International Association of Risk and Compliance Professionals (IARCP)
1200 G Street NW Suite 800, Washington DC, 20005-6705 USA
Tel: 202-449-9750, Web: www.risk-compliance-association.com

Monday, May 23, 2022

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

Dear members and friends,

Supply chain disruption continues. Now it is the time to turn crisis into opportunity, by making supply chains more reliable and resilient.

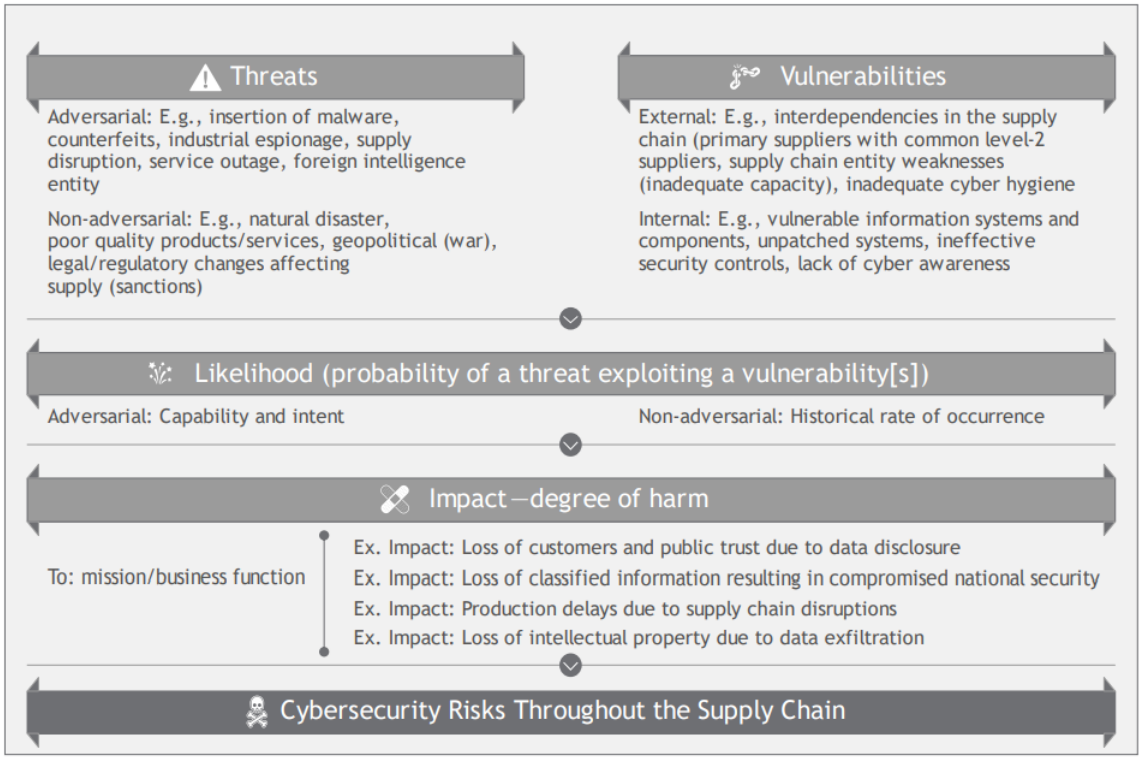
Cybersecurity risks throughout the supply chain refers to the potential for harm or compromise that arises from the cybersecurity risks posed by suppliers, their supply chains, and their products or services.

This is part of the new paper, *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations*, from the National Institute of Standards and Technology (NIST). According to the paper, examples of these risks include:

- Insiders working on behalf of a system integrator steal sensitive intellectual property,resulting in the loss of a major competitive advantage.

- A proxy working on behalf of a nation-state inserts malicious software into supplierprovided product components used in systems sold to government agencies. A breach occurs and results in the loss of several government contracts.
- A system integrator working on behalf of an agency reuses vulnerable code, leading to a breach of mission-critical data with national security implications.
- An organized criminal enterprise introduces counterfeit products onto the market, resulting in a loss of customer trust and confidence.
- A company is on contract to produce a critical component of a larger acquisition, but the company relabels products from an unvetted supplier. A critical component that cannot be trusted is deployed into operational systems, and there no trusted supplier of replacement parts.

Risks such as these are realized when threats in the cybersecurity supply chain exploit existing vulnerabilities. The figure below depicts supply chain cybersecurity risks resulting from the likelihood that relevant threats may exploit applicable vulnerabilities and the consequential potential impacts.



Supply chain cybersecurity vulnerabilities may lead to persistent negative impacts on an enterprise's missions, ranging from a reduction in service levels leading to customer dissatisfaction to the theft of intellectual property or the degradation of critical mission and business processes.

It may, however, take years for such vulnerabilities to be exploited or

discovered. It may also be difficult to determine whether an event was the direct result of a supply chain vulnerability.

Vulnerabilities in the supply chain are often interconnected and may expose enterprises to cascading cybersecurity risks. For example, a large-scale service outage at a major cloud services provider may cause service or production disruptions for multiple entities within an enterprise's supply chain and lead to negative effects within multiple mission and business processes.

The phrase *"persistent negative impact"* in the paper is very interesting. I remember that Albert Einstein believed that *reality is merely an illusion, albeit a very persistent one.*

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

U.S. SECURITIES AND EXCHANGE COMMISSION

Number 6 (Page 23)

U.S. Treasury Issues First-Ever Sanctions on a Virtual Currency Mixer, Targets DPRK Cyber Threats

Number 7 (Page 29)

NIST Publishes Review of Digital Forensic Methods

Report documents the scientific foundations of digital evidence examination and recommends ways to advance the field.

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

Number 8 (Page 32)

"A 'New' New Era:" Prepared Remarks Before the International Swaps and Derivatives Association Annual Meeting

SEC Chair Gary Gensler

Number 9 (Page 35)

How we make every day safer with Google

Jen Fitzpatrick, SVP, Core

Google

Number 10 (Page 38)

Active Cyber Defence, the 5th Year: Summary of Key Findings

National Cyber Security Centre

Number 1

Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations

Jon Boyens, Angela Smith, Nadya Bartol, Kris Winkler, Alex Holbrook, Matthew Fallon

Information and communications technology (ICT) and operational technology (OT) rely on a complex, globally distributed, extensive, and interconnected supply chain ecosystem that is comprised of geographically diverse routes and consists of multiple levels of outsourcing.

This ecosystem is composed of public and private sector entities (e.g., acquirers, suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers) that interact to research, develop, design, manufacture, acquire, deliver, integrate, operate, maintain, dispose of, and otherwise utilize or manage ICT/OT products and services.

These interactions are shaped and influenced by a set of technologies, laws, policies, procedures, and practices. This ecosystem has evolved to provide a set of highly refined, cost-effective, and reusable solutions.

Public and private sector entities have rapidly adopted this ecosystem of solutions and increased their reliance on commercially available products, system integrator support for custom-built systems, and external service providers.

This, in turn, has increased the complexity, diversity, and scale of these entities.

In this document, the term *supply chain* refers to the linked set of resources and processes between and among multiple levels of an enterprise, each of which is an acquirer that begins with the sourcing of products and services and extends through the product and service life cycle.

Given the definition of supply chain, cybersecurity risks throughout the supply chain refers to the potential for harm or compromise that may arise from suppliers, their supply chains, their products, or their services.

