variety of legal and quasi-legal methods, including mergers and acquisitions, investment, joint ventures, partnerships, and talent recruitment programs to acquire U.S. technology and innovation.

Ultimately, FIEs seek to degrade our economic power and national security, compromise our critical infrastructure, and undermine our democratic institutions.

This new form of conflict is not fought on a foreign battlefield but in our power grids, our computer networks, our laboratories and research facilities, our financial institutions, our healthcare systems, and our federal, state, local, and tribal governments.

This challenge can be met only by hard work, determination and diligence, and public and private sector partnership.

NCSC is working closely with partners to implement holistic, integrated enterprise risk mitigation (ERM) programs to develop a “blended” enterprise approach, actively engaging the entire enterprise to protect their organizations.

Our citizens as well as our government and institutions need capabilities that deter our adversaries capabilities. These capabilities can be provided by an integrated and layered ERM program.

This document includes links to risk mitigation information that can help organizations enhance their physical security, personnel security, operations security (OPSEC), cybersecurity, defensive counterintelligence (CI), insider threat mitigation capabilities, and supply chain risk management (SCRM).

ERM programs mitigate vulnerabilities to protect critical assets from collection, theft, disruption, and exploitation.

A well-developed program likely will have the added benefit of protecting the organization against criminal exploitation as well. Successful threat mitigation requires leveraging the workforce at all levels across an organization.

Threat Overview

Some foreign governments combine civilian and military capabilities with criminal activity to steal information to gain an advantage.

These practices illustrate the blurred lines between traditional intelligence collection and economic espionage. Rapid technological advancements are enabling FIEs to refine cyber capabilities and target organizations in the United States.

Their cyber operations penetrate our government and private sector in pursuit of policy insights, research, intellectual property, military and trade secrets, and personal identifiable information (PII), all to obtain a competitive advantage.

There are also significant risks associated with our nation's ever-increasing reliance on interconnected information technologies, particularly across critical infrastructure sectors such as the defense industrial base, energy, finance, healthcare, and telecommunications.

Additionally, many state actors view economic espionage—often using commercial enterprises owned or influenced by the state—as essential to achieving their own national security and economic goals. This comes at our expense.

FIEs attempt to exploit vulnerabilities in government and industry supply chains to steal our intellectual property, corrupt our software, surveil our critical infrastructure, and carry out other malicious activities through cyber or technical operations.

FIE tactics have included elicitation, economic espionage, human targeting, and cyber intrusions. We are increasingly concerned about state and nonstate-sponsored attempts to control or debilitate critical infrastructure systems, corrupt supply chains, or gain access to systems that control our nation's critical infrastructure.

The systemic and persistent vulnerabilities continue to grow, intensifying traditional FIE threats, placing critical infrastructure and emerging and proprietary technologies at risk, eroding competitive advantage, and weakening our global influence.

The federal workforce is one of our nation's greatest assets, but it faces an increasingly challenging risk environment ranging from insider threats, unauthorized disclosures, workplace violence, and being targeted by adversaries.

These workforce challenges will persist. Threat actors are conducting malicious influence campaigns that employ cyber operations, propaganda, and manipulation to try to sow divisions in society and undermine confidence in democratic institutions.

To read more:
https://www.dni.gov/files/NCSC/documents/products/Risk_Mitigation_Web_2023.pdf

