O mundo da segurança de informação vem passando por transformações profundas. A cada dia surgem novas tecnologias que impactam diretamente os pilares fundamentais da área. Exemplos de invasão de sistemas e difusão de dados pessoais de usuários e empresas inundam as manchetes dos meios especializados. A discussão vem se tornando cada vez mais séria, devido ao processo de automatização em que se encontram veículos e aeronaves. Há alguns meses, um especialista em segurança anunciou na Internet que havia conseguido invadir o sistema de controle de um avião a partir do seu sistema de entretenimento. A notícia causou forte impacto. Ora, se um hacker consegue dominar um avião em pleno voo, quais as consequências que isso poderia gerar em larga escala? Outro exemplo aconteceu em meados de 2015, quando dois pesquisadores de segurança da informação e também especialistas em sistemas embarcados conseguiram invadir e controlar o computador de bordo de um veículo durante sua passagem por um trecho de rodovia. Durante o teste, os especialistas fizeram o carro frear sozinho e afirmaram, ainda, que o exemplo não se restringia a usar os freios. Eles poderiam enviar qualquer comando ao carro, desde acelerar, desligar o motor, mudar a direção do veículo e até mesmo causar uma forte colisão, se assim desejassem. Isso evidencia que um especialista motivado e financiado pode causar estragos a outros, de acordo com sua vontade. Outro exemplo mais recente está no uso de ransomware. A ideia é sequestrar dados e solicitar pagamento para liberação. O sequestro se dá por meio da encriptação dos dados com algoritmos simétricos e assimétricos, dependendo do caso. O fato é que existem informações divulgadas em meios especializados de que empresas já foram vítimas de ransomware e de que elas pagaram a hackers para ter seus dados de volta. A tendência, em curto prazo, é só piorar, pois a segurança da informação não é assunto que faz parte do dia a dia dos usuários comuns de sistemas computacionais.