ZDMP Blog

Why Cybersecurity Risk Assessment Matters in Industry 4.0

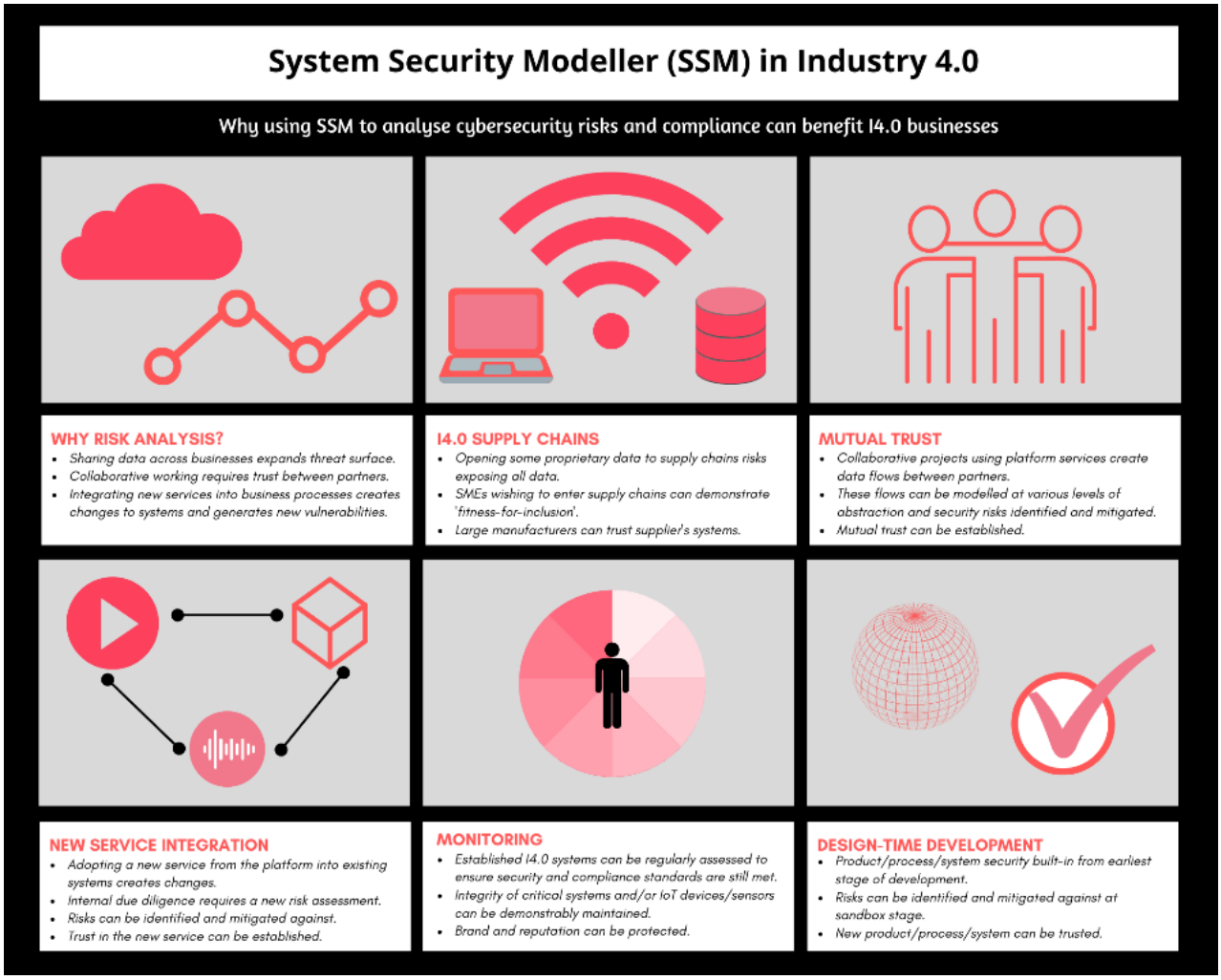
By Nic Fair, Knowledge Engineer & Juri Papay, Senior Enterprise Fellow, IT Innovation, University of Southampton

Some questions for you

- Do you share any type of proprietary, sensitive or process data with any of your suppliers or other third parties in any way? (or do they share data with you?)
- Do you ever integrate new services into your existing IT systems and/or production processes?
- When was the last time you undertook due diligence by conducting a cybersecurity and GDPR compliance risk analysis?
- Do you consider the risks to your business from cyber-attacks or IT system misbehaviours?