Number 8

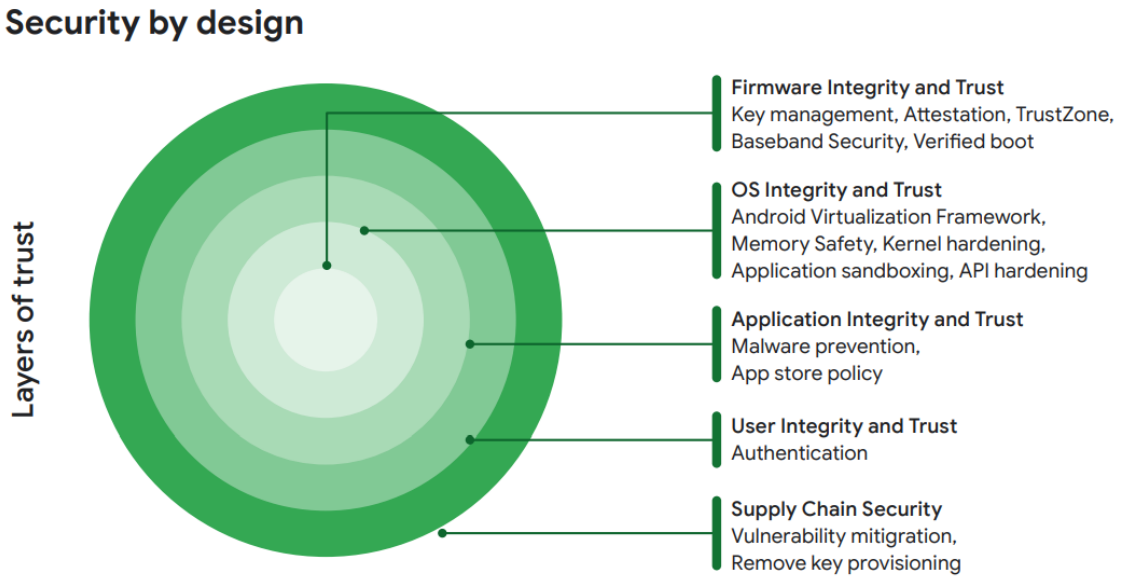
Piloting new ways of protecting Android users from financial fraud

Google Security Blog

From its founding, Android has been guided by principles of openness, transparency, safety, and choice. Android gives you the freedom to choose which device best fits your needs, while also providing the flexibility to download apps from a variety of sources, including preloaded app stores such as the Google Play Store or the Galaxy Store; third-party app stores; and direct downloads from the Internet.

Keeping users safe in an open ecosystem takes sophisticated defenses. That's why Android provides multiple layers of protections, powered by AI and backed by a large, dedicated security & privacy team, to help to protect our users from security threats while continually making the platform more resilient.

We also provide our users with numerous built-in protections like Google Play Protect, the world's most widely deployed threat detection service, which actively scans over 125 billion apps on devices every day to monitor for harmful behavior. That said, our data shows that a disproportionate amount of bad actors take advantage of select APIs and distribution channels in this open ecosystem.



Elevating app security in an open ecosystem

While users have the flexibility to download apps from many sources, the safety of an app can vary depending on the download source. Google Play, for example, carries out rigorous operational reviews to ensure app safety, including proper high-risk API use and permissions handling.

Other app stores may also follow established policies and procedures that help reduce risks to users and their data. These protections often include requirements for developers to declare which permissions their apps use and how developers

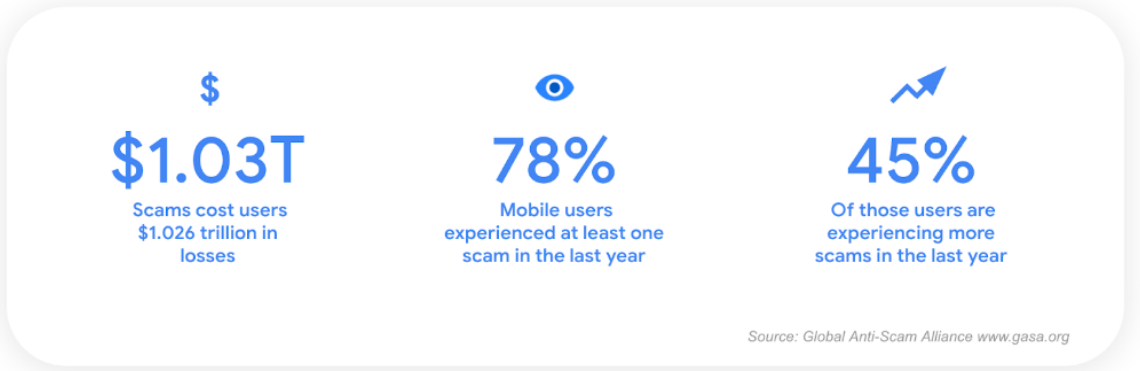
plan to use app data. Conversely, standalone app distribution sources like web browsers, messaging apps or file managers – which we commonly refer to as Internet-sideloading – do not offer the same rigorous requirements and operational reviews. Our data demonstrates that users who download from these sources today face unusually high security risks due to these missing protections.

