DACH

CompTIA COMMUNITY

HERZLICH WILLKOMMEN

zum zweiten DACH Community Meeting

Am 17.11.2023

Kartellrecht, Anti-Belästigung und Diversität

- **Kartellrecht**
  CompTIA verfolgt eine Politik der strikten Einhaltung der Kartellgesetze auf Bundes- und Landesebene https://www.comptia.org/membership/communities-and-councils/antitrust-statement

- **Anti-Belästigung**
  CompTIA ist bestrebt, bei allen Veranstaltungen ein sicheres und einladendes Umfeld zu schaffen, und verbietet unerwünschtes Verhalten, das auf der Rasse, der Hautfarbe, der Religion, dem Geschlecht, der Geschlechtsidentität, der nationalen Herkunft, dem Alter, einer geistigen oder körperlichen Behinderung, dem Staatsbürgerstatus oder einem anderen geschützten Status einer Person beruht. https://www.comptia.org/contact-us/harassment-complaint

- **Diversität**
  Eine diverse Mischung von Stimmen führt zu besseren Diskussionen, Gesprächen, Entscheidungen und Ergebnissen für alle.
  https://comptia.informz.net/COMPTIA/pages/CompTIAATTD

WE ARE THE CompTIA COMMUNITY

MJ Shoer
Chief Community Officer
and
CEO, CompTIA Spark

Christina Allmeroth
Director, Business
Development DACH and
CEE at CompTIA

Sameera Deen
Senior Specialist,
Member Relations at
CompTIA

Katrin Giza
Manager, Member
Communities DACH
at CompTIA

CompTIA COMMUNITY

Wer ist CompTIA?

Die Computing Technology Industry Association (CompTIA) ist eine führende Organisation und Fürsprecherin des globalen IT-Ökosystems im Wert von 5 Billionen US-Dollar und der geschätzten 75 Millionen IT- und Industriefachkräften, die die Technologie, die die Weltwirtschaft antreibt, entwickeln, implementieren, verwalten und schützen. Durch Community, Aus- und Weiterbildung, Zertifizierung, Interessenvertretung, Philanthropie und Marktforschung ist CompTIA die Drehscheibe für die Erschließung des Potenzials der Tech Branche und ihrer Arbeitskräfte. **connect.comptia.org**

CompTIA®

CompTIA ist hersteller-neutral, ein non-profit Verband

Community Meeting

CompTIA COMMUNITY

DACH

Der heutige Tag

Seeheim am 16. November 2023

09:30-10:00	Registrierung und Kaffee
10:00-10:10	**CompTIA Begrüßung** Katrin Giza – CompTIA
10:10-10:25	**Einführung in die CompTIA Community** Otto Schobert [Thefi], René Claus – Arcserve
10:25-11:00	**Keynote - Das Metaverse: Revolutionizing Communication and Collaboration** Christian Glessner - Hololux
11:00-11:15	**Fireside Chat**: Christian Glessner - Hololux & Norbert Neudeck - MailStore
11:15-11:30	Kurze Kaffeepause
11:30-11:50	**Women in Tech oder warum die IT weibliche Superkräfte braucht** Sandra Steinert-Ramirez – Women in Tech e.V.
11:50-12:10	**Panel Diskussion: Warum Frauen in Tech wichtig sind** Susanne Pfister - Niteflite, Géraldine Fricke-Bonin - Pax8, Rebecca Quinlain – Synaxon, Sandra Steinert-Ramirez – Women in Tech e.V.
12:10-13:15	Mittagessen im "Eat & Meet"
13:15-13:45	**AI im Marketing: Von Wundertools und Wirklichkeit mit Q&A** Annabelle Atchison - IONOS
13:45-15:00	**DACH Community World Café:** Cybersecurity - Stephan Schmidt – TCI Rechtsanwälte & Jürgen Ebner – Ebner e.U. / Workforce – René Claus – Arcserve / KI im Marketing – Annabelle Atchison IONOS
15:00-15:30	Kaffeepause
15:30-15:50	**Was sind die CompTIA Member Benefits?** Sameera Deen - CompTIA
15:50-16:15	**Zertifizierungspfade und das Partnerprogramm** Christina Allmeroth - CompTIA
16:15-16:45	**Keynote - Sailing the oceans of leadership & talent management** Hans Demeyer – Supplier of Optimism & Inspiration at Breinpiraten
16:45-17:00	**DACH Community – Zusammenfassung des Tages** Otto Schobert - [Thefi] and René Claus – Arcserve
17:00-22:00	Drinks, Networking und Abendessen ab 18:15 in der Bar „Last Call"

