CompTIA COMMUNITY

Welcome

UK&I Cybersecurity Interest Group
Presents: The Untold Story Of A Cyber Attack

18 Jan 2024

WE ARE THE

CompTIA®

COMMUNITY

Leanne Johnson

CompTIA

WE ARE THE CompTIA COMMUNITY

Kris Nagamootoo
CompTIA

Sam Ross
CompTIA

CompTIA COMMUNITY

Antitrust, Diversity, and Anti-Harassment

- Antitrust
  You must not engage in discussions that could result in an unreasonable restraint of trade.
  https://connect.comptia.org/about-us/antitrust-statement

- Diversity
  We promote an inclusive environment that respects and values all individuals.
  https://connect.comptia.org/about-us/dei-policy

- Anti-Harassment
  This is a respectful and safe environment for all. Any verbal, physical, or psychological harassment will not be tolerated.

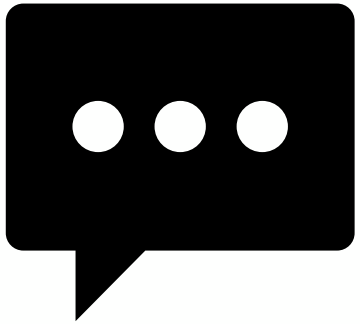
  https://www.comptia.org/contact-us/harassment-complaint

Please report any violation of the above policies to CompTIA staff immediately.
Violators will be removed from the event or meeting.

CompTIA COMMUNITY

WIFI: MP_conference

Password:
Conference2022@MP



CompTIA COMMUNITY

- 1:00pm Welcome **Leanne Johnson**, CompTIA
- 1:10pm CompTIA Communities and Committees **Dan Scott**, ConnectWise (UK&I Community Chair)
- 1:25pm CompTIA's Cyber Ready Program **Zeshan Sattar**, CompTIA
- 1:35pm MSP & Cyber Threat Landscape **Greg Jones**, Datto/Kaseya (UK&I Cybersecurity Committee Chair)
- 1:45pm The BIG Customer Hack **Andrew Allen**, Aabyss
- 2:05pm Understanding the Why & What Behind An Attack **Lewis Warner**, Pentiq
- 2:50pm The BIG MSP Hack **Greg Jones**, Datto/Kaseya and **Ken Roulston** Ex2 Consultancy
- **3:20pm NETWORKING BREAK until 3:50pm**

CompTIA COMMUNITY

- **3:20pm NETWORKING BREAK until 3:45pm**
- 3:50pm A Regional Perspective **Hollie Whittles**, Purple Frog Systems (UK&I Community Vice Chair)
- 4:05m What Happens In The Event Of An Attack? **Trevor Cornbill**, TechInsure
- 4:20pm What You Need In Place From A PR Perspective **Rahme Mehmet**, TechComms
- 4:40pm What Does CompTIA Offer That Could Help You? **Wayne Selk**, CompTIA
- 5:10pm Top Cyber Resources and Takeaways **Kyle Torres**, Sophos (UK&I Cybersecurity Vice Chair)
- **6:00pm NETWORKING DRINKS & CANAPES**

WE ARE THE

CompTIA®

COMMUNITY

Dan Scott
ConnectWise

CompTIA COMMUNITY

Global Communities

ANZ
ASEAN
Benelux
DACH
North America
UK&I

Industry Advisory Councils

Artificial Intelligence
Blockchain & Web3
Channel Development
Cybersecurity
IoT
SaaS Ecosystem

CompTIA ISAO

Executive Steering Council

Committees

with New Global Task Force

Cybersecurity
DEI
Emerging Technology
Managed Services

Technology Interest Groups

Artificial Intelligence
Blockchain
DEI
Drone
IoT

- 1:25pm CompTIA's Cyber Ready Program **Zeshan Sattar**, CompTIA
- 1:35pm MSP & Cyber Threat Landscape **Greg Jones**, Datto/Kaseya (UK&I Cybersecurity Committee Chair)
- 1:45pm The BIG Customer Hack **Andrew Allen**, Aabyss
- 2:05pm Understanding the Why & What Behind An Attack **Lewis Warner**, Pentiq
- 2:50pm The BIG MSP Hack **Greg Jones**, Datto/Kaseya and **Ken Roulston**, Ex2 Consultancy
- **3:20pm NETWORKING BREAK until 3:45pm**

WE ARE THE

CompTIA®

COMMUNITY

Zeshan Sattar
CompTIA

CompTIA Cyber Ready

SC 2022 awards EUROPE WINNER

Try Hack Me

Department for Science, Innovation & Technology

Foreign, Commonwealth & Development Office

Cyber First

UK CYBER SECURITY COUNCIL

Department for Education

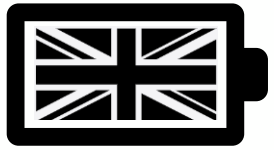
GREATER MANCHESTER DOING DIGITAL DIFFERENTLY

DIGITAL SKILLS PARTNERSHIP LANCASHIRE

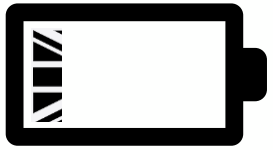
West Midlands Combined Authority

CyberReadyTIA

Background: The need for Cyber Ready

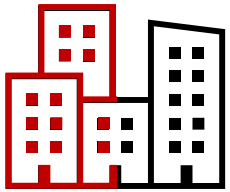


The UK needs 18,200 Cyber Security Professionals annually



Currently there is an annual shortfall of 11,200 Professionals

37% of Vacancies are unfilled due to lack of **T**echnical skills



50% of UK businesses lack basic **T**echnical skills

17% of the UK cyber workforce are Women*

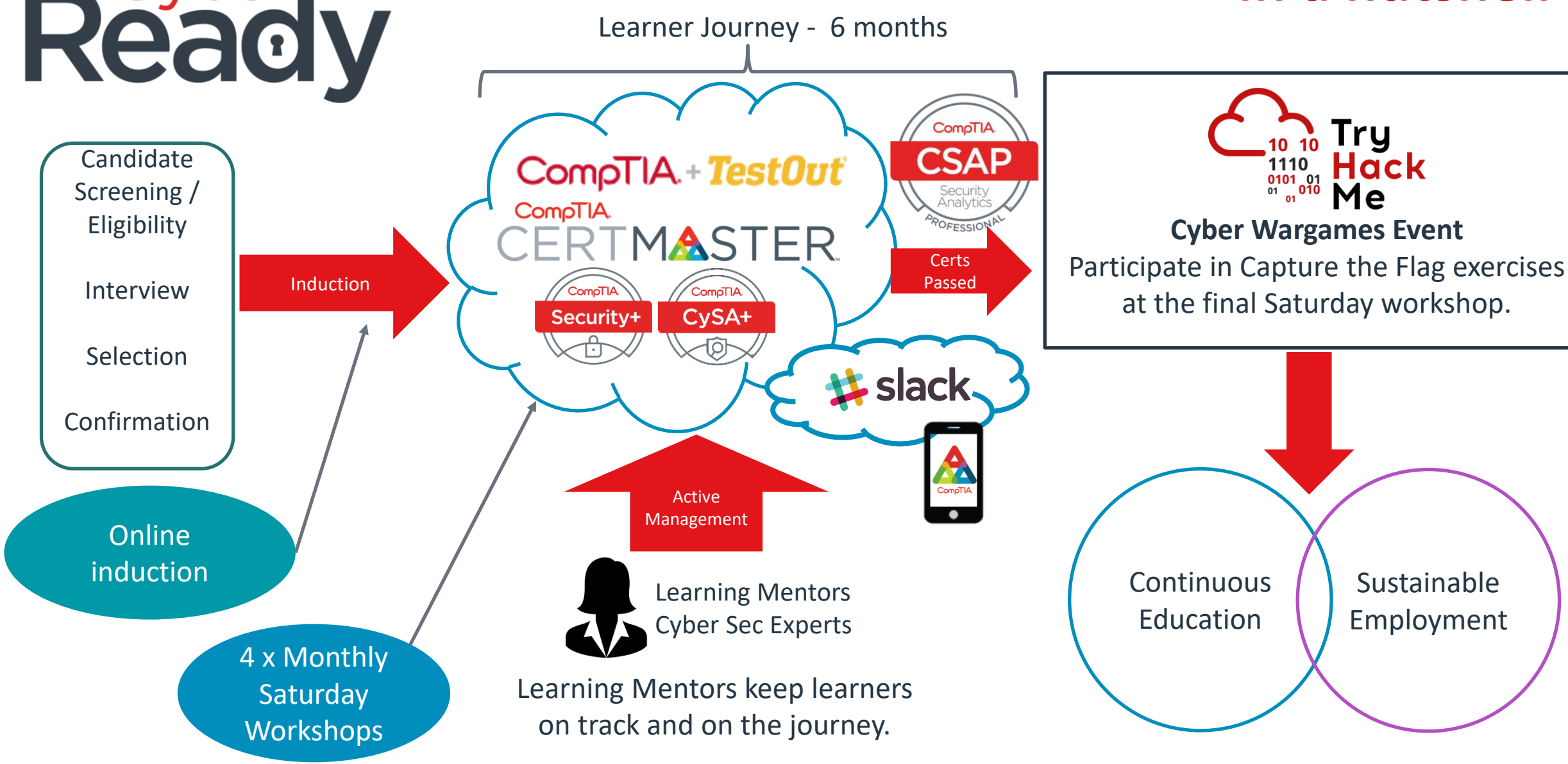
22% of the UK cyber workforce are from Ethnic Minorities*

