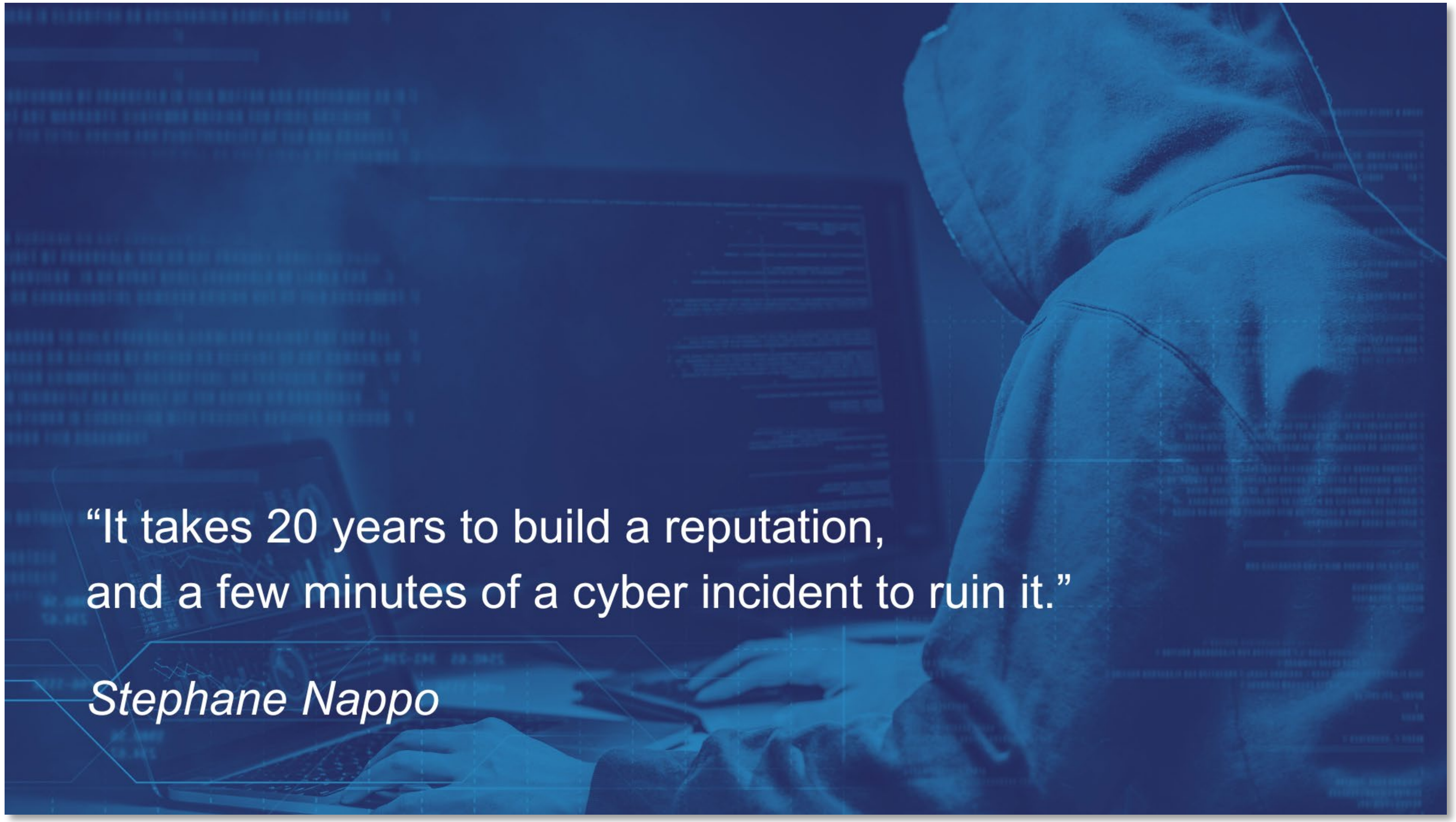
Cyber Essentials:

Proving You Take Security Seriously

MOORE ClearComm

Today's Webinar

- Current Cyber Threat
- Supply Chain Risk
- Contracts, Bids and Tenders
- Cyber Essentials Scheme
- The Five Controls
- Opportunity for Questions



"It takes 20 years to build a reputation, and a few minutes of a cyber incident to ruin it."

