UK BUSINESSES AND IT/ CYBERSECURITY SPEND

CYBER FACTS & OBSERVATIONS

This insight comes against a backdrop of increasing engagement from Government on the subject, driven by the NCSC and the DCMS. Earlier this year various focus groups were held to try and get a better understanding from businesses as to where they see the roadblock to be, in their spending and engagement in all things cyber.

The target audience was (non-technical) main board Directors who ultimately have the responsibility and budgets. Around 200 companies were involved across the country.

THEIR TOP FIVE QUESTIONS WERE:

- What should we be spending our money on to make the most difference?
- How do we know that what we are spending our money on adds any value or truly protective benefits?
- How can we manage our IT Teams when we don't really understand what or how they do things? How can we better manage and protect our own responsibilities from a board perspective?
- What technology infrastructure changes can we make operationally, both internally and within our supply chains, that will have the most benefit on our information security and risk posture?
- If we had better guidance, we would definitely spend more money on this, as we would turn it to a competitive advantage. Our reputation is our most valuable asset. How can technology protect that?

> ***"Changes to regulation offer real opportunities too. The NIS Directive that came into effect last year will force the UK's most critical industries to ensure their cybersecurity is adequate or risk hefty fines"***
>
> Jeremy Fleming - Director GCHQ

Businesses need to look at these points carefully and work them into their Cyber Risk & Compliance strategy.

The **Essential 8** solution from Edge IT Group fits squarely within this domain set and could be used as a tool of reference to answer those various questions with the definitive metrics and trust/authority needed. The point being there is no silver bullet, no one size fits all, no one application that will save everything.

Despite cries from the think-tank of the nanny state from some quarters, people are still looking to Government for advice as fundamentally they trust them.

The provenance of **Essential 8** and brand association with Australia / Australian Government, is powerful and compelling.

EDGE IT GROUP LTD

FUTURE THINKING TECHNOLOGY

Huntsman®

Defence-Grade Cyber Security

Huntsman®
Defence-Grade Cyber Security

The Australia initiative has been incredibly successful with international polls suggesting people trust Australian company's brands, culture, global competitiveness and ease of doing business. For the first time Australia has ranked in the Top 10 Soft Power Nation States with the value of its nation brand. This is especially recognised in innovation and technology.

A collective criticism from the panel was that the technology market is full of snake oil salesmen selling variations of vapourware. The panel wanted tools that provided a definitive benchmark and scoring that could be relied upon, that are tamper-proof.

The conversation ultimately turned to Brexit and the 'Brexit Backlash'. This throws up some other useful intelligence, and a clear indication that companies remain open for business and the top three areas of focus for technology spend are:

- Data Loss Prevention
- Endpoint Protection
- Cyber Regulation and Compliance

This was supported by the NCSC who recommend spending a minimum of 2.5% of turnover on IT/Information Security/ Cyber Security with a guideline ideal of circa 4%; whilst the DCMS and Cabinet Office acknowledges that many highly regulated companies spend up to 11% on regulation and compliance.

Importantly the pricing of the **Essential 8** scorecard solution is typically less than an FTE but is on duty 24/7.

Importantly all these cyber solutions ultimately depend on full knowledge of the Network Topology and Inventory, given you can manage what you know, which plays to the functional strengths of the Edge **Black Swan** solution.

"It's about embracing the unexpected and seeing into the future"

On key Security Controls:

"When implemented correctly, we know it makes these companies much harder targets for commodity cyber-attacks"

Jeremy Fleming - Director GCHQ

Cabinet Office

Department for Culture Media & Sport

National Cyber Security Centre

GCHQ

EDGE IT GROUP LTD

FUTURE THINKING TECHNOLOGY

0800 808 5270
https://edge.org.uk
enquiries@edge.org.uk