NUMBER 71 | OCTOBER 2022

NTT DATA
Trusted Global Innovator

Radar

Cybersecurity magazine

GOVERNANCE, RISK AND COMPLIANCE AS A FUNDAMENTAL SUPPORT IN THE RISK MANAGEMENT OF COMPANIES

The real growth potential of companies is compromised by the increasing identification of risks they face on a daily basis. This context has changed in large part due to the Covid-19 crisis which highlighted risks (environmental, technological, cyber, financial, etc.). Companies must therefore take new measures to manage them appropriately in order to prevent them from threatening their continuity.

The implementation of these new measures in risk analysis and risk treatment involves different activities such as:

- Analysis of strategic objectives: verifying the alignment of the processes that deliver and process information to achieve these objectives and leverage them with GRC management.
- Diagnosis: Identifying the current state of the processes and business areas that contribute to GRC, identifying scenarios to evaluate and opportunities.
- Approach: The definition of objectives and diagnosis establishes the line of business, risks and processes involved.

Organisations that have prioritised the implementation of GRC have been able to better achieve their objectives, optimise resources and improve the capabilities of their infrastructure and teams.

All of this means a constant improvement that allows the company's teams to have sufficient tools in case of an eventuality.

The great acceptance and openness of the market has allowed organisations in other sectors that, due to their type of operation, did not have GRC within their organisation, to implement it internally or with the support of external entities such as NTT DATA.

Yakeline Prieto Ballesteros

Cybersecurity Leader at NTT Data Colombia

CYBER NEWS

Internet browsers are the gateway to most of the queries we make in our day to day, being Google Chrome one of the most used. To get the greatest possible benefit out of them we usually make use of extensions, which are created and developed with the purpose of having greater functionality and agility.

McAfee recently published on its official blog a list of malicious extensions that may have affected more than 1.4 million users by stealing browsing data and storing it on servers owned by the extensions' creator.

> "A list of malicious extensions has been published that could have affected more than 1.4 million users".

How do these identified malicious extensions operate? They track user browsing activity and then insert code, modifying cookies on e-commerce sites that have been visited. The purpose is for the authors of the extensions to receive the payments that the user has made on those sites.

The above used manifest.json which sets the background page as bg.html. This HTML file loads b0.js and is responsible for sending the visited URL and injecting code into e-commerce sites; it also uses the POST method to collect information such as the URL, user ID, device location (country, city, postcode) and an encoded referrer URL.

What are the extensions involved? These extensions offered functionalities such as watching content from the Netflix platform together, coupons on websites, taking screenshots, etc. More specifically, five identified extensions are the following: Netflix Party, Netflix Party 2, FlipShope - Price Tracker Extension, Full Page Screenshot Capture – Screenshotting and AutoBuy Flash Sales.

This situation exposed by McAfee is an explicit violation of consumer privacy, as browsing data is being shared. It is therefore recommended that we pay attention to the installations we make, validate their authenticity, check the functionalities of the extensions and the permissions that are being requested and assess the privacy risk to which we are exposing ourselves.

We often do not read or pay attention to the small print, but it is really important and can save us from situations like this.

THE CHALLENGE FOR ORGANIZATIONS TO HAVE A RISK MANAGEMENT, RISK AND COMPLIANCE (GRC) MODEL IN PLACE

By: NTT DATA

We are currently observing that different sectors are becoming more aware of risk identification. There is a growing need for strategic IT governance to guide processes and a focus on compliance with the organisation, control bodies and customers.

What is a GRC system in an organisation and why is it important?

It can be established as a management model that helps to manage the organisation's functions, led by corporate governance and integrating the functions of risk management and compliance responsibilities. It is also considered as a strategy that is implemented to transfer corporate governance and enterprise risk management effectively and efficiently, managed from an organisational approach.

An organisation's GRC model provides a management model that integrates the activities and functions of corporate governance, risk management, performance management and accountability to ensure that its activities are conducted in accordance with the laws and regulations facing the organisation. This enhances the ability of companies to achieve their business objectives.

GRC is considered as a model that enables a company or institution to consistently achieve its objectives by including governance, risk, and compliance management in its processes.

