Cloud Cyber Security: How Hard Can It Be?

Bob Duncan
Computing Science
University of Aberdeen
Aberdeen, UK
Email: bobduncan@abdn.ac.uk

CLOUD COMPUTING 2017, the Eighth International Conference on Cloud Computing, GRIDs, and Virtualization, 19 February 2017 - 23 February 2017, Athens, Greece

UNIVERSITY OF ABERDEEN
BUSINESS SCHOOL

Cloud Cyber Security: How Hard Can It Be?

1. Introduction
2. A Possible Approach
3. Weaknesses
4. Future Improvements
5. Conclusion

CLOUD COMPUTING 2017, the Eighth International Conference on Cloud Computing, GRIDs, and Virtualization, 19 February 2017 - 23 February 2017, Athens, Greece

UNIVERSITY OF ABERDEEN
BUSINESS SCHOOL

Cloud Cyber Security: How Hard Can It Be?

1. Introduction

Cloud Computing - A Novel Concept.

Let us take all our important corporate information and run it in somebody else's computer system.

What could possibly go wrong?

CLOUD COMPUTING 2017, the Eighth International Conference on Cloud Computing, GRIDs, and Virtualization, 19 February 2017 - 23 February 2017, Athens, Greece

UNIVERSITY OF ABERDEEN
BUSINESS SCHOOL

Cloud Cyber Security: How Hard Can It Be?

2. A Possible Approach

Develop a conceptual cloud security assurance model with:

- Declarative Layer
- Operational Layer
- Assurance Layer
- Audit Layer

UNIVERSITY OF ABERDEEN
BUSINESS SCHOOL

Cloud Cyber Security: How Hard Can It Be?