Cybersecurity risks throughout the supply chain are the results of threats that exploit vulnerabilities or exposures within products and services that traverse the supply chain or threats that exploit vulnerabilities or exposures

within the supply chain itself. Examples of cybersecurity risks throughout the supply chain include:

1) A widget manufacturer whose design material is stolen in another country, resulting in the loss of intellectual property and market share.

2) A widget manufacture that experiences a supply disruption for critical manufacturing components due to a ransomware attack at a supplier three tiers down in the supply chain.

3) A store chain that experiences a massive data breach tied to an HVAC vendor with access to the store chain's data-sharing portal.

Note that SCRM and C-SCRM refer to the same concept for the purposes of NIST publications. In general practice, C-SCRM is at the nexus of traditional Supply Chain Risk Management (SCRM) and traditional Information Security. Organizations may employ different terms and definitions for SCRM outside of the scope of this publication. This publication does not address many of the non-cybersecurity aspects of SCRM.

Technology solutions provided through a supply chain of competing vendors offer significant benefits, including low cost, interoperability, rapid innovation, and product feature variety.

Whether proprietary, government-developed, or open source, these solutions can meet the needs of a global base of public and private sector customers. However, the same factors that create such benefits also increase the potential for cybersecurity risks that arise directly or indirectly from the supply chain.

Cybersecurity risks throughout the supply chain are often undetected and impact the acquirer and the end-user. For example, deployed software is typically a *commercial off-the-shelf (COTS)* product, which includes smaller COTS or open source software components developed or sourced at multiple tiers.

Updates to software deployed across enterprises often fail to update the smaller COTS components with known vulnerabilities, including cases in which the component vulnerabilities are exploitable in the larger enterprise software.

Software users may be unable to detect the smaller known vulnerable components in larger COTS software (e.g., lack of transparency, insufficient vulnerability management, etc.).

The non-standardized nature of C-SCRM practices adds an additional layer of complexity as this makes the consistent measurement and management of cybersecurity risks throughout the supply chain difficult for both the organization and members of its supply chain (e.g., suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers).

When engaging with suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers, agencies should carefully consider the breadth of the Federal Government's footprint and the high likelihood that individual agencies may enforce varying and conflicting C-SCRM requirements.

Overcoming this complexity requires interagency coordination and partnerships.

The passage of the Federal Acquisition Supply Chain Security Act (FASCSA) of 2018 aimed to address this concern by creating a government-wide approach to the problem of supply chain security in federal acquisitions by establishing the Federal Acquisition Security Council (FASC).

The FASC serves as a focal point of coordination and information sharing and a harmonized approach to acquisition security that addresses CSCRM in acquisition processes and procurements across the federal enterprise.

In addition, the law incorporated SCRM into FISMA by requiring reports on the progress and effectiveness of the agency's supply chain risk management, consistent with guidance issued by the Office of Management and Budget (OMB) and the Council.

Note that this publication uses the term "enterprise" to describe Level 1 of the risk management hierarchy. In practice, an organization is defined as an entity of any size, complexity, or positioning within a larger enterprise structure (e.g., a federal agency or company).

By this definition, an enterprise is an organization, but it exists at the top level of the hierarchy where individual senior leaders have unique risk management responsibilities [NISTIR 8286].

Several organizations may comprise an enterprise. In these cases, an enterprise may have multiple Level 1s with stakeholders and activities defined at both the enterprise and the organization levels.

Level 1 activities conducted at the enterprise level should inform those activities completed within the subordinate organizations.

Enterprises and organizations tailor the C-SCRM practices described in this publication as applicable and appropriate based on their own unique enterprise structure.

There are cases in this publication in which the term “organization” is inherited from a referenced source (e.g., other NIST publication, regulatory language). Refer to NISTIR 8286, Integrating Cybersecurity and Enterprise Risk Management (ERM), for further guidance on this topic.

Purpose

Cybersecurity Supply Chain Risk Management (C-SCRM) is a systematic process for managing exposure to cybersecurity risks throughout the supply chain and developing appropriate response strategies, policies, processes, and procedures.

The purpose of this publication is to provide guidance to enterprises on how to identify, assess, select, and implement risk management processes and mitigating controls across the enterprise to help manage cybersecurity risks throughout the supply chain.

The content in this guidance is the shared responsibility of different disciplines with different SCRM perspectives, authorities, and legal considerations.

The C-SCRM guidance provided in this document is not one-size-fits-all. Instead, the guidance throughout this publication should be adopted and tailored to the unique size, resources, and risk circumstances of each enterprise.

Enterprises adopting this guidance may vary in how they implement C-SCRM practices internally.

To that end, this publication describes C-SCRM practices observed in enterprises and offers a general prioritization of C-SCRM practices (i.e., Foundational, Sustaining, Enabling) for enterprises to consider as they implement and mature C-SCRM.

However, this publication does not offer a specific roadmap for enterprises to follow to reach various states of capability and maturity.

The processes and controls identified in this document can be modified or augmented with enterprise-specific requirements from policies, guidelines, response strategies, and other sources.

This publication empowers enterprises to develop C-SCRM strategies tailored to their specific mission and business needs, threats, and operational environments.

Target Audience

C-SCRM is an enterprise-wide activity that should be directed as such from a governance perspective, regardless of the specific enterprise structure.

This publication is intended to serve a diverse audience involved in C-SCRM, including:

• Individuals with system, information security, privacy, or risk management and oversight responsibilities, including authorizing officials (AOs), chief information officers, chief information security officers, and senior officials for privacy;

• Individuals with system development responsibilities, including mission or business owners, program managers, system engineers, system security engineers, privacy engineers, hardware and software developers, system integrators, and acquisition or procurement officials;

• Individuals with project management-related responsibilities, including certified project managers and/or integrated project team (IPT) members;

• Individuals with acquisition and procurement-related responsibilities, including acquisition officials and contracting officers;

• Individuals with logistical or disposition-related responsibilities, including program managers, procurement officials, system integrators, and property managers;

• Individuals with security and privacy implementation and operations responsibilities, including mission or business owners, system owners, information owners or stewards, system administrators, continuity planners, and system security or privacy officers;

• Individuals with security and privacy assessment and monitoring responsibilities, including auditors, Inspectors General, system evaluators, control assessors, independent verifiers and validators, and analysts; and

• Commercial entities, including industry partners, that produce component products and systems, create security and privacy technologies, or provide services or capabilities that support information security or privacy.