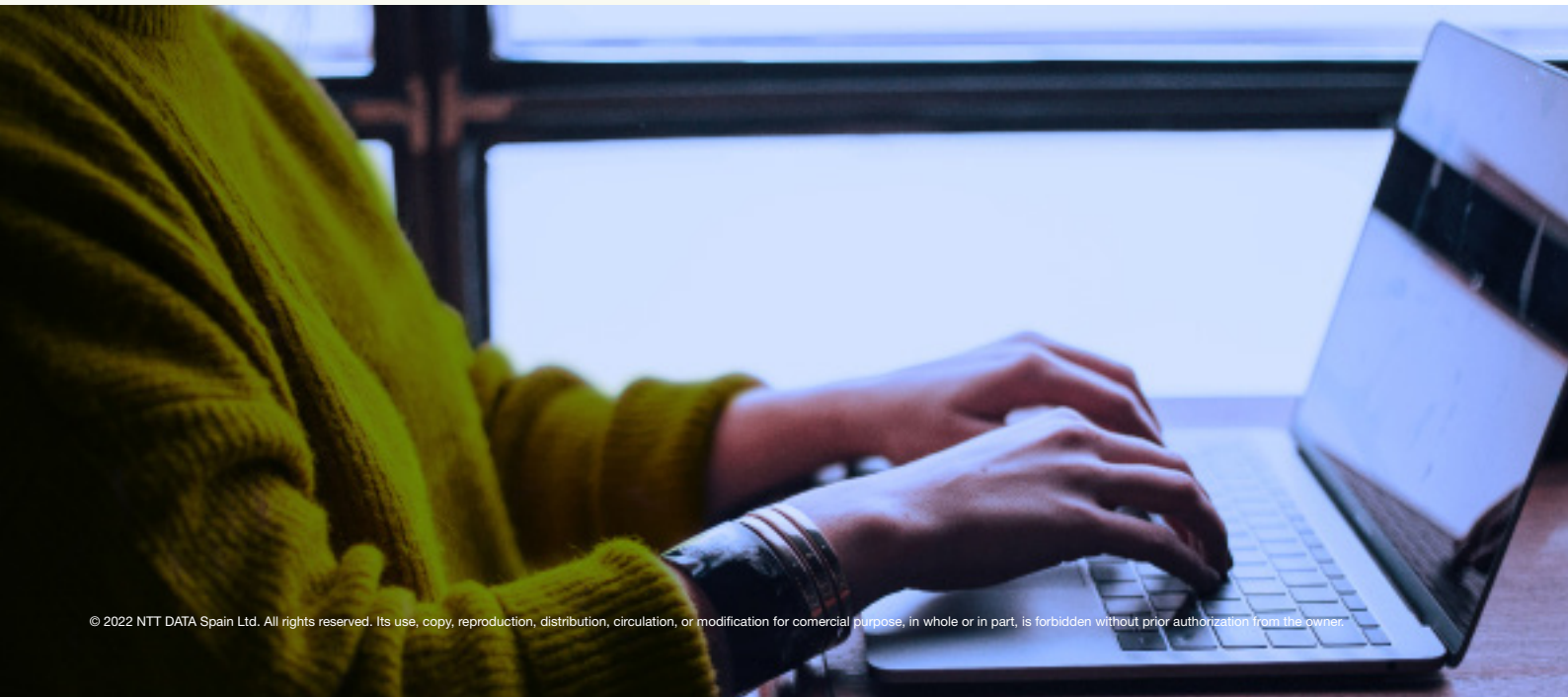
Governance supports the strategic objectives of the organisation since this is where the operational strategies are structured and generated in order to achieve the organisational objectives.

Risk management is also linked to objectives and performance. In an organisation there are different types of risks: legal, operational, technological, reputational, among others; if these risks are not managed, it is likely that the established objectives will be impacted.

In order to carry out an organisational inclusion, risks are identified and the order in which they should be addressed is established according to how they affect the achievement of organisational objectives.

Once the business model has been defined in terms of strategies, processes, technology, and workforce, GRC helps companies to create value. This is achieved by transforming those risks into opportunities, controlling, or mitigating them, within the regulatory framework of laws, regulations, and international standards; always fulfilling the agreements with customers, employees, providers, and stakeholders.

Having a GRC system in place within organisations allows for tools to be put in place to protect systems, networks and infrastructure from potential cyber-attacks that seek to access, modify, or destroy company information.



How is the management model developed in organisations?

Within organisations we can observe the need and demand for a better integrated and collaborative organisational structure, which allows for greater control over the management of situations that may impact on organisational achievements or objectives. It becomes a challenge to prioritise management, comply with regulations and at the same time be the starting point of information for decision making within the organisation.

