Information Security from an Enterprise Perspective - Abstract of presentation

Lars Magnusson
Faculty of Technology, Department of Informatics
Linnaeus University, Sweden
lars.magnusson@lnu.se

Since 2010, the world has seen a strong increase in containment failures or thefts of personal data. From 2014 and onwards around one billion records have been reported stolen or otherwise disclosed to outsiders for criminal or impersonation usage. Not all publicized cases have presented a public root cause analysis, but many have presented such analyses to allow formulating a reasonable failure trending. Though a fair amount of the cases has been related to technological deficiencies, the primary root cause in the presented cases has been sub-standard ICT management and haphazard management procedures. The technology flaws have simply been the vehicle to give the perpetrators a, for the situation, maximized penetration. In most cases, fraudulent access could have been totally avoided if the victimized organization have had a governance model with an understanding of the complexity of its ICT landscape.

Also, among others, and prior to the event of the General Data Protection Regulation (GDPR), accountability for the leadership was nil, while today it often is a CEO work history termination. Losing thousands of personal data records is no longer acceptable in western world organizations, leading to a new paradigm for information management, accountability. But still, there is an urgent need for a new ICT governance perspective, and new management models; moving from systems management to information management. A need for more systemic models, illustrating standardized work, process maps, and information flows, aligning with a modern fractal organizational structure. Therefore, this writer is building on Stafford Beer's Viable System Model and the emerging Information Logistics Model, as a baseline for standardized work and processes. Models that enables mapping of modern enterprise system complexity and information flow logistics. But, it also provides tools for auditing and, thus, enable increasing information protection compared to today's organizational requirements in search of fulfilling legal demands like GDPR and CCPA (California Consumer Privacy Act.

We need to use overall enterprise processes, like the Viable System Model and Information Logistics, if to survive the emerging wave of sensors and Internet of Thing data flows. ITIL, Cobit, and other older single system focused management models need to give away to large-scale, enterprise convoluted system thinking.

Keywords: System thinking, enterprise, governance, management, information logistics, GDPR