Seeheim am 17. November 2023

09:30-10:00	Registrierung und Kaffee
10:00-10:05	**CompTIA Begrüßung** Katrin Giza - CompTIA
10:05-10:20	**Einführung in die CompTIA Community** Maximilian Pfister – Niteflite, Otto Schobert - [Thefi], René Claus – Arcserve
10:20-10:50	**Keynote: MSP Cybersecurity: Lessons from the past and how to approach the future** Mostyn Thomas – Pax8
10:50-11:10	**Q&A** with Mostyn Thomas and Max Pfister
11:10-11:30	Kaffeepause
11:30-11:50	**CompTIA Cybersecurity Programs – with a special focus on ISAO** MJ Shoer - CompTIA
11:50-12:30	**ISO27001 für MSPs – sinnvolle Investition oder rausgeschmissenes Geld?** Max Pfister
12:30-13:30	Mittagessen im "Eat & Meet"
13:30-14:45	**MSP-Verträge - was ist drin enthalten, was nicht? Ein Erfahrungsaustausch.** Markus Rex - Synaxon
14:45-15:00	**DACH Community – Zusammenfassung des CompTIA Tages** René Claus – Arcserve
15:00-16:00	Networking bei Kaffee & Kuchen

#CompTIACommunity

Executive Council

CompTIA COMMUNITY

DACH

Bernd Ramgeus
Inhaber
dassys GmbH

Geraldine Fricke-Bonin
Team Lead DACH
Pax8

Jürgen Ebner
Geschäftsführer & IT Sicherheitsexperte
ICTE GmbH

Markus Rex
GM SYNAXON Services,
SYNAXON AG

Markus Bauer
Senior Technology Evangelist EMEA
Acronis Germany GmbH

Maximilian Pfister
CEO, Niteflite Networxx GmbH

Norbert Neudeck
Director of Sales
MailStore Software GmbH

Otto Schobert
Geschäftsführender Gesellschafter
[thefi.com] GmbH & Co KG

Peter Feige
Geschäftsführender Gesellschafter
TechnoSoft Consulting GmbH

René Claus
EMEA Sales Director
Arcserve

Robert Sieber
Inhaber
MSP-Support GmbH

Together, We Are The CompTIA COMMUNITY

Otto Schobert

Geschäftsführender Gesellschafter
[thefi.com] GmbH & Co KG
CompTIA DACH Community
Executive Council Chair

René Claus

Technology Professional
CompTIA DACH Community
Executive Council Vice Chair

Maximilian Pfister

Maximilian Pfister
CEO Niteflite
Networxx GmbH

Together,
We Are The CompTIA
COMMUNITY

MSP Cybersecurity:

