TTI Summer Forum | Strategies for Survival and Beyond

6point6 Cyber | Moving to Secure Working |
Peter Barnsley, Cyber Security Director

18 June 2020

Introductions

A little bit about us...

My name is **Peter Barnsley** and I am the **Director of Cyber Security** at **6point6**. I have over 10 years of experience in **Cybersecurity** and a further 10 years in wider IT disciplines including Information Assurance, Governance, Infrastructure, Networking and Software Engineering.

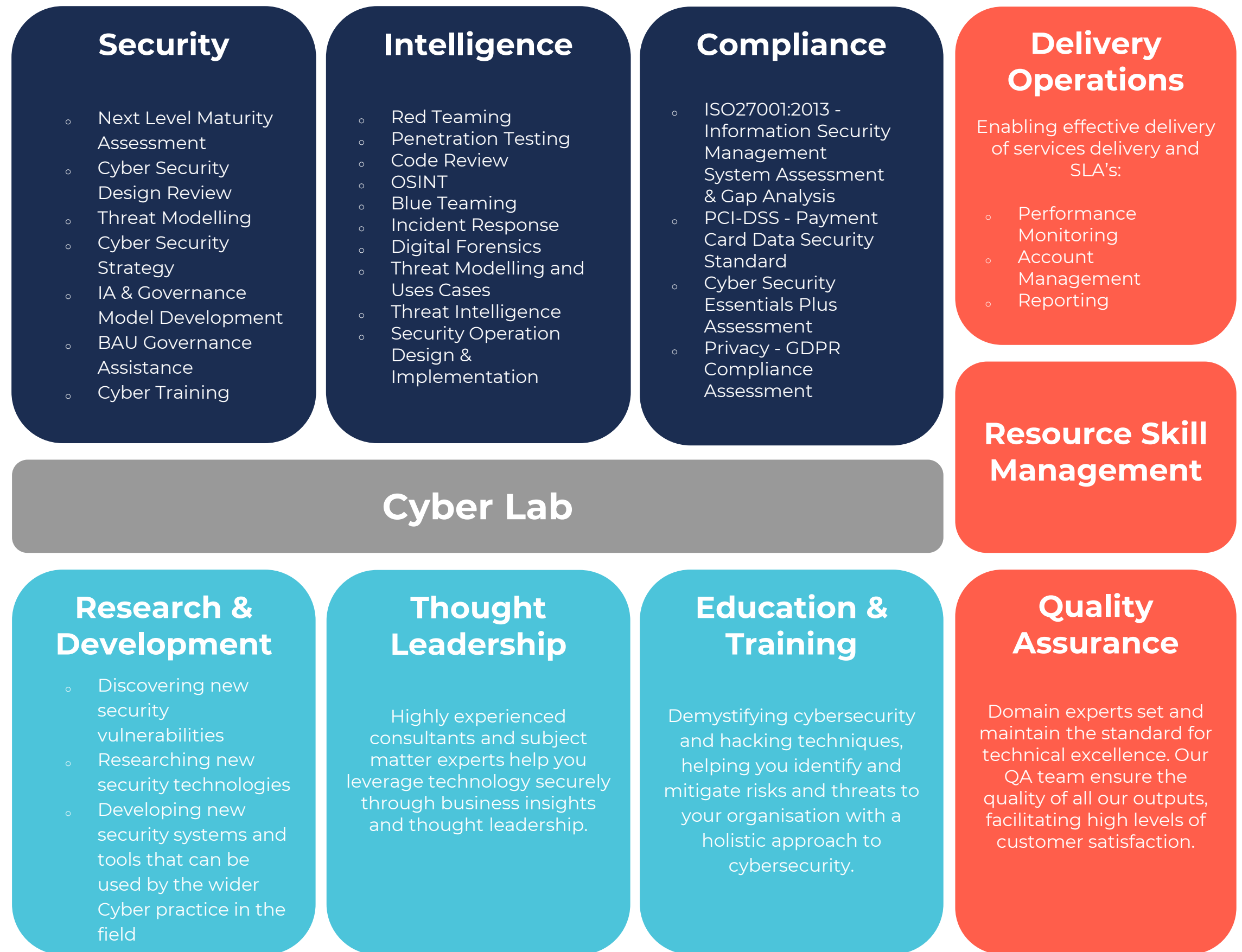Before joining 6point6, I worked for the Home Office, Ministry of Justice and MoD.
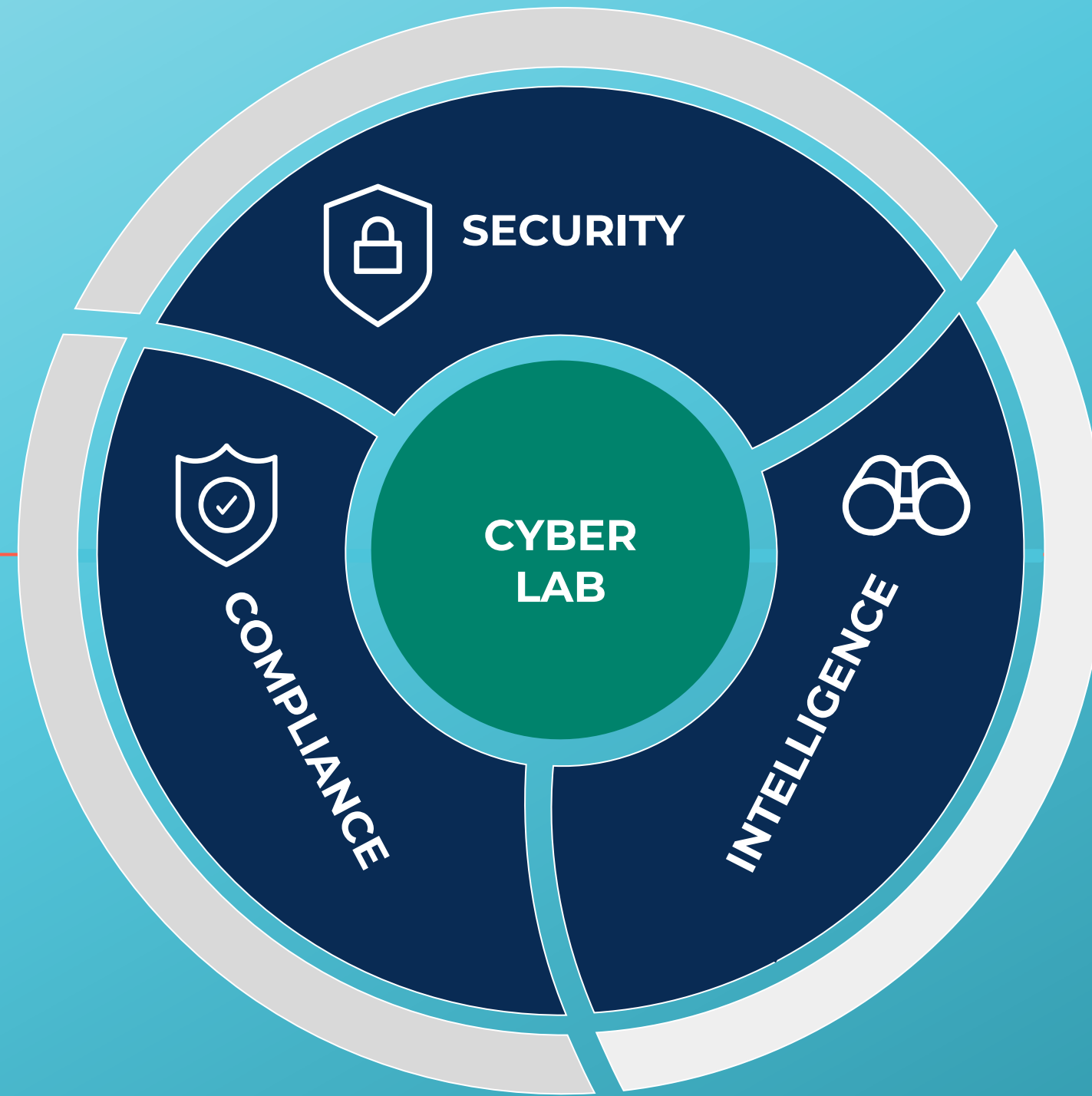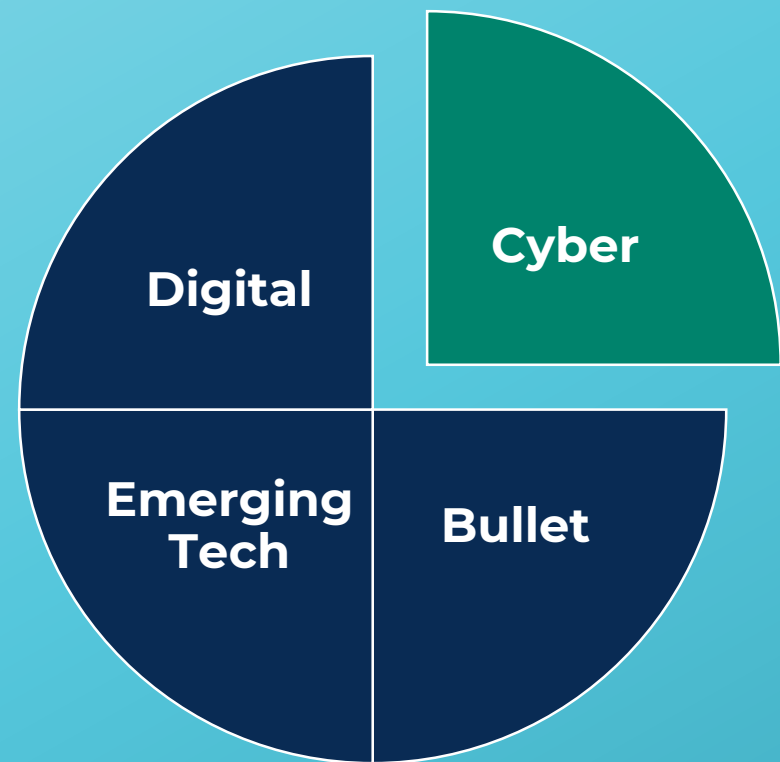
Our holistic approach to cybersecurity