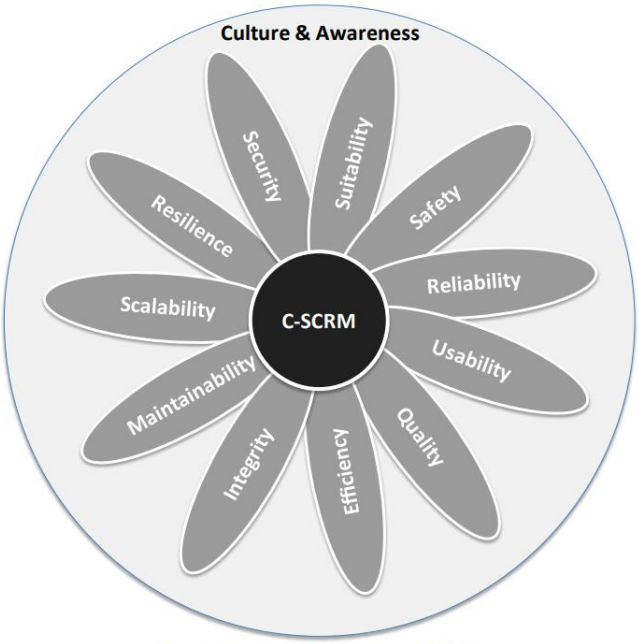


Fig. 1-1: Dimensions of C-SCRM

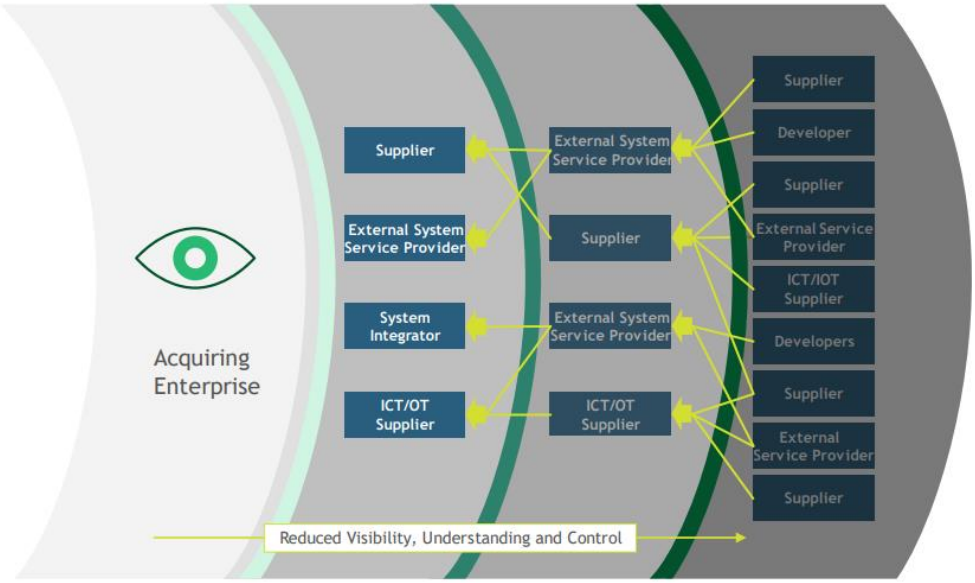


Fig. 1-2: An Enterprise's Visibility, Understanding, and Control of its Supply Chain

To read more:
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1.pdf

Number 2

Computers and money: the work of the Basel Committee on cryptoassets

Pablo Hernández de Cos, Chair of the Basel Committee on Banking Supervision and Governor of the Bank of Spain, at the 36th Annual General Meeting of the International Swaps and Derivatives Association, Madrid.

Introduction

Good morning, and thank you for inviting me to speak at your 36th Annual General Meeting (AGM). On a personal level, let me welcome all of you to Madrid. I hope that you will have the time to visit and enjoy all that it has to offer. It's great to see meetings and events slowly taking place in-person once again.

I understand that the last time ISDA held an in-person AGM was in April 2019. I don't think it's an understatement to say that the world has changed profoundly since then.

A global pandemic, heightened geopolitical tensions and rising stagflationary pressures, to name just a few developments, will continue to shape the risk environment for the banking system over the coming months and years. Vigilance continues to be the watchword for both banks and their supervisors.

But there are also medium-term structural trends and developments that have continued to grow in importance. Most notably, the twin forces of digitalisation and climate-related financial risks will be at the centre of the Basel Committee's priorities over the coming years.

Add to this the growing interconnections between banks and non-bank financial intermediation (NBFI) and rising debt (both public and private), and you have no shortage of vulnerabilities that need careful monitoring and management.

I will focus my remarks today on a subset of these structural trends, namely, the Committee's work on digitalisation, with a particular emphasis on cryptoassets. But before I do so, let me first mention another pivotal element of the Basel Committee's work over the coming years.

As just discussed in the previous session, implementing all aspects of the Basel III framework in a full, timely and consistent manner is an imperative for our member jurisdictions.

Events over the past two years, including the pandemic and the Ukraine conflict, have once again highlighted the importance of having a prudent and robust global regulatory framework in place.

These events have also underlined how we cannot afford to leave unaddressed the remaining fault-lines in the regulatory framework. We may not always have as much fiscal and monetary space available to respond to future crises as was the case over the past two years. Banks' self-resilience will therefore depend even more critically on their own capital and liquidity resources.

A key aspect of the outstanding Basel III reforms is the revised market risk framework. As you know, the revised framework seeks to address a number of shortcomings related to banks' trading books that were painfully exposed during the Great Financial Crisis, including:

A porous boundary between the trading and banking book, resulting in exploitative regulatory arbitrage. The gravity of this behaviour during the GFC made it the textbook example for regulatory arbitrage.

The revised framework introduces more prescriptive requirements when it comes to the scope of instruments that may, or may not, be included in the trading book.

Internal models that lacked robustness and could not account for the magnitude of extreme financial shocks.

More than a decade since the GFC, we continue to see how existing value-at-risk (VaR) models are incapable of capitalising against such events: the number of VaR breaches by major internationally active banks in response to market volatility over the past two years exceeded pre-pandemic breaches by an order of magnitude.

This time is certainly not different. The revised framework replaces VaR with an expected shortfall model that better captures tail risks and limits the discretion available for banks to determine capital requirements.

The lack of an appropriate standardised approach to serve as a credible fallback to internal models, thus increasing the incentives for aggressive modelling behaviour and lowballing modelled capital requirements. A fundamentally redesigned standardised approach will bring greater risk

sensitivity and serve as the basis for calculating market risk requirements for the "output floor". This, in turn, will help ensure that banks' modelled capital requirements do not fall below a certain level. It will also facilitate the comparability of banks' market risk profiles within and across jurisdictions.

It is in our collective interests to see the Basel III reforms implemented in full and consistently. ISDA and its members can contribute to locking in these financial stability benefits by doubling down their efforts and focus towards implementing these standards.

In that regard, allow me to be somewhat blunt: the time for negotiations and lobbying is over. The Committee will in due course evaluate the impact of all of its reforms after they are implemented.

Cryptoassets and DeFi: some progress, but much more work needed

There was a quip about three years ago that described cryptoassets as "everything you don't understand about money combined with everything you don't understand about computers". I think it's fair to say that, since then, our understanding of both the economic and technological dimensions of cryptoassets has deepened.

Despite our better understanding of cryptoassets and DeFi, the jury is still out when it comes to ascertaining how best to harness their oft-cited promises and benefits, while mitigating their risks and safeguarding financial stability. The shortcomings of the existing financial architecture are well known, including at times high costs, low speed, limited access and insufficient transparency.

The purported aims of DeFi and cryptoassets of a seamless, open, inclusive and transparent financial system are certainly noble. Some might also sympathise with the idea of a robust network characterised by its "unstructured simplicity", as originally envisioned by Satoshi Nakamoto.

To read more: https://www.bis.org/speeches/sp220512.htm

Number 3

Joint ESA Supervisory Statement on expectations regarding the 'What is this product?' section of the key information document for packaged retail and insurancebased investment products

2. CONTEXT AND OBJECTIVE

2.1. The objective of this Supervisory Statement is to achieve a high, effective and consistent level of regulation and national supervision promoting a level playing field and the protection of retail investors.