To achieve the above, it is strategic to have an organised management framework, for which it is recommended to implement GRC under guidelines and good practices defined in methodologies that can be selected according to the organisation's control objectives.

Methodology use

The implementation of methodologies such as Fair (Factor Analysis of Information Risk), NIST, Cobit 5.0 and ISO27001, has as its main objective to identify the likely risks, as well as the chances that these risks will move from a potential risk situation to an actual situation. Having this foresight can allow companies to take corrective measures to anticipate or mitigate risks.

The study of probability offers the opportunity to understand the level of certainty and impossibility for each scenario analysed. Probability implies that an incident may occur, but it may also not occur, depending on the corrective and preventive actions that a company will exercise.

NIST Methodology

The NIST Cybersecurity Framework helps all organisations of all sizes to better understand their cybersecurity risks, manage and reduce their risks, and protect their networks and data. The Framework provides organisations with best practices to help them decide where they need to focus the efforts of their staff and the organisation's business environment to improve cybersecurity processes and protections.

The framework is composed of five simultaneous and continuous functions: Identify, Protect, Detect, Respond and Recover.

Identify: Identification is made by means of a list of all equipment and software programs used, including computers, laptops, smartphones, tablets, and devices used in each communication channel.

Protect: The protection of the network of assets and devices is sought, considering the following validations:

- Controlling who accesses the network and the use of connected devices.
- Use of data protection security software.
- Updating security software on a regular basis.
- Performing backups.
- Encryption of sensitive data in transit and storage process.
- Implementation of formal policies for secure disposal of information.
- Training of internal staff and board of directors in the use of cybersecurity policies on the use of implementations and their exposure to the network.

Detect: Within the activities set out in the standard, detection activities are established, initially relating to the monitoring of computers and networks to control access by unauthorised personnel, the use of devices for support or storage and the use of USB data or software that may be present during the operational process.

In addition, consideration should be given to reviewing the network to monitor the detection of unauthorised users and connections, as well as investigating unusual connections or use of information.

Respond: The incident response process should be taken into account within the implementation by considering the processes of:

- Notifying customers, employees and other data that may generate risk.
- Maintaining the functioning of business operations.
- Reporting the attack to those in charge of compliance with legal guidelines.

Recover: The last consideration is related to the recovery process after the infrastructure and network is affected by external or internal attacks affecting equipment and network segments.

In addition, it is required that all staff and customers be kept informed of the activities that will be executed during an attack or recovery scenario.

FAIR Methodology

With new market needs arising on a daily basis, the need for risk assessment, identification of controls and the establishment of governance has become evident.

The importance of quantifying cyber risk, be it to manage it with senior management, business units or even insurers, brings to the table the real need to assess cyber risks as objectively as possible. The challenge is twofold: to gain relevance and legitimacy.

The FAIR model is divided into four key components, with the main objective of accurately identifying risk scenarios and their correlation with each other:

Threats: provides an adequate profile of potential threats to better understand the scale and magnitude of the damage they can inflict.

Assets: can be tangible, such as computers, services and other electronic devices connected to an organisation's IT framework, or intangible, such as data files.

The organisation: the organisation is the entity that is observed and analysed for risks, especially if any of these risk situations, or a combination of them, may cause damage to the company.

The external environment: You also have external factors to contend with, which may or may not be within your control, but which may nevertheless represent likely risk factors. These include industry competitors,

legislative obstacles, regulatory frameworks and the like.

COBIT 5.0 Framework

The use of frameworks in organisations has become an important point of reference to obtain better value and optimal performance, taking into account the resource utilisation and risk levels assumed. COBIT 5 enables IT to be governed and managed holistically across the organisation, taking into consideration business and functional areas, as well as internal and external stakeholders. COBIT 5 can be applied to organisations of all sizes, whether in the private sector, public sector, or any type of business entity.

Figura 2—Principios de COBIT 5

ISO 27001:2013

It is known as a standard for information security approved and published as an international standard in October 2005 by the International Organisation for Standardisation and the International Electrotechnical Commission. It specifies the requirements necessary to establish, implement, maintain, and improve an information security management system according to the well-known “Deming Cycle”: denoted by the acronym PDCA - Plan, Do, Check, Act.