Lessons from the past and how to approach the future

Mostyn Thomas

Pax8

MSP Cybersecurity:
Lessons from the past and how to approach the future

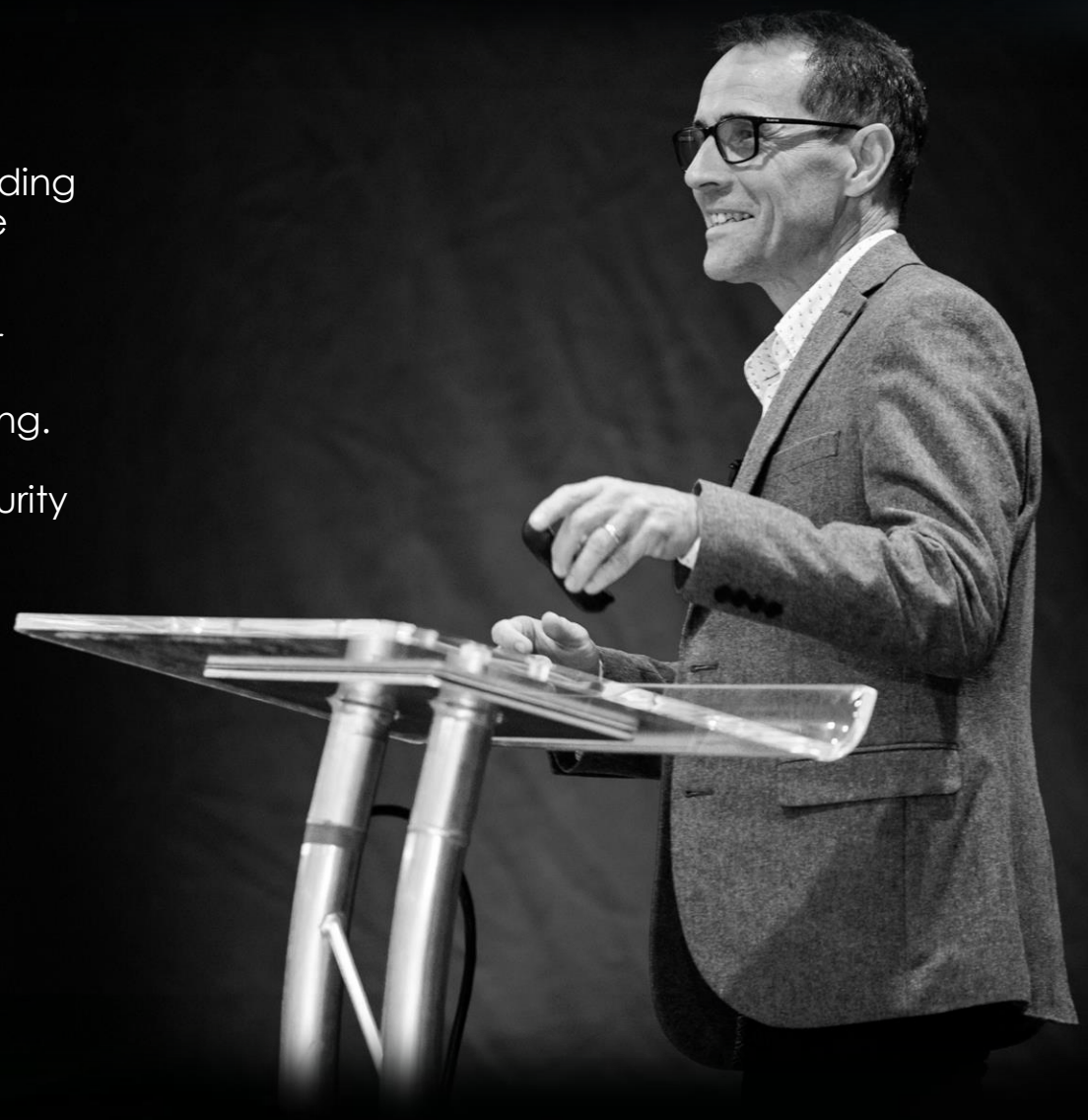
Mostyn Thomas

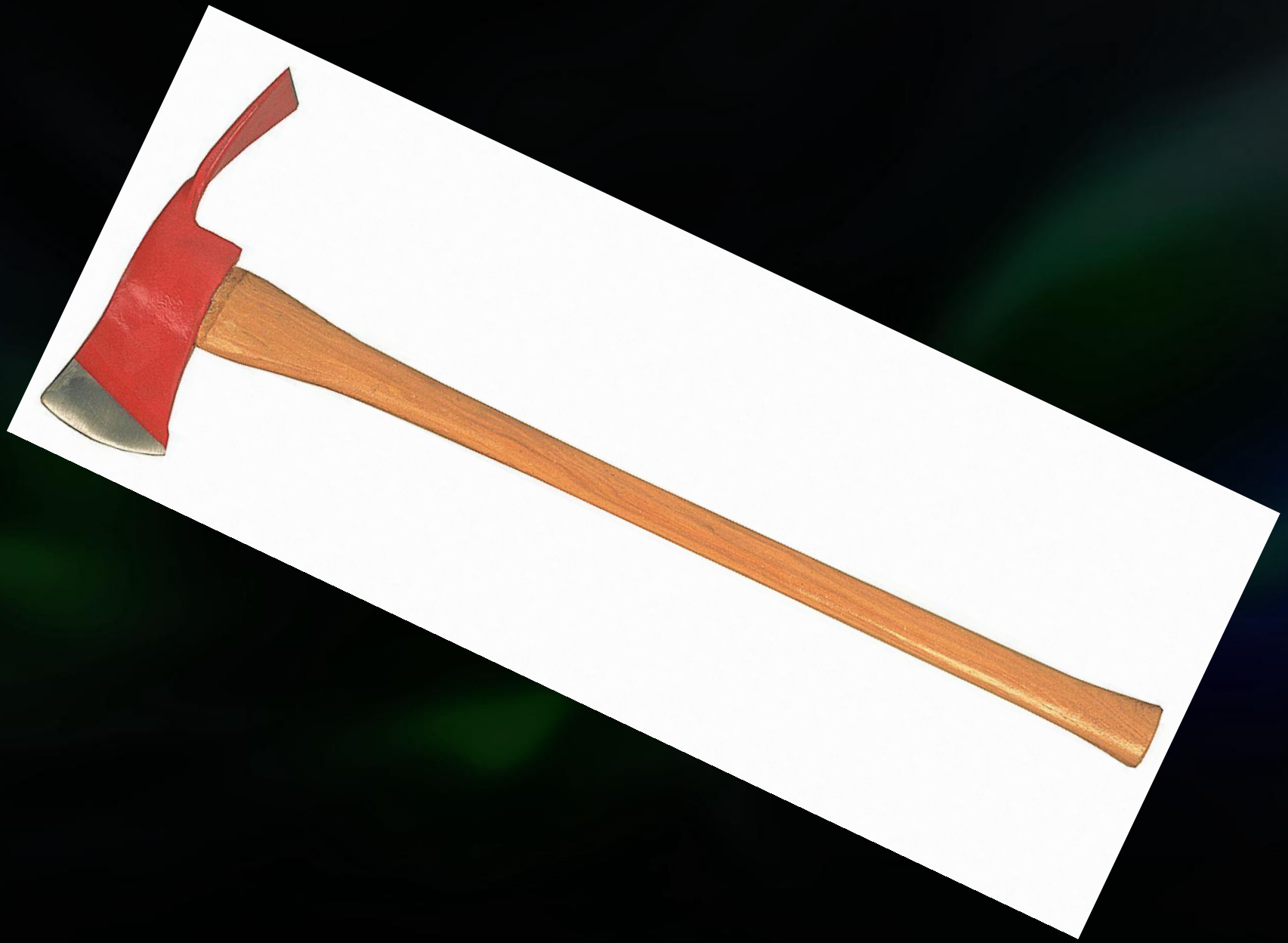
Senior Director of Security, Pax8

20 years experience working with MSPs, including founding and running Astrix integrated systems in 2001, which he sold in 2018 to concentrate on cyber security.

Much of his work with MSPs is to deliver effective cyber security solutions to the MSP company itself and their customers through best practice and awareness training.

In addition to his unique experience, Mostyn holds security certifications from Comptia, british computer society, national cyber security centre and is a qualified cyber essentials assessor.





MANN GULCH FIRE

National Register of Historic Places

On August 5th, 1949, a lightning caused wildfire entrapped a smokejumper crew in this steep canyon. Before it was controlled it took the lives of 13 men and burned nearly 5,000 acres.

The lessons learned from this tragic event continue to influence wildland fire fighting.

FOREST SERVICE
US
DEPARTMENT OF AGRICULTURE

Helena National Forest


VENTURA COUNTY
FIRE DEPT.

© Getty Images/M. Tama


IRON MOUNTAIN
0800 270 270
www.ironmountain.co.uk

Causes of Lehman Bros Bankruptcy

1. **Risk** - $639b assets - $613b in debt - trouble was the assets were difficult to sell and when they needed the case they had no cash flow.