We recently launched enhanced Google Play Protect real-time scanning to help better protect users against novel malicious Internet-sideloaded apps. This enhancement is designed to address malicious apps that leverage various methods, such as AI, to avoid detection. This feature, now deployed on Android devices with Google Play Services in India, Thailand, Singapore and Brazil, has already made a significant impact on user safety.

As a result of the real-time scanning enhancement, Play Protect has identified 515,000 new malicious apps and issued more than 3.1 million warnings or blocks of those apps. Play Protect is constantly improving its detection capabilities with each identified app, allowing us to strengthen our protections for the entire Android ecosystem.

A new pilot to combat financial fraud

Cybercriminals continue to invest in advanced financial fraud scams, costing consumers more than $1 trillion in losses. According to the 2023 Global State of Scams Report by the Global Anti-Scam Alliance, 78 percent of mobile users surveyed experienced at least one scam in the last year. Of those surveyed, 45 percent said they're experiencing more scams in the last 12 months. The Global Scam Report also found that scams were most often initiated by sending scam links via various messaging platforms to get users to install malicious apps and very often paired with a phone call posing to be from a valid entity.



Scammers frequently employ social engineering tactics to deceive mobile users. Using urgent pretenses that often involve a risk to a user's finances or an opportunity for quick wealth, cybercriminals convince users to disable security safeguards and ignore proactive warnings for potential malware, scams, and phishing. We've seen a large percentage of users ignore, or are tricked into dismissing, these proactive Android platform warnings and proceed with installing malicious apps.

This can lead to users ultimately disclosing their security codes, passwords, financial information and/or transferring funds unknowingly to a fraudster.

To help better protect Android users from these financial fraud attacks, we are piloting enhanced fraud protection with Google Play Protect. As part of a continued strategic partnership with the Cyber Security Agency of Singapore (CSA), we will launch this first pilot in Singapore in the coming weeks to help keep Android users safe from mobile financial fraud.

This enhanced fraud protection will analyze and automatically block the installation of apps that may use sensitive runtime permissions frequently abused for financial fraud when the user attempts to install the app from an Internet-sideloading source (web browsers, messaging apps or file managers).

This enhancement will inspect the permissions the app declared in real-time and specifically look for four runtime permission requests: RECEIVE_SMS, READ_SMS, BIND_Notifications, and Accessibility. These permissions are frequently abused by fraudsters to intercept one-time passwords via SMS or notifications, as well as spy on screen content.

Based on our analysis of major fraud malware families that exploit these sensitive runtime permissions, we found that over 95 percent of installations came from Internet-sideloading sources.

During the upcoming pilot, when a user in Singapore attempts to install an application from an Internet-sideloading source and any of these four permissions are declared, Play Protect will automatically block the installation with an explanation to the user.

Collaborating to combat mobile fraud

This enhanced fraud protection has undergone testing by the Singapore government and will be rolling out to Android devices with Google Play services.

“The fight against online scams is a dynamic one. As cybercriminals refine their methods, we must collaborate and innovate to stay ahead, “ said Mr Chua Kuan Seah, Deputy Chief Executive of CSA. “Through such partnerships with technology players like Google, we are constantly improving our anti-scam defenses to protect Singaporeans online and safeguard their digital assets.”

Together with CSA, we will be closely monitoring the results of the pilot program to assess its impact and make adjustments as needed. We will also support CSA by continuing to assist with malware detection and analysis, sharing malware insights and techniques, and creating user and developer education resources.