It also ensures the security, confidentiality and integrity of data and information, as well as of the systems that process it.

Which or what combination of frameworks best suits your organisation? Each company must look at itself and decide the frameworks through which it wants to manage and measure in order to evolve its risk mitigation and continue to leverage its strategic objectives.

HOW WELL PROTECTED ARE OUR INDUSTRIAL PROTECTION AND OT SYSTEMS?

By: NTT DATA

Although there is a lot of information available on cybersecurity of ICSs (Industrial Control System) in general, not much research has been done on how to apply this knowledge to systems specific to industries producing goods in various sectors and utility companies. Many of them are in the early stages of protecting their assets and operating technologies against cybersecurity threats.

Before implementing any security strategy, policy or technology, the assets that require protection and the threats that jeopardise the security of these assets must be identified. Therefore, the focus should be on cyber threats and vulnerabilities, not on strategy or policy setting. Only when the threats and the risks they pose have been covered, can the necessary countermeasures be designed and implemented.

The use of industrial control systems (ICSs) has been spreading in different sectors of industry due to their characteristics of remote monitoring and management of an industrial process, facilitating the execution of routine and complex services, storage of historical records, availability of information on screen and maintenance access. At the beginning, ICSs were designed to work in isolated environments and were used in plants with complex and large-scale processes. Nowadays, the massification of technology and the economy of scale has made them available to companies of different sizes, from SMEs to large companies.

The coverage of ICSs in different industries, together with their functionality to control some kind of process or at least gather some kind of process information in real time, has turned them into a focus of attention and a target for possible cyber-attacks with various motivations, creating threats that were not originally conceived, given that they were designed to work in isolated environments. The availability of relevant information for different levels of companies housed in ICSs has meant that they are currently connected to corporate networks, or sometimes even public networks such as the Internet. This has led to an increase in the threats applicable to this type of system.

Another of the characteristics of ICSs that is conceived as a cause of risk leading to the generation of threats is the priority that these systems give to maintaining a continuous service, preventing in many cases the adequate updating of these systems. In addition, the current trend of migration of the technological platforms used towards general use technologies extends the risks of conventional technology to this type of systems, while multiplying the number of possible attackers with sufficient knowledge to produce damage.

On the other hand, compounding the scenario, there is a tendency to underestimate the risks, which is widespread among those in charge of managing ICSs. There is a belief that no attacker could be motivated to target these systems. This belief is countered by pointing out the possible motivations of potential attackers, ranging from disgruntled employees or former employees to terrorists or ideologically motivated attackers.

According to a survey conducted by Kaspersky Lab, the most common cyber threats faced by businesses include spam, malware, phishing, network intrusion, mobile device theft and DoS (denial of service) attacks.

According to another Kaspersky Lab report [1] focusing on ICSs, 35% of malicious code in ICS networks is spread from the corporate office network, 29% from remote access connections and 9% directly from the Internet, while in the remaining incidents the ICS network is accessed directly. This means that approximately three out of four attacks use connections to other networks in the delivery phase.

In many cases, because ICSs control and monitor processes of vital importance to society (such as water distribution or power generation and distribution), they are conceived as systems that are functionally designed to work continuously. The availability of the service provided is the absolute priority.

Unlike traditional ICT (Information and Communication Technology) systems, ICSs have a different approach to the CIA (Confidentiality, Integrity, Availability) pyramid of priorities. In an ICS, the primary objective is to guarantee the availability of the service and the system, whereas in a traditional ICT system, the scale of the pyramid of priorities is based on confidentiality, then integrity and finally, availability.

The standardisation of cybersecurity in ICS networks is not straightforward, as there are several applicable standards and best practice guidelines developed by various organisations that vary in their applicability depending on the sector where the infrastructure to be protected is located, as well as specific standards for industrial control systems. ISO/IEC 62443, which includes the earlier ISA99 standard, is a security standard for industrial automation and control systems. In addition, the National Institute of Standards and Technology (NIST) has a number of Special Publications (SP) on different aspects of SCADA and ICS security. Especially NIST SP 800-82 entitled Guide for the Security of Industrial Control Systems is worth mentioning. However, we can take these standards as best practices to take the first steps towards consciously and continuously protecting our technological infrastructure.

TRENDS

Updates to the ISO 27000 standard

The ISO 27000 standard and its family of standards allows us to know and adopt the best implementation and control practices in terms of Information Security Management Systems. Its evolution over time has been marked by the transformation of technologies and the adaptability of the standard to the sectors where it has been applied.

