Trustworthy Computing:
Privacy, Security & Usability

HIPAA – Summit West II

Coordinating Security & Privacy

Richard Purcell

Corporate Privacy Officer

Microsoft Corporation

What is Privacy?

- It’s about me
  - Who I am, where I am, what I do
- It’s about being in control
  - I control who gets access
  - Let me be the judge about use
- It’s about being left alone
  - Don’t bug me
- It’s about respect
  - Like I said, don’t bug me

What is the Value of My Information?

- For me:
  - Defines WHO I am as an individual
  - Defines WHAT I do and WANT
  - Defines WHERE I am and WHEN
- For others:
  - In emergencies, it’s critical
  - In communities, it’s important
  - In business, it’s convenient
  - In some cases, I’d rather be invisible
- Most importantly – it’s empowering!

When Information is Critical

- Don’t expect any privacy
  - Emergencies like 911
  - Identify-based services, like passports
  - Use of others’ resources as employees
  - Legal actions like taxes and divorce
  - Law enforcement like stop signs

When Information is Important

- Financial dealings like bank and credit accounts
- Job applications like resumes and references
- Airline travel
- Medical services
- Contracted services
- Government protections

When Information is Convenient

- Business transactions like catalog purchases
- Local/national directories like phone books and church directories
- Retail sales like tailored clothing
- Personal preferences like nutritional requirements

This is Easy, Right?

- Nope – it’s way complicated
- Privacy requires Security, but not too much
  - Security doesn’t require privacy at all
- Gov’ts compel information …
  - …and promises to reveal it, too!
- No one really can agree on what privacy means
  - No one-size-fits-all formula

How Hard Could It Be?

- Do you want your government to know about you?
  - To tax me to the max? *Rather not!*
  - Public services? *OK!*
  - Protective services? *Darned right!*

Keep this Stuff Secure!

- Different kinds of data require different protections
  - Name & address – some, but not a lot
  - Shopping behaviors – a bit more
  - Finances – a lot
  - Health – quite a lot
  - Political, sexual, racial – lots & lots
- Configuring security can be quite complicated
- Data types and potentials uses (and abuses) are the key

Oh, yeah, Make it Easy for Me to Use, Too!

- High security means high difficulty
  - That's the point – security makes it hard to get to the data
- If it's hard for someone else to get to my data, then it's hard for me to get to it, too
- Base Points:
  - Recognition is not enough
  - Authentication is often required
  - Authorization has to be based on verified identity

This Really is Hard

- Privacy is very personal
  - Who can decide what is the right balance for everyone?
- Governments have to be intrusive, and provide open access, too
  - Really hard balance, particularly for the judiciary
- Business cannot succeed without customer trust
  - More clear today then ever before

The Elements of Trust

- Data Protection
  - Privacy
  - Security
  - Control of Information
  - Control of Devices
  - Choice re: Content
- Goal: empower people