2. **Culture** - Management rewarded excessive risk-taking – too much Profit driven

3. **Overconfidence** investing in complex high risk products that they did not really understand the risk and how the market was moving

4. **Regulator inaction** – authorities knew but did not do anything – "Too big to fail"

Cybersecurity statistics you need to know

43%	43% of EU Cyber Attacks target Small Business
99.9%	Attempted Microsoft account hacks blocked when MFA in place
74%	74% of the ransomware attacks on German companies were via phishing emails
70	German employees use an average of 70 passwords each. Average of 13 reused.
€92,700	The average EU BEC attack attempted to steal €92,700

Poll

Do you use a password management tool?

Are you currently implementing MFA?

Multi Factor Authentication

- Something you ***know***, such as a password or PIN
- Something you ***have***, or possess, such as a badge or smartphone
- Things you ***are***, such as a biometrics (fingerprints or face recognition)

When Given an option

- **60%** of consumers enable MFA for online banking
- **61%** of consumers enable MFA for online healthcare portals and apps
- **60%** of consumers enable MFA to access insurance accounts

- **73%** of consumers do not enable MFA for cryptocurrency accounts
- **70%** of consumers do not enable MFA when using social media
- **80%** of consumers do not enable MFA when online gambling
- **77%** of consumers do not enable MFA when using streaming services

Prove Identity MFA report 2023

What do they have in common?