2.2. The 'What is this product?' section is the first descriptive section of the KID and is an essential part of the document to enable retail investors to understand the key features of the product.

It is also a largely "free text" section within the KID template, where it is the responsibility of the PRIIP manufacturer to use appropriate text or language and there are not pre-defined narrative explanations.

2.3. The answer to the question 'What is this product?' must be provided according to five elements:

- the type of the PRIIP ('Type');
- its objectives and the means for achieving them, including by means of direct or indirect exposure to the underlying assets ('Objectives');
- the description of the type of retail investor to whom the PRIIP is intended to be marketed ('Intended retail investor');
- where applicable, details of the insurance benefits; and
- the term of the PRIIP ('Term').

2.4. Taking into account different approaches taken by certain PRIIP manufacturers to describe the main features of the product, including approaches which are considered to go against the aims of the KID to provide retail investors with information that is accurate, fair, clear and not misleading, the ESAs consider it important to clarify their expectations regarding the 'What is this product?' section of the KID.

2.5. In particular, as highlighted in recitals 13 and 14 of the PRIIPs Regulation, given difficulties many retail investors have in understanding specialist financial terminology, particular attention should be paid to the vocabulary and style of writing used in the document.

It is, therefore, necessary to ensure that clear and understandable language is used, which is accessible to retail investors and that the description of how the investment objectives are achieved, including the description of the financial instruments used, avoids financial jargon and terminology which is not clear to retail investors.

The ESAs' supervisory experience since the implementation of the KID has shown that these standards relating to the use of clear and understandable language, are often not adhered to by PRIIPs manufacturers.

2.6. This Supervisory Statement applies to all types of PRIIPs. However, a number of the issues identified so far during the supervision of the KID concern product features that are not relevant to all types of PRIIPs, and in particular are only relevant for certain types of structured products or derivatives.

These features include, for example, autocallability, the possibility for early termination, and the payment of coupons or leverage. Products with these features are usually offered directly, but in some jurisdictions might also be offered as underlying investment options in a PRIIP offering a range of options for investment.

In this context, in most cases, the issues are only applicable to the specific information on relevant underlying investment options, rather than the generic key information document.

2.7. At this stage, the ESAs have considered those elements of the 'What is this product?' section that apply to all types of PRIIPs, including the 'Type', 'Objectives' and 'Intended retail investor' and 'Term'.

This does not mean that there are not issues relating to current practices for the part of this section on the insurance benefits, or indeed regarding other "free text" sections of the KID.

The ESAs may, in a next step, set out their views and expectations regarding these other parts of the KID.

2.8. For each of the issues identified, a description is provided of some of the current practices observed, with reference to specific examples drawn

from KIDsthat are included in an Annex, followed by the ESAs expectations regarding how to improve the clarity and comparability of KIDs.

To read more:
https://www.eiopa.europa.eu/document-library/supervisory-statement/joint-esa-supervisory-statement-expectations-regarding-what_en

Number 4

Threat report on application stores

The risks associated with the use of official and third party app stores.

National Cyber Security Centre
a part of GCHQ

Introduction

Over the last decade there has been an enormous increase in the availability and use of smartphones and smart devices.

Many of these devices feature application stores ('app stores'), which allow users to download additional applications and content.

The vast majority of users, particularly on mobile platforms, download apps via these app stores.

There's also been increased demand for apps, primarily as a result of the COVID-19 pandemic as more people work, shop, and stay in touch online. Since there is a great variety of devices (and supporting app stores), there are a number of disparate and complex security issues that can expose consumers and enterprises to online threats.

This report summarises the risks associated with the use of official and third party app stores.

It includes links to detailed guidance that describe how to mitigate the main threats.

This report was compiled to inform Department for Digital, Culture, Media & Sport's (DCMS) review on current threats associated with app stores.

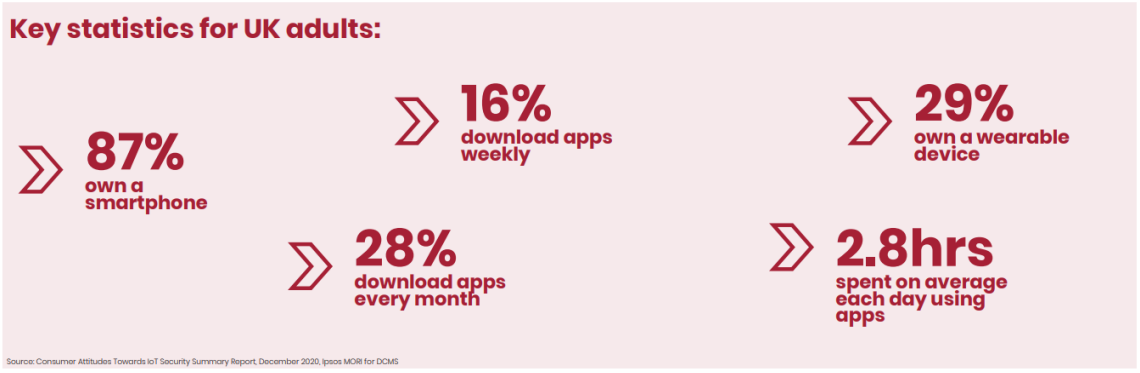
The report will aid in the development of policy interventions that will seek to improve app stores' security and privacy controls to protect both UK consumers and enterprises.

It will also be of particular interest to the following audiences:

• developers of applications for both mobile and other connectable consumer devices (such as smart TVs and wearables)

• administrators responsible for managing the use of applications within their organisations (for example in BYOD scenarios)

• other governments with an interest in implementing policy to improve their security posture of app stores to protect their consumers and enterprises.



This report identifies systemic vulnerabilities that have been used by attackers to exploit app stores.

It includes a selection of case studies which describe how users of official and third party app stores have been affected, as well as users of smartwatches, smart TVs, and voice assistants.

An application, or app, is a software package that users can install or are pre-installed on a device to provide extra functionality or content to their

device. Most people will be familiar with downloading apps for their smartphones and tablets, but they can also be installed on laptops, computers, games consoles, wearable devices (such as smartwatches or fitness trackers), smart TVs, smart speakers (such as Alexa devices), and IoT (internet of things) devices.

Apple and Google provide their users with access to a dedicated app store (Apple's App Store, Google's Play Store) where they can download free and paid apps. Original equipment manufacturers (OEMs) also provide stores, such as the Huawei AppGallery, the Samsung Galaxy Store, or Amazon's App Store.

Users of IoT devices typically are only able to download apps onto their devices via a manufacturer-supported store. The UK is amongst the leading nations for consumer spends and downloads on Apple's App Store and the Google Play Store.

A survey conducted by Ipsos MORI6 on behalf of DCMS reveals that the majority of users download applications using official app stores for their smartphone/tablets. 52% of UK consumers have downloaded apps from Google Play Store. 44% of UK consumers have downloaded apps from Apple's App Store.

To read more:
https://www.ncsc.gov.uk/files/Threat-report-on-application-stores-web-v2.pdf

Number 5

SEC Nearly Doubles Size of Enforcement's Crypto Assets and Cyber Unit

U.S. SECURITIES AND EXCHANGE COMMISSION

The Securities and Exchange Commission announced the allocation of 20 additional positions to the unit responsible for protecting investors in crypto markets and from cyber-related threats.