How developers can prepare

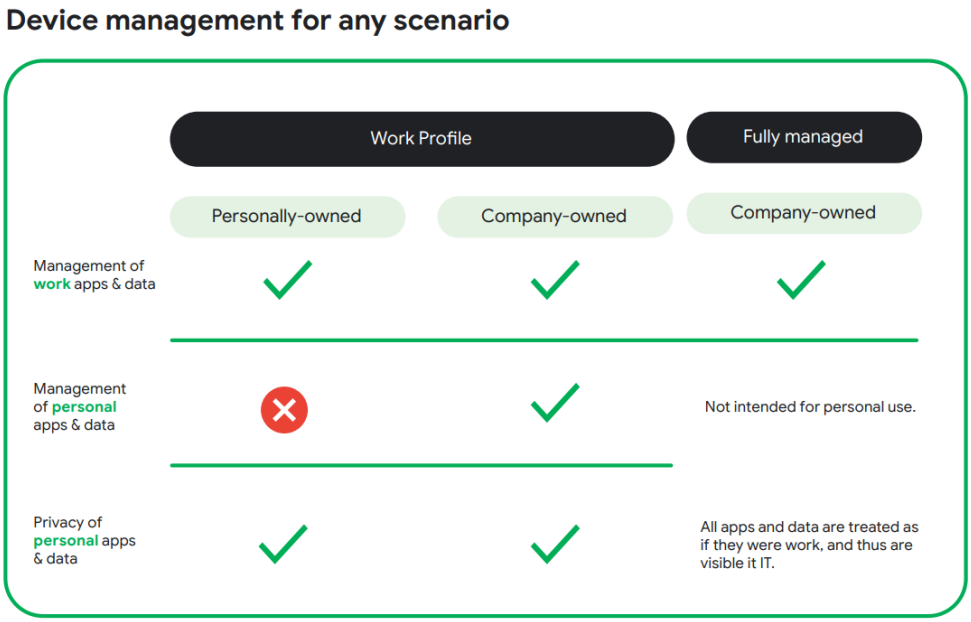
For developers distributing apps that may be affected by this pilot, please take the time to review the device permissions your app is requesting and ensure you’re following developer best practices. Your app should only request permissions that

the app needs to complete an action and ensure it does not violate the Mobile Unwanted Software principles. Always ensure that your app does not engage in behavior that could be considered potentially harmful or malware.

If you find that your app is affected by the app protection pilot you can refer to our updated developer guidance for Play Protect warnings for tips on how to help fix potential issues with your app and instructions for filing an appeal if needed.

Our commitment to protecting Android users

We believe industry collaboration is essential to protect users from mobile security threats and fraud. Piloting these new protections will help us stay ahead of new attacks and evolve our solutions to defeat scammers and their expanding fraud attempt. We have an unwavering commitment to protecting our users around the world and look forward to continuing to partner with governments, ecosystem partners and other stakeholders to improve user protections.



To read more:
https://security.googleblog.com/2024/02/piloting-new-ways-to-protect-Android-users-from%20financial-fraud.html

https://services.google.com/fh/files/misc/android-enterprise-security-paper-2023.pdf

Number 9

DARPA's REMA Program to Add Mission Autonomy to Commercial Drones

From concept to contract in 70 business days: Companies collaborate to add capabilities for off-the-shelf drones to carry out predefined missions without need for operator connection

DARPA DEFENSE ADVANCED RESEARCH PROJECTS AGENCY

Commercial drone technology is advancing rapidly, providing cost-effective and robust capabilities for a variety of civil and military missions.

DARPA's Rapid Experimental Missionized Autonomy (REMA) program aims to enable a drone to autonomously continue its predefined mission when connection to the operator is lost.

The program is focused on constantly providing new agnostic drone autonomy capabilities for transition in one-month intervals to outpace adversarial countermeasures. REMA progressed from program announcement to contract awards in just 70 business days.

"REMA is the demonstrator for rapid ideation and tech development," said Dr. Lael Rudd, REMA program manager. "The five performers under contract are working as a conglomerate without firewalls to create common solutions to achieve the program goals."

As small aerial vehicles play increasingly important military roles on the battlefield, REMA will render ineffective adversaries' electromagnetic countermeasures intended to disrupt communication links between operator and drone to abort missions and cause crashes.

"REMA is focused on creating autonomous solutions to maximize effectiveness of stock commercial and small military drones on the battlefield," said Rudd.

“Through creating an autonomy adapter that works with all commercial drones, regardless of manufacturer, and by developing mission-specific autonomy that is constantly refreshed and easy to upload prior to a mission, we aim to give drone operators the advantage in fast-paced combat operations.”

The 18-month, single-phase program is divided into two technical areas:

1) A drone-autonomy adapter interface and

2) mission-specific autonomy software.

REMA will be able to agnostically detect the drone type when connected and apply autonomy to increase the drone’s capability. REMA will be completed in development cycles starting at three-month intervals and accelerating to one-month intervals, to repeatedly provide new and improved autonomy for direct transition.

Contracts for the drone-autonomy adapter interface technical area have been awarded to Anduril and RTX. Contracts for the mission-specific autonomy software technical area have been awarded to Leidos, Northrop Grumman, and SoarTech.