facebook

540 Million

500 Million

106 Million

myfitnesspal

151 Million

Zaun
Fencing

Strix Group
Kettles

Optus
Communication

Gateley
Law

Uber
Travel

Neopets
Virtual Community

Small Business Examples

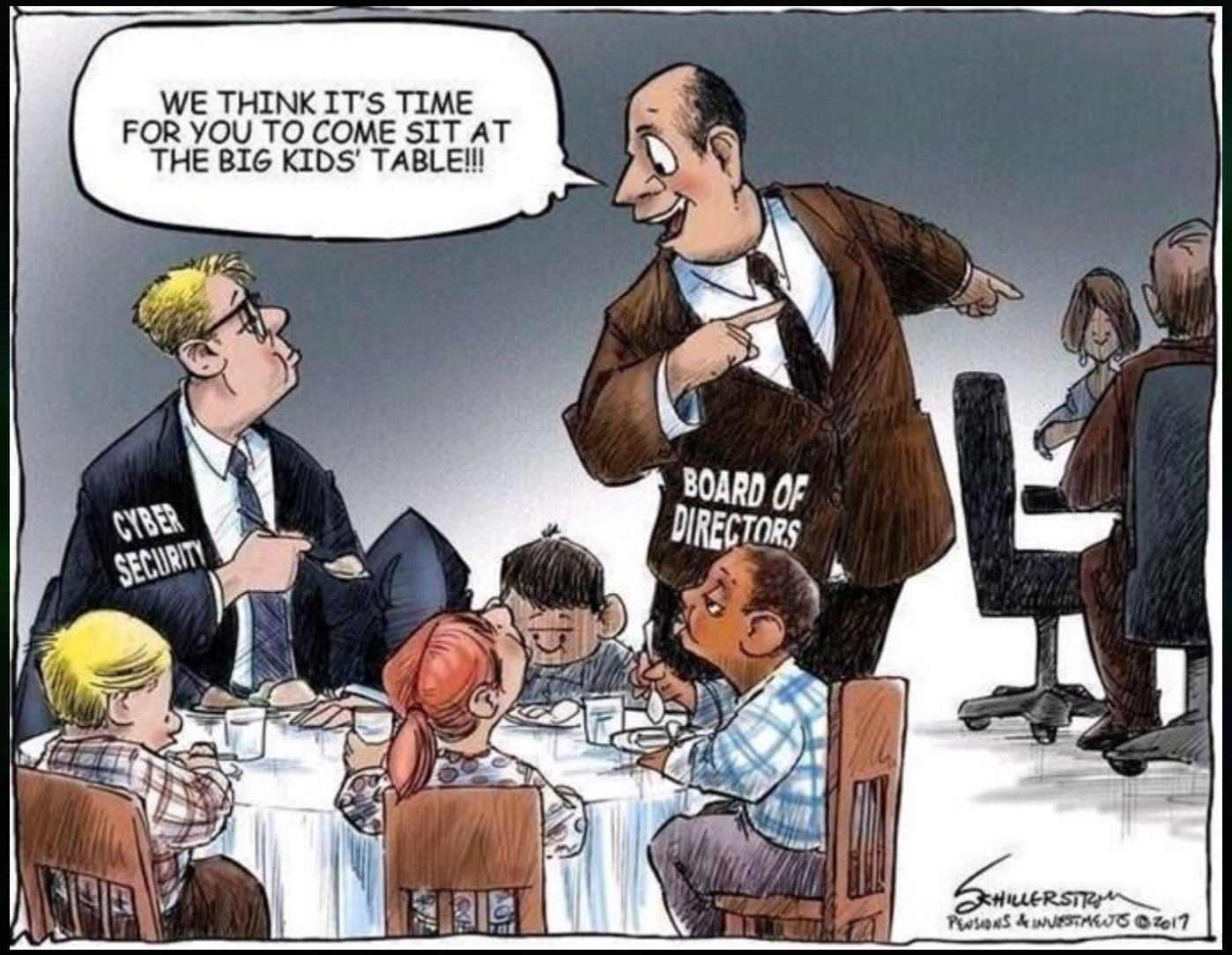
- Scottish based engineering company
- Had 2FA in place – app based
- No cyber insurance
- Not clear if user had admin permissions
- Phishing email
- Aitm attack : session cookies/proxy to setup second MFA device
- Supply chain fraud: threat actor waited until the right moment to interact with victim's clients

£130,000
Legal fees
Reputation
Tech costs

Observations on MSP cyber security

- Not getting the basics right – at least not consistently
- Technical staff still logging on as admin
- No separate admin accounts for PC, servers etc
- Lack of visibility of vulnerabilities on their network
- Often no detailed risk register or breach plan
- Recording and retaining logs not common
- Internal user awareness training or testing missing
- MSP supply chain is NOT secure
- Not following a recognised Cybersecurity framework

Building best practice and the changing role of the MSP



Building best practice and the changing role of the MSP

Get your own house in order – Make sure your MSP Cybersecurity is effective

Embrace Governance, Risk and Compliance (GRC)

Frameworks and certification

Get to those clients Board tables

Follow the data

Continuous learning and research

Partnerships

Hurdles for changing the cyber security approach

The essentials of cyber security

CIS Controls

CIS Controls v8:

There are 3 levels of Implementation Group :

IG1: Basic Cyber Hygiene

IG2: Includes IG 1 plus further controls

IG3 Includes IG1&2 and all the controls and safeguards

CIS Controls v8:

There are 18 areas of control :

The IASME Cyber Baseline Standard

The Cyber Baseline scheme is designed to improve the basic cybersecurity practices of organisations in the same way that the Cyber Essentials Scheme does in the UK and provide a certification scheme to prove compliance.