12% of the UK cyber workforce are neurodivergent*

*Only 14% of Women and 14% of those from an Ethnic Minority background are in Senior Roles

Cyber Ready

"In a nutshell"



Cyber Ready

Reaching Individuals from Diverse Backgrounds

Our programme is aimed at increasing diversity in the cyber workforce, and we actively attract:

Returnees to the workforce (carers) who have prior IT experience

People working in a different sector but are **IT hobbyists**

Unemployed or facing redundancy due to volatile economic conditions or job loss due to automation

Individuals **working in first-line IT roles** and looking to progress

Graduates who have undertaken a tech degree but are unable to find employment

- We actively promote the programme to hard-to-reach groups, including:
  - Women
  - Ethnic Minorities
  - Neuro Diversity
  - Socially mobile individuals

Cyber Ready

Skills Gained with Cyber Ready

Cyber Ready

Approx. **200** Candidates Reached across UK & Middle East

100	68	25	43	33
Ethnic Minority Candidates	Female Candidates	Neuro Diverse Candidates	Socially Mobile Candidates	Average Age

Cyber Ready >> Successes to date

96% CompTIA Security+ Certified!

83% CompTIA CySA+ Certified!

85% of candidates secured Cyber Security roles at **Airbus**, **BAE Systems**, **Claranet**, **DWP**, **ECSC**, **Fujitsu**, **Lloyds Banking Group**, **Ministry of Defence**, **NHS**, **Racing Post** **Sainsburys**, **Sellafield**, **Thales**, **Tata Consultancy Services**, or have been recognised and added value to their current organisation.

Get involved - Cyber Ready is back in 2024!

- Our focus areas are:
  - Lancashire
  - West Midlands
  - West Yorkshire
- We need your help to:
  - Become guest speakers at our workshops
  - Promote the programme to potential candidates
    - Can be your staff!

Share our Cyber Ready webpage

- https://www.comptia.org/content/lp/cyber-ready
- Please talk to me if you want to be a guest speaker
- Share our promotional activity on social media

- 1:35pm MSP & Cyber Threat Landscape **Greg Jones**, Datto/Kaseya (UK&I Cybersecurity Committee Chair)
- 1:45pm The BIG Customer Hack **Andrew Allen**, Aabyss
- 2:05pm Understanding the Why & What Behind An Attack **Lewis Warner**, Pentiq
- 2:50pm The BIG MSP Hack **Greg Jones**, Datto/Kaseya and **Ken Roulston**, Ex2 Consultancy
- **3:20pm NETWORKING BREAK until 3:45pm**

WE ARE THE

CompTIA®

COMMUNITY

Greg Jones
Kaseya / Datto

MSP / SMB Cyber Threat Landscape Update

Greg Jones
VP of Business development EMEA

Kaseya / Datto

Living in a golden age of tech

Surely this is a good thing?

Attacks/Breaches | 5 MIN READ | NEWS

Attackers Are Already Exploiting ChatGPT to Write Malicious Code

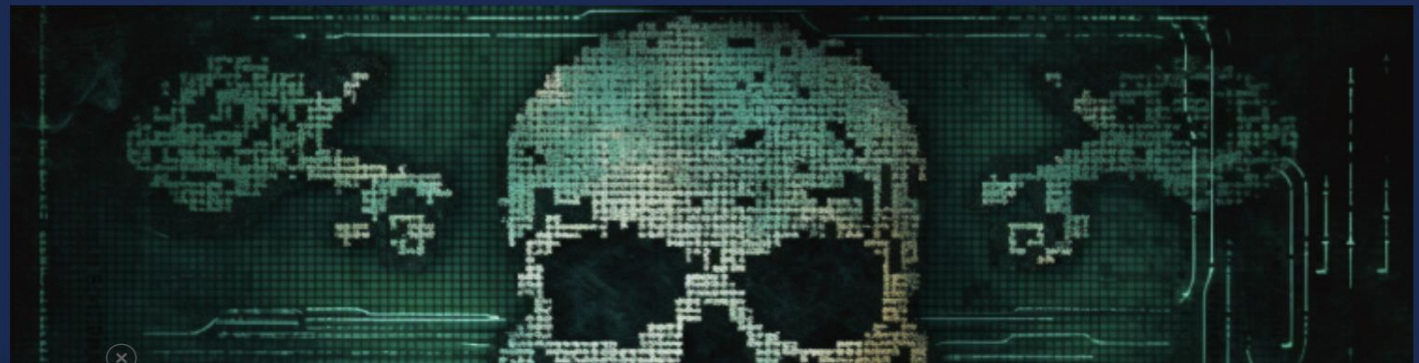
The AI-based cha
malware.

AI-Powered Malware Holds Potential For Extreme Consequences

Could Artificial Intelligence Be a Black Ball

Home / AI & Machine Learning / AI-Powered Malware Holds Potential For...

AI-powered malware is a growing security concern, CyberArk survey finds



Attacks Continue to Rise

300%

Increase in reported CyberCrimes since Covid-19

92.7%

Ransomware attacks have nearly doubled

59%

MSPs said remote work increased ransomware attacks

Who are the Bad guys?

Who Are The Threats…

Hacking Collectives
Ethical hackers — break into systems to help make technology more secure. “white-hat hackers”

IoT Hackers
Think your Alexa is safe?

Ransomware Developers
Over £7 Billion pounds in damages since 2018

Nation State
Countries that don’t seem to like the UK

Organized Crime
Gangs, mobs, and things that go bump in the night

Insider Threats
£19 billion lost every year in secrets

Script Kiddies
Lacks programming knowledge - uses existing software to launch attacks. Uses programs without knowing how they work or what they do.

Hacktivist
Hackers with a political goal

Malware Developers
Starting as low at £30 - you to can own a copy of any popular Malware

Mobile Malware
Have an iPhone or Android phone? Think you’re safe? Think again.

RYUK

CONTI

TRICKBOT

How Modern Threats Have Evolved

Attackers have adopted new methods to bypass endpoint protection

Modern trends include:

Living Off The Land - “Why deliver my malicious program when I can make your existing admin tools do the work for me?”

Staged Malware & Attacks - Individually, each stage is benign

Disabling Endpoint Protection - Many attacks seek to disable AV and defensive tools before dropping their final stage (e.g. Ransomware)


DXRACER

Casino Gets Hacked Through Its Internet-Connected Fish Tank Thermometer

Sunday, April 15, 2018 Wang Wei

Ask yourself:

Are you ready.....

We hope today's event brings you one step closer to saying YES!

- 1:45pm The BIG Customer Hack **Andrew Allen**, Aabyss
- 2:05pm Understanding the Why & What Behind An Attack **Lewis Warner**, Pentiq
- 2:50pm The BIG MSP Hack **Greg Jones**, Datto/Kaseya and **Ken Roulston**, Ex2 Consultancy
- **3:20pm NETWORKING BREAK until 3:45pm**

WE ARE THE

CompTIA®

COMMUNITY

Andrew Allen
Aabyss

- 2:05pm Understanding the Why & What Behind An Attack **Lewis Warner**, Pentiq
- 2:50pm The BIG MSP Hack **Greg Jones**, Datto/Kaseya and **Ken Roulston**, Ex2 Consultancy
- **3:20pm NETWORKING BREAK until 3:45pm**

WE ARE THE

CompTIA®

COMMUNITY

Lewis Warner
Pentiq

in/lewiswarner/

CREST Registered Penetration Tester (CRT Pen)
CREST - www.crest-approved.org

Offensive Security Certified Professional (OSCP)
Offensive Security

Cyber Essentials Assessor
The IASME Consortium

Cyber Essentials PLUS Assessor
The IASME Consortium

IASME Governance Assessor
The IASME Consortium

TigerScheme Qualified Security Team Member (QSTM/CTM)
University of South Wales

CompTIA Security+
CompTIA

Cisco Certified Network Associate (CCNA)
Cisco

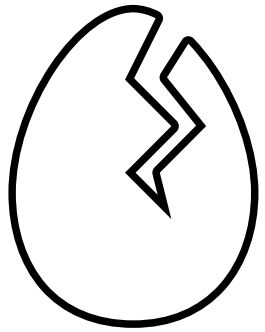
$~: whoami

CompTIA COMMUNITY

- Common Terminology.
- The Who and Why.
- Changes in the Security Landscape.
- The Mindset of an Attacker.
- Common Vulnerabilities in MSP environments.
- Closing thoughts before a brief Q&A

What are we going to cover?