The impact of cyber attacks

The insurers Hiscox spoke to 5,400 small, medium and large businesses in the UK, Germany, the US, Belgium, France, the Netherlands and Spain [1]. They found that the number of cyberattacks rose significantly in 2019, with 60% of businesses reporting one or more attack in 2019 (up from 45% in 2018). Official UK government statistics from the National Cyber Security Council (2019) [2] indicate that 31% of UK small businesses identified a cyber breach or attack last year (mainly phishing emails, impersonations and malware). The impact of these attacks included lost files, lost network access, websites taken down and software systems corrupted or damaged – at an average financial cost of £3,650 p.a. to fix [2]. Therefore, as suggested in a Deloitte's Insights article "*organizations should perform risk assessments across their environment, including enterprise, Digital Supply Networks, industrial control systems, and connected products, and use those assessments to determine or update their cyber risk strategies*" [3].



Data is everything

In an Industry 4.0 manufacturing environment, typified by large quantities of proprietary data moving rapidly between and within businesses, effective cybersecurity has become central – because where there are data flows there is security risks. Whether it is a SmartFactory scenario, featuring highly distributed data processing architectures; or a SmartProduct process, using advanced AI and analytics for closed-loop interactions at all stages of a product lifecycle; or a Smart Supply Chain environment, with data shared up and down the chain; data sovereignty, data security and data integrity matter [4].

Trust as result of risk assessment

For example, in the Smart Supply Chain scenario, large manufacturers want the confidence to enter into dynamic, ad-hoc collaborations with a range of SME suppliers, and SMEs want to prove they are cybersecure to large manufacturers in order to enter into the supply chain.

Yet, becoming cybersecure is often seen as a complex and expensive process for SMEs, many of whom may lack the expertise in-house to conduct extensive risk assessments. For example, 68% of SMEs have no cybersecurity policies or risk management processes and 70% have not conducted any risk assessment in the past year [2]. This can put them at a competitive disadvantage when compared with large suppliers.

What will ZDMP achieve

The System Security Modeller (SSM) tool, provided as one of the component services available to SMEs, and others, on the ZDMP platform, can help overcome these barriers (see infographic above).

In general terms, using the SSM tool to model and assess your systems can help demonstrate to others that your business is cybersecure and trustworthy. It can also help IT Managers to trust that the integration of new services, such as zApps, into existing systems is secure. Equally, risk assessment can be undertaken mutually, in an end-to-end process, by manufacturer and supplier together. This can develop strong mutual trust in each other's systems and promote positive collaborations. In LoveData Week 2020, in an age where the most valuable part of many businesses is the data it generates, yet I4.0 standards and processes requires the sharing of that data with others, it is vital that all parties can demonstrate their data trustworthiness to others through effective, timely and on-going cyber security risk assessment.

ZDMP Links

• Architecture Component(s)	System Security Modeller
• Work Package	WP6 – ZDMP Platform Building
• Tasks	T6.2 – Secure Business Cloud T6.4 – Platform Integration and Federation

References

[1] BBC News, 23rd April 2019. *'More than half of British firms 'report cyber-attacks in 2019'* [Available on: https://www.bbc.co.uk/news/business-48017943]

[2] UK Government Official Statistics, 2019, *Cyber Security Breaches Survey 2019: Micro/Small Business findings'*. National Cyber Security Council. [available on: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/791943/CSBS_2019_Infographics_-_Micro_and_Small_Businesses.pdf]

[3] Waslo et. al., 2017. *Industry 4.0 and cybersecurity: Managing risk in an age of connected production.* Deloitte Insights Article. [Accessed on https://www2.deloitte.com/us/en/insights/focus/industry-4-0/cybersecurity-managing-risk-in-age-of-connected-production.html]

[4] Big Data Value Association, 2020. *Big Data Challenges and AI in Smart Manufacturing* [in publication]