2. A Possible Approach

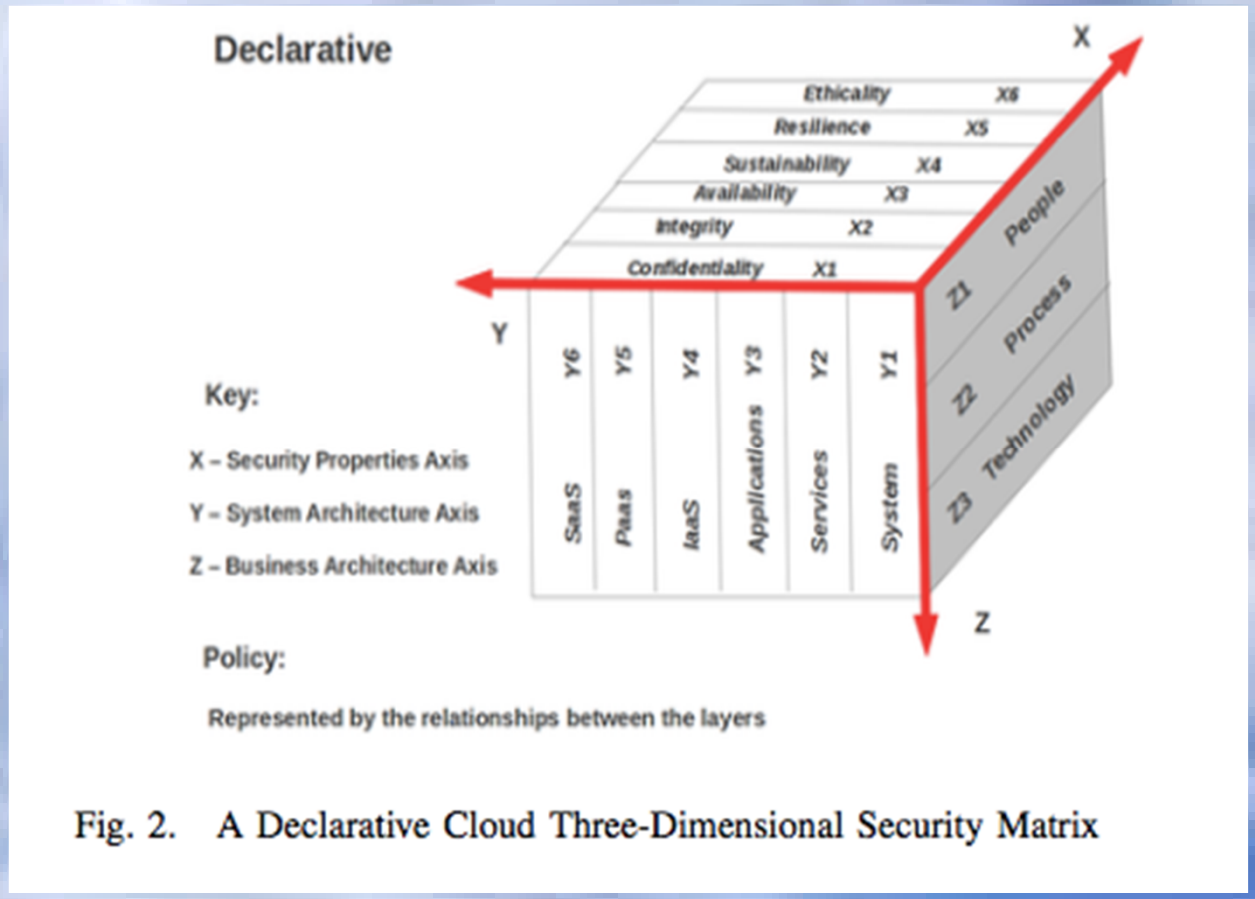


Fig. 2. A Declarative Cloud Three-Dimensional Security Matrix

CLOUD COMPUTING 2017, the Eighth International Conference on Cloud Computing, GRIDs, and Virtualization, 19 February 2017 - 23 February 2017, Athens, Greece

UNIVERSITY OF ABERDEEN BUSINESS SCHOOL

Cloud Cyber Security: How Hard Can It Be?

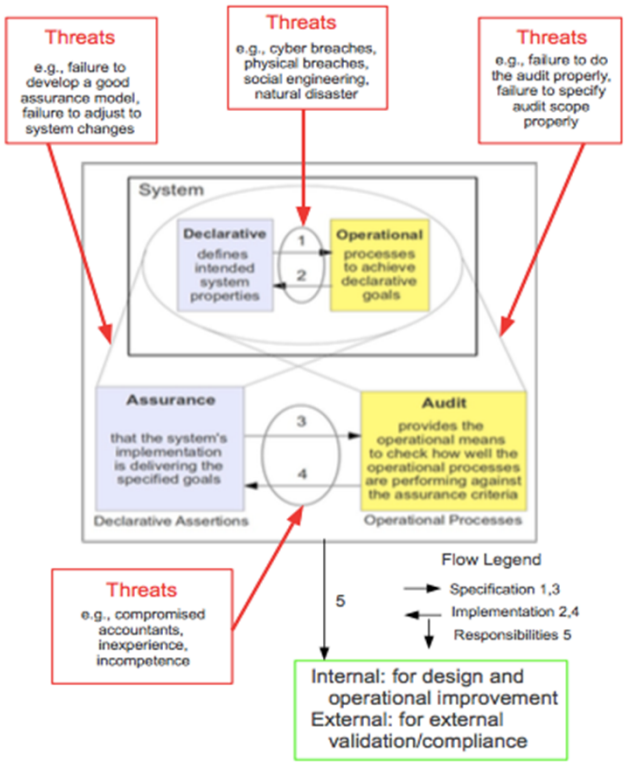


Fig. 3. The Declarative/Operational/Assurance/Audit Layers (see Subsection IV(E) for notes

CLOUD COMPUTING 2017, the Eighth International Conference on Cloud Computing, GRIDs, and Virtualization, 19 February 2017 - 23 February 2017, Athens, Greece

UNIVERSITY OF ABERDEEN
BUSINESS SCHOOL

Cloud Cyber Security: How Hard Can It Be?

3. Weaknesses

1. Definition of security goals
2. Compliance with standards
3. Audit issues
4. Management approach
5. Technical complexity of cloud
6. Lack of responsibility and accountability
7. Measurement and monitoring
8. Management attitude to security
9. Security culture in the company
10. The threat environment

UNIVERSITY OF ABERDEEN
BUSINESS SCHOOL

Cloud Cyber Security: How Hard Can It Be?

3. Weaknesses

1. Definition of security goals

UNIVERSITY OF ABERDEEN
BUSINESS SCHOOL

Cloud Cyber Security: How Hard Can It Be?