- Based mainly on CIS 8.0 controls
- Aimed at any country outside of UK, Europe particularly
- Will have a certification scheme
- Will be seeking Certifying bodies in every country
- Launched on 9th Oct 2023

IASME CYBER BASELINE

IASME CONSORTIUM

What have we observed?

Face facts:
Perform an honest and realistic appraisal on your cyber risk, think like a hacker

Culture:
Aim to have all staff onboard with cybersecurity practice by altering the culture of the organisation.

Back to basics:
Although new and sophisticated tools and techniques are out there, start with getting the basics done really well

Use your own knowledge:
Be like Wag and think what will work for your organisation and what will not work

Monitor yourself:
In the absence of regulation, be your own regulator, follow a framework relevant to you

5 Laws of cybersecurity

Law 1: If there is a vulnerability, it will be exploited, no exceptions

Law 2: Everything is vulnerable in some way

Law 3: Humans can trust when they shouldn't

Law 4: With Innovation comes opportunity for exploitation

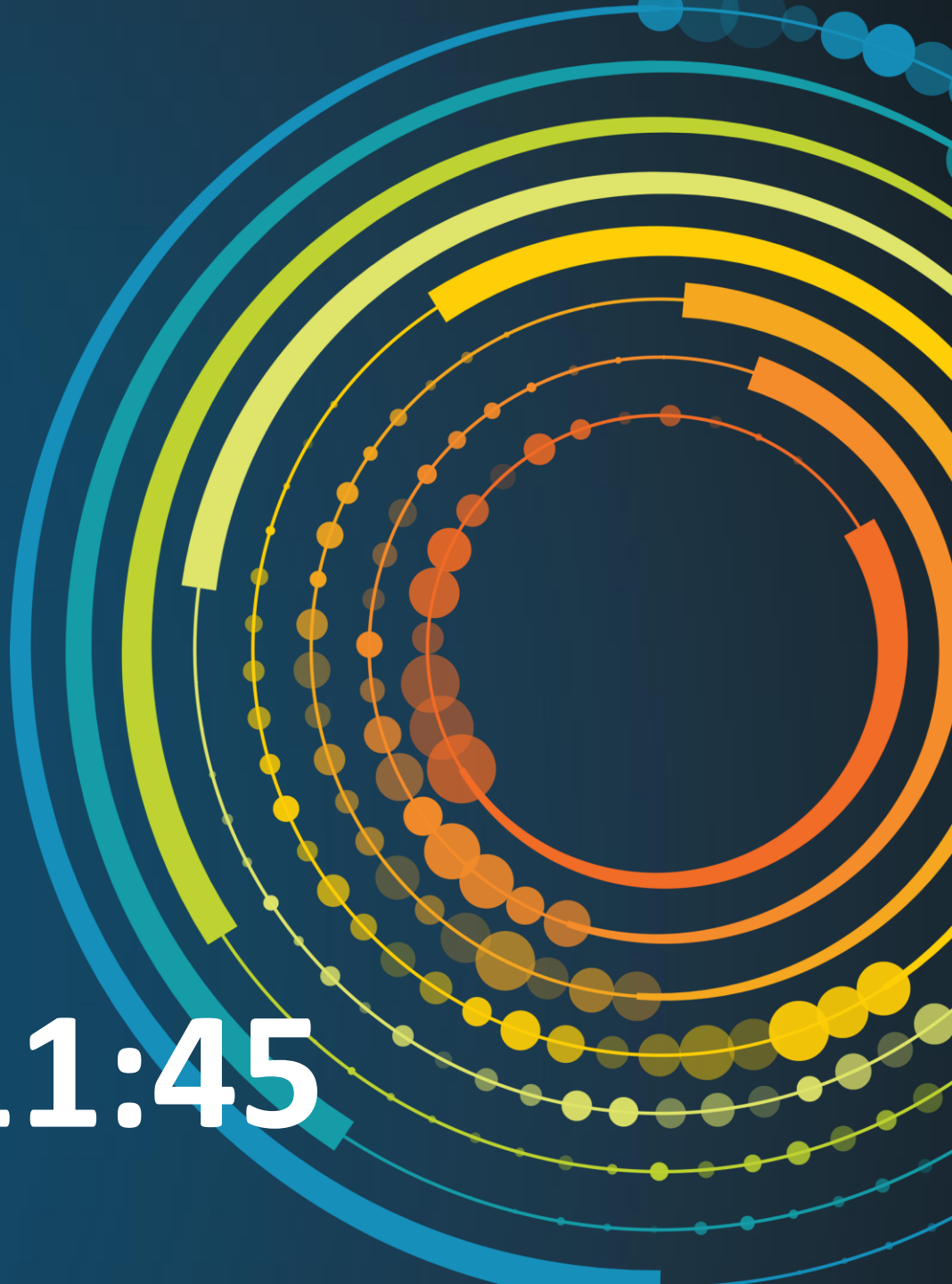
Law 5: When in doubt, see Law 1

Credit Mark Espinosa

Cybersecurity Masterclass

With Mostyn Thomas
6th December 2023
Frankfurt

‘Really excited from today's in-person event with the team here at Pax8. Working on some amazing solutions around **#cybersecurity** for clients in an open workshop collaborating with other IT businesses.’



