ESSENTIAL 8
THE CYBER SCORECARD

OBJECTIVES

- ***Essential 8*** *provides businesses with a non-technical oversight of 8 key Cyber KPI's*
- ***Essential 8*** *is a technological 'truth-serum' for what your IT functions or external IT support provider (MSP) should be doing, or claim to be doing*
- ***Essential 8*** *is a Risk audit assessment tool, run monthly, producing a non-technical scorecard analysis*

AN EXECUTIVE PERSPECTIVE

- **Essential 8** is a unique product from Huntsman Security, a world-renowned Cyber Security Analytics solution developer and provider
- Huntsman is an Australian company that evolved through their relationship with the Australian Signals Directorate, the equivalent of the UK's GCHQ
- Huntsman provide Cyber Security Analytics capabilities, globally to the highest levels of Nation State Government and Defence
- **Essential 8** offers military-level Cyber technology solutions at mid-market prices
- This solution has been packaged for ease of deployment, to reduce costs and deliver immediate and accurate visibility.

WHAT DOES ESSENTIAL 8 DO?

- **Essential 8** monitors and reports on your key Cyber Security KPI's, by taking constant readings from multiple technologies already deployed within your IT infrastructure
- Independent research conducted by the ACSC found that 85% of breaches had their root cause in a failure to actively address the key components of **Essential 8**
- Most of the 'news-worthy' Cyber incidents could have been stopped or minimised if the **Essential 8** measures had been in place
- **Essential 8** monitors and reports on, what your Cyber/IT team should be doing, or claims to be doing.

WHY BUSINESSES NEED ESSENTIAL 8?

- Essential 8 gives non-technical Executives the truth, not a technical 'smoke-screen'
- The dashboard will provide a percentage KPI reading against a predetermined matrix
- It will identify problems and provide the necessary indicators to structure remediation plan(s)
- Essential 8 is run monthly to give businesses a rolling & trending view of Cyber Security performance
- This technology will empower businesses to challenge their Security/IT function
- It will seamlessly deliver the intelligence Executives need to make sound decisions about Cyber risk.

EDGE IT GROUP LTD
FUTURE THINKING TECHNOLOGY

Huntsman®
Defence-Grade Cyber Security

WHAT'S THE BENEFIT AND ROI?

BENEFITS

- ***Essential 8*** *delivers clear and objective management metrics on the performance of key controls that mitigate 85% of Cyber Risks*
- *It allows Executives to understand how well they are preventing attacks, how much they can limit the extent of a breach and how easy it would be to recover from a Cyber attack.*

TWO COMPARISONS

01 ESSENTIAL 8 V'S FTE

- Given the importance of the task and the skills required, the remuneration level of a suitable FTE would be circa £60k plus employment costs
- For a large or multi-site enterprise there would be a requirement for 2 or more FTE's.

02 COST OF A BREACH

- Figures for the average costs of a breach vary dramatically and are industry specific, ranging from thousands to many millions; there is no-shortage of news scare-stories
- The anticipated cost of a breach should never be a surprise to a business. The definition of an enterprise's Cyber posture must include a range of potential liability costs and the possibility of those occurring; this will determine the appropriate levels of investment in Cyber
- It is only through knowledge of these Risks that businesses can determine the appropriate level of investment in Cyber Security
- **Essential 8** will be one of the least expensive components in your Cyber posture but probably one of the most effective.