ISO 27002 - 2022 Update

As we discussed in previous editions, the most recent update was applied to ISO 27002:2022 Information security, cybersecurity, and privacy protection - Information security controls; where new aspects such as threat intelligence, information security for the use of cloud services and data leakage prevention are addressed, enabling organisations to maintain control over security against the various natures of cyber-attacks.

Likewise, the control domains of the 2013 edition were changed from 14 to the following 4 categories: Technological, Organisational, People and Physical. This allows organisations, when adopting the standard, to focus on the context of application of the control in accordance with the new categories and to facilitate the definition of responsibilities for the management of information security, cybersecurity, and privacy protection.

As for Annex A, where we initially had 114 controls, this version consolidates 93: the result of the merger of several controls and the inclusion of controls regarding constant changes in the use of technology and data protection, controls for sensitive data and recognition of the role of technology in business resilience.

ISO 27001- Next update

The update of the ISO27001 standard is expected to be released by the end of 2022 and will be closely aligned with ISO27002, with moderate changes and focused on having a more agile and simplified process in its implementation. Adjusting to a restructuring and reduction of controls. However, organisations, technology and cybersecurity guilds are expectant about the new features that it may introduce.

What can we do?

With the update available, it is recommended that you maintain best practices for information security, cloud security and data security by reviewing your risk assessment, current controls and assessing whether you want to move forward with additional implementations, ensuring alignment with the new guidance. In this way, your organisation will be in a better position to overcome future risks. In addition, as this change provides for a realignment to ISO 27001, you will be preparing your organisation for an update of its certificate.

VULNERABILITIES

Cognex

CVE-2022-38100,-36385,-38069,-38453,-3027-1368,-1522,-1525
Date: 07/09/2022

Description. The affected Cognex product suffers from several critical vulnerabilities. One of these vulnerabilities allows the password of an operator's account to be changed. This is done by monitoring the web socket from an unauthenticated session, from which it is possible to execute different web server commands. In addition, another critical vulnerability allows circumvention of web access controls by attackers modifying password-protected source code.

Link: https://www.cisa.gov/uscert/ics/advisories/icsa-22-249-03
https://www.incibe-cert.es/alerta-temprana/avisos-sci/multiples-vulnerabilidades-producto-cognex

Affected Products. Cognex 3D-A1000 Dimensioning System, firmware version 1.0.3 (3354) and prior versions

Solution: Upgrade to version 1.2 PR26

Contec

CVE-2022-38100;-36385;-38069;-38453;-3027;-38453
Date: 02/09/2022

Description. The vulnerability identified as high risk implies that with access to the network a malicious UDP request can be issued in such a way that the device can crash and thus require a physical reboot. A denial of service can also occur on all CMS8000s connected to the same network.