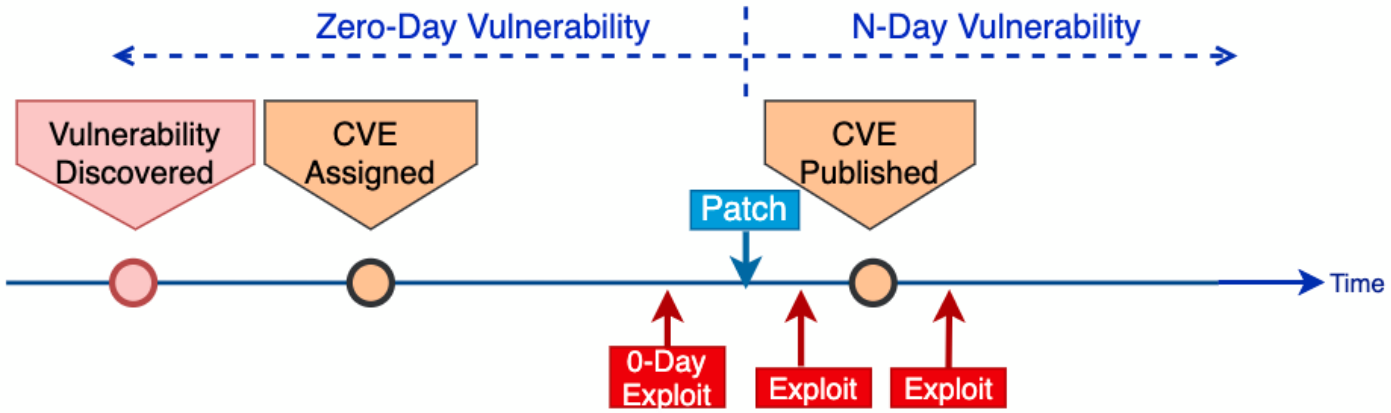
- Asset
- Threat
- Vulnerability



CVSS
COMMON VULNERABILITY SCORING SYSTEM

Risk =

A + T + V



Common Terminology

CompTIA COMMUNITY

"A Cyber Threat Actor (CTA) is a participant (person or group) in an action or process that is characterised by malice or hostile action (intending harm) using computers, devices, systems, or networks. CTAs are classified into one of five groups based on their motivations and affiliations:"* *https://www.cisecurity.org/

Cyber Threat Actors

CompTIA COMMUNITY

ANNUAL REVIEW

NCSC Annual Review 2023

This year we received an all-time high of 2005 reports*, an increase of almost 64% from last year's 1226.

The NCSC issued 24.48 million notifications, informing organisations that they were experiencing a cyber incident, through our automated Early Warning service.

327 incidents involving the exfiltration/extortion of data (18.5% increase on last year.)

- **Compliance** (ISO27001, ISO22301, PCI-DSS, Cyber Essentials, SOC 2).
- **GDPR/Data Protection Laws**
- **Supply Chain and Client Requirements**
- **To protect your Organisation**

Why?

CompTIA COMMUNITY

Infrastructure
(Cloud, Routers, Firewalls, Switches, …)

Network Services
(SSH, VPN, SNMP, SMTP, Telnet, FTP, DNS, SNMP, …)

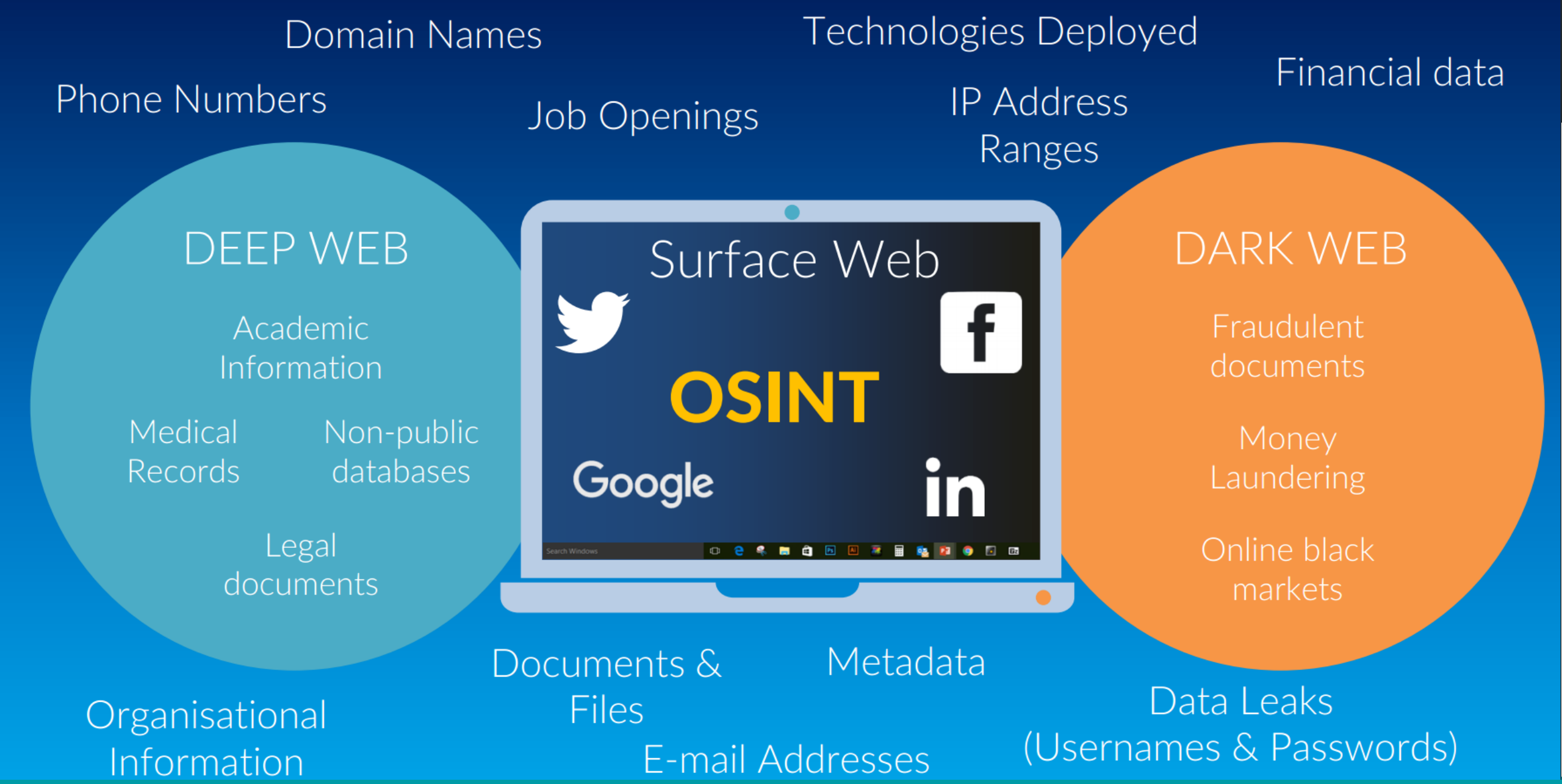
Servers & Endpoints
(Operating System, Services, and applications)

Web Applications
(Web Technologies, Frameworks, Content Management Systems, Databases)

Internal & Wireless Networks
(VLANs, Passwords, Privileges, On-Prem/Hybrid, Remote Working.)

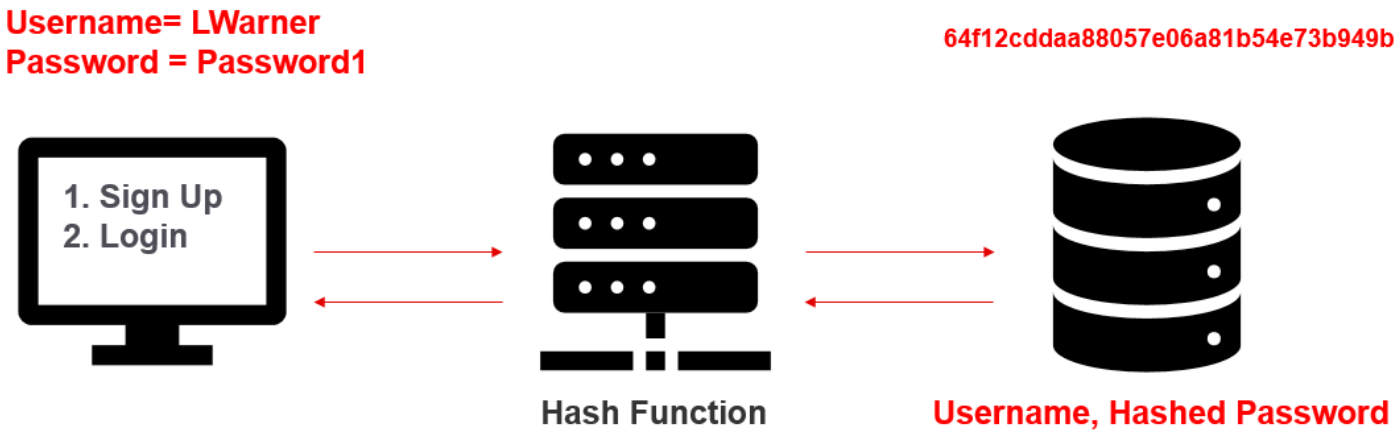
Employees
(Social Engineering, Phishing, Insider Threat)