Spanning the lifecycle of your security journey

Security

- Next Level Maturity Assessment
- Cyber Security Design Review
- Threat Modelling
- Cyber Security Strategy
- IA & Governance Model Development
- BAU Governance Assistance
- Cyber Training

Intelligence

- Red Teaming
- Penetration Testing
- Code Review
- OSINT
- Blue Teaming
- Incident Response
- Digital Forensics
- Threat Modelling and Uses Cases
- Threat Intelligence
- Security Operation Design & Implementation

Compliance

- ISO27001:2013 - Information Security Management System Assessment & Gap Analysis
- PCI-DSS - Payment Card Data Security Standard
- Cyber Security Essentials Plus Assessment
- Privacy - GDPR Compliance Assessment

Delivery Operations

Enabling effective delivery of services delivery and SLA's:

- Performance Monitoring
- Account Management
- Reporting

Cyber Lab

Resource Skill Management

Research & Development

- Discovering new security vulnerabilities
- Researching new security technologies
- Developing new security systems and tools that can be used by the wider Cyber practice in the field

Thought Leadership

Highly experienced consultants and subject matter experts help you leverage technology securely through business insights and thought leadership.

Education & Training

Demystifying cybersecurity and hacking techniques, helping you identify and mitigate risks and threats to your organisation with a holistic approach to cybersecurity.

Quality Assurance

Domain experts set and maintain the standard for technical excellence. Our QA team ensure the quality of all our outputs, facilitating high levels of customer satisfaction.

6POINT6

The agenda

What we're going to cover in today's talk…

- 15 – 20 minute talk around the topics of **Secure Remote Working** and **Cyber Resiliency**
- 10 minute **Q&A session** to follow

Talking points:

- COVID-19 | A new world
- Secure remote working
- Supply chain resilience
- COVID-19 | Lessons learned in business continuity
- Shadow IT
- What next?

COVID-19 | A new world

The short and long-term impact of COVID-19

COVID-19 has forced organisations to find **alternative means** of **operating**. For most, this has meant **remote working**. The haste with which this change needed to occur created a raft of security concerns for organisations of all sizes and from all industries. **Security** was often neglected or ignored altogether as organisations went into **survival mode**.

Commons challenges

- o Rapid deployment of new capabilities
- o Automation and autoscaling of internal services and tools
- o Data management

Where to start

- o Management of credentials - MFA
- o Securing your network – VPN's
- o Education - Process and governance

Post COVID-19 | What can we expect?

Is your IT ready for what is to follow?

COVID-19 has prompted a sharper shift in attitude regarding remote or flexible working. It has demonstrated that the **benefits** to the organisation, its **supply chain**, **employees** and, most importantly, its **customers** can be significant if implemented correctly.

It has also facilitated a change in our consumer habits too. These trends are likely to continue beyond the COVID-19 pandemic. **Organisations need to embrace these changes if they are to survive and thrive.**

Overwhelming demand caused the temporary **shut-down** of **websites** across the **retail** and **hospitality** sectors during the COVID-19 pandemic:

Secure remote working

How to securely support a distributed workforce post COVID-19

Key things to consider

- o Account security
- o Endpoint security
- o Phishing protection
- o Network security
- o IT Support
- o Embrace new ways of working

Supply chain resilience

Is the cybersecurity of my supply chain robust enough?

Almost **all** organisations rely upon third parties to **operate** and **deliver their services** to customers.

- How does an organisation ensure the **controls** for their third parties are **proportionate**?
- How does an organisation understand what third parties are doing with their **data** and ensure they adhere to **legal requirement**?
- What level of responsibility do third parties have in providing **assurance** to their customer?
- How can organisations begin to understand the effectiveness of third party **BCDR plans** and responses?
- How can an organisation integrate third party **assurance** into **BAU** activities?

COVID 19 | Lessons learned in business continuity

A time to reflect, learn and ACT

The impact of COVID-19 on the travel, hospitality and leisure sectors has been well documented. **How can the damage be minimised?**

Plan for ongoing business impact

- o Reduce and refine service offerings
- o Consider new means of reaching your market – leverage technology to help
- o Embrace change. Don't fight it!

Continuity of the supply chain

- o Early and regular communication
- o Support your supplier and partners
- o Identify alternatives

Remote working is here to stay

- o Remote working likely to increase
- o Assess IT impact of workers utilising remote access
- o Identify and embrace new ways of working

The human element

- o Priority remains well being of staff
- o Keeping staff motivated and engaged
- o Sensitivity to personal supply chains

Shadow IT

The challenges created by the rise of shadow IT

1) What is shadow IT?

2) Shadow IT was already on the rise prior to COVID-19. What prompted this?

3) What issues can this cause if unchecked?
   - Increase in cybersecurity and compliance risks and issues
   - Data security
   - Increased IT costs
   - Inefficiency and technical debt

4) Reducing risk
   - Monitoring cloud and network resources
   - IT project governance guidelines should be highlighted
   - Allowing limited shadow IT

What next?

How do we address the cybersecurity concerns we have?

6point6 offer a range of cybersecurity services to help organisations, big and small, identify and understand the specific threats and risks to their business and sector, including:

- o Regular Risk Assessments
- o Incident Response: Prepare
- o Penetration Testing
- o Maturity Assessment
- o ISO27001 Assessments

About 6point6

Founded in 2012, 6point6 is a technology consultancy with strong expertise in digital, emerging technology and cyber. We bring a wealth of hands-on experience to help businesses, including financial service providers, media houses and government, achieve more with digital. Using cutting edge technology and agile delivery methods, we help organisations reinvent, transform and secure a brighter digital future.

Visit us on **www.6point6.co.uk**
Email us at **cyber@6point6.co.uk**
Twitter: **6point6ltd**
LinkedIn: **linkedin.com/company/6point6**

6POINT6