The newly renamed Crypto Assets and Cyber Unit (formerly known as the Cyber Unit) in the Division of Enforcement will grow to 50 dedicated positions.

"The U.S. has the greatest capital markets because investors have faith in them, and as more investors access the crypto markets, it is increasingly important to dedicate more resources to protecting them," said SEC Chair Gary Gensler. "The Division of Enforcement's Crypto Assets and Cyber Unit has successfully brought dozens of cases against those seeking to take advantage of investors in crypto markets. By nearly doubling the size of this key unit, the SEC will be better equipped to police wrongdoing in the crypto markets while continuing to identify disclosure and controls issues with respect to cybersecurity."

Since its creation in 2017, the unit has brought more than 80 enforcement actions related to fraudulent and unregistered crypto asset offerings and platforms, resulting in monetary relief totaling more than $2 billion.

The expanded Crypto Assets and Cyber Unit will leverage the agency's expertise to ensure investors are protected in the crypto markets, with a focus on investigating securities law violations related to:

- Crypto asset offerings;
- Crypto asset exchanges;
- Crypto asset lending and staking products;
- Decentralized finance ("DeFi") platforms;
- Non-fungible tokens ("NFTs"); and
- Stablecoins.

In addition, the unit has brought numerous actions against SEC registrants and public companies for failing to maintain adequate cybersecurity controls and for failing to appropriately disclose cyber-related risks and incidents.

The Crypto Assets and Cyber Unit will continue to tackle the omnipresent cyber-related threats to the nation's markets.

"Crypto markets have exploded in recent years, with retail investors bearing the brunt of abuses in this space. Meanwhile, cyber-related threats continue to pose existential risks to our financial markets and participants," said Gurbir S. Grewal, Director of the SEC's Division of Enforcement. "The bolstered Crypto Assets and Cyber Unit will be at the forefront of protecting investors and ensuring fair and orderly markets in the face of these critical challenges."

The infusion of 20 additional positions into the Crypto Assets and Cyber Unit will bolster the ranks of its supervisors, investigative staff attorneys, trial counsels, and fraud analysts in the agency's headquarters in Washington, DC, as well as several regional offices.

To read more: https://www.sec.gov/news/press-release/2022-78

Number 6

U.S. Treasury Issues First-Ever Sanctions on a Virtual Currency Mixer, Targets DPRK Cyber Threats

The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) sanctioned virtual currency mixer Blender.io (Blender), which is used by the Democratic People's Republic of Korea (DPRK) to support its malicious cyber activities and money-laundering of stolen virtual currency.

On March 23, 2022, Lazarus Group, a DPRK state-sponsored cyber hacking group, carried out the largest virtual currency heist to date, worth almost $620 million, from a blockchain project linked to the online game Axie Infinity; Blender was used in processing over $20.5 million of the illicit proceeds.

Under the pressure of robust U.S. and UN sanctions, the DPRK has resorted to illicit activities, including cyber-enabled heists from cryptocurrency exchanges and financial institutions, to generate revenue for its unlawful weapons of mass destruction (WMD) and ballistic missile programs.

"Today, for the first time ever, Treasury is sanctioning a virtual currency mixer," said Under Secretary of the Treasury for Terrorism and Financial Intelligence Brian E. Nelson. "Virtual currency mixers that assist illicit transactions pose a threat to U.S. national security interests. We are taking action against illicit financial activity by the DPRK and will not allow state-sponsored thievery and its money-laundering enablers to go unanswered."

Treasury is also updating the List of Specially Designated Nationals and Blocked Persons (SDN List) to identify additional virtual currency addresses used by the Lazarus Group to launder illicit proceeds.

Treasury is committed to exposing components of the virtual currency ecosystem, like Blender, that are critical to the obfuscation of the trail of stolen proceeds from illicit cyber activity. OFAC sanctioned the Lazarus Group on September 13, 2019, pursuant to Executive Order (E.O.) 13722, and identified it as an agency, instrumentality, or controlled entity of the Government of the DPRK, based on its relationship to the U.S.- and

UN-designated Reconnaissance General Bureau, the DPRK's premiere intelligence organization, which is also involved in conventional arms trade.

Blender.io (Blender) is a virtual currency mixer that operates on the Bitcoin blockchain and indiscriminately facilitates illicit transactions by obfuscating their origin, destination, and counterparties.

Blender receives a variety of transactions and mixes them together before transmitting them to their ultimate destinations. While the purported purpose is to increase privacy, mixers like Blender are commonly used by illicit actors.

Blender has helped transfer more than $500 million worth of Bitcoin since its creation in 2017. Blender was used in the laundering process for DPRK's Axie Infinity heist, processing over $20.5 million in illicit proceeds.

OFAC's investigation also identified Blender's facilitation of money-laundering for, among others, Russian-linked malign ransomware groups including Trickbot, Conti, Ryuk, Sodinokibi, and Gandcrab.

Blender is being designated pursuant to E.O. 13694, as amended, for having materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services to or in support of, a cyber-enabled activity originating from, or directed by persons located, in whole or in substantial part, outside the United States that is reasonably likely to result in, or has materially contributed to, a significant threat to the national security, foreign policy, or economic health or financial stability of the United States and that has the purpose or effect of causing a significant misappropriation of funds or economic resources, trade secrets, personal identifiers, or financial information for commercial or competitive advantage or private financial gain.

While most virtual currency activity is licit, it can be used for illicit activity, including sanctions evasion, through mixers, peer-to-peer exchangers, darknet markets, and exchanges. This includes the facilitation of heists, ransomware schemes, and other cybercrimes.

Treasury continues to use its authorities against malicious cyber actors in concert with other U.S. departments and agencies, as well as our foreign partners, to disrupt financial nodes tied to illicit payments and cyber-attacks.

Those in the virtual currency industry play a critical role in implementing appropriate Anti-Money Laundering/Countering the Financing of Terrorism (AML/CFT) and sanctions controls to prevent sanctioned

persons and other illicit actors from exploiting virtual currency to undermine U.S foreign policy and national security interests.

The virtual currency mixers that assist criminals are a threat to U.S. national security interests. Treasury will continue to investigate the use of mixers for illicit purposes and consider the range of authorities Treasury has to respond to illicit financing risks in the virtual currency ecosystem.

For example, in 2020, Treasury's Financial Crime Enforcement Network (FinCEN) assessed a $60 million civil money penalty against the owner and operator of a virtual currency mixer for violations of the Bank Secrecy Act (BSA) and its implementing regulations. You may visit: https://www.fincen.gov/sites/default/files/enforcement_action/2020-10-19/HarmonHelix%20Assessment%20and%20SoF_508_101920.pdf

UNITED STATES OF AMERICA
FINANCIAL CRIMES ENFORCEMENT NETWORK
DEPARTMENT OF THE TREASURY

IN THE MATTER OF:	)	
	)	
	)	Number 2020-2
Larry Dean Harmon	)	
d/b/a Helix	)	
	)	
Akron, Ohio	)	