ROI SUMMARY

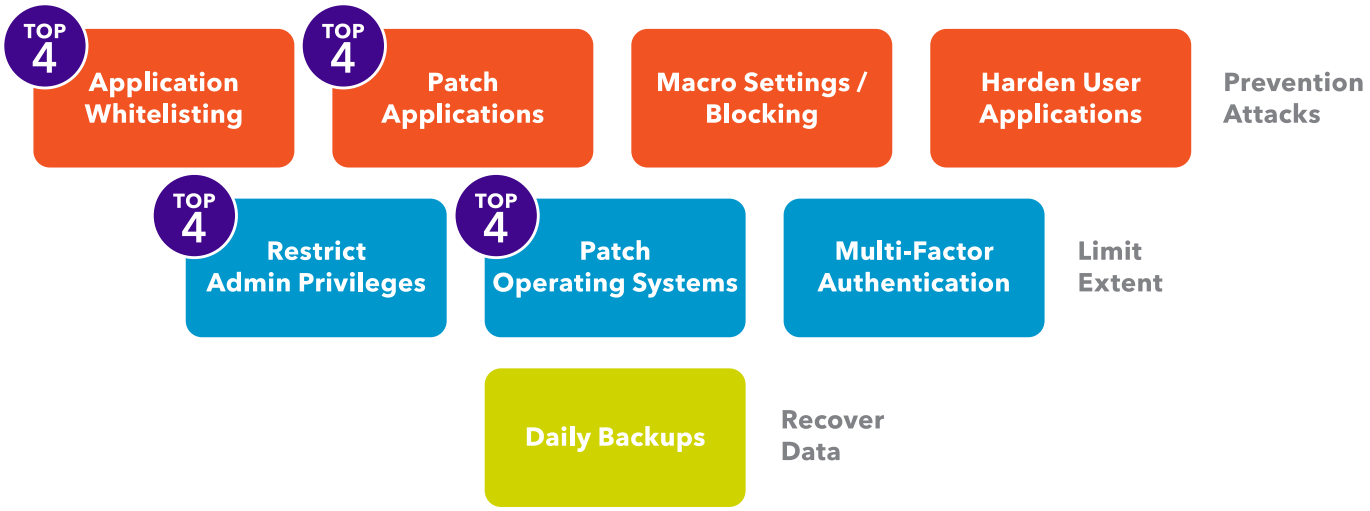
01 TECHNOLOGY V'S FTE

- A FTE would be more expensive and cannot deliver the same level of Cyber Security Analytics KPI integrity and reporting that **Essential 8** will deliver
- Manual, sample-based audits give less clarity for more effort than automated analysis.

02 COST OF A BREACH

- Assuming the threat of a Cyber-attack is accepted and the enterprise wishes to provide a holistic Cyber protection strategy, the cost of **Essential 8** is relatively insignificant in comparisons to the cost of a breach, even a small or contained one.

WHAT ARE THE ESSENTIAL 8?



HOW DO WE PROCEED?

The implementation of **Essential 8** is a three-phase process:

01 ON-BOARDING

- Interviews to review & understand the current high-level Cyber posture
- A high-level review of the current process, procedures and policies
- Understand Infrastructure landscape (by location) including current monitoring tools
- Current Cyber architecture
- If tools are not in place, make recommendations on 'best of breed' toolsets
- Report on findings to Executives', including short-term, quick-win improvements and GRC focused recommendations.

02 ACTIVATION

- Set the **Essential 8** Security KPI's
- Install the platform, linking to current monitoring tools
- Take initial readings to baseline the current position.

03 ON-GOING REPORTING

- Monthly remote monitoring of the integrity of the **Essential 8** implementation
- Establish the reporting regime for Execs and GRC & IT functions if required.

EDGE IT GROUP LTD
FUTURE THINKING TECHNOLOGY

Huntsman®
Defence-Grade Cyber Security

Huntsman®
Defence-Grade Cyber Security

THE CONTROLS IN DETAIL

01 APPLICATION WHITELISTING

- What applications should be on our system?
- Identify unapproved or malicious applications
- Stop the system executing unapproved applications

02 PATCHING APPLICATIONS

- Is the enterprise totally patched up to date?
- Have all patches been installed within 48 hours of receipt to prevent 'zero-day attacks'?

03 DISABLING UNTRUSTED MICROSOFT MACROS?

- Have they been identified and blocked?

04 APPLICATION HARDENING

- Has each and every application been secured to prevent tampering?
- Has the Operating system been properly protected?
- Do you have a successful application of end-point policies?

05 PATCH OPERATING SYSTEMS

- Is the Operating System patched up to date?
- Are you running unsupported Operating System Versions?

06 ADMINISTRATIVE PRIVILEGES

- Are admin privileges for email, web access and restricted software in place?

07 DAILY BACKUP OF DATA

- Are back-ups started and complete?
- Backup failures identified
- Failures identified with 24 hours

08 MULTI-FACTOR AUTHENTICATION (MFA)

- Is MFA in place for all remote access users?

EDGE IT GROUP LTD

FUTURE THINKING TECHNOLOGY

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