Microprocessor-based relays protecting against fault current have revolutionized power automation industry. The leverage using commercially available information communication technologies has been the currency for future cyberinfrastructure deployment, which enables plausible electronic manipulation that can affect system operation. The bus differential protection has been recognized as one of the most critical protection schemes, if compromised, that would disconnect a large number of components within a substation. A hypothesized substation outage is the worst case scenario of intrusion attack events. This paper proposes an impact analysis of critical cyber assets in substations that capture historical load and topology conditions. This is to identify critical substations and other “nightmare” hypothesized combinations for security protection planning. The proposed metrics of attack scenarios incorporate electronic instrumentation in relation to the physical system for impact and dependency evaluation. Combinatorial verification of these hypothesized events based on the proposed reverse pyramid model (RPM) is validated using IEEE 30- and 118-bus systems.