3. Weaknesses

1. Definition of security goals

Often, company managers have difficulty understanding what their security goals ought to be.

UNIVERSITY OF ABERDEEN
BUSINESS SCHOOL

Cloud Cyber Security: How Hard Can It Be?

3. Weaknesses

2. Compliance with standards

UNIVERSITY OF ABERDEEN
BUSINESS SCHOOL

Cloud Cyber Security: How Hard Can It Be?

3. Weaknesses

2. Compliance with standards

Compliance with standards is a laudable aim. Since cloud began, over 30 agencies have been working on cloud standards. Despite all this good work, there are currently no complete cloud security standards in existance.

UNIVERSITY OF ABERDEEN
BUSINESS SCHOOL

Cloud Cyber Security: How Hard Can It Be?

3. Weaknesses

3. Audit issues

Compliance is often achieved through audit. However, the practical meachanisms frequently deployed to achieve audit place an over reliance on checklists, rather than on carrying out proper due diligence, leading to poor audit quality.

UNIVERSITY OF ABERDEEN
BUSINESS SCHOOL

Cloud Cyber Security: How Hard Can It Be?

3. Weaknesses

4. Management approach

Management approaches can generally be grouped into two main categories:-

4.1 Managers who work under Agency Theory, and

4.2 Managers who work under Stewardship Theory

It is well known that Agency Theory completely fails to handle the effects of greed, leading to weakness in management goals.

Cloud Cyber Security: How Hard Can It Be?

3. Weaknesses

5. Technical complexity of cloud

UNIVERSITY OF ABERDEEN
BUSINESS SCHOOL

Cloud Cyber Security: How Hard Can It Be?

3. Weaknesses

5. Technical complexity of cloud

Cloud presents a far more complex environment for companies to operate in. Complexity is not the friend of security. Over the years, cloud has become ever more complex, leading to ever more needless vulnerabilities appearing in cloud systems.

UNIVERSITY OF ABERDEEN
BUSINESS SCHOOL

Cloud Cyber Security: How Hard Can It Be?

3. Weaknesses

6. Lack of responsibility and accountability

There is a great tendency for both cloud service providers and cloud users to wriggle out of their responsibilities when if comes to ensuring a high level of cloud security and privacy can be maintained. When no-one stands accountable for their actions, or inactions, this usually impacts adversely on the standard of security being achieved.

UNIVERSITY OF ABERDEEN
BUSINESS SCHOOL

Cloud Cyber Security: How Hard Can It Be?

3. Weaknesses

7. Measurement and monitoring

CLOUD COMPUTING 2017, the Eighth International Conference on Cloud Computing, GRIDs, and Virtualization, 19 February 2017 - 23 February 2017, Athens, Greece

UNIVERSITY OF ABERDEEN
BUSINESS SCHOOL

Cloud Cyber Security: How Hard Can It Be?

3. Weaknesses

7. Measurement and monitoring

A common weakness in many compromised systems is a singular lack of any measurement and monitoring to ensure systems are behaving as expected. Current estimates suggest that it takes on average 200 days for corporates to realise they have suffered a breach. Proper measurement and monitoring would clearly allow for much faster discovery. In 2018, the EU General Data Protection Regulation will come into force, whereby failure to disclose a breach within 72 hours will result in punitive fines.

UNIVERSITY OF ABERDEEN
BUSINESS SCHOOL

Cloud Cyber Security: How Hard Can It Be?

3. Weaknesses

8. Management attitude to security

UNIVERSITY OF ABERDEEN
BUSINESS SCHOOL

Cloud Cyber Security: How Hard Can It Be?

3. Weaknesses

8. Management attitude to security

Where management have a poor attitude to security, this tends to filter down through the organisation, leading to the view that “If management don't seem to care, why should we?”

Cloud Cyber Security: How Hard Can It Be?

3. Weaknesses

9. Security culture in the company

UNIVERSITY OF ABERDEEN
BUSINESS SCHOOL

Cloud Cyber Security: How Hard Can It Be?

3. Weaknesses

9. Security culture in the company

Where management do not seem to care about security, this can lead to the evolution of a poor security culture in the company. A proper level of security depends on both the security culture in the company and the actions of every single employee in the company. Without the right security culture in place, the company effectively aids the attacker to exploit the company much more easily than would otherwise be the case.