Kaffeepause bis 11:45

Together,
We Are The CompTIA
COMMUNITY

CompTIA Cybersecurity Programs

Sameera Deen
Senior Specialist,
Member Relations at
CompTIA

- Connecting to an incredibly powerful network of more than 800 tech vendors, MSPs/solution providers and business technology consultants on the front lines of cybersecurity.
- Gaining allies that are working together to share information about the latest cybersecurity risks.
- Thwarting the malicious attacks that threaten our businesses, our customers and the credibility of our industry.
- Enhancing your reputation and thought leadership in the tech and security industries.
- Demonstrating social and cybersecurity responsibility.

CompTIA ISAO - FREE to ALL MSP/solution provider members

- Cyber Forum – online forum, safe space for discussion and collaboration
- Informational and Actionable Threat Reports
  - Easy to understand, with threat analysts comment
  - Access to Splunk / TruStar Threat Intelligence Management
- Access to Sophos X-Ops Intelix
- Access to Cyber Risk Rating powered by Security Scorecard
- Monthly Member Meetups every 3rd Wednesday, 2 sessions for our global members
- Access CompTIA ISAO Cyber Forum from my.CompTIA.org

ne
erWeekly Podcast
king News! Podc...
er Risk Rating
ms
s Feeds
ources
hos X-Ops Intelix
eat Reports
TAR Login
nbers
CompTIA
Documents
erence Center

Forum list | Threads | Latest activity 10+ | Posts | Questions | Resources

Create

1 2 3 ... 146 Next ›

Set default

INFORMATIONAL TLP:GREEN Zero-Days in Edge Devices Become China's Cyber Warfare Tactic of Choice
Cariza Schiavone · Yesterday at 3:03 PM · Threat Intelligence
China's Cyber Warfare Tactics
0 ratings
Updated: Yesterday at 3:03 PM

ACTIONABLE Severity: Medium TLP:GREEN LockBit Ransomware Exploits Citrix Bleed in Attacks, 10K Servers Exposed
Asim Subedi · Yesterday at 2:36 PM · Threat Intelligence
Ransomware Attack
0 ratings
Updated: Yesterday at 2:36 PM

INFORMATIONAL TLP:GREEN 82% of Attacks Show Cyber-Criminals Targeting Telemetry Data
Asim Subedi · Yesterday at 2:35 PM · Vendor Reports
82% of Attacks Show Cyber-Criminals Targeting Telemetry Data
0 ratings
Updated: Yesterday at 2:35 PM

INFORMATIONAL Severity: Medium TLP:GREEN BlackCat Ransomware Gang Targets Businesses Via Google Ads
Jonathan Braley · Yesterday at 10:34 AM · Threat Intelligence
Ransomware
0 ratings
Updated: Yesterday at 10:34 AM

INFORMATIONAL Severity: Low TLP:GREEN DDoS Attacks Underscore the Vulnerability of Public Systems
Asim Subedi · Tuesday at 4:53 PM · Threat Intelligence
DDoS Attack
0 ratings
Updated: Tuesday at 4:53 PM

Filter

In category:
- Cyber Forum Policies
- Cyber Genius Videos
- Help Documents
- Member Resources
- Threat Reports

- Watched resources
- Watched categories
- All
- People you follow
- People that follow you

Save

CompTIA CYBERSECURITY Emergency Response Team

- MSP911.org
- Launched in North America March 2023
- Free assistance to any MSP/solution provider experiencing a cybersecurity incident
- Launched by victims of the July 2022 Kaseya attack
- This is NOT incident response
- Provides a coach to help you through the critical initial hours/days
- Live call center 24/7

CompTIA CYBERSECURITY Trustmark

- Organizational Accreditation designed specifically for MSPs/solution providers to establish a foundational security program for their organisation
- Based on industry accepted best practices across varying controls from globally recognized frameworks
- Includes access to a GRC Platform
- Participant discussion in the CompTIA ISAO Cyber Forum (private group)
- Weekly calls with Platform Partners, FortMesa and Cybersecurity Program Team members to help you succeed
- Join over 800 companies from 25 countries!

Thank you!