Thinking like an Attacker

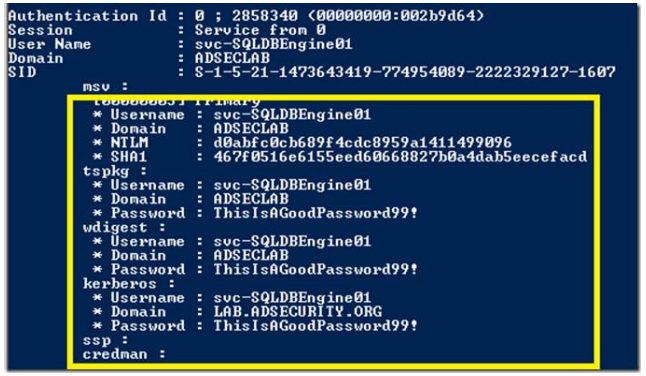

Domain Names
Technologies Deployed
Financial data
Phone Numbers
Job Openings
IP Address Ranges
DEEP WEB
Academic Information
Medical Records
Non-public databases
Legal documents
Surface Web
OSINT
Google
DARK WEB
Fraudulent documents
Money Laundering
Online black markets
Documents & Files
Metadata
Organisational Information
E-mail Addresses
Data Leaks (Usernames & Passwords)

How?

- Interception
- Brute force
- Key logging
- Manual guessing
- Shoulder surfing
- Stealing passwords
- Stealing hashes
- Phishing & coercion
- Data breaches
- Password spraying

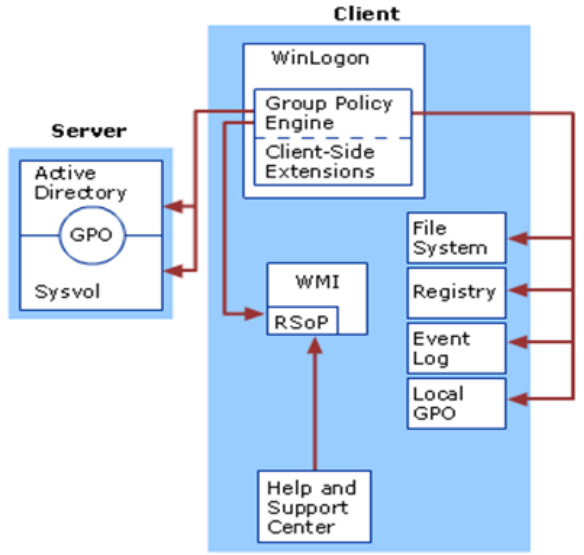


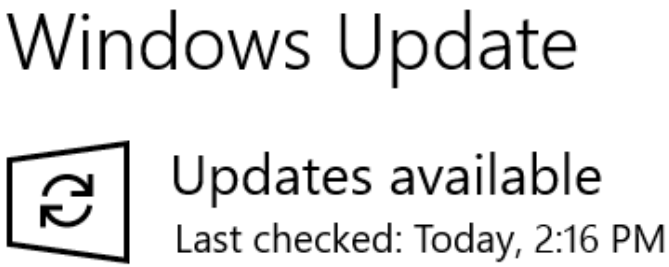
NTLM Cracker Page - Over 312.072 billion cracked NTLM hashes ...
https://hashkiller.co.uk/Cracker/NTLM
Please input the **NTLM** hashes that you would like to look up. ... This allows you to input an **NTLM** hash and search for its corresponding plaintext ("found") in our database of already-cracked hashes. ... NT (New Technology) LAN Manager (**NTLM**) is a suite of Microsoft security protocols that ...



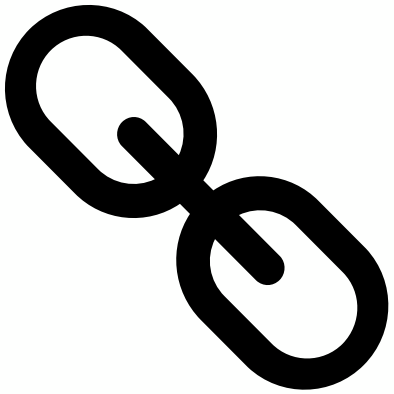
Passwords

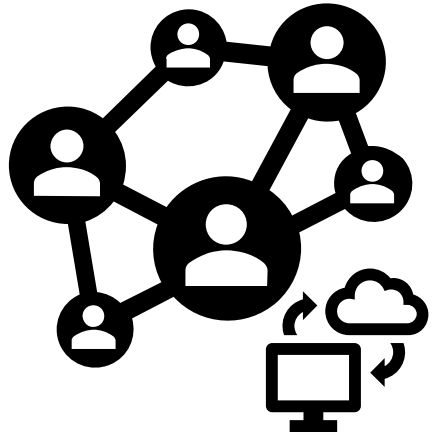
CompTIA COMMUNITY





Updates & Misconfigurations





In Closing

WE ARE THE
CompTIA
COMMUNITY

Lewis Warner
Chief Hacking Officer
PENTIQ
Be Assured. Be Secured.

Thank you

Questions?

- 2:50pm The BIG MSP Hack **Greg Jones**, Datto/Kaseya and **Ken Roulston**, Ex2 Consultancy
- **3:20pm NETWORKING BREAK until 3:45pm**

WE ARE THE CompTIA COMMUNITY

Greg Jones

Kaseya / Datto

Ken Roulston

Ex2 Consultancy

CompTIA COMMUNITY

CompTIA COMMUNITY

- 3:50pm A Regional Perspective **Hollie Whittles**, Purple Frog Systems (UK&I Community Vice Chair)
- 4:05pm What Happens In The Event Of An Attack? **Trevor Cornbill**, TechInsure
- 4:20pm What You Need In Place From A PR Perspective **Rahme Mehmet**, TechComms
- 4:40pm What Does CompTIA Offer That Could Help You? **Wayne Selk**, CompTIA
- 5:10pm Top Cyber Resources and Takeaways **Kyle Torres**, Sophos (UK&I Cybersecurity Vice Chair)
- **6:00pm Networking Drinks & Canapes**

WE ARE THE

CompTIA®

COMMUNITY

Hollie Whittles
Purple Frog Systems

We Are The CompTIA COMMUNITY

#CompTIACommunity

West Midlands cyber focus

with Hollie Whittles

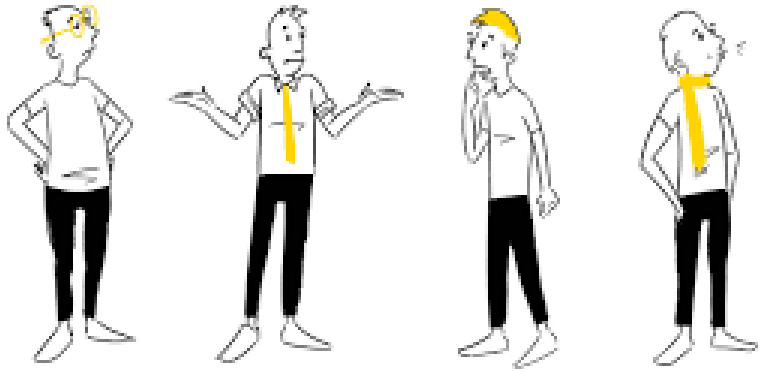
21% of West Midlands businesses report cyber attack

West Midlands Cyber Resilience Centre

Some ‘not so fun’ facts

- Small businesses subject to 10,000 cyber-attacks a day, according to UK’s largest business group, the Federation of Small Businesses
- Victims are frequently subject to phishing attempts, with 530,000 small firms suffering from such an attack over the past 2 years
- Hundreds of thousands of businesses also report incidences of
  - malware (374,000)
  - fraudulent payment requests (301,000) and
  - ransom-ware (260,000)

Your responsibilities



Business owners and leaders have a responsibility to ensure employees are using systems and devices safely, whilst protecting customer data from the likes of phishing attacks or data breaches

A Digital Roadmap to catapult the region

The West Midlands Digital Roadmap has 5 key missions for 2021 – 2026

- Securing access for everyone to digital opportunities, particularly those in poverty
- Sharing and using data to improve people's lives
- Becoming the UK's best-connected region
- Realising the potential of digital to transform our economy and build economic resilience
- Using digital public services to build a fairer, greener, healthier region