The first development cycle, or “spiral challenge,” started in December 2023, is focused on developing platforms with agnostic autonomy features. The performers are expected to demonstrate a full working solution to the first challenge in March 2024.

To read more: https://www.darpa.mil/news-events/2024-02-08

Number 10

DOD Releases List of People's Republic of China (PRC) Military Companies in Accordance With Section 1260H of the National Defense Authorization Act for Fiscal Year 2021

U.S. Department of Defense

The Department of Defense released an update to the names of "Chinese military companies" operating directly or indirectly in the United States in accordance with the statutory requirement of Section 1260H of the National Defense Authorization Act for Fiscal Year 2021.

Updating the Section 1260H list of "Chinese military companies" is an important continuing effort in highlighting and countering the PRC's Military-Civil Fusion strategy.

The PRC's Military-Civil Fusion strategy supports the modernization goals of the People's Liberation Army (PLA) by ensuring it can acquire advanced technologies and expertise developed by PRC companies, universities, and research programs that appear to be civilian entities.

Entities Identified as Chinese Military Companies Operating in the United States in accordance with Section 1260H of the William M. ("Mac") Thornberry National Defense Authorization Act for Fiscal Year 2021 (Public Law 116-283)**

360 Security Technology Inc. (Qihoo 360)*

Advanced Micro-Fabrication Equipment Inc. China (AMEC)

Aerospace CH UAV Co., Ltd (S-SEA)*

Aviation Industry Corporation of China Ltd. (AVIC)*
- AVIC Aviation High-Technology Company Limited (AVIC Aviation Hi-Tech)*
- AVIC Heavy Machinery Company Limited (AVIC Heavy Machinery)*
- AVIC Jonhon Optronic Technology Co., Ltd. (AVIC Jonhon)*
- AVIC Shenyang Aircraft Company Limited (AVIC Shenyang)*
- AVIC Xi'an Aircraft Industry Group Company Ltd. (AVIC Xi'an)*
- Jiangxi Hongdu Aviation Industry Co., Ltd. (Hongdu Aviation)*
- Zhonghang Electronic Measuring Instruments Company Limited (ZEMIC)*

Beijing Megvii Technology Co., Ltd. (Megvii)

Beijing Zhidao Chuangyu Information Technology Co., Ltd. (Knownsec)*

BGI Genomics Co., Ltd. (BGI)*

Chengdu JOUAV Automation Tech Co., Ltd. (JOUAV)

Chengdu M&S Electronics Technology Co., Ltd. (M&S Electronics)

China Aerospace Science and Industry Corporation Limited (CASIC)*
Aerosun Corporation (Aerosun)*

China Communications Construction Group (Limited) (CCCG)*
China Communications Construction Company Limited (CCCC)*

China Construction Technology Co., Ltd. (CCTC)

China Electronics Corporation (CEC)*

China Electronics Technology Group Corporation (CETC)*
Hangzhou Hikvision Digital Technology Co., Ltd. (Hikvision)*

China General Nuclear Power Corporation (CGN)*

China Mobile Communications Group Co., Ltd. (China Mobile Comm)*
China Mobile Limited (China Mobile)*

* Denotes entities previously identified as Chinese Military Companies operating in the United States in accordance with Section 1260H of the William M. ("Mac") Thornberry National Defense Authorization Act for Fiscal Year 2021 (Public Law 116-283)

** Subsidiaries Listed with Parent Companies

Section 1260H directs the Department to begin identifying, among other things, Military-Civil Fusion contributors operating directly or indirectly in the United States.

The Department will continue to update the list with additional entities as appropriate. The United States Government reserves the right to take additional actions on these entities under authorities other than section 1260H.

The list is available at:
https://media.defense.gov/2024/Jan/31/2003384819/-1/-1/0/1260H-LIST.PDF

To read more:
https://www.defense.gov/News/Releases/Release/Article/3661985/dod-releases-list-of-peoples-republic-of-china-prc-military-companies-in-accord/

Disclaimer

The Association tries to enhance public access to information about risk and compliance management.

Our goal is to keep this information timely and accurate. If errors are brought to our attention, we will try to correct them.

This information:

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

- should not be relied on in the 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 an interpretative document;

- 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.

