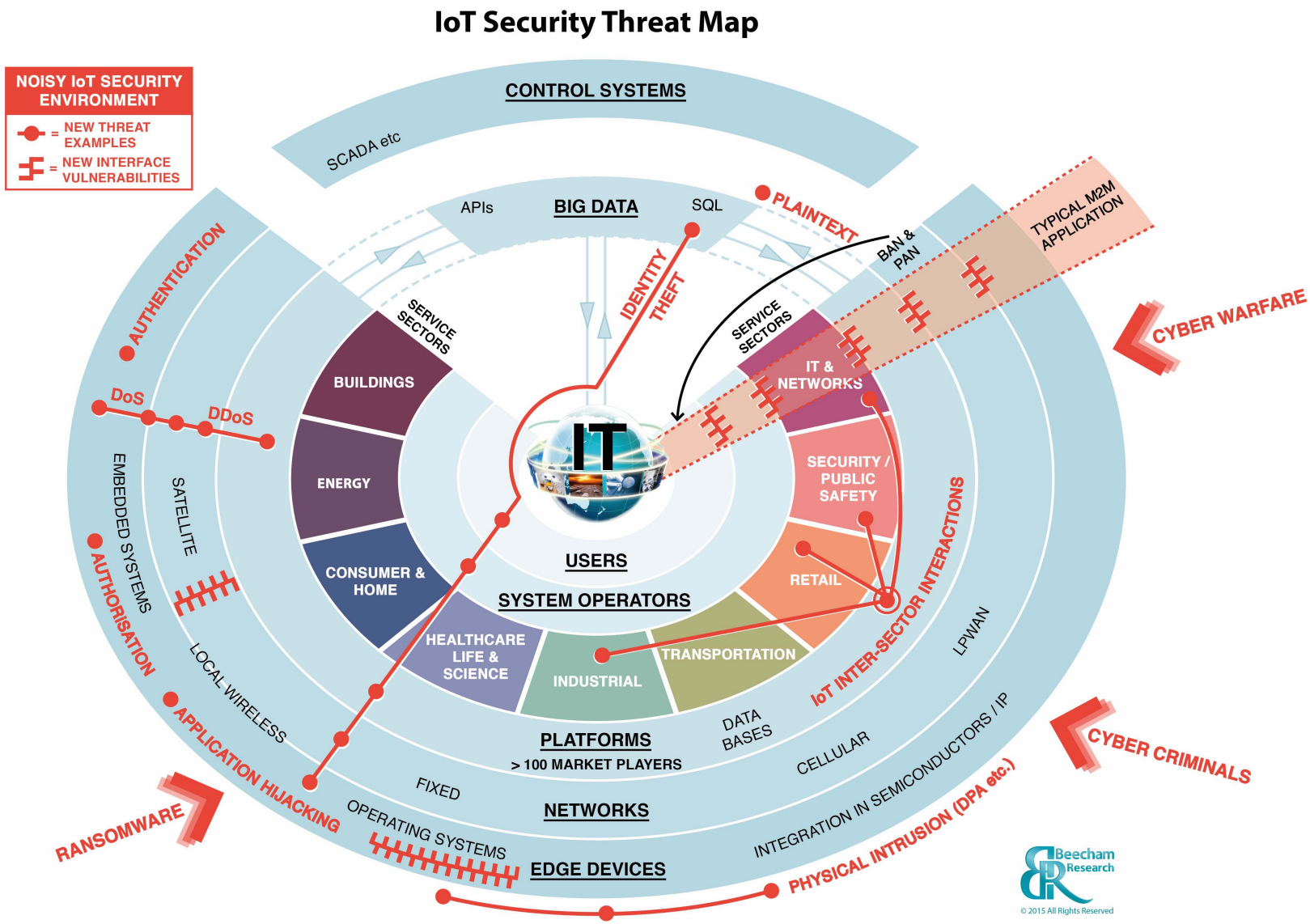
IoT Security Threat Map

A new view of attacks and essential defences

Beecham's new IoT Security Threat Map



Beecham's new IoT Security Threat Map

Our new IoT Security Threat Map provides an overlayed summary of the full set of threat and vulnerability analyses that Beecham uses to help clients shape their strategies. This complex Threat Map "summary" features many of the top 5 features from each of those analyses.

One analysis focuses on external threats that are increasing and have the potential to become most problematic for IoT solutions including cyber warfare, cyber criminality, the use of ransomware, identity theft and physical intrusion attacks on edge devices.

Top internal vulnerabilities of IoT applications are analysed and include: The potential for applications inside edge devices to be hijacked; increasing accessibility through communications enabling Denial of Service attacks; The current necessity for searchable databases in the new Big Data arena to be stored in unprotected Plaintext; The complexities of IoT systems targetting multiple sector verticals; and The proliferation of internal interfaces and their introduction of weaknesses in advanced IoT solutions.

The other areas of threat and vulnerability analysis featured that are major factors in the risks for IoT systems include: Needs for robust authentication, authorisation & confidentiality; The features and interactions between multiple networks used together in IoT; The complexities of combining Service Sector optimised capabilities of differing Service Enablement Platforms; and The implementation and defences of edge device operating systems, chip integration and the associated Root of Trust.

Beecham's new IoT Security Threat Map

- The move towards IoT from simpler M2M scenarios increases the Threats

- There were few threats aimed at, or that "can compromise", M2M solutions
- - M2M solutions are usually a slice through a vertical / sector
- - Limited appeal or monetary gain as a target
- - Clearly controllable solutions with well understood interfaces
- - Made secure by M2M security experts when key Elements of Security are used with care

- IoT solutions are aimed at wider applications
- - Connecting many users and target sectors
- - Providing access to higher value combinations of information & control
- - Promising greater value & impact to users, operators and **attackers**

- M2M built correctly requires right-sized security levels, to match the selected vertical and application. Sufficient security but only what is necessary within the delivered-value budget

- IoT solutions also require right-sized and affordable security BUT will encounter complexities of differing value, threats and budgets in the multiple connected verticals, networks, and edge device technologies