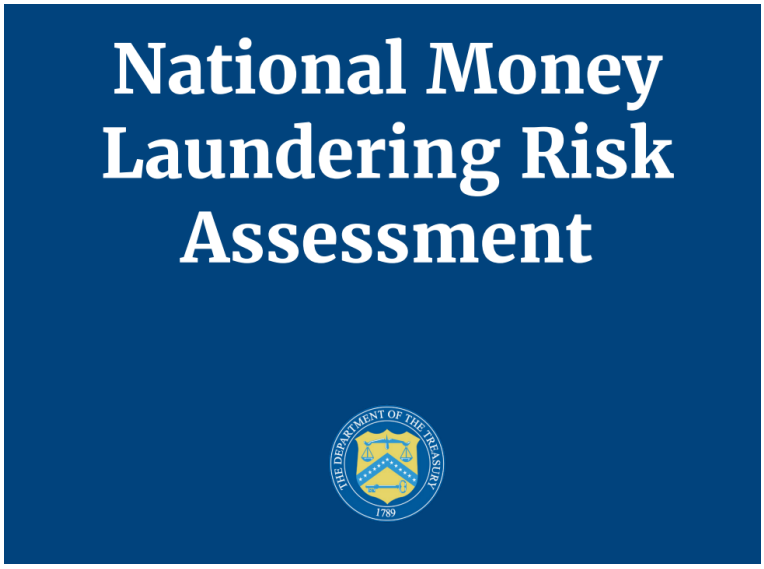
ASSESSMENT OF CIVIL MONEY PENALTY

I. INTRODUCTION

The Financial Crimes Enforcement Network (FinCEN) has determined that grounds exist to assess a civil money penalty against Larry Dean Harmon, as the primary operator of Helix, and as the Chief Executive Officer (CEO) and primary operator of Coin Ninja LLC (Coin Ninja), pursuant to the Bank Secrecy Act (BSA) and regulations issued pursuant to that Act.[1]

Criminals have increased use of anonymity-enhancing technologies, including mixers, to help hide the movement or origin of funds. Additional information on illicit financing risks associated with mixers and other anonymity-enhancing technologies in the virtual asset ecosystem can be found in the 2022 National Money Laundering Risk Assessment. You may

visit:
https://home.treasury.gov/system/files/136/2022-National-Money-Laundering-Risk-Assessment.pdf



ADDITIONAL LAZARUS GROUP WALLET

OFAC is identifying four additional virtual currency wallet addresses used by the Lazarus Group to launder the remainder of stolen proceeds from the March 2022 Axie Infinity heist. This builds upon OFAC's April 14, 2022, attribution of DPRK's Lazarus Group as the perpetrators of the Axie Infinity heist and identification of the original getaway wallet address. Treasury is committed to tracing illicit virtual currency and blocking associated wallets and addresses wherever found.

SANCTIONS IMPLICATIONS

As a result of today's action, all property and interests in property of the entity above, Blender.io, that is in the United States or in the possession or control of U.S. persons is blocked and must be reported to OFAC. In addition, any entities that are owned, directly or indirectly, 50 percent or more by one or more blocked persons are also blocked. All transactions by U.S. persons or within (or transiting) the United States that involve any property or interests in property of designated or otherwise blocked persons are prohibited unless authorized by a general or specific license issued by OFAC, or exempt. These prohibitions include the making of any contribution or provision of funds, goods, or services by, to, or for the benefit of any blocked person and the receipt of any contribution or provision of funds, goods, or services from any such person.

For identifying information on the entity sanctioned:
https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20220506

For information on complying with virtual currency sanctions, see OFAC's Sanctions Compliance Guidance for the Virtual Currency Industry at:
https://home.treasury.gov/system/files/126/virtual_currency_guidance_brochure.pdf

OFAC
Office of Foreign Assets Control

Number 7

NIST Publishes Review of Digital Forensic Methods

Report documents the scientific foundations of digital evidence examination and recommends ways to advance the field.

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

The National Institute of Standards and Technology (NIST) has published *Digital Investigation Techniques: A NIST Scientific Foundation Review*. This draft report, which will be open for public comment for 60 days, reviews the methods that digital forensic experts use to analyze evidence from computers, mobile phones and other electronic devices. You may visit: https://www.nist.gov/forensic-science/digital-investigation-techniques-scientific-foundation-review

NISTIR 8354-DRAFT

Digital Investigation Techniques: *A NIST Scientific Foundation Review*

The purpose of NIST scientific foundation reviews is to document and evaluate the scientific basis for forensic methods. These reviews fill a need identified in a landmark 2009 study by the National Academy of Sciences, which found that many forensic disciplines lack a solid foundation in scientific research.

To conduct their review, the authors examined peer-reviewed literature, documentation from software developers, test results on forensic tools, standards and best practices documents and other sources of information.

They found that "digital evidence examination rests on a firm foundation based in computer science," and that "the application of these computer science techniques to digital investigations is sound."

"Copying data, searching for text strings, finding timestamps on files, reading call logs on a phone. These are basic elements of a digital investigation," said Barbara Guttman, leader of NIST's digital forensics research program and an author of the study. "And they all rely on

fundamental computer operations that are widely used and well understood."

The report also discusses several challenges that digital forensic experts face, including the rapid pace of technological change. "Digital evidence techniques don't work perfectly in all cases," Guttman said. "If everyone starts using a new app, forensic tools won't be able to read and understand the contents of that app until they are updated. This requires constant effort."

To address this challenge, the report recommends better methods for information-sharing among experts and a more structured approach to testing forensic tools that would increase efficiency and reduce duplication of effort across labs.

The report also recommends increased sharing of high-quality forensic reference data that can be used for education, training, and developing and testing new forensic tools.

NIST's Digital Forensics Research Program, which was launched in 1999, develops methods for testing digital forensics tools and provides access to high-quality reference datasets.

NIST also maintains a vast archive of published software, the National Software Reference Library, that is a critical resource for investigating computer crimes.

NIST scientific foundation reviews help laboratories identify appropriate limitations on the use of forensic methods, identify priorities for future research, and suggest steps for moving the field forward.

These reviews are conducted as part of NIST's Forensic Science Program, which works to strengthen forensic practice through research and improved standards. In 2018 Congress directed NIST to conduct these scientific reviews and appropriated funding for them.

Readers can submit comments on the draft report through July 11, 2022. NIST will host a webinar about the draft report on June 1, 2022. Instructions for submitting comments and registration information for the webinar are available on the NIST website.

To read more: https://www.nist.gov/digital-evidence

https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8354-draft.pdf

Number 8

"A 'New' New Era:" Prepared Remarks Before the International Swaps and Derivatives Association Annual Meeting

SEC Chair Gary Gensler

Thank you for the kind introduction. It's good to be back with the International Swaps and Derivatives Association (ISDA) again.

As is customary, I'd like to note that I'm not speaking on behalf of my fellow Commissioners or the SEC staff.

Swaps emerged in the 1980s to provide producers and merchants with a way to lock in the price of commodities, interest rates, and currency rates. Our economy benefits from a well-functioning swaps market, as it's essential that companies have the ability to manage their risks.

When I first appeared before this group, as Chair of the Commodity Futures Trading Commission (CFTC), Washington was still developing the regulatory response to the 2008 financial crisis. At the time, I had the honor of working with then-CFTC Commissioner Scott O'Malia, now the CEO of ISDA, on reforms to the swaps market. A decade ago, I called it a "new era for the swaps marketplace."

The financial crisis had many chapters, but a form of security-based swaps — credit default swaps, particularly those used in the mortgage market — played an important role throughout the story.

International banks were using credit default swaps to lower regulatory capital requirements and to hedge their bank loan portfolios — or so they thought.

