Cyber Essentials & DSPT

- Compare
- Contrast
- Compliment

Intro:

- Trevor Bradfield
- Founder/Director of Unity IT Ltd (2004)
- Cyber Essentials Assessor
- Cyber Essentials Certifying Body
- Rugby Referee
- Rubiks Puzzle Champion!


currency XTRA
MUNEMARK
Wine Merchant

Cyber Essentials & DSPT

- Compare
- Contrast
- Compliment

Feature	DSPT	Cyber Essentials
Primary purpose	Demonstrate compliance with data protection & information governance in health/social care	Demonstrate baseline cyber security protection against common threats
Scope	**Broad**: covers digital + paper records, staff behaviour, policies, governance, incident handling	**Narrower**: focuses on technical cyber security controls only
Target audience	UK health & social care organisations (e.g. NHS, care providers)	All organisations across any sector
Key focus areas	Data protection, confidentiality, training, governance, processes, IT security	**5 Controls**: firewalls, secure config, access control, malware protection, patching
Type of assessment	Self-assessment toolkit (no mandatory audit)	Certification (self-assessment + optional independent audit for Plus)

CERTIFICATION BODY CYBER ESSENTIALS

CYBER ESSENTIALS CERTIFIED

National Cyber Security Centre
a part of GCHQ

unity

Feature	DSPT	Cyber Essentials
Mandatory?	Required for NHS and often for social care contracts	No, but often required for government contracts
Sector-specific?	Yes – tailored to care sector requirements	No – generic, not sector-specific
Covers paper records & verbal info?	Yes	No (digital only)
Certification output	“Standards Met” / “Standards Exceeded”	Formal Cyber Essentials certificate
Insurance included?	No (can support claims)	Includes £25k Cyber Insurance
Regulatory recognition	Recognised by NHS, CQC, local authorities	Recognised by UK government (NCSC-backed scheme)
Relationship to each other	Broader framework; can incorporate Cyber Essentials evidence	Can support DSPT; Cyber Essentials Plus can help achieve higher DSPT rating
Cost	Free (government-funded support programme)	Paid certification £320-£600

CERTIFICATION BODY
CYBER ESSENTIALS

5 Controls / Areas

1. Firewalls & Routers
2. Secure Configuration
3. Security Updates
4. Access Control
5. Malware Protection

CYBER ESSENTIALS
CERTIFIED

National Cyber Security Centre
a part of GCHQ

unity

1. Firewalls & Routers

- **Improper configuration** – Leaving default settings or not customizing rules, which can allow unauthorized traffic.
- **Ignoring updates** – Failing to apply firmware updates or patch vulnerabilities.
- **Ports that are open** – Is there a documented business case to have these open?

CERTIFICATION BODY CYBER ESSENTIALS

CYBER ESSENTIALS CERTIFIED

National Cyber Security Centre
a part of GCHQ

unity

2. Secure Configuration

- **Using default passwords** – Not changing factory credentials.
- **When staff leave** – Disabling accounts, revoking access.
- **Disabling AutoRun** – When you plug in a USB drive, DON'T let it auto run.

CERTIFICATION BODY CYBER ESSENTIALS

CYBER ESSENTIALS CERTIFIED

National Cyber Security Centre
a part of GCHQ

unity

A disgruntled ex-employee at a Singaporean IT firm caused carnage after deleting over 180 servers

The staff member was angry about his dismissal and sought to get his own back

A disgruntled ex-employee deleted 180 virtual servers from his company's systems in rage following his dismissal, dealing significant damage to the company.

The company in question, IT firm NCS, suffered damages of $918,000 Singaporean dollars, equivalent to roughly $678,000 US dollars.

The employee, Kandula Nagaraju, has been sentenced to two years and eight months in jail on one count of unauthorized access to computer material, with another charge taken into consideration for sentencing, according to reporting from *CNA*.

Nagaraju reportedly exploited his prior access to NCS' quality assurance system to carry out the breach. Following his dismissal in 2022, he used administrator login credentials to gain unauthorized access to the system from between January and March 2023.

3. Security Updates

- **Delaying updates** – Ignoring update prompts or postponing patches.
- **Using unsupported systems** – Continuing to use software or operating systems that no longer receive security updates.
- **Not automating updates** – Relying on manual updates and missing critical patches.

CERTIFICATION BODY CYBER ESSENTIALS

CYBER ESSENTIALS CERTIFIED

National Cyber Security Centre
a part of GCHQ

unity

CERTIFICATION BODY
CYBER ESSENTIALS

Co-op cyber attack affects customer data, firm admits, after hackers contact BBC

“We’re patching like mad!”

CYBER ESSENTIALS
CERTIFIED

National Cyber Security Centre
a part of GCHQ

unity

4. Access Control

- **User Account Separation** – Have a separate admin account with elevated privileges and a standard account for day to day work.
- **Privilege creep** – Letting users retain access they no longer need.
- **Weak password practices** – Reusing passwords or using easily guessed ones.

CERTIFICATION BODY CYBER ESSENTIALS

CYBER ESSENTIALS CERTIFIED

National Cyber Security Centre
a part of GCHQ

unity

5. Malware Protection

- **Clicking suspicious links or attachments** – Falling for phishing or drive-by download attacks.
- **Disabling antivirus software** – To speed up the computer or run untrusted software.
- **Ignoring alerts** – Overlooking or not reporting malware warnings or unusual system behaviour.

Why become Cyber Essentials Certified?

92%
fewer insurance claims made by orgs with Cyber Essentials controls in place

78%
would recommend certifying to Cyber Essentials to other orgs like theirs

79%
of users believe the scheme has a positive impact on the confidence of their own clients and customers

1.1%
failure rate for Cyber Essentials; dropping for the 4th straight year

69%
of organisations with Cyber Essentials believe that it has increased their market competitiveness

80%
believe being certified can reduce the financial cost to their org of an unsophisticated cyber attack

95%
of customers said they would recertify to Cyber Essentials next year

82%
are confident that the technical controls provide protection against common cyber threats

CERTIFICATION BODY CYBER ESSENTIALS

CYBER ESSENTIALS CERTIFIED

National Cyber Security Centre
a part of GCHQ

unity

DSPT & Cyber Essentials

Key Takeaway

DSPT = governance + people + process + data + tech

Cyber Essentials = technical cyber security fundamentals

CERTIFICATION BODY CYBER ESSENTIALS

CYBER ESSENTIALS CERTIFIED

National Cyber Security Centre
a part of GCHQ

unity

DSPT & Cyber Essentials

How they work together

(They are complementary, not competing!)

Many organisations:

- Use Cyber Essentials for technical controls
- Use DSPT for full compliance (especially in health/social care)

Having Cyber Essentials Plus can:

- Reduce effort in DSPT
- Help achieve a higher DSPT rating (“Standards Exceeded”)

CERTIFICATION BODY CYBER ESSENTIALS

CYBER ESSENTIALS CERTIFIED

National Cyber Security Centre
a part of GCHQ

unity

DSPT & Cyber Essentials

When to use each

Choose **DSPT** if you:

- Work with NHS or social care data
- Need to meet regulatory/data protection obligations

Choose **Cyber Essentials** if you:

- Want a baseline cyber security certification
- Need it for government contracts or assurance

Use **both** if you:

- Are in health/social care AND want strong cyber posture

CERTIFICATION BODY CYBER ESSENTIALS

CYBER ESSENTIALS CERTIFIED

National Cyber Security Centre
a part of GCHQ

unity

Trevor Charles Bradfield

Certified Cyber Security Assessor

Thank you!!!

Any questions?