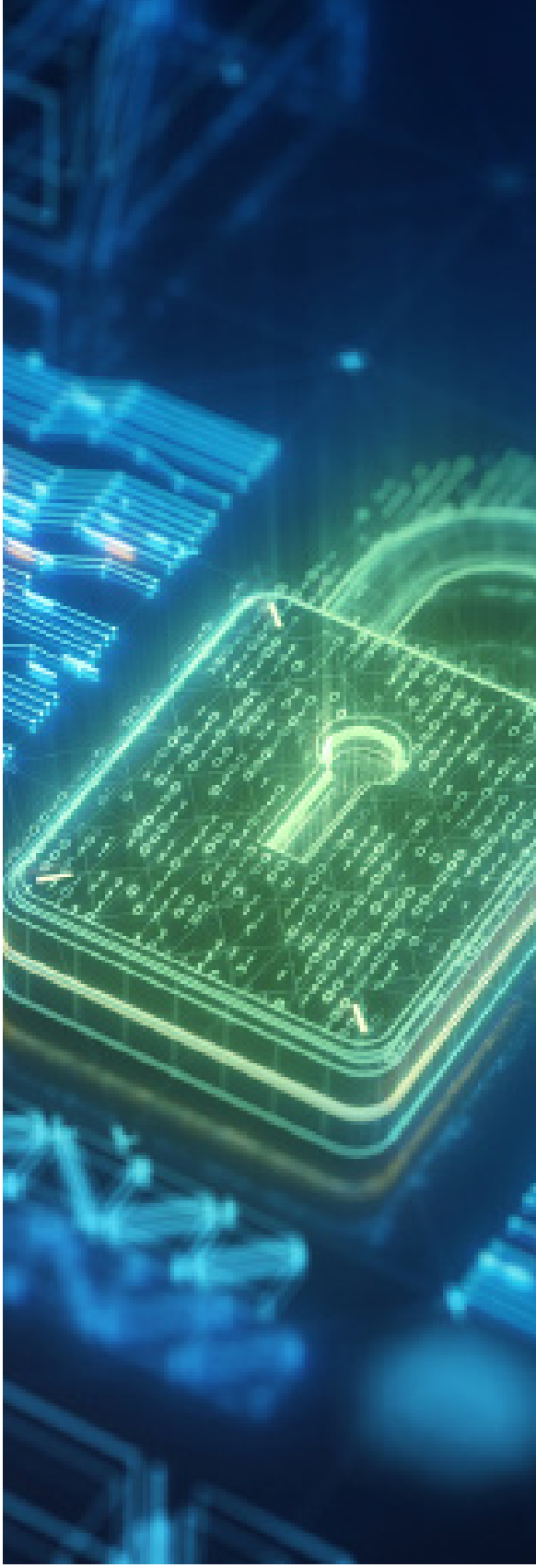
Link: https://www.cisa.gov/uscert/ics/advisories/icsma-22-244-01
https://www.incibe-cert.es/alerta-temprana/avisos-sci/multiples-vulnerabilidades-contec-health-cms8000

Affected Products.
Contec Health CMS8000 CONTEC ICU CCU Vital Signs Patient Monitor

Solution: CISA recommends the following:

- Disable UART functionality at CPU level.
- Enforce one-time authentication of the device before granting access to the terminal/bootloader.
- As far as possible, apply a secure boot.
- Tamper indicators on the device housing to know when a device has been opened.

PATCHES



Hitachi

Date: 07-09-2022

Description. A series of security patches have been released to fix vulnerabilities in multiple Hitachi Energy TXpert Hub CoreTec4 products. Such vulnerabilities could allow an attacker to change an existing user's password and gain access to the system. In addition, the attacker can inject commands into the system and through a vulnerability in the file upload an attacker could gain access to the system. The manufacturer makes a number of additional recommendations:

- Avoid exposing process control systems to the Internet.
- Use firewalls limiting open ports.
- Perform removable storage analysis before connecting them to the systems.

Link: https://www.incibe-cert.es/alerta-temprana/avisos-sci/multiples-vulnerabilidades-hitachi-energy-txpert-hub-coretec-4
https://www.cisa.gov/uscert/ics/advisories/icsa-22-249-04

Affected Products:
TXpert Hub CoreTec 4 versions 2.0.0, 2.0.1, 2.1.1, 2.1.2, 2.1.3, 2.2.0 and 2.2.1.

Solution: Upgrade TXpert Hub CoreTec 4 to version 2.3.0 or higher.

Aveva

Date: 06-09-2022

Description. The AVEVA Software Security Response Centre team reported several vulnerabilities related to insecure deserialisation, and an attacker would be able to execute code by manipulating files in a given project. AVEVA has released the HF 2020.2.00.40 patch that addresses the vulnerabilities detected. In addition to the patch, they recommend the following:

- Include access control lists for projects
- Maintain a chain of custody of project files
- Train users to verify that a project's origin is legitimate

Link:https://www.aveva.com/content/dam/aveva/documents/support/cyber-security-updates/SecurityBulletin_AVEVA-2022-005.pdf
https://www.cisa.gov/uscert/ics/advisories/icsa-22-249-02

Affected Products: AVEVA Edge 2020 R2 SP1 and prior.

Solution:

- Use the HF 2020.2.00.40 patch for AVEVA Edge 2020 R2 SP1.
- For AVEVA Edge 2020 R2, first upgrade to AVEVA Edge 2020 R2 SP1 and then apply the HF 2020.2.00.40 patch.

EVENTS

Identity Week America 2022

4 - 5 october 2022 |

Focusing on identity, this conference covers topics such as secure physical credentials, digital identity, and advanced authentication technologies such as biometrics.