These derivatives were at the core of what led to the $180 billion bailout of AIG, whose near-failure accelerated the crisis.

More than a decade later, we've continued to see the relevance of this market. For instance, in light of Russia's invasion of Ukraine, many market participants are closely watching the credit default swaps related to Russian companies and sovereign debt.

The security-based swap market comprises also includes single-name and narrow-based equity swaps, some of which are called total return swaps.

Hedge funds and other asset managers increasingly have been using total return swaps to express a position that then may be held on the balance sheet of their prime broker or bank.

In March 2021, a month before I was sworn in as SEC Chair, Archegos Capital Management failed. Archegos used total return swaps based on large concentrated positions in underlying stocks, and prime brokers had significant exposure to that family office. In April, we charged Archegos Capital Management and affiliated individuals with committing fraud and manipulating stock prices using total return swaps.

Ten years before the collapse of AIG, in 1998, Long-Term Capital Management failed. It brought with it more than $1 trillion of derivatives contracts, many of which were total return swaps. I was serving at the U.S. Department of the Treasury at the time, sent along with the Federal Reserve to examine the impending failure of this firm.

Thus, the role of security based swaps in the market jitters in 1998, 2008, and 2021 help inform how I think about security-based swaps.

When Congress decided to bring reforms to the overall swaps market, they assigned the bulk of the swaps market to our sibling agency, the CFTC, which I had the honor of chairing. They assigned authority over security-based swaps, however, to the SEC, as these derivatives were related to the securities, issuers, and markets at the core of our remit.

Congress sought to align key aspects of the security-based swap market with our policy perimeter for other aspects of the securities markets: reducing risk, increasing transparency, and enhancing market integrity.

While we have adopted many reforms to the security-based swap market, we have work to do to further fulfill our obligations under Dodd-Frank and update rules for this marketplace. Thus, we are embarking on yet another "new era."

Risk Reduction

The reforms included two main ways to reduce risk. First, dealers would have to register with the SEC. In doing so, they'd need to have key back-office controls and adequate cushions against losses.

Last year, in November, security-based swap dealers and major security-based swap participants were required to register with the Commission for the first time.

The requirements for the 47 conditionally registered security-based swap dealers include new counterparty protections, requirements for capital and margin, internal risk management, supervision and chief compliance officers, trade acknowledgement and confirmation, and recordkeeping and reporting procedures.

The other part of Dodd-Frank's risk-reduction regime was central clearing.

In 2016, we adopted new rules for clearinghouses. The SEC now regulates three clearinghouses that clear security-based swaps, in particular credit default swaps.

To read more:
https://www.sec.gov/news/speech/gensler-remarks-swaps-and-derivatives-association-annual-meeting-051122

Number 9

How we make every day safer with Google

Jen Fitzpatrick, SVP, Core

Google

Every day, we work to create a safer internet by making our products secure by default, private by design, and putting you in control of your data. This is how we keep more people safe online than anyone else in the world.

Secure by default in the face of cyber threats

Today, more cyberattacks than ever are happening on a broader, global scale. The targets of these attacks are not just major companies or government agencies, but hospitals, energy providers, banks, schools and individuals. Every day, we keep people's data safe and secure through industry-leading security technology, automatic, built-in protections, and ongoing vulnerability research and detection.

Our specialized teams work around the clock to combat current and emerging cyber threats. Google's Threat Analysis Group (TAG), for example, has been tracking critical cyber activity to help inform Ukraine, neighboring countries in Europe, and others of active threat campaigns in relation to the war. We've also expanded our support for Project Shield to protect the websites of 200+ Ukrainian government entities, news outlets and more.

Cybersecurity concerns are not limited to war zones — more than 80% of Americans say they're concerned about the safety and privacy of their online data. That's why we built one of the world's most advanced security infrastructures to ensure that our products are secure by default.

Now, that infrastructure helps keep people safer at scale:

- *Account Safety Status:* We're adding your safety status to your apps so you never have to worry about the security of your Google Account. These updates will feature a simple yellow alert icon on your profile picture that will flag actions you should take to secure your account.

- *Phishing protections in Google Workspace:* We're now scaling the phishing and malware protections that guard Gmail to Google Docs, Sheets, and Slides.

- *Automatic 2-Step Verification:* We're also continuing our journey towards a more secure, passwordless future with 2-Step Verification

(2SV) auto enrollment to help people instantly boost the security of their Google Accounts and reduce their risk of getting phished. This builds on our work last year to auto enroll 150+ million accounts in 2SV and successfully reduce account takeovers.

- *Virtual Cards:* As people do more shopping online, keeping payment information safe and secure is critically important. We're launching virtual cards on Chrome and Android. When you use autofill to enter your payment details at checkout, virtual cards will add an additional layer of security by replacing your actual card number with a distinct, virtual number.

  This eliminates the need to manually enter card details like the CVV at checkout, and they're easy to manage at pay.google.com — where you can enable the feature for eligible cards, access your virtual card number, and see recent virtual card transactions. Virtual cards will be rolling out in the US for Visa, American Express, Mastercard and all Capital One cards starting this summer.

Helpful products that are private by design

We're committed to designing products that are helpful and protect people's privacy. Our engineers have pioneered and open-sourced numerous privacy preserving technologies, including Federated Learning and Differential Privacy, which we made more widely available earlier this year when we started offering our Differential Privacy library in Python as a free open-source tool — reaching almost half of developers worldwide.

Now, we're expanding this work with the introduction of Protected Computing, a growing toolkit of technologies that transform how, when, and where data is processed to technically ensure the privacy and safety of your data. We do this by:

- *Minimizing your data footprint:* Leveraging techniques like edge processing and ephemerality, we shrink the amount of your personally identifiable data.

- *De-identifying data:* Through blurring and randomizing identifiable signals, to adding statistical noise, we use a range of anonymization techniques to strip your identity from your data.

- *Restricting access:* Through technologies like end-to-end encryption and secure enclaves, we make it technically impossible for anyone, including Google, to access your sensitive data.

Today, Protected Computing enables helpful features like Smart Reply in Messages by Google and Live Translation on Pixel. And while we're continuing to innovate new applications across our products, we're equally focused on using Protected Computing to unlock the potential of data to benefit society more broadly — for example, by enabling even more robust aggregated and anonymized datasets so we can safely do everything from help cities reduce their carbon footprint, to accelerate new medical breakthroughs.

To read more:
https://blog.google/technology/safety-security/how-we-make-every-day-safer-with-google/

Number 10

Active Cyber Defence, the 5th Year: Summary of Key Findings

National Cyber Security Centre

What is Active Cyber Defence?

The UK continues to be one of the most digitally advanced countries in the world, with our lives being online more than ever before.

As this digitisation continues, it is vital that the UK remains able to protect its organisations, business and citizens against cyber crime.

The aim of Active Cyber Defence (ACD) is to "Protect the majority of people in the UK from the majority of the harm caused by the majority of the cyber attacks the majority of the time."

It was launched in 2017 and continues to protect the UK, in a relatively automated way, from a significant proportion of commodity cyber attacks.

The ACD programme is one of the NCSC's most successful ways to help bring about a real-world, positive impact against threats.

The programme seeks to reduce high-volume cyber attacks, such as malware, ever reaching UK citizens, and aims to remove the burden of action from the user.

The ACD programme's core services include Takedown, Protective DNS, Early Warning and Exercise in a Box.