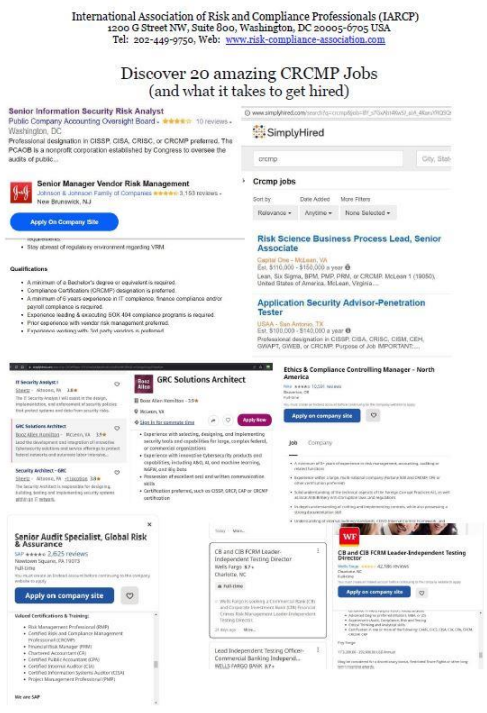
The Association accepts no responsibility regarding such problems incurred because of using this site or any linked external sites.

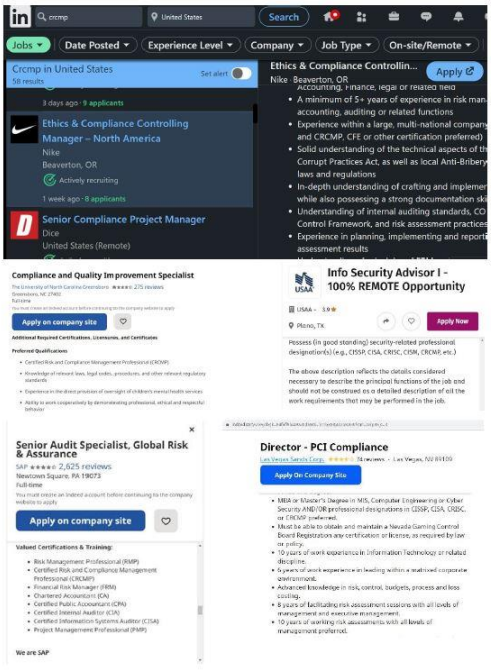
Our training and certification programs:

1. Certified Risk and Compliance Management Professional (CRCMP), distance learning and online certification program. You may visit: https://www.risk-compliance-association.com/Distance_Learning_and_Certification.htm

The CRCMP has become one of the most recognized certificates in risk management and compliance. There are CRCMPs in 57 countries. Companies and organizations around the world consider the CRCMP a preferred certificate.

You can find more about the demand for CRCMPs at: https://www.risk-compliance-association.com/CRCMP_Jobs_Careers.pdf





2. Certified Information Systems Risk and Compliance Professional (CISRCP), distance learning and online certification program. You may visit: https://www.risk-compliance-association.com/CISRCP_Distance_Learning_and_Certification.htm

3. Certified Risk and Compliance Management Professional in Insurance and Reinsurance CRCMP(Re)I, distance learning and online certification program. You may visit: https://www.risk-compliance-association.com/CRCMP_Re_I.htm

4. Certified Cyber (Governance Risk and Compliance) Professional CC(GRC)P, distance learning and online certification program. You may visit: https://www.risk-compliance-association.com/CC_GRC_P_Distance_Learning_and_Certification.htm

5. Travel Security Trained Professional (TSecTPro), distance learning and online certification program. You may visit: https://www.risk-compliance-association.com/TSecTPro_Distance_Learning_and_Certification.htm

The International Association of Risk and Compliance Professionals (IARCP) is a business unit of Compliance LLC, incorporated in Wilmington NC and offices in Washington DC, a provider of risk and compliance training and executive coaching in 57 countries. To learn more: https://www.risk-compliance-association.com/Privacy.htm

You may contact:

Lyn Spooner
Email: lyn@risk-compliance-association.com

George Lekatis
President of the IARCP
1200 G Street NW Suite 800,
Washington DC 20005, USA
Email: lekatis@risk-compliance-association.com
Web: www.risk-compliance-association.com
HQ: 1220 N. Market Street Suite 804,
Wilmington DE 19801, USA