Link: https://www.terrapinn.com/exhibition/identity-week-america/index.stm

(ISC)2 Security Congress

10-12 october 2022 |

The (ISC)2 Security Congress brings together cybersecurity professionals to discuss the latest developments in the cyber domain driven by the mission to promote innovation, leadership, and growth for cybersecurity professionals at every stage of their careers.

Link: https://www.isc2.org/#

IAPP Privacy. Security. Risk. 2022

11 - 14 october 2022 |

This conference focuses on the intersection of privacy and technology with sessions focusing on ad tech, artificial intelligence, and cybersecurity, among others.

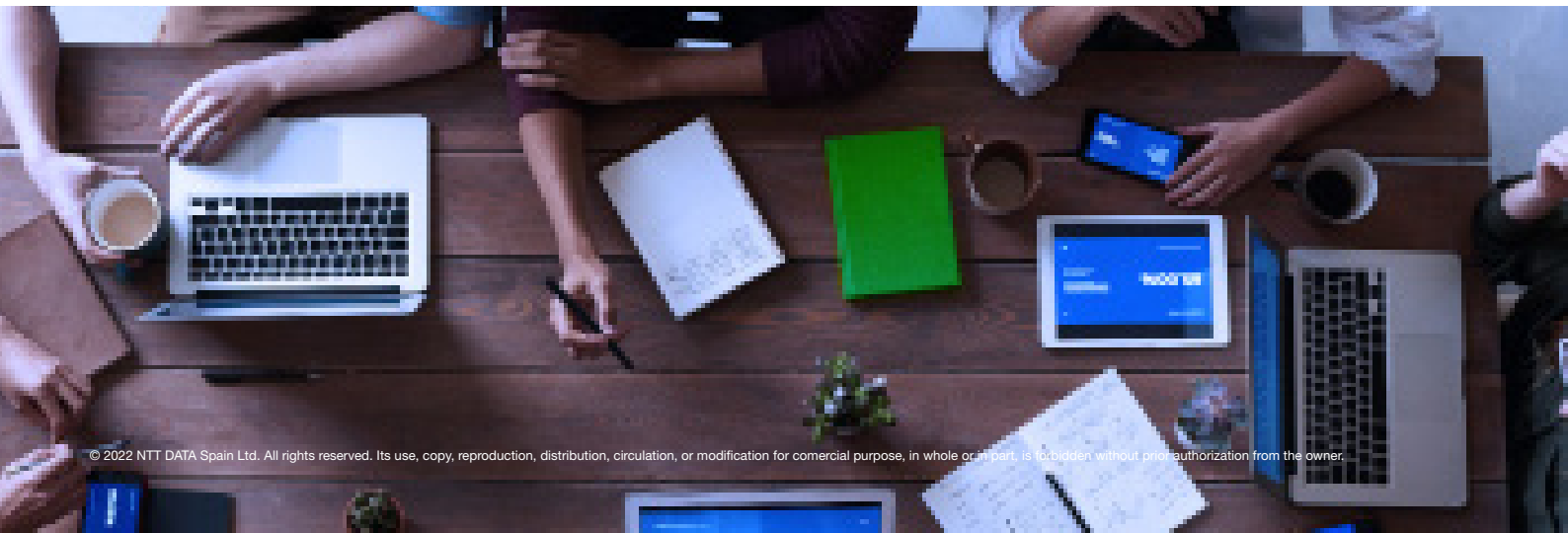
Link: https://iapp.org/conference/iapp-privacy-security-risk/

Hackers to Hackers Conference

22 october 2022 |

It is a conference organised by people working or directly involved in research and development in the field of information security, whose main objective is to enable the dissemination, discussion, and exchange of knowledge on information security among the participants and also among the companies involved in the event.

Link: https://www.h2hc.com.br/h2hc/pt/



RESOURCES

GITHUB

GitHub announces the general availability of the new and improved Projects, developed by GitHub Issues. Since the beta release published last year, the platform has listened to feedback and delivered 15 change logs every two to three weeks.