This document summarises some of the key findings from the fifth year of the NCSC´s ACD programme. A fuller report, covering all of the services within the ACD programme, will be published shortly.

Takedown Service
www.ncsc.gov.uk/information/takedown-service

The Takedown Service finds malicious sites and sends notifications to the host or owner to get them removed from the internet before significant harm can be done.

The NCSC centrally manages the service, so departments automatically benefit without having to sign up.

Key findings from the Takedown Service

In total, 2.7M campaigns (3.1M URLs) were taken down in 2021. This is a significant increase when compared with 2020's tally (700,595 campaigns and 1,448,214 URLs) and is principally due to the prolonged period we have been performing takedowns against extortion mail server and celebrity - endorsed investment scams throughout 2021.

These attacks are widely distributed and generate a proportionally large number of takedown records.

Table 1: Total takedowns by attack campaign group, 2020 and 2021

Attack Type	2020	2021
Extortion Mail Server	179,008 (Nov-Dec)	1,867,435
Celeb Endorsed Investment Scams	290,345 (Apr-Dec)	607,723
Fake Shop	160,295 (Apr-Dec)	107,251
Phishing URL	33,964	54,382
Web Shell	5,323	26,060
Advance Fee Fraud	27,346	19,197
Technical Support Scam	1,450 (Nov-Dec)	14,448
Advance Fee Fraud Mail Server	2,686	6,632
Malware Infrastructure URL	4,755	4,668
Vulnerable Application	-	4,050
Phishing URL Mail Server	6,849	53,437
Malware Attachment Mail Server	7,839	2,580
Malware Distribution URL	5,198	2,188

To read more:
https://www.ncsc.gov.uk/files/ACD-The-Fifth-Year-Summary-of-Key-Findings.pdf

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.

International Association of Risk and Compliance Professionals (IARCP)

You can explore what we offer to our members:

1. *Membership* – Become a standard, premium or lifetime member.

You may visit:
https://www.risk-compliance-association.com/How_to_become_member.htm

2. *Weekly Updates* - Visit the *Reading Room* of the association at:
https://www.risk-compliance-association.com/Reading_Room.htm

3. *Training and Certification* – Become:

- a Certified Risk and Compliance Management Professional (CRCMP),

- a Certified Information Systems Risk and Compliance Professional (CISRCP),

- a Certified Cyber (Governance Risk and Compliance) Professional - CC(GRC)P,

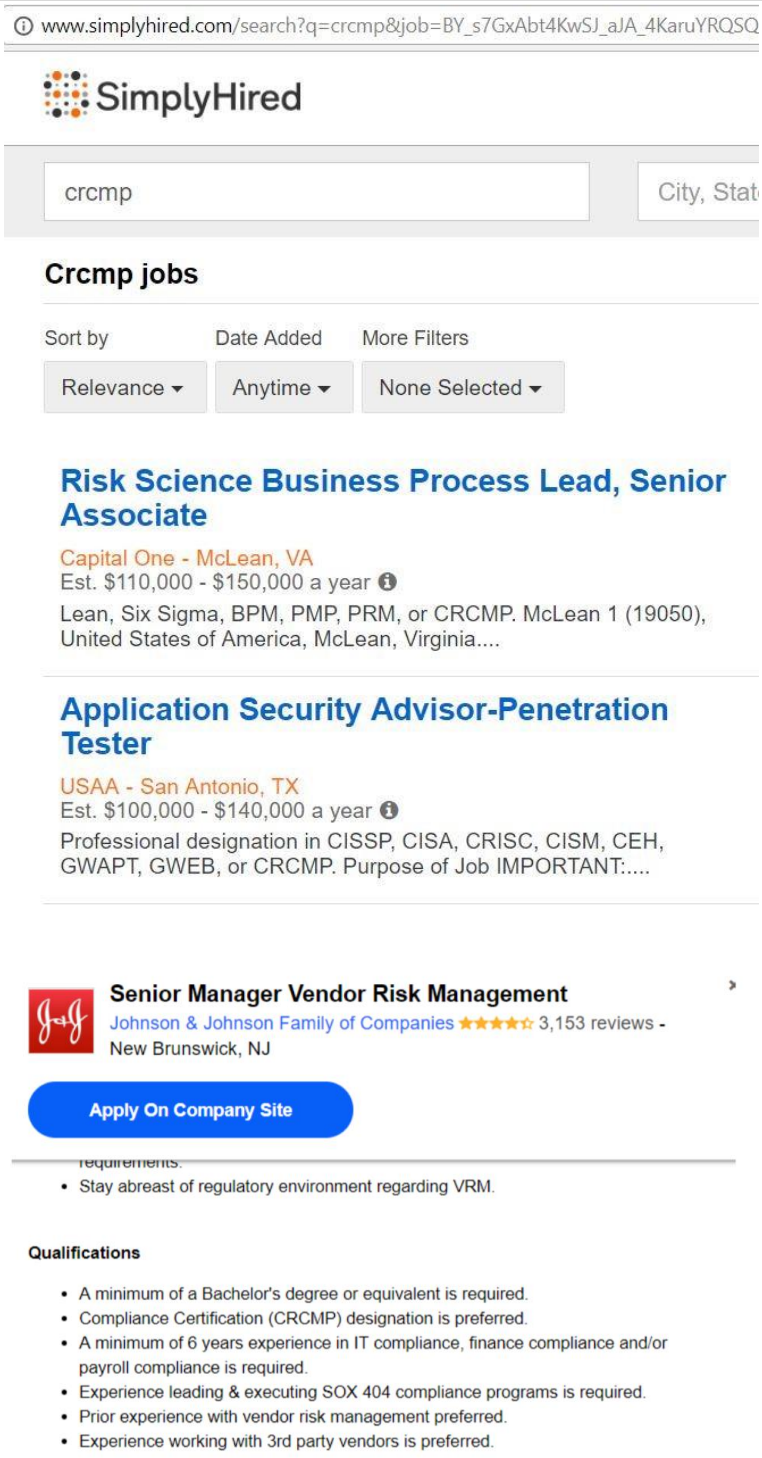
- a Certified Risk and Compliance Management Professional in Insurance and Reinsurance - CRCMP(Re)I,

- a Travel Security Trained Professional (TSecTPro).

The CRCMP has become one of the most recognized certificates in risk management and compliance. There are CRCMPs in 32 countries.

Companies and organizations around the world consider the CRCMP a preferred certificate:

Senior Information Security Risk Analyst
Public Company Accounting Oversight Board - ★★★★☆ 10 reviews - Washington, DC
Professional designation in CISSP, CISA, CRISC, or CRCMP preferred. The PCAOB is a nonprofit corporation established by Congress to oversee the audits of public...



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

For the 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

For the 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

For the 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

For the 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

For the 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

Certified Cyber (Governance Risk and Compliance) Professionals - CC(GRC)Ps, have a 50% discount for the Travel Security Trained Professional (TSecTPro) program ($148 instead of $297).

You have a $100 discount after you purchase one of our programs. The discount applies to each additional program. For example, you can purchase the CRCMP program for $297, and then purchase the CISRCP program for $197 (instead of $297), the CC(GRC)P program for $197 (instead of $297), the CRCMP(Re)I program for $197 (instead of $297), and the TSecTPro program for $197 (instead of $297).

For *instructor-led* training, you may contact us. We can tailor all programs to meet specific requirements.