Stephane Nappo

MOORE ClearComm

Today`s Panellists:
Maritz Cloete and Paras Shah

The Cyber Threat

Global Cyber Crime Data

- ✓ Global cost expected to surge to $23.84 trillion by 2027 ($8.44 trillion in 2022) *(Statista, the FBI and IMF)*
- ✓ 34.5% report their organizations' accounting and financial data were targeted by cyber adversaries in 2023 *(Deloitte Center for Controllership Poll)*
- ✓ Artificial Intelligence threats are growing at a compound annual growth rate (CAGR) of 23.6%
- ✓ AI crime will reach a market value of $46.3 billion by 2027 *(International Data Corporation)*
- ✓ Authorised "Push Payment" fraud (APP) in the UK: generated losses of £485.2 million in 2022 *(UK Gov)*
- ✓ 50% of mobile phone owners (worldwide) are exposed to a phishing attack every quarter *(Lookout)*

National Cyber Security Centre: Cyber Security Breaches Survey 2023

32% of businesses and 24% of charities experienced a breach or attack in 2023:

- Medium businesses: 59%
- Large businesses: 69%
- High-income charities*: 56%

- Proportion of micro businesses saying cyber security is a high priority, decreased from 80% to 68%
- Qualitative evidence: cyber security has dropped down the priority list for smaller organisations
- Relative to wider economic concerns (inflation and socioeconomic uncertainty)

* More than £500k in annual revenue

National Cyber Security Centre: Cyber Security Breaches Survey 2023

Evidence of a decline in cyber hygiene:

✗ Use of password policies:	79% in 2021 vs 70% in 2023
✗ Use of network firewalls:	78% in 2021 vs 66% in 2023
✗ Restricting admin rights:	75% in 2021 vs 67% in 2023
✗ Software security updates (14 days):	43% in 2021 vs 31% in 2023

☠ Cyber Threat is Increasing + Defence is Decreasing ↘

Cyber Essentials Scheme

Cyber Essentials: Scheme Overview

- ✓ Developed by UK Gov / IASME Consortium and Information Security Forum (ISF)
- ✓ Set of key technical controls to help organisations protect themselves (and their supply chains) against common online security threats
- ✓ Scheme enables organisations to gain one of two Cyber Essentials badges
- ✓ Backed by the FSB, CBI and several insurance organisations
- ✓ Suitable for all organisations, of any size, in any sector

CYBER ESSENTIALS

CYBER ESSENTIALS PLUS

IASME CYBER ASSURANCE

Cyber Essentials: Business Benefits

- ✓ Protect your organisation from most known cyber threats
- ✓ Strengthen your internal and external supply chain resilience
- ✓ Reassure your customers, prospects and suppliers that you take cyber security seriously
- ✓ Become listed on the IASME Directory of organisations awarded Cyber Essentials certification
- ✓ Attract new business with assurance that you have (and can prove) cyber security measures in place
- ✓ Gain access to some government contracts, that may require Cyber Essentials certification
- ✓ Benefit from £25k of cyber liability insurance*

* Business turnover dependent

The Five Controls

Five Controls

Firewalls provide technical protection between your network devices and the Internet, referred to in the question set as boundary firewalls.

Computers and cloud services are often not secure upon default installation or setup. Cyber Essentials demands you choose the most secure settings on your new devices and software

To protect your organisation, you should ensure that all your software is always up to date with the latest security updates.

It is important to only give users access to the resources and data necessary for their roles, and no more.

Malware protection should include detection facilities (updated as frequently as possible). Anti-malware products can help confirm whether websites you visit are malicious.

Supply Chain Risk

Supply Chain Vulnerability

Supply Chain attacks will target:

- Third party software providers
- Website builders
- Third party data stores

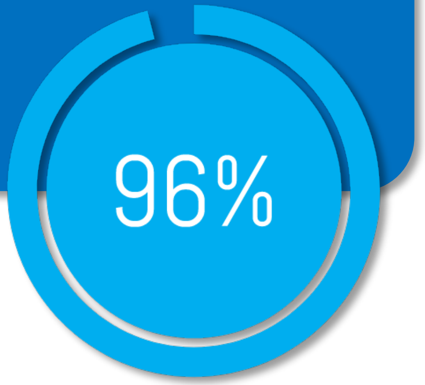
- 98% of companies have been negatively impacted by a breach that occurred at a company in their network *(Ponemon Institute)*
- 633% year-on-year increase in software supply chain attacks, since 2022 *(Boston Consulting Group)*
- Only 13% of businesses review the risks posed by **immediate** suppliers
- Only 7% review the risks posed by their **wider** supply chain
- 59% of SMEs do not fully understand the components or links in their own supply chain
- 9% admit they have **no** knowledge or understanding of their supply chain or business customers

Contracts, Bids and Tenders

Contracts, Bids and Tenders

- ✓ Increasingly, Cyber Essentials is a pre-requisite for bidding in public sector contracts
- ✓ Ministry of Defence (MoD) and most government projects demand that suppliers hold Cyber Essentials certification
- ✓ Local authorities and funding bodies now require Cyber Essentials / Cyber Essentials Plus as a fixed requirement at the beginning of the bidding process
- ✓ Many private sector contracts are now asking for Cyber Essentials as part of baseline requirements

> *"Reviewing over 50 tenders we've had access too in the last 6 months, all but two specifically asked about Cyber Essentials - and all asked questions about both cyber security and data protection."*
>
> *HBP Group*



QUESTIONS

maritz.Cloete@mooreclearcom

paras.shah@mooreclear.com

richard.jackson@mooreclear.com

Our next webinar

IT Audits and Best Practice (Episode #7)

