My answers to all the collaborative discussions

Collaborative discussion 1

Based on your reading of the case study (Kovaitė and Stankevičienė, 2019) answer the following questions in the discussion forum:

- *What do the authors mean by the term 'Industry 4.0' - give two examples.*
- *Give two real-world examples of risks that fit into the authors categories.*
- *Find another journal article that either supports or contradicts the points made in the cited study.*

<u>Peer 1 answer to the question</u>

> Industry 4.0 refers to the fourth industrial revolution, which combines machines, people, and physical assets into an integrated digital ecosystem that creates, analyses, and transmits data without human interaction, and occasionally takes action based on that data. It places a strong emphasis on connection, automation, machine learning, and real-time data. The Industrial Internet of Things (IIoT) and smart manufacturing are components of Industry 4.0. It integrates physical production and operations with intelligent digital technology, machine learning, and big data to build more linked systems for manufacturing and supply chain management-focused businesses.
>
> Industry 4.0 is anticipated to change the industrial world, much as steam power did in the 1800s. The number of networked devices in use today is a chance to gather data and enable enhanced management and technological decision-making, which will significantly enhance output. Industry 4.0 facilitates the actionability of data. If used correctly, the availability of information across a system or systems may become a potent weapon.
>
> Four Key Areas of Industry 4.0
>
> - Cyber-Physical Systems (CPS) and Cobots
> - Internet of Things (IoT) and Big Data
> - Cloud Manufacturing (CMfg)
> - Automation
>
> Communications and cybersecurity cannot be seen as separate processes with Industry 4.0. To fully benefit from the possibilities that Industry 4.0 presents, firms of all sizes will need to comprehend its capabilities and possible dangers.
>
> The risks that industry 4.0 would face would be those directly of the IT infrastructure and more. Notable attacks would be attacks on Web & Application, Network & Infrastructure, and direct threat to internet connected devices (IIoT)

My answer to peer 1

I think you are highlighting a crucial aspect of industry 4.0, as data becomes the new gold. As for example, I bought a new phone and there were features like ‘personalized service’ and ‘Android System Intelligence’ which are designed to provide services better tailored to the customers’ preferences. These settings are a double edge sword; as a customer, I like to have tailored settings that are relevant to me and takes away the unnecessary ‘noise’. However, I also profoundly dislike that my data are collected, which are in turn used to refine my preferences and others’ preferences. The price to pay for convenience is our data that are been collected and as you mentioned Yash, it can become a potent weapon.

Peer 2 answer to the question

What is Industry 4.0?

Industry 4.0 (I4.0) is a new phase in the industrial revolution that introduce intelligent networking of machines and processes for industry with the help of information, communication and networking technology. "In the new world, it is not the big fish which eats the small fish, it's the fast fish which eats the slow fish" (Klaus Martin Schwab, 2020)

I4.0 Digitalization Risks in Supply Chain and Logistics:

As per (Kersten, Blecker, Ringle, 2017) HICL submission research paper, analyzes the current literature on risk management in European seaports and digitalization in Supply Chain Management and Logistics. They have detailed about the risk factors, types of risk assessments in supply chain management and sea logistics during digitalisation I4.0. They tailored to quantitative and qualitative risk assessment and risk management methods that could be used by the various stakeholders in the different operations and sources of risk at seaports. This is one of the best real time example for this discussion.

I4.0 Digitalization Risks in HealthCare:

The I4.0 Revolution is advancing healthcare to unprecedented comfort levels. Telemedicine is a rather modern trend that became especially popular during the COVID-19 pandemic. Technologically, this kind of telecommunication provided the direct transmission of medical information in various formats. Healthcare is a prime target for cyberattacks. With progress in big data, IOT and its advancement into medical innovation, there are potential risks to patient data privacy. As per (Popov, Elena, Kudryavtseva, Andrei Shishkin, Stepanov, and Saurav 2022) "Industry 4.0 and Digitalization in Healthcare" research paper they have detailed about the risks involved during healthcare digitalization and its mitigations.

My answer to peer 2

Very informative the part on digitalization risks in supply chain and logistics in the seaports sector! For the part on digitalization risks in healthcare industry, Karatas et al. (2022) highlights issues in Big Data for Healthcare industry 4.0. The article collects and discusses multiple published papers on the Healthcare sector and Big Data linked to it in the private and public sectors. As mentioned before, patients' data privacy has become a vector for risk management in Health care sector. The article discusses developing a healthcare system framework which incorporate cloud-based Big Data-driven Industry 4.0 concepts. The system is divided in three layers: data acquisition, cloud Big Data analytics and application layer. The second layer tends to mitigate the leak of clients' data by compressing, storing, and formatting. Moreover, the Dutch national Digital Society Research Programme had organized a conference to help researchers, health care providers, and eHealth developers on how to handle privacy and legal matters in eHealth (Zegers et al. 2021) because data privacy presents a massive risk in the industry 4.0.

Reference:
Karates et al. (2022). Big Data for Healthcare Industry 4.0: Applications, challenges and future perspectives. Available from https://www-sciencedirect-com.uniessexlib.idm.oclc.org/science/article/pii/S0957417422003499 [Accessed on September 5th 2022].

Zegers et al. (2021). Mind Your Data: Privacy and Legal Matters in eHealth. Available from: https://formative.jmir.org/2021/3/e17456 [Accessed on 5th September 2022]

Peer 3 answer to the question

According to (Kovaite & Stankeviciene, 2019), Industry 4.0 has greatly influenced digitization thus rapidly changing people’s behaviour and companies.

