Will encryption fail when quantum computers are viable?

Every time the topic of cyber-security is discussed, the mischievous 13-year-old inside of me immediately starts thinking about how to disrupt or disable that security protection. Maybe I watched too many cartoons as a kid, but I always wonder what tools a movie's evil genius would employ to crack into the hero's base and cause havoc? In the case of modern encryption, the best possible tool of destruction seems to be a powerful quantum computer. Once a thing of comic books and science fiction, quantum computing is right around the corner. In fact, it is a top priority of cyber security experts (and, let's be honest, spies) in the National Security Agency. “According to documents provided by former NSA contractor Edward Snowden, the effort to build 'a cryptologically useful quantum computer' – a machine exponentially faster than classical computers' (Rich) is part of a $79.7 million research program led by the agency. The goal: to design a machine with the capability to break virtually any code in the world and protect U.S. security interests.

In Matt Hottell's lecture on cyber-security, the class was introduced to the three principles that form the foundation of information security: Confidentiality, Data Integrity, and System Availability (Hottell). More importantly, we saw through specific examples, how closely these principles are tied together. It is extremely likely that if safeguards on one fail, all three eventually fail. Cryptography is the key to keeping our
data safe and our own. Currently, we have every reason in the world to feel secure. Assuming proper password protocols, standard computers would take about 10.79 quintillion years to break the billions of possible keys in a normal 128-bit AES cipher (Wood). What happens when computers are fast enough to handle that code-breaking task in a manner of months, or weeks? This topic is explored in an article by Sophie Curtis for the UK's Telegraph. Curtis begins by explaining the difference between standard computers and quantum computers. Standard computers require data to be encoded into bits, either a one or a zero, while quantum computers use qubits, which represent both zero and one values. “If these qubits are placed in an ‘entangled’ state—physically separated but acting as thought they are connected—they can represent a vast number of values simultaneously” (Curtis). This structure removes the limitations of standard computers, allowing them to solve mathematical problems in a fraction of the time. Curtis quotes security expert Brian Snow as describing quantum computers as a ‘wonderful gift for the scientific community’ but clarifying that ‘they also pose a ‘monstrous threat to the security functions running on the World Wide Web’ (Curtis). At the point when a practical quantum computer exists, Snow feels vulnerabilities in the control engines that transfer data across national borders will make financial transactions impossible to keep safe. Beyond banking, a massive attack to electrical power infrastructure could bring down the entire World Wide Web and even cause thousands of deaths.

The good news for governments, Internet shoppers, and super heroes (especially those with super-secret hide-outs), is that much of what can be done with quantum computers is still theoretical. The odds are very likely that what has been true with
traditional computers will remain true; as processing power increases, so will security measures to keep to every one's data safe. It is impossible to say where computing and data security will stand in the decades it will take for quantum computers to become mainstream tools; however, we can be assured the entire landscape of information technology will be completely transformed.