A Trust Taxonomy

Goals

Availability
At advertised levels

Suitability
Features fit function

Integrity
Against data loss or alteration

Privacy
Use & Access authorized by end-user

Reputation
System and provider brand

Means

Security
Resists unauthorized access

Quality
Performance criteria

Dev Practices
Methods, philosophy

Operations
Guidelines and benchmarks

Business Practices
Business model

Policies
Laws, regulations, standards, norms

Execution

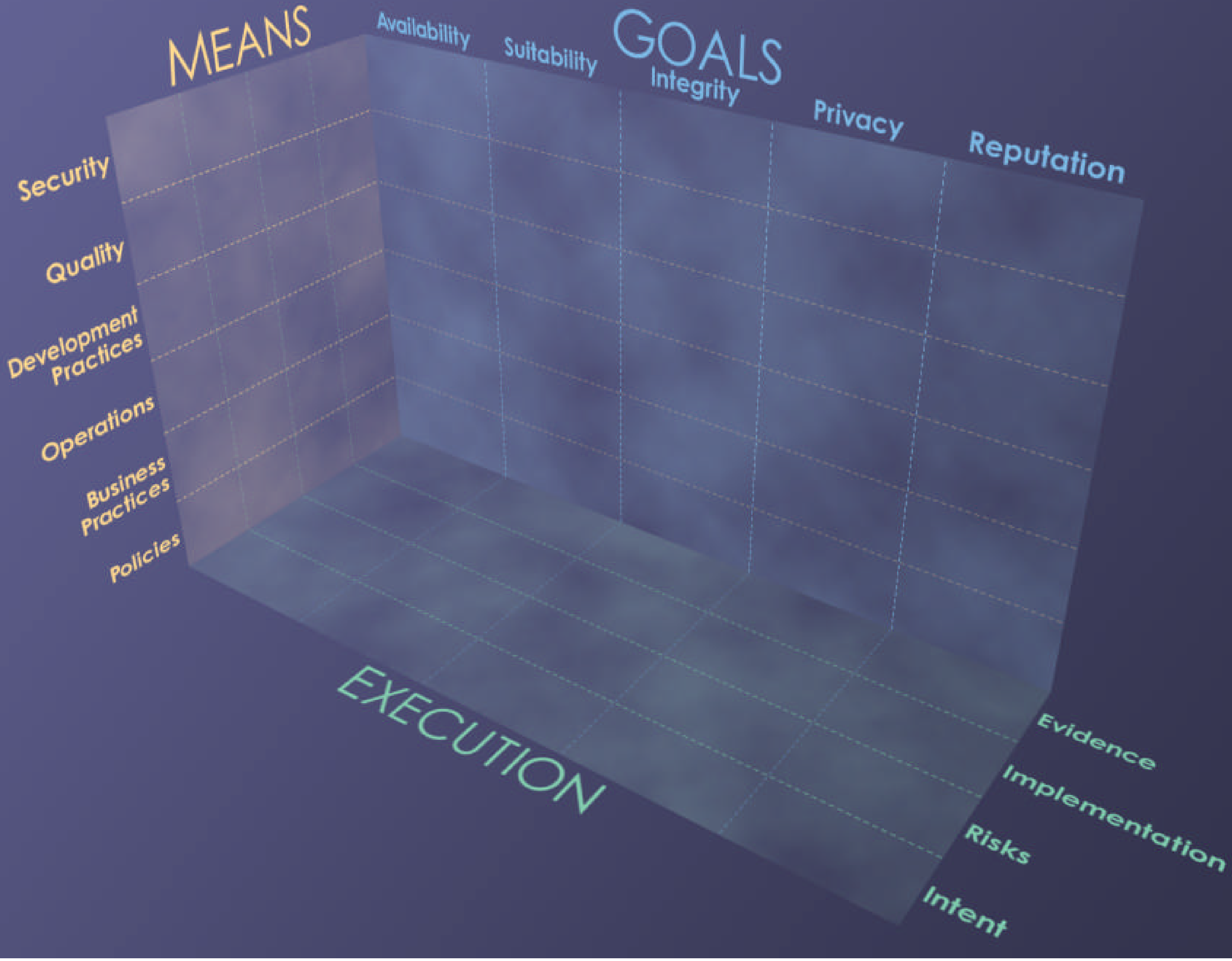
Intent
Management assertions

Risks
What undermines intent, causes liability