The Cyber Engine of the UK

£9m Cyber Quarter facility located in Hereford, on the UK's Defence and Security Enterprise Zone

https://www.cyberquarter.co.uk

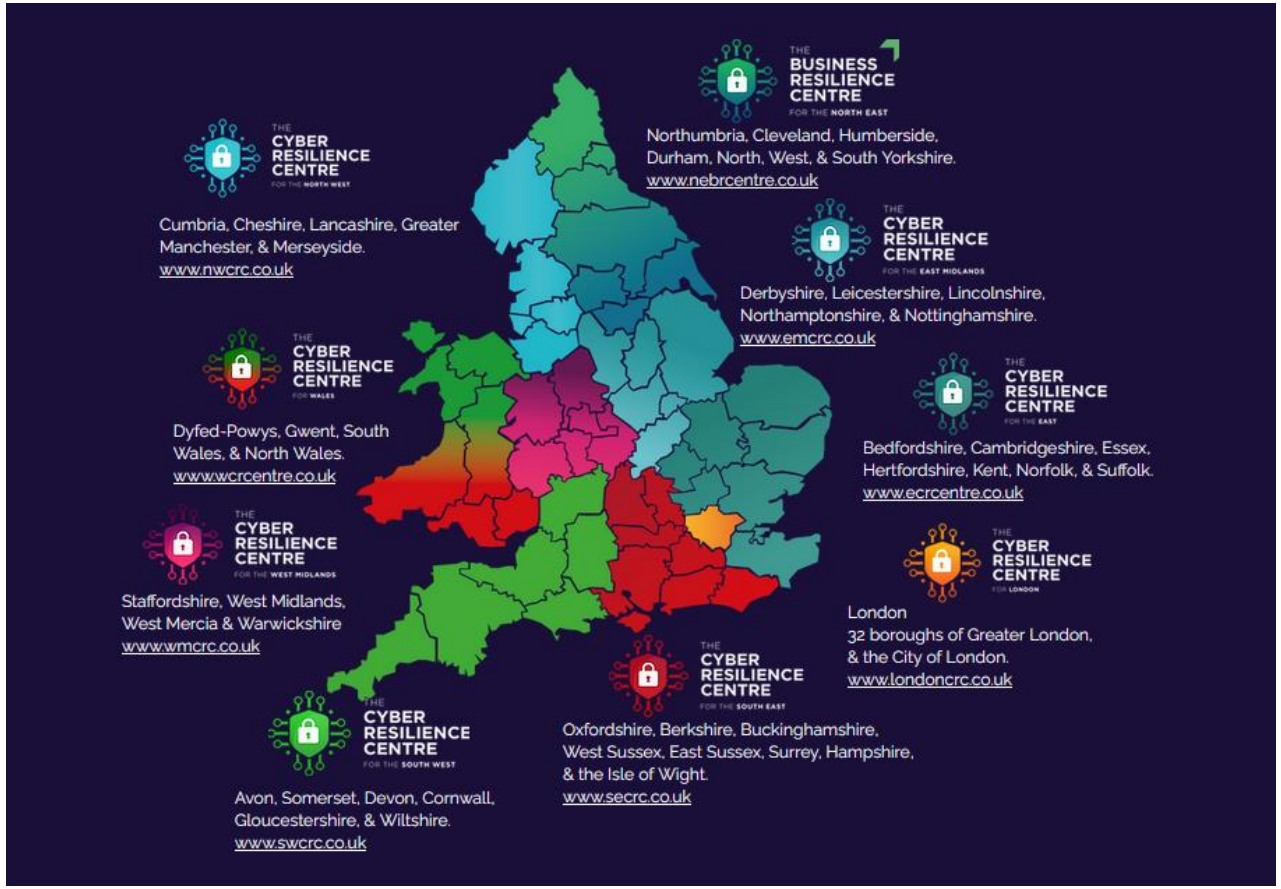
The Cyber Engine of the UK

- The West Midlands is delivering national and internationally recognised cyber security services
- The launch of the UK's National Cyber Strategy 2022 in Birmingham brought these activities to light:
  - A competitive and collaborative ecosystem
  - Cyber for young minds
  - Nationally significant academic capabilities
  - Critical National Infrastructure & commerce
  - A Growing Base of Cyber Expertise

Cyber Resilience Centre for the West Midlands

The Cyber Resilience Centre for the West Midlands is a trusted resource for support to protect businesses and third sector organisations in the West Midlands region

https://www.wmcrc.co.uk



State of Cybersecurity 2024

If you haven't already, download the latest report from CompTIA:

https://www.comptia.org/content/research/cybersecurity-trends-research

We Are The CompTIA COMMUNITY

#CompTIACommunity

THANK YOU

Hollie Whittles

CompTIA COMMUNITY

- 4:05pm What Happens In The Event Of An Attack? **Trevor Cornbill**, TechInsure
- 4:20pm What You Need In Place From A PR Perspective **Rahme Mehmet**, TechComms
- 4:40pm What Does CompTIA Offer That Could Help You? **Wayne Selk**, CompTIA
- 5:10pm Top Cyber Resources and Takeaways **Kyle Torres**, Sophos (UK&I Cybersecurity Vice Chair)
- **6:00pm Networking Drinks & Canapes**

WE ARE THE

CompTIA®

COMMUNITY

Trevor Cornbill
TechInsure

By Trevor Cornbill

Cyber Insurance

Techinsure
part of the cleargroup

Cyber Insurance

Hints and tips to help limit the chances of your claim being declined!!!!

- Business description
- Interpretation of the questions
- Clear understanding
- Regular reviews

What happens in the event of claim?

Step 1 - Notification

What happens in the event of claim?

Step 2 - Assessment

What happens in the event of claim?

Step 3 - Forensics

What happens in the event of claim?

Step 4 - Recovery

What happens in the event of claim?

Step 5 - Settlement

Contact Details

Tel: **01789 338071**
Email: **cyberinsurance@thecleargroup.com**

Techinsure
part of the cleargroup

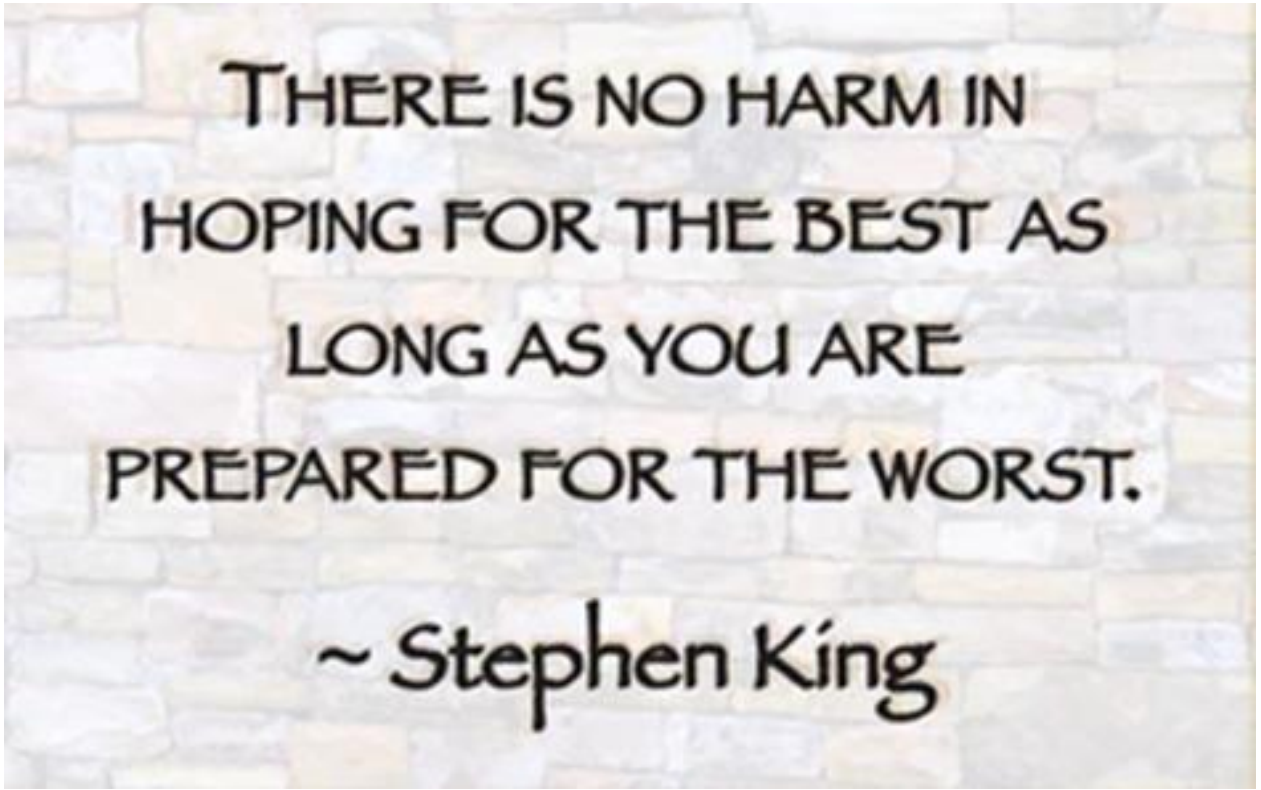
- 4:20pm What You Need In Place From A PR Perspective **Rahme Mehmet**, TechComms
- 4:40pm What Does CompTIA Offer That Could Help You? **Wayne Selk**, CompTIA
- 5:10pm Top Cyber Resources and Takeaways **Kyle Torres**, Sophos (UK&I Cybersecurity Vice Chair)
- 6:00pm **Networking Drinks & Canapes**

WE ARE THE

CompTIA®

COMMUNITY

Rahme Mehmet
TechComms



Be Prepared!