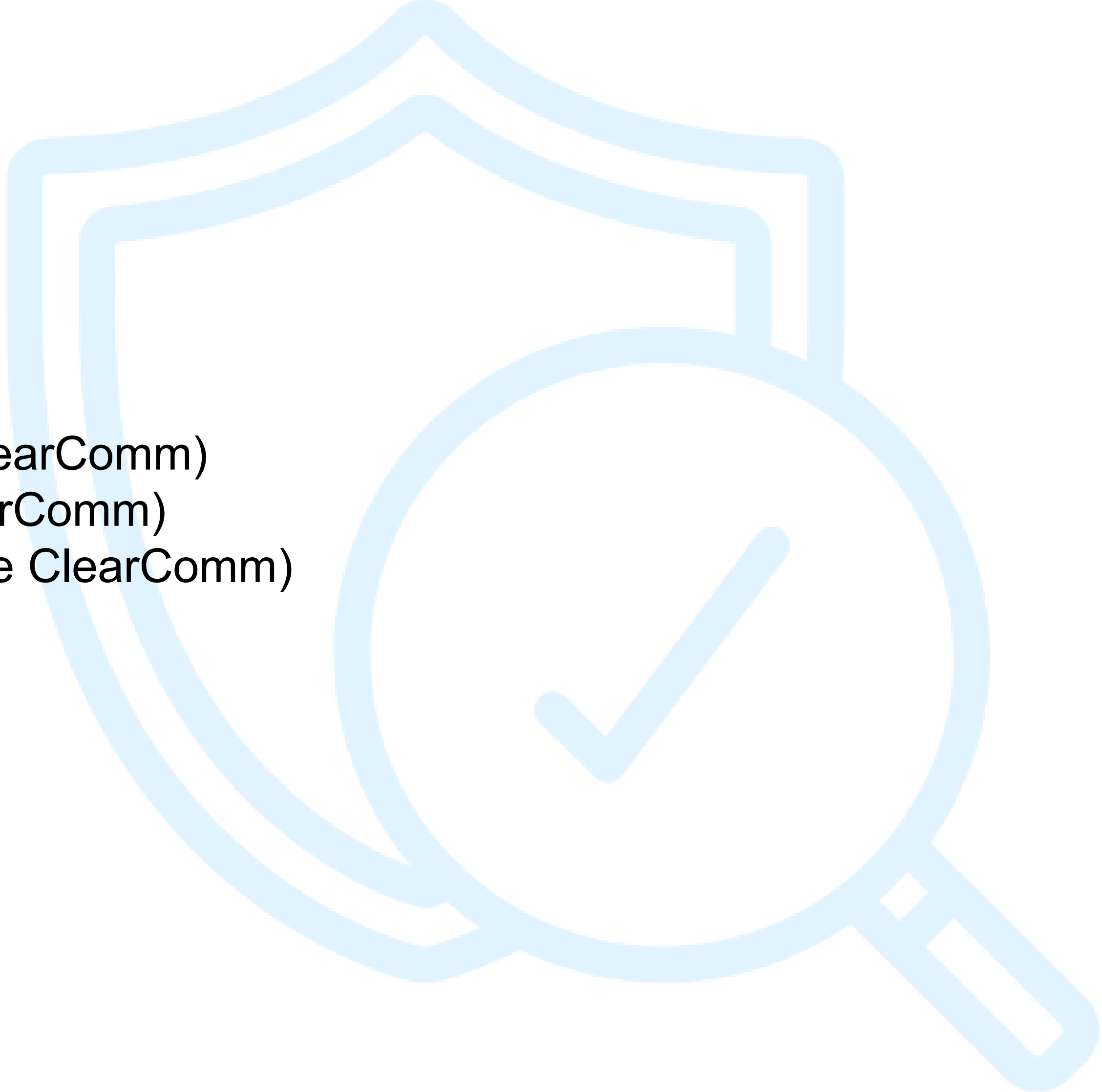
Date: Wednesday 20th March
Time: 10.00am-11.00am

Panel:

- Rich Jackson, Strategic Business Manager (Moore ClearComm)
- Maritz Cloete, Director of Cyber Services (Moore ClearComm)
- Benjie Ocquaye, IT Assurance Senior Manager (Moore ClearComm)

Location: Zoom

Previous Episodes: ▶



MOORE ClearComm

Moore ClearComm
9 Appold Street
London
EC2A 2AP
t: +44 (0)20 45821983

www.mooreclear.com

Any assumptions, opinions and estimates expressed in the Information contained in this content constitute the judgment of Moore Kingston Smith LLP and/or its associated businesses as of the date thereof and are subject to change without notice. This Information does not constitute advice and professional advice should be taken before acting on any information herein. No liability for any direct, consequential, or other loss arising from reliance on the Information is accepted by Moore Kingston Smith LLP, or any of its associated businesses.

Moore Kingston Smith LLP is regulated by the Institute of Chartered Accountants in England & Wales. Certain activities of the LLP and/or its associated businesses are authorised and regulated by the Financial Conduct Authority or the Solicitors Regulation Authority. More details are available on our website at www.mooreks.co.uk

MOORE ClearComm