They further explain how the use of computers and internet was introduced in 3rd Industrial Revolution and the 4th Industrial Revolution picked up from there by including technological drivers like: Internet of Things (IoT), Cloud Computing, Big Data, Cloud computing, Artificial Intelligence, Robotics and exploration of decentralized communication between people and machines.

A few examples of 4.0 Industries as from (Anon, N.D.) include: Mechanica AI that that provides production-grade AI for industrial operations, ULS Robotics that develops an exoskeleton technology platform that reduces physical strains from a working wearer.

(Kovaite & Stankeviciene, 2019) goes on to state the risks that tend to rise from Industry 4.0, that include:

> - Behavioural risks, that is whether it is from within or outside the organisation, for example end-users require cybersecurity training so as to minimise and combat cyber-threats that are to be faced.
> - Competence risks, lack of professionals who can adopt to the new technologies like cloud computing.
> - Financial risks, the cost to be covered on the adaptation of new technologies.
> - Data security risks, how safe will the data be from data losses, data errors, etc.
> - Technical risks, implementation and adaptation of new technologies.
>
> (Rajnai & Kocsis, 2017) points out how in the future (beyond 2030), highly educated workers with the knowledge of the newest technologies, and up-to-date digital skills will be needed.

<u>My answer to peer 3</u>

I like the last point you made about skilled workers and their importance in mastering new technologies in the years to come. Moreover, the enormous need in the future for companies to have those workers can be felt right now.

Even though, human is the only reason for technological incidents/failure, as human error or hackers or misconfiguration...., companies have a massive role to play in managing risks in their entities. A company can have the most educated worker and still face risks,
* as there is a need for the company to do a screening of the worker to make sure
1- the worker is not a hacker or industrial spy
2- the worker has the right skilled for the position and the environment it will be in contact with
* as on-proper boarding can lead to incidents
* as a on-trained employees can become a liability for a company
* as a company has the moral duty to implement and maintain policies and procedures to mitigate risks
(Chapple et al., 2021)
I hear often the rhetoric about the companies focusing mostly on recruiting the best and sharpest IT workers, to the detriment of putting enough efforts in the development risk management within the organisation.

Reference:

Chapple et al. (2021). (ISC)2 CISSP Certified Information Systems Security Professional Official Study Guide, 9th Edition, 1248 pages.

Collaborative discussion 2

Read Spring et al (2021) and then answer the following questions:

1. *What characteristics of CVSS do the authors criticise? Do you agree with the critique? Justify your answer with academic references.*
2. *The authors also discuss a number of alternatives to CVSS. Select one of these alternatives and post an argument for why it should replace CVSS.*

Peer 1 answer to the question

> The Common Vulnerability Scoring System (CVSS) is a framework which provides a data points for cybersecurity and stakeholders (Dashchenko, N.D)
>
> While the Common Vulnerability Scoring System (CVSS) was developed to quantify the technical impact of a vulnerability, it is commonly misapplied to rank vulnerabilities and assign risk ratings. The scoring algorithm lacks the justification and openness necessary for the community to understand its function. (Shick, 2018)
>
> The CVSS score helps describe how severe an issue is and gives an idea of how quickly an application or organization that is affected by the issue should react to it. The CVSS scores have been used by many companies to determine which security holes need to be addressed first. (Robinson, 2019)
>
> Spring et al. offer a few additional recommendations, including one called the Stakeholder-Specific Vulnerability Categorization (SSVC). While I support a new system, While I support a new system, I am skeptical of its widespread adoption, given the popularity and mass acceptance of CVSS. SSVC address some of the problems with CVSS and authors suggests others to test and improve the methods.
>
> However, the current problem with SSVC is that the proposal could cause stakeholders who depend on each other to have different priorities. Different stakeholders can come to very different conclusions because they each use different factors and decision trees. (Akbar, 2020)

My answer to peer 1

I enjoyed reading your post. I like your summary about CVSS, but mostly your point of view about SSVC. I think you highlighted a very important point by addressing the issue of considering so many points of view from different stakeholders. So what is your answer to the original question: what do you propose for alternative to CVSS?

Peer 2 answer to the question

> Spring et al (2021) highlight a number of inconsistencies with respect to the CVSS scoring. In their view the CVSS formula is not properly justified and its robustness is not documented. Some methodological questions also arise as equations seem to be derived from methods of uncertain validity such as parametric regression, which may or may not be valid in the context of CVSS. Besides the methodological uncertainties highlighted there seems to be also a lack of clarity regarding the initial ranking of vulnerabilities which unavoidably affects the resulting equation for assigning CVSS scores.
>
> Wortman and Chandy counter argue that Spring et al does not examine the effect of CVSS scores on actual risk assessment, but only on the correctness of their application to vulnerability management (Wortman and Chandy, 2022). Despite any weaknesses identified the framework still forms the basis for assessments in IT and vulnerability management often supplemented by additional metrics. Applicability also varies by area of application. For example, Lorenzo et al (2021) have highlighted how CVSS lacks the necessary elements to be applied to industrial environments and IoT.
>
> Spring et al make a few alternative suggestions such as the Stakeholder-Specific Vulnerability Categorisation (SSVC). Personally whereas I embrace a new system I am also pessimistic on its widespread adoption considering the popularity of CVSS and its widespread adoption.

My answer to peer 2

I love that you are realistic about the wilde adoption of CVSS and know that even if SSVC seems like a great alternative it does not have the same embrace in the practice. So maybe the alternative to CVSS is not SSVC, but more like plugs-in to CVSS.

Look at: Kioskli, K., & Polemi, N. (2022). Estimating Attackers’ Profiles Results in More Realistic Vulnerability Severity Scores for example.