18 January 2024

Our Agenda

1. Introduction to our Agency
2. What is a PR Crisis?
3. Effective Crisis Management

Who We Are

TechComms is a marketing and communications agency renowned for its extensive experience and expertise in the B2B technology sector. Our specialised knowledge spans a range of key markets, including security, mobile & telecoms, enterprise tech, retail & eCommerce, video, and collaboration technology.

TechComms was born within a virtual environment. We are a team of senior marketing and communications experts - dedicated to helping companies – large and small – develop their profile and messaging, establish their market position, grow their sales and channel networks, and build on their brand and market awareness.

Our B2B Experience

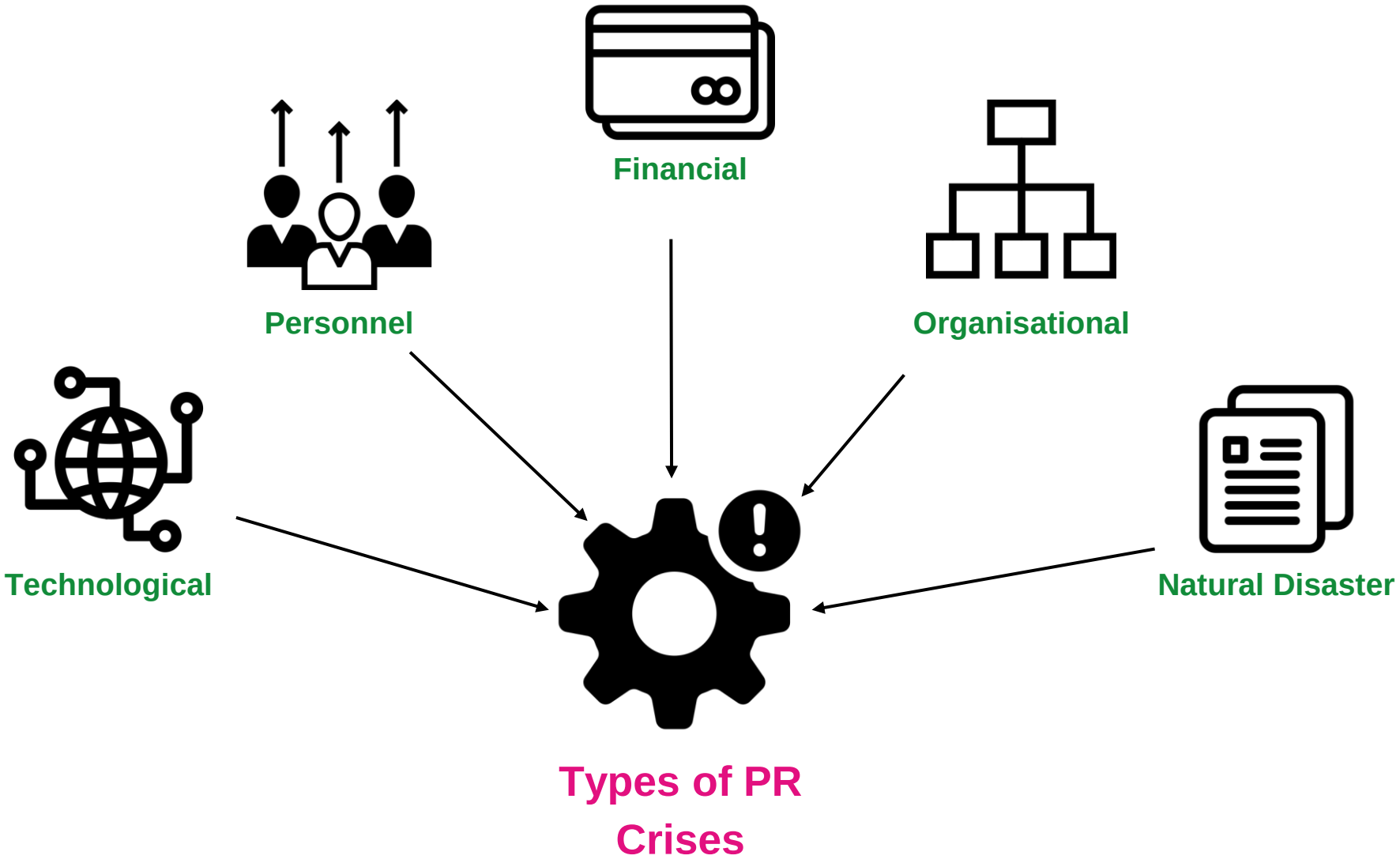
We understand complex technology, we have worked with leading technology providers and can help clients identify their proposition and communicate it to target audiences, generating increased awareness and credibility


TechComms International

What is a PR Crisis?

Negative Public Attention

Types of PR Crises



UK Businesses May Lack Readiness for a Communications Crisis

In the last 12 months, 39% of UK businesses identified a cyber attack*

- Around one in five (21%) identified a more sophisticated attack type such as a denial of service, malware, or ransomware attack.
- Only 19% of businesses have a formal incident response plan.

Source: Cyber Security Breaches Survey, 2022

Seven in 10 respondents to the Chartered Institute of Public Relations (CIPR) survey 2022 have a crisis communications plan

- 63.3% used a PR agency in July 2022
- 69.7% said their business in July 2022 had a plan for identifying and tackling reputation risk

What proportion of business leaders do you think cited reputation risks as their number one concern?

- 2021 it was **5.7%**
- 2022 it was **?**

Source: ** CIPR survey with 300 business leader

How Gender Pay Gap Bot works?

- The bot searches X (formerly Twitter) to match the company names from the government data to their Twitter accounts.
- It ‘listens’ for various keywords related to International Women’s Day to find relevant posts.
- When it finds a relevant post from a company listed in the government data, a quote tweet is published with their gender pay gap information.

Organisational PR Crisis Example (March 2023):

Companies can highlight its failings by newsjacking

International Women’s Day (IWD) - 8 March.
Many companies got caught out by Gender Pay Gap Bot (@PayGapApp), a bot created to highlight that employers’ supportive social media posts are rarely backed up by action.

International Women’s Day

Caught out by Gender Pay Gap Bot!!!! News Coverage

Gender Pay Gap Bot @PayGapApp

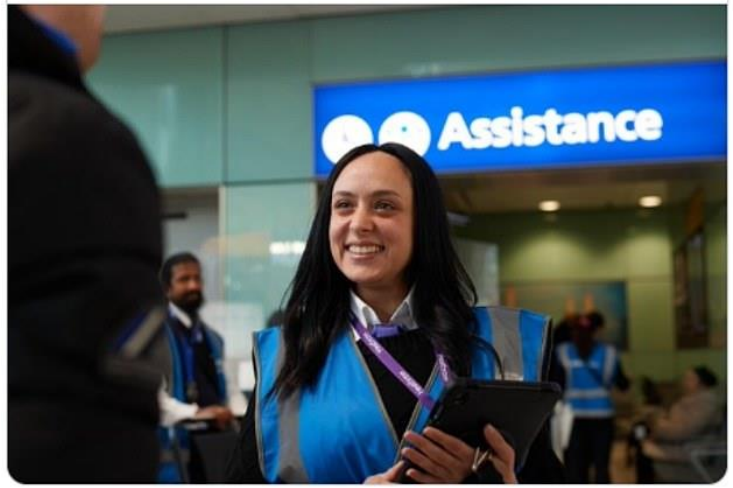
In this organisation, women's median hourly pay is 14% lower than men's. The pay gap is 9.5 percentage points wider than the previous year.

Heathrow Airport @HeathrowAirport · 3h

Good morning and Happy International Women's Day!!! 👧 ✨

You can read a few stories from the women at Heathrow here: heathrow.com/heathrow-blog/...

Feel free to tweet @ us or drop us a direct message if you have any airport or travel queries.



Gender Pay Gap Bot @PayGapApp

In this organisation, women's median hourly pay is 9.8% lower than men's. The pay gap is 9.8 percentage points wider than the previous year.

Department for Culture, Media and Sport @DCMS · 2h

On #IWD2023, we are highlighting the importance of providing equal opportunities for girls in sport

@JillScottJS8 reflects on progress made due to investment in grassroots facilities across England and her hopes for the future of women's football

More gov.uk/government/new...

Mail Online

Women share @paygapapp to mark International Women's Day: Twitter account shames companies for claiming to celebrate IWM - while female staff suffer huge disparity in pay compared to men

- **The Gender Pay Gap Bot shares the median pay difference at various companies**
- **Women have slammed some of the worst offenders with gaps near to 70 percent**

By ELIZABETH HAIGH
PUBLISHED: 10:35, 8 March 2023 | **UPDATED:** 14:17, 8 March 2023

Share 19 shares 478 View comments

Women around the UK are marking **International Women's Day** as they share tweets from **Twitter** accounts highlighting pay disparities at organisations compared to male colleagues.