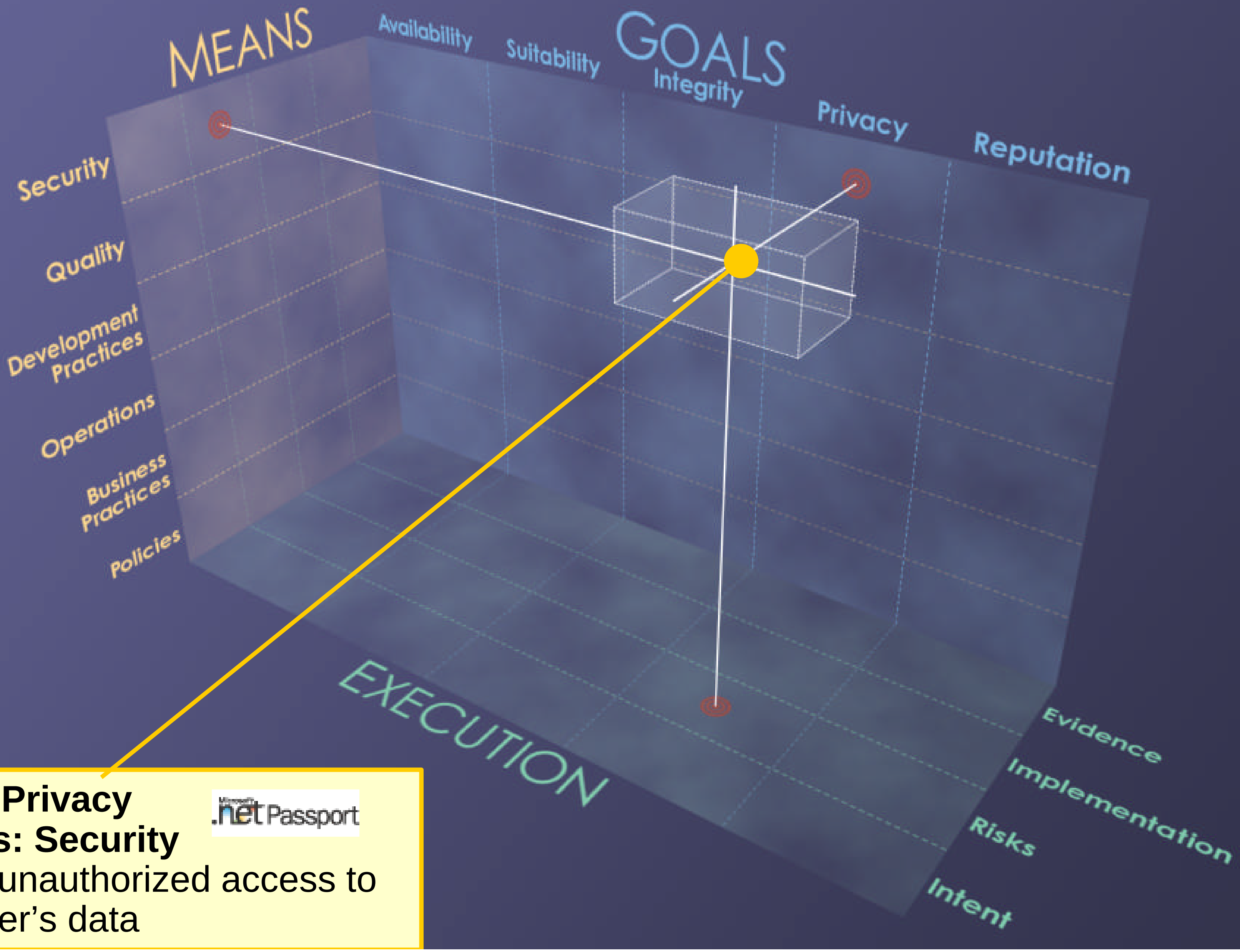
Implementation
Steps to deliver intent

Evidence
Audit mechanisms

A Trust Scorecard: 120 Grades



Passport Anxiety: Will My Data Be Safe?



Goal: Privacy
Means: Security
Risk: unauthorized access to the user’s data

.net Passport

TCI Process for Privacy

- Privacy Directive
  - 100+ page policy documentation
- Privacy Checklist
  - Training module required for all staff
- Privacy Health Index
  - Assessment tool required for targeted product, systems, and services managers
- Scorecard – you can’t manage what you can’t measure

Thank You!