UNIVERSITY OF ABERDEEN
BUSINESS SCHOOL

Cloud Cyber Security: How Hard Can It Be?

3. Weaknesses

10. The threat environment

Cloud Cyber Security: How Hard Can It Be?

3. Weaknesses

10. The threat environment

We can consider 5 main areas of threat:

10.1 State sponsored attack;
10.2 Industrial espionage;
10.3 Hacktivists;
10.4 Professional criminals;
10.5 Amateur hackers.

UNIVERSITY OF ABERDEEN
BUSINESS SCHOOL

Cloud Cyber Security: How Hard Can It Be?

3. Weaknesses

10. The threat environment

They work 24/7 365 days a year. Some, such as the state-sponsored actors are exceptionally talented and extremely well resourced. Others, such as hacktivists, are highly motivated. Even amateurs can be highly skilled. It is no longer a question of IF you will be hacked, rather it is simply a question of WHEN!

UNIVERSITY OF ABERDEEN
BUSINESS SCHOOL

Cloud Cyber Security: How Hard Can It Be?

3. Weaknesses

11. The Internet of Things

CLOUD COMPUTING 2017, the Eighth International Conference on Cloud Computing, GRIDs, and Virtualization, 19 February 2017 - 23 February 2017, Athens, Greece

UNIVERSITY OF ABERDEEN
BUSINESS SCHOOL

Cloud Cyber Security: How Hard Can It Be?

3. Weaknesses

11. The Internet of Things

To this unhappy list, we can now add the Internet of Things (IoT). The weaknesses of cloud pale into insignificance when we consider the IoT. With up to 50 billion IoT devices forecast to be in use by 2020, no security standards on the horizon, devices riddled with poor or non-existant security, and with full access to our “secure” networks, what could possibly go wrong?

UNIVERSITY OF ABERDEEN
BUSINESS SCHOOL

Cloud Cyber Security: How Hard Can It Be?

4. Future Improvements

FAST-CCS?

UNIVERSITY OF ABERDEEN
BUSINESS SCHOOL

Cloud Cyber Security: How Hard Can It Be?

4. Future Improvements

FAST-CCS?

This could provide a good starting point. Once a breach occurs, the attacker seeks to delete the audit trail, to remove all trace of their visit. Ensuring proper audit and forensic trails are properly maintained can provide a good starting point, especially if the weaknesses from Section 3 are properly addressed.

UNIVERSITY OF ABERDEEN
BUSINESS SCHOOL

Cloud Cyber Security: How Hard Can It Be?

4. Future Improvements

Unikernels?

CLOUD COMPUTING 2017, the Eighth International Conference on Cloud Computing, GRIDs, and Virtualization, 19 February 2017 - 23 February 2017, Athens, Greece

UNIVERSITY OF ABERDEEN
BUSINESS SCHOOL

Cloud Cyber Security: How Hard Can It Be?

4. Future Improvements

Unikernels

We can use unikernel solutions to help reduce the complexity of cloud systems in order to make security more effective and simpler to achieve. A useful by product is the reduced running costs which can be offered by unikernel systems. Thanks to their minuscule footprint, they might also be adapted for IoT security.

UNIVERSITY OF ABERDEEN
BUSINESS SCHOOL

Cloud Cyber Security: How Hard Can It Be?