Information is being shared online about the gender pay gap at governmental bodies, emergency services, educational institutions and corporate firms.

Women also shared experiences of inequality or sexual harassment in the workplace on social media, as well as wishing one another a happy International Women's Day.

Financial PR Crisis Example: How Silicon Valley Bank Collapsed in 36 Hours

- One of the most significant PR disasters of 2023 (March 2023).
- SVB released a statement sharing recent losses.
- SVB did not communicate that it was cash positive despite the losses on the bonds……

Silicon Valley Bank: News Coverage

Leaders | Lessons from a bank collapse

What really went wrong at Silicon Valley Bank

America must plan better for the failure of banks that are large but not enormous

IMAGE: AP

Mar 13th 2023 Share

SHED NO TEARS for investors in Silicon Valley Bank (SVB). On March 10th the bank, which had $212bn of assets, failed with spectacular speed, making it the biggest lender to collapse since the global financial crisis of 2007-09. Most of SVB's depositors were Bay Area tech startups with accounts holding well in excess of the $250,000 that is insured by the federal government. They had fled and their panic was rational. By loading up on long-term bonds, SVB had taken an enormous unhedged bet on interest rates staying low. That bet went wrong, leaving the bank insolvent (or near enough). The fact that shareholders have been wiped out and bondholders will take big losses is not a failure of the financial system. A bad business has been allowed to go bust.

THE WALL STREET JOURNAL.

How Silicon Valley Bank Collapsed in 36 Hours: What Went Wrong

WSJ
March 15, 2023 13

Silicon Valley Bank collapsed in less than two days. In that time, the bank's stock price fell over 60%, and customers tried to withdraw $42 billion. Here's how the SVB's collapse became the second-largest U.S. bank failure ever, and what it means for customers in the future. Photo Illustration: Alexandra Larkin

The Economist

yahoo!news

Economics Observatory.

The Guardian
Newspaper of the year

FINANCIAL TIMES

The New York Times

CTV NEWS

CNN BUSINESS.

Technological PR Crisis Example:

SME Book Publisher Retained Trust With Clients During Crisis

What happened?

- Fraudsters sent emails to clients requesting invoice payments

What did they do?

- Identified the incident (IT audit) and new security measures where put in place
- Stopped and prevented it from moving forward
- Informed their customers and provided instructions on what to do

Don’t LOSE your relationships!!!

- Proactive communications - address concerns to help strengthen trust

MASCOT BOOKS

est. 2003

Effective Crisis Management Plan

Successful Crisis Management

Two Key Components:

1. Actions that you take to respond and manage the incident to radiate the threat

2. Good Communications - timely, factual, empathic, and clear

The Role of a Crisis Communication Plan in Cybersecurity Incidents

- Being prepared – preparation can quickly restore a good reputation.
- Social media and mobiles – the digital landscape has transformed.
- Ensure that relevant audiences are correctly identified, and establish key contacts at relevant agencies - example, Information Commissioner's Office (ICO).
- Work with a PR crisis communications expert to help you create a crisis communications strategy/plan and manage the execution of the communications process.

Crisis Communications

Key Steps

1. Establish the FACTS

2. Develop a CLEAR communication strategy (objective, spokespeople, questions, etc.)

3. Communicate IMMEDIATELY and directly

- **Be specific -** what happened, how it affects everyone, and what you're doing to rectify the situation.
- **Show remorse** and articulate how seriously you are taking the situation.
- **Answer any potential questions that you can -** ask yourself critical questions.
- **Focus on the relationship with stakeholders** and how you can strengthen it.

4. MONITOR and evaluate the effectiveness and impact of your communication efforts.

Tips for Your Official Statement

1. Tell your story.
Proactive storytelling to shape the narrative around the crisis.

2. Give the media the true story to use.
Accurate information helps in controlling the narrative.

3. Focus on building and strengthening your relationships.
Engage with stakeholders, acknowledging their concerns, and work towards rebuilding trust.

4. Be honest, transparent, and compassionate.
Maintain credibility and demonstrating a commitment to ethical communication.

5. Share what you have done, and what you will be doing.
What are the consequences of the breach? What actions have already been taken? What are the ongoing and future measures to manage the crisis?

6. Answer all foreseeable questions.
Demonstrates preparedness by anticipating and addressing potential questions and responses,

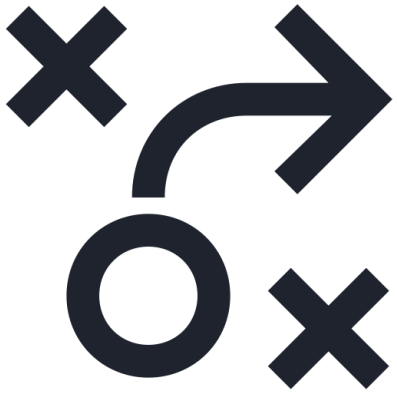
7. Update the statement as more questions get answered.
As information becomes available, ensure stakeholders are kept informed.

8. Title the statement with keywords for search optimisation.
Use relevant and searchable keywords in the statement title to make it easily discoverable.

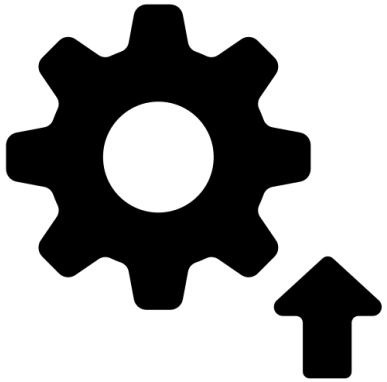
Ask Yourself Some Critical Questions

Before saying anything about a crisis……

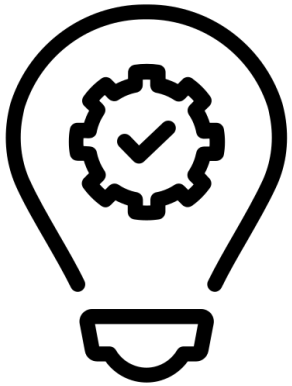
Your answers can help ensure that communications and decisions about the crisis will be….



Strategic



Effective



Efficient

Questions - What, When, Who…..etc

What

- What do we know about the situation?
- What is the source of information about the crisis, and how trustworthy is that source? Is it accurate, credible, and current?
- What don’t we know about the situation, and when will we know it?
- What will be the impact when we tell people what we know about the crisis? Could it make matters better, worse, or have no effect?
- What questions could we be asked about the crisis, and do we have answers to those queries? If not, why not?
- What steps will we take to address the crisis, and what will we tell people about those actions?
- What resources do we have —or have access to— to respond to the crisis?
- What’s the worst that could happen if we stay quiet about it, and are we prepared for the possible consequences?

Questions - What, When, Who…..etc

When, Who, Where, Why and How?

When

- When will we announce what we know about the situation?

Who

- Who are the most important audiences that we should tell about the crisis?
- Who will be our spokesperson for the crisis, and why?
- Who should we give a heads-up that we will make the announcement?
- Who can we get to be surrogates to help tell our side of the story about the situation?

Where

- Where will we make the announcement?

Why

- Why will we share the information about the crisis?

How

- How will we share that information?

Thank You

Rahme Mehmet
Managing Director
+44 (0) 7886 015 222
rmehmet@techcomms.co.uk

- 4:40pm What Does CompTIA Offer That Could Help You? **Wayne Selk**, CompTIA
- 5:10pm Top Cyber Resources and Takeaways **Kyle Torres**, Sophos (UK&I Cybersecurity Vice Chair)
- 6:00pm **Networking Drinks & Canapes**

WE ARE THE CompTIA COMMUNITY

Wayne Selk
CompTIA

CompTIA is More Than Certifications

We can help you grow and thrive as a Solution Provider

Reduce Risk – Grow Revenues

Don’t get left behind

- Legislation impacts on profitability
  - GDPR
  - NIS2
- Designed to reduce risk for Clients and Governments
  - 41% of the organizations that suffered a material incident in the past 12 months say it was caused by third-party
  - 54% of organizations have an insufficient understanding of cyber vulnerabilities in their supply chain

“Alignment between cyber and business is becoming more common” – Source: World Economic Forum Global Cybersecurity Outlook 2024

“For any organization, the partners in its ecosystem are both the greatest asset and the biggest hinderance to a secure, resilient and trustworthy digital future” – Source: World Economic Forum Global Cybersecurity Outlook 2024