CompTIA
CYBERSECURITY
Trustmark

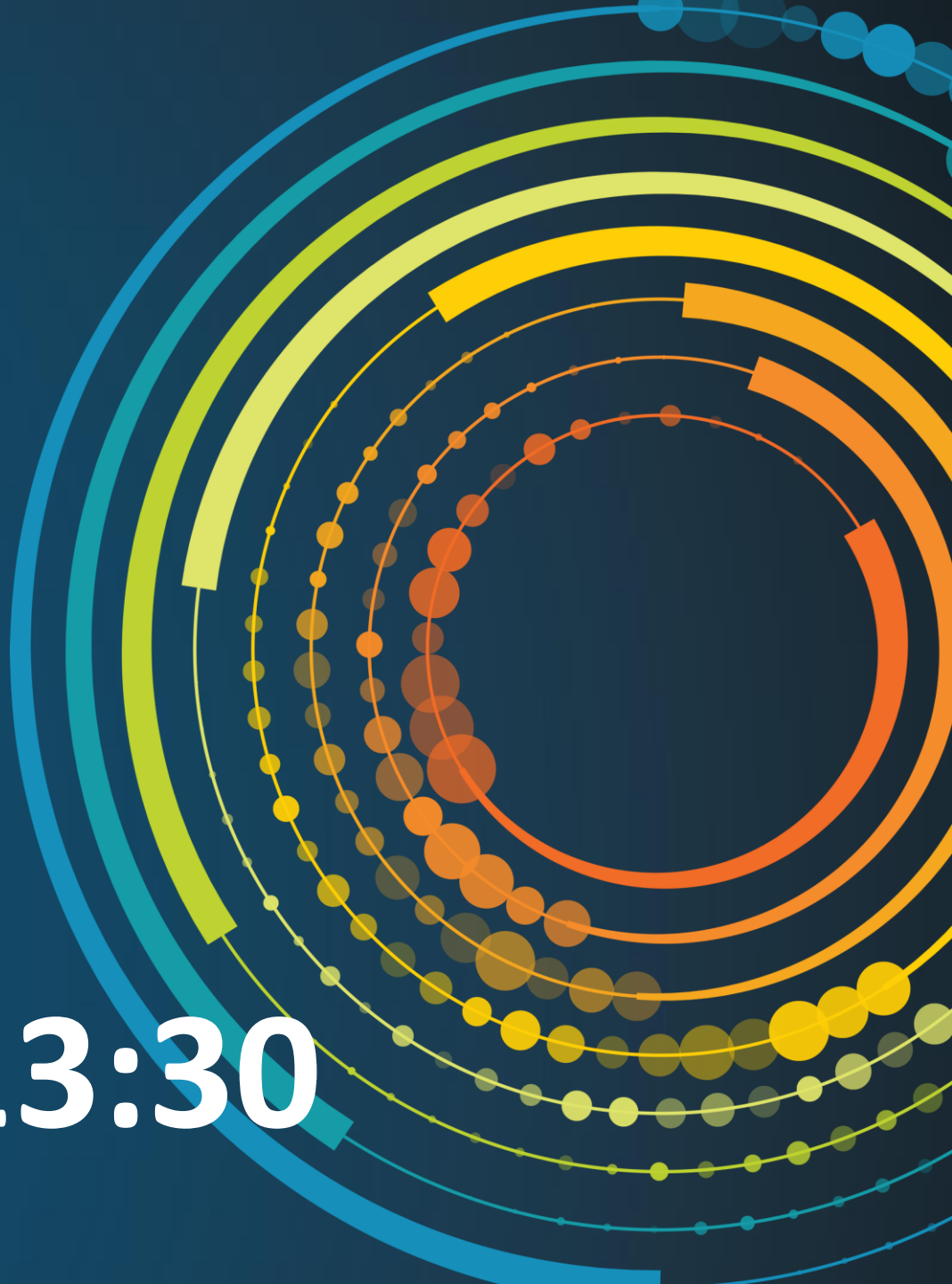
Learn more and join the waitlist!

Together,
We Are The CompTIA
COMMUNITY

ISO27001 für MSPs – sinnvolle Investition oder rausgeschmissenes Geld?

Max Pfister

Niteflite Networxx GmbH



Mittagessen bis 13:30

Together,
We Are The CompTIA
COMMUNITY

MSP-Verträge - was ist drin enthalten, was nicht? Ein Erfahrungsaustausch.

Markus Rex

Synaxon AG

Together,

We Are The CompTIA COMMUNITY

René Claus

Technology Professional

CompTIA DACH Community

Executive Council Vice Chair

Rückblick

- Zusammenfassung
- Meine “Key-Takeaways”
- Danke an alle Teilnehmer und Beteiligten!

Networking bei Kaffee und Kuchen

We Are The CompTIA COMMUNITY

VIELEN DANK!