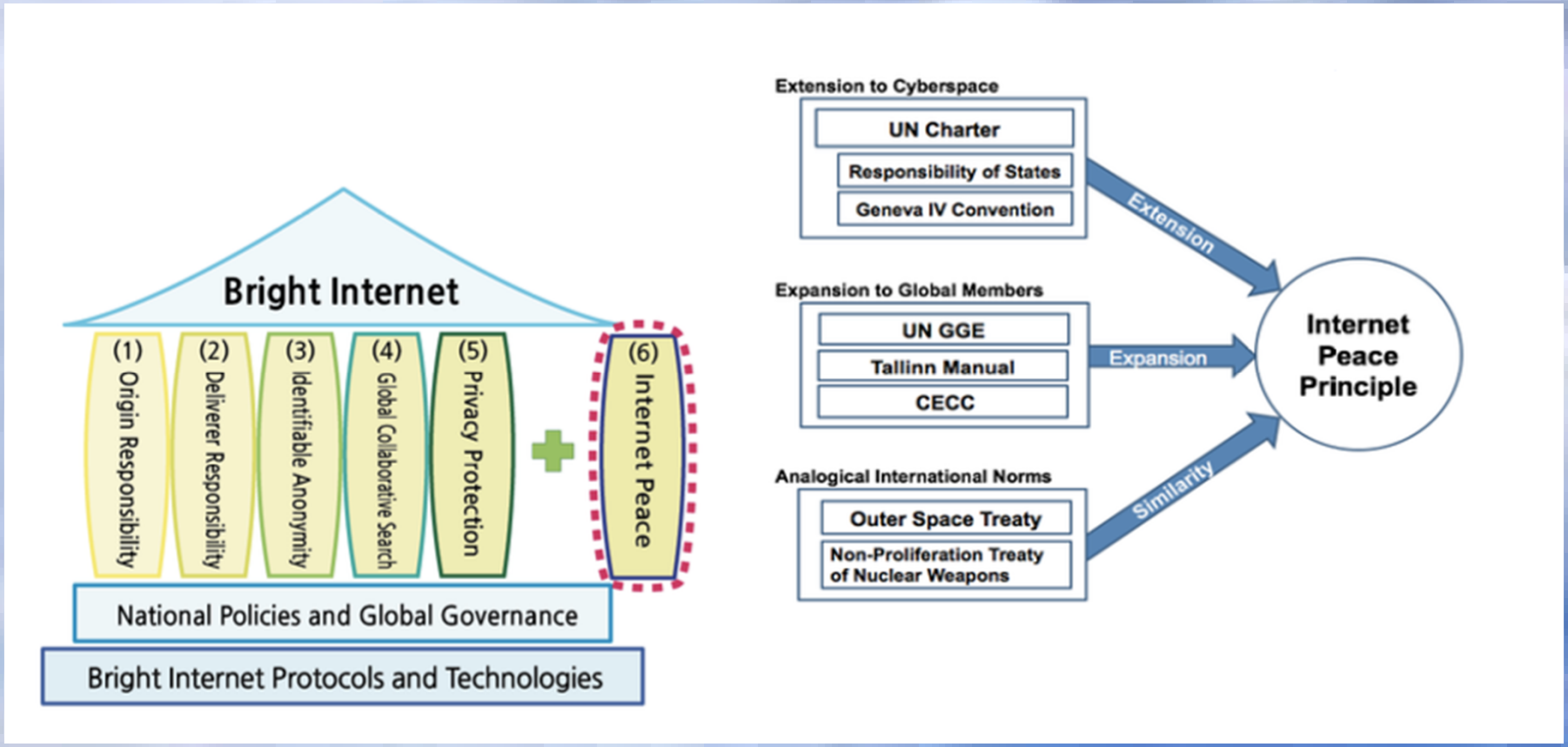
4. Future Improvements

The Bright Internet

CLOUD COMPUTING 2017, the Eighth International Conference on Cloud Computing, GRIDs, and Virtualization, 19 February 2017 - 23 February 2017, Athens, Greece

Cloud Cyber Security: How Hard Can It Be?

