Supply chain cyber security

Introduction – why focus on supply chain cyber security

28 September 2022

Presenters: Maritz Cloete and Richard Jackson, Moore ClearComm

© ICAEW 2022

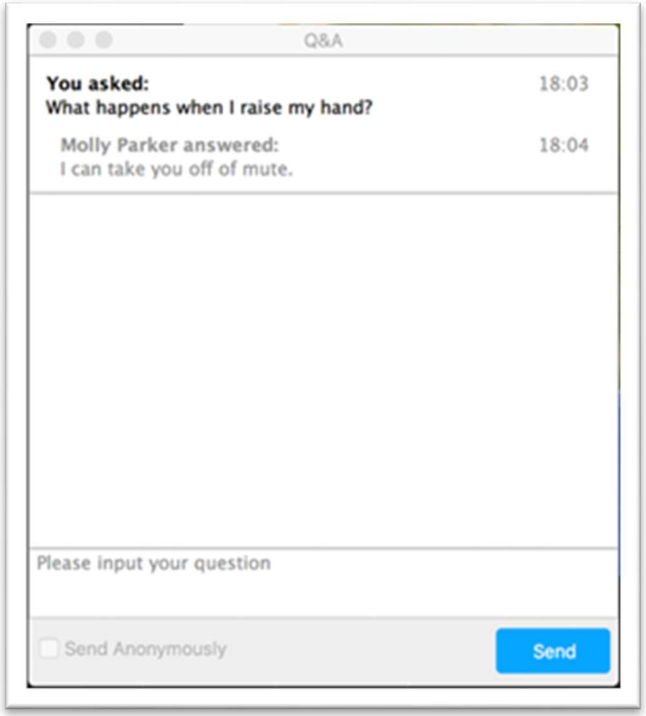
Today’s presenters

Maritz Cloete
Director, Cyber Security & IT Assurance Services
MooreClearComm

Richard Jackson
Partnership manager
MooreClearComm

© ICAEW 2022

Ask a question



You asked: 18:03
What happens when I raise my hand?

Molly Parker answered: 18:04
I can take you off of mute.

Please input your question

Click on the Q&A button in the bottom toolbar to open the submit question prompt.

Type in your question and click send.

Note. If you wish to ask anonymously tick the send anonymously box shown on the illustration to the left.

© ICAEW 2022

“With the increase in the remote workforce and ongoing COVID pandemic, there has been a 300% increase in cyberattacks on accounting practices of **all sizes**.”

Accounting Today (2022)

© ICAEW 2022

Accounting Today

- Attackers are sophisticated and often strike when accountants are busy and have deadlines to meet

- Such as at year-end or when tax return deadlines are looming

- In all cases, cyber criminals will exploit the weakness in:

1) Your systems

2) Your supply chain

3) Employee diligence

© ICAEW 2022

AAT Comment

- Smaller practices are seen as a softer target
- They are less likely to have the right technical / IT controls in place
- Minimal focus on supply chain best practice or vendor risks
- Their staff less likely to be trained in cyber awareness
- Partners/Owners do not perceive the firm to be a likely target

© ICAEW 2022

Supply Chain: High Risk and High Impact

- Supply Chain is a major threat source for all businesses
- All accountants now rely heavily on third-party suppliers, in respect of digital service and processing of client data
- Vendor Risk Assessments (VRA) are a business essential, in 2022