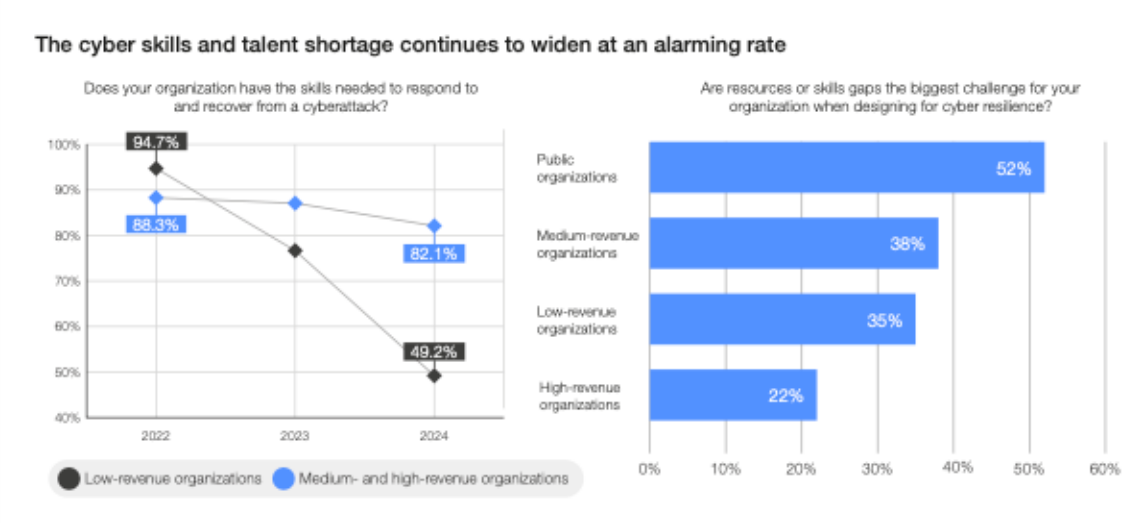
“60% of executives agree that cyber and privacy regulations effectively reduce risk in their organization’s ecosystem – up 12% since 2022” – Source: World Economic Forum Global Cybersecurity Outlook 2024

CompTIA CYBERSECURITY Programs

Skills Gap – Train Talent

The right people matter

- Talent is Hard to Find, even Harder to Keep
- Unsure of the skills needed
- Unable to afford to hire



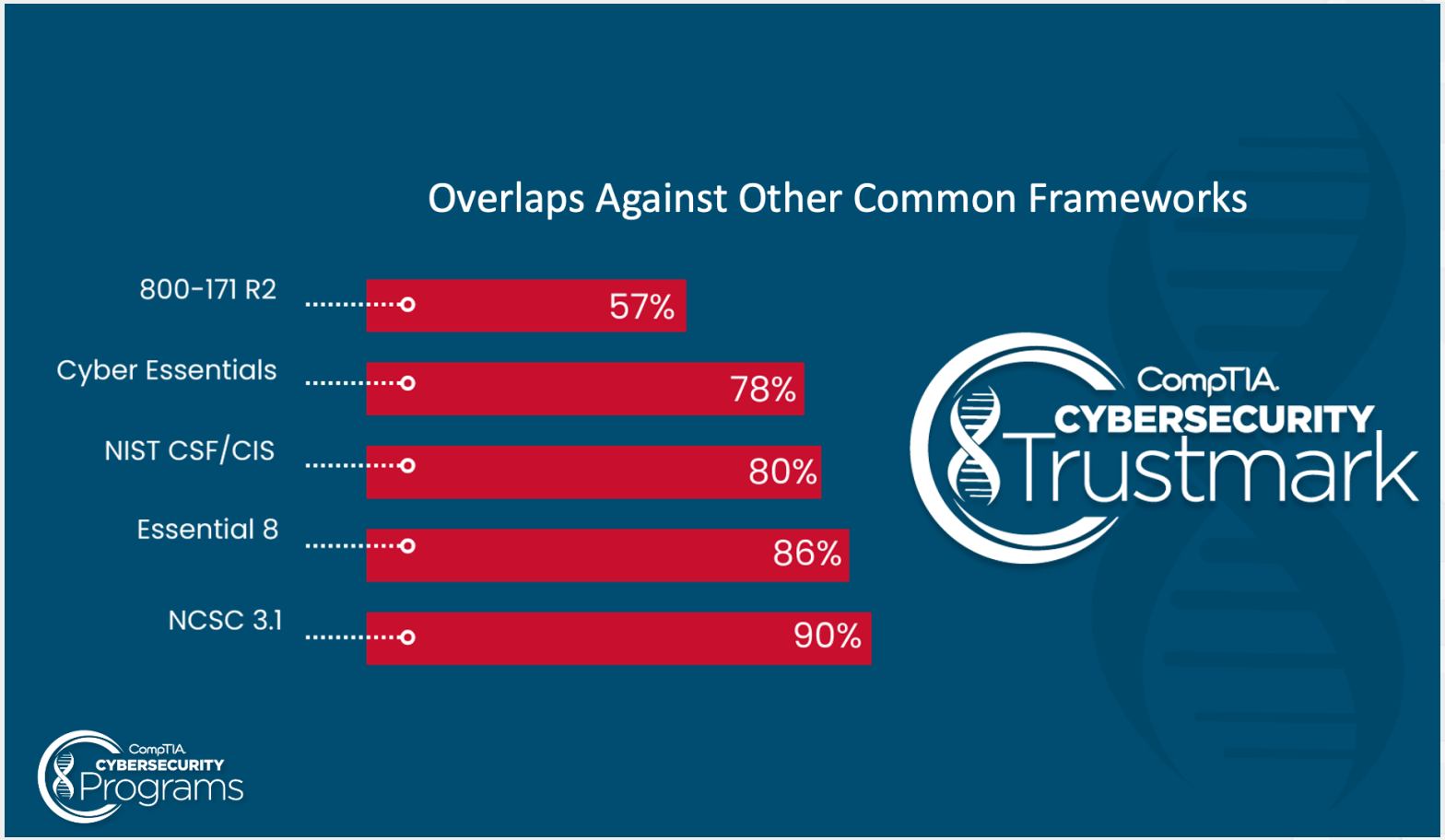
"Cyber-skills and talent shortage continues to widen at an alarming rate" – Source: World Economic Forum Global Cybersecurity Outlook 2024

"Only 15% of all organizations are optimistic that cyber skills and education will significantly improve in the next two years" – Source: World Economic Forum Global Cybersecurity Outlook 2024

CompTIA CYBERSECURITY Programs

Creating Opportunity – Cybersecurity Programs

Efficiency and effectiveness drive revenues



CompTIA CYBERSECURITY Programs

Cybersecurity Trustmark

Set yourself apart

- Set the business up to lower the impact of risk
- Create a security-first culture in your organization (or improve it)
- Align your organization to meet NIS2
- Grow your revenue, Grow your business

CompTIA CYBERSECURITY Programs

What's Coming in 2024

Cybersecurity Programs

- Third-party Vendor Risk Management Program
- CISO Advisory Program
- Emergency Response Team for UK&I (Need volunteers)
- Trustmark Vendor and End Client Profiles
- Cybersecurity Global Task Force

CompTIA CYBERSECURITY Programs

Other CompTIA Benefits

You may not be aware of…

- 15% Discount on Exam Vouchers
- 10-40% Discount on Courseware
- Marketing and Legal Toolkits
- CompTIA Research (State of the Channel, State of Cybersecurity, etc.)
- Events are FREE to attend (Pay only air and lodging)
- Councils and Regional Groups (Networking)

CompTIA CYBERSECURITY Programs

We are here to help

Questions?

- 5:10pm Top Cyber Resources and Takeaways **Kyle Torres**, Sophos (UK&I Cybersecurity Vice Chair)
- 6:00pm **Networking Drinks & Canapes**

WE ARE THE

CompTIA®

COMMUNITY

Kyle Torres
Sophos

Cyber Resources & Takeaways

Resources

- CompTIA ISAO – Information Sharing & Analysis Organization
- CompTIA Resource Library – State of Cybersecurity, Embedding Security into Company Culture, others
- Emergency Response Team (ERT)

Cyber Resources & Takeaways

Takeaways

- The BIG Hacks:
  - Customer
  - MSP
- Understanding the why and what behind attacks: How can we be proactive against these threats?
- Insurance & Press: What should you have in place?

- Growth & Development
  - What are your next steps?
  - Internal/External Enablement
  - Ready to monetise

We Are The CompTIA
COMMUNITY

#CompTIACommunity

THANK YOU

CompTIA COMMUNITY

https://surveys.comptia.org/s3/2024-January-UK-I-Cybersecurity-Committee-Meeting

We Value Your Feedback

CompTIA COMMUNITY

CompTIA IT Industry Outlook 2024

- ***Why*** – Helps you and your business understand what trends are coming in 2024 and stay ahead of the curve
- ***Who*** – Anyone in the business who wants to understand the latest stats and industry trends, so please share around your organisations
- ***How*** – Download here or use the QR code - https://connect.comptia.org/content/research/it-industry-trends-analysis
- ***Useful Info*** –
  - Has stats for all the regional communities
  - Any information can be taken from it and shared on your resources as long as you cite the source
  - Members can co-brand with their logo to share with partners and clients
  - Vendor and Distributor members can have this delivered to their partners, either at a live event or on a webinar at no cost

CompTIA Research Report Highlight

#CompTIACommunity

CompTIA
COMMUNITY

18:00 - 19:00 Networking Drinks and Canapes