The Software Supply Chain Business Case

Duncan K. Sparrell
sFractal Consulting
Oakton, VA, USA
duncan@sFractal.com

15-minute Presentation

***Abstract*—Building trust in critical digital systems costs money. Or does it save money? The definition of a business case is "a justification for a proposed project or undertaking on the basis of its expected commercial benefit". This presentation will help the audience understand, and quantify, the commercial benefits of understanding your software supply chain, as well as the work, the tools, and the costs necessary to do so. The author will begin by describing the threats to critical systems and the risks of not addressing them – including how to quantify those risks for your particular business. Use cases will be reviewed, building on the work in the National Telecommunications and Information Administration (NTIA) and Cybersecurity and Infrastructure Security Agency (CISA) working groups. Example use cases will be shown from vulnerability management, licensing, regulatory compliance, and end of life; including how to leverage across all these use cases to build your business case; and how to craft the business case in terms a Board would understand and relate with. Work in various standards development organizations (SDO's) will be reviewed, including reviewing the alphabet soup of acronyms in this space as well as various recent events such as SBOMarama and the Cybersecurity Automation Village. But understanding our supply does take investment in both staff and money. Various costs will be reviewed that must be taken into account, and tradeoffs among alternatives. The presentation will conclude by summarizing the elements to your business case for establishing the right level of investment to establish the right level of trust for your particular business.**

Keywords—Software Transparency, Software Bill of Materials, Supply Chain Risk, Business Case

About the author

Duncan's mission is to make the world a safer place. He has 45+ years of expertise in software and has been involved in cybersecurity since 1990, including building the first Security Operations Center and coining the term "SOC". After retiring as AT&T's Chief Security Architect, Duncan volunteers most of his time to cybersecurity standards including cochairing the Open Cybersecurity Alliance Cybersecurity Automation Sub-Project. He has been advocating software bill of materials (SBOM) literally for decades. Duncan was awarded the Intelligence Community Seal Medallion, the AT&T Science and Technology Medal, the OASIS Distinguished Contributor Award, and 18 patents. Duncan's tagline is "Think evilly, act ethically". For more info about Duncan, see https://www.linkedin.com/in/sfractal/