4. Future Improvements

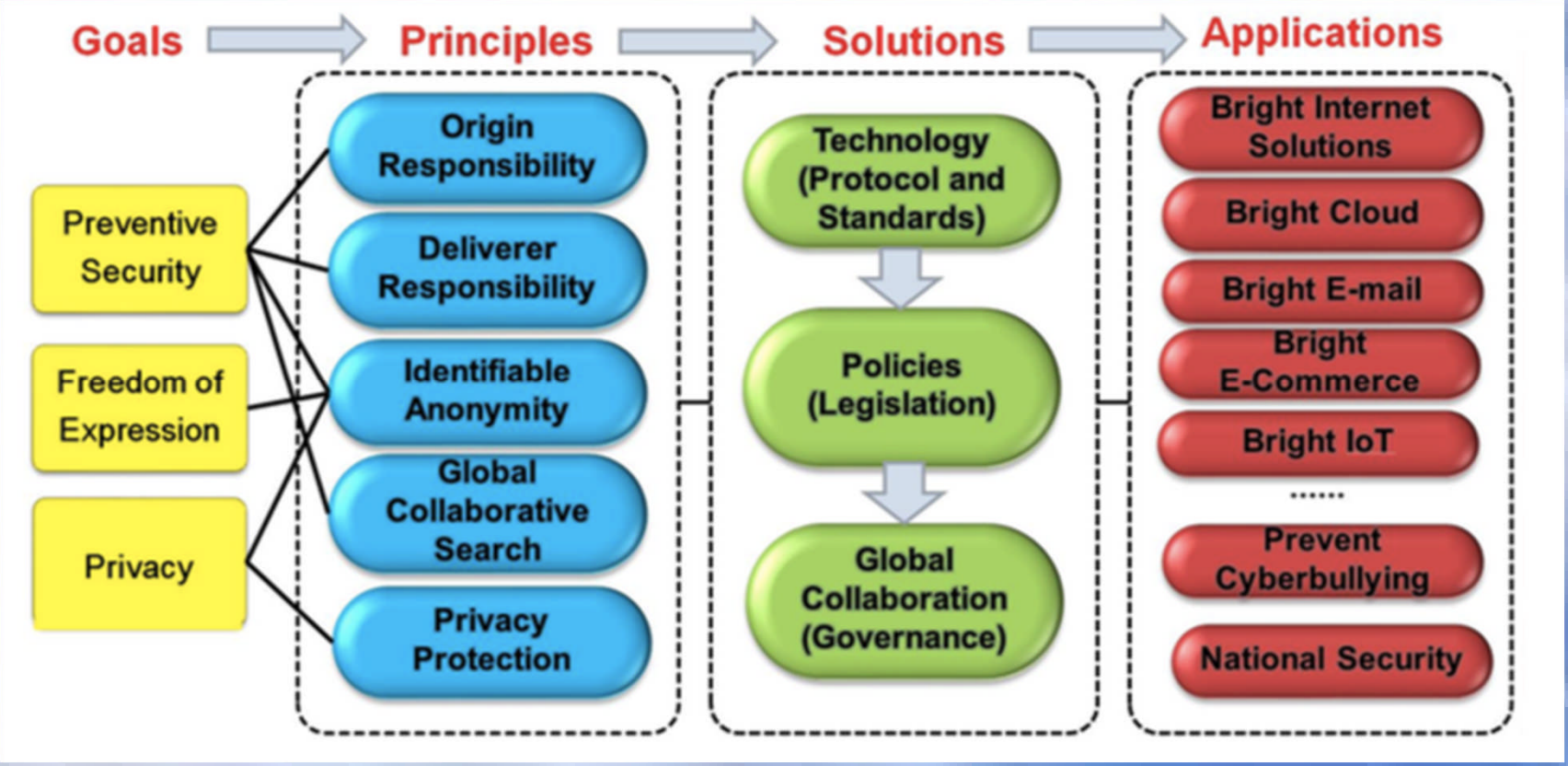


CLOUD COMPUTING 2017, the Eighth International Conference on Cloud Computing, GRIDs, and Virtualization, 19 February 2017 - 23 February 2017, Athens, Greece

UNIVERSITY OF ABERDEEN
BUSINESS SCHOOL

Cloud Cyber Security: How Hard Can It Be?

4. Future Improvements



CLOUD COMPUTING 2017, the Eighth International Conference on Cloud Computing, GRIDs, and Virtualization, 19 February 2017 - 23 February 2017, Athens, Greece

UNIVERSITY OF ABERDEEN
BUSINESS SCHOOL

Cloud Cyber Security: How Hard Can It Be?

4. Future Improvements

- **Traditional Destination Driven Protective Solution**

- **Bright Internet Approach: Bright Cloud**
  - **Origin Driven Preventive Solution: Reverse Engineering**

CLOUD COMPUTING 2017, the Eighth International Conference on Cloud Computing, GRIDs, and Virtualization, 19 February 2017 - 23 February 2017, Athens, Greece

UNIVERSITY OF ABERDEEN
BUSINESS SCHOOL

Cloud Cyber Security: How Hard Can It Be?

5. Conclusion

What do you think?

UNIVERSITY OF ABERDEEN
BUSINESS SCHOOL