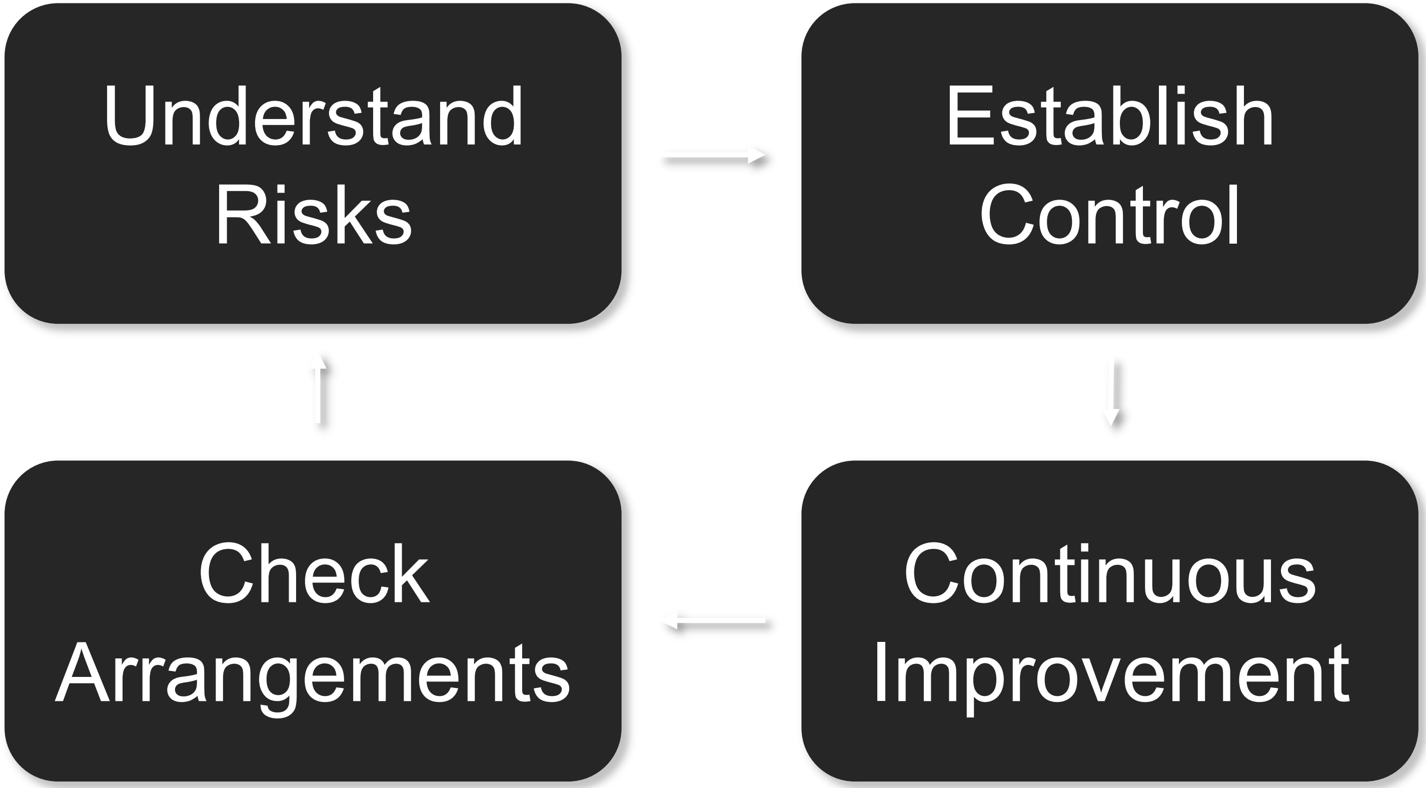
Thought:

Has your practice carried out a
risk assessment of its supply chain?

© ICAEW 2022

National Cyber Security Centre
a part of GCHQ

Supply Chain Risk Principles



MOORE ClearComm

© ICAEW 2022

BlueVoyant Survey:

3rd Party Cyber Risk Management (Oct 2021)

- 93% of respondents had suffered a direct cyber security breach because of weaknesses in their supply chain

- 37% year-on-year increase

- 38% said they had “no way of knowing when or if an issue arises with a third-party”

© ICAEW 2022

NIST
National Institute of
Standards and Technology

Key Cyber Supply Chain Risks

- Third party service providers or vendors: from office cleaning to software engineering
- Poor information security practices by lower-tier suppliers
- Compromised software or hardware purchased from suppliers
- Software security vulnerabilities in supply chain management or supplier systems
- Hardware with embedded malware
- Third party data storage or data aggregators

© ICAEW 2022

Supply chain cyber security webinar series

05 Oct: Understanding the risk your supply chain poses to you

12 Oct: Embedding security in agreements

19 Oct: Managing a supplier assessment and oversight programme

02 Nov: Recap and question and answer session

- **https://events.icaew.com/pd/25435**

© ICAEW 2022

Thank you for attending

Please take the time to fill out our short survey

Phone: +44 (0)20 7920 8526
Email: faculties@icaew.com

© ICAEW 2022

ICAEW

© ICAEW 2022