# KARL'S SECURITY REVIEW

Send Email

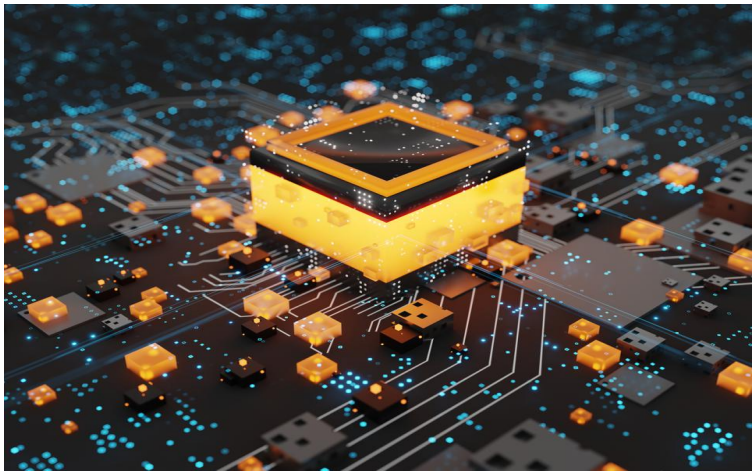
## Hi, I'm Karl! Blog Posts

Welcome, and thank you for taking the time to visit my page. I am a Cybersecurity Professional that is seeking to learn, grow, and master my craft.

# Who should have the final say on product security decisions, the business or the security department?

## security, decision, business

Some of the goals of a business are to increase profit, decrease production costs, improve customer relations, and grow. There are may opportunities that will present themselves to achieve these goals, but will also introduce more security risk. The potential risks grow exponentially with the introduction of information technology. According to a financesonline.com report "the cost of cybercrime around the globe is in the billions of dollars." Cybercrime is on the rise and is expected to more than double by 2025. According to Omer Rana's article, "10 Concerning Cybercrime Statistics For 2022", "Global security spending is expected to hit $133.7 Billion is 2022; and ransomware attacks are increasing by more than 350% each year." This has made Cybersecurity essential to the survival of business. However, security is only a factor in the ultimate goal of a business. It is the responsibility of the business owners and excecutives to collect all the factors, assume the risks, and make the make the final say in product security decisions.
**https://financesonline.com/cybercrime-statistics/**
**https://www.linkedin.com/pulse/10-concerning-cybercrime-statistics-2022-omer-rana/**



# How could quantum computing affect cybersecurity?

## quantum computing, cybersecurity

Quantum computing is the development of computer-based technologies centered around the principles of quantum theory. Quantum theory explains the nature and behavior of energy and matter on the quantum level. Unlike our current day computers, quantum computers can perform tasks using a combination of 0's and 1's simultaneously, thus giving it much more powerful processing speed and power. Quantum computing will unlock many cutting-edge possibilities in the future of medical research, artificial intelligence, weather forecasting, etc. The promise of these great breakthroughs will come with a significant risk to cybersecurity. Our modern cryptography will be easily broken by the potential computing power that quantum computers possess. There currently is not a quantum computer that has that kind of power yet, but it is imminent. The National Academies of Sciences, Engineering, and Medicine stated in a 2018 report that there are still more significant technical advances that are required before they will be able to break strong codes. The future code-breaking quantum computers will need 100,000 times more processing power and an error rate 100 times better than today's best quantum computers have achieved. There is no timeline as to when this will happen, and it probably will not happen within a decade. Researchers have been working the last several years to develop "quantum-safe" encryption, such as "post-quantum cryptography (PQC) and "Quantum key distribution" (QKD). The future of Quantum computing will have a profound effect on cybersecurity with our current forms of encryption. The best way that is known to mitigate the threat is to change how we secure our data and start now.

**https://www.americanscientist.org/article/is-quantum-computing-a-cybersecurity-threat**
**https://www.techtarget.com/whatis/definition/quantum-computing**
**https://quantumxc.com/blog/quantum-computing-impact-on-cybersecurity/#:~:text=The%20Quantum%20Threat%20to%20Cybersecurity,data%20and%20the%20Internet's%20infrastructure.**