



Webinars for Cold Chain Professionals

**FOOD SECURITY WEEK DAY 1: THE RISING THREAT  
OF CYBER CRIME TO THE COLD CHAIN**

**STARTING AT 10:30AM**

SUPPORTED BY:



TOM SOUTHALL  
POLICY DIRECTOR  
COLD CHAIN FEDERATION



# INTRODUCTION

## Russian hackers targeting opponents of Ukraine invasion, warns GCHQ chief

Russian operatives trying to escalate online conflict and seeking targets in countries opposing war, says Jeremy Fleming

● [Russia-Ukraine war: latest updates](#)

## KP Snacks hit by ransomware attack with retailers warned of crisps and nuts shortage

Stocks of Skips, Nik Naks, Hula Hoops, McCoy's crisps and KP Nuts themselves could be in tight supply until "the end of March at the earliest".



Alexander Martin

## BUSINESS

CORONAVIRUS | GULF | MENA | WORLD | BUSINESS | OPINION | LIFESTYLE | ARTS & CULTURE | TRAVEL | SPORT | PODCASTS | WEEKEND

on | Economy | Energy | Money | Cryptocurrencies | Property | Banking | Technology | Markets | Travel and Tourism | Start-Ups | Road to Net Zero | F

## THE COST OF A MALWARE INFECTION? FOR MAERSK, \$300 MILLION

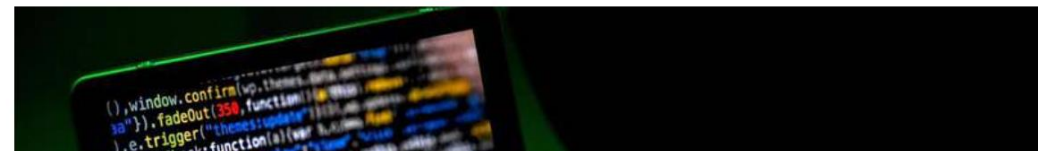


Nate Lord

Last Updated: Friday August 7, 2020

## Cyber crime rate in the UK higher last year than in other developed nations

► Data from online security company Surfshark reveal the number of cyber crimes grew 40 per cent in Britain last year, compared to a global rate of 8 per cent




# SCHEDULE

10:35 – 10:50	Current trends in cyber security & support available	 National Cyber Security Centre
10:50 – 11:10	The need for increased cybersecurity throughout the food chain	
11:10 – 11:30	Protect your business with the right software	 mercurius information technology


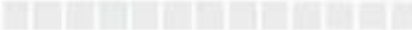


File View Help



Audio

Sound Check  ?

☒ Computer audio  
☐ Phone call  
☐ No audio

Microphone Array (Conexant SmartA... ▼

Speakers (Conexant SmartAudio HD) ▼


Talking: **Shane Brennan**

Questions

[Enter a question for staff]

Send

**CCF - COVID 19 - INTELLIGENCE EXCHANGE**  
Webinar ID: 308-161-843

 GoToWebinar

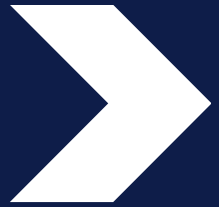
# CURRENT TRENDS IN CYBER CRIME & SUPPORT AVAILABLE



National Cyber  
Security Centre



National Cyber  
Security Centre  
a part of GCHQ



# Introduction to the National Cyber Security Centre

# National Cyber Security Centre

---

The National Cyber Security Centre (NCSC), a part of GCHQ, is the UK's technical authority for cyber threats.

Our vision is to make the UK the safest place to live and work online.

We support the most critical organisations in the UK, the wider public sector, industry, SMEs as well as the general public.

When incidents do occur, we provide effective incident response to minimise harm to the UK, help with recovery, and learn lessons for the future.

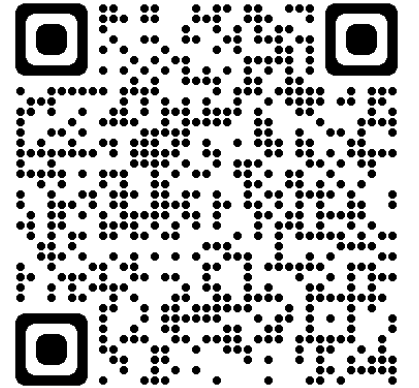




# NCSC Update

---

- **Guidance** – Actions to take when the cyber threat is heightened
- **News** – UK joins international partners to issue advice on latest Russian cyber threat
- **Blog Post** – Use of Russian technology products and services following the invasion of Ukraine
- **Sign up to our Subscription Centre** (Threat Reports & Advisories) to receive real time alerts





*39% of businesses...report  
having any kind of cyber  
security breach or attack in  
the last 12 months*

Cyber Security Breaches Survey 2022





## Take your email security to another level

### Action 1

Use a strong and different password for your email using 3 random words

### Action 2

Turn on 2-Step Verification (2SV) for your email

### Follow on Actions

- Save passwords in your browser
- Backup your data
- Update your devices
- Get your free Cyber Action Plan



# Small Business Guide



## Cyber Security Small Business Guide

Small  
Business  
Guide  
Collection

How to improve your cyber security;  
affordable, practical advice for businesses



- Backing up your data
- Protecting your organisation from malware
- Keeping your smartphones (and tablets) safe
- Using passwords to protect your data
- Avoiding phishing attacks

# Response and Recovery Guide

Guidance to help business prepare their response to and plan their recovery from a cyber incident



- Prepare for incidents
- Identify what's happening
- Resolve the incident
- Report the incident to wider stakeholders
- Learn from the incident

## Exercise in a Box

---



An online tool which helps organisations find out how resilient they are to cyber attacks and practise their response in a safe environment





# 10 Steps to Cyber Security