Link: About Projects - GitHub Docs

CLOUD SECURITY ALLIANCE

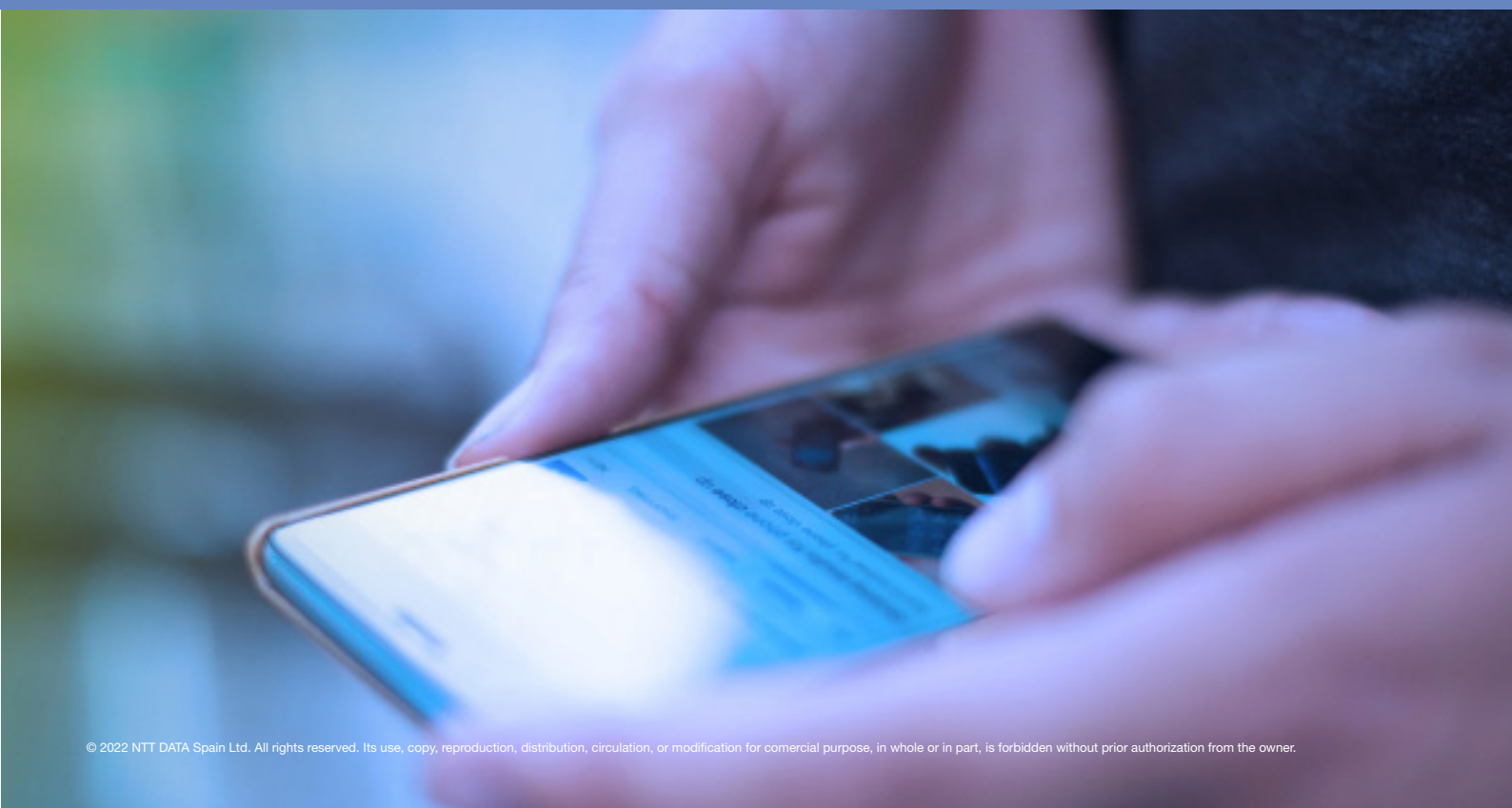
The Cloud Security Alliance (CSA), a non-profit organisation that promotes research into best practices for securing computing and the use of cloud technologies, provides this resource on the top concerns of IT and security professionals in terms of cloud and web threat concerns, strategy, and methods for protecting against cloud and web threats, and current cloud governance strategies.

Link: Cloud and Web Security Challenges in 2022

Security Guidelines for Providing and Consuming APIs

The objective of this document is to provide a framework for securely connecting external entities such as customers or third parties. The document provides a usable list of security considerations in order to estimate the risk involved in specific connectivity (first part of the document) and a technical checklist for the implementation of security controls (second part of the document).

Link: Security Guidelines for Providing and Consuming APIs - Korean | CSA (cloudsecurityalliance.org)




NTT DATA
Trusted Global Innovator
powered by the
cybersecurity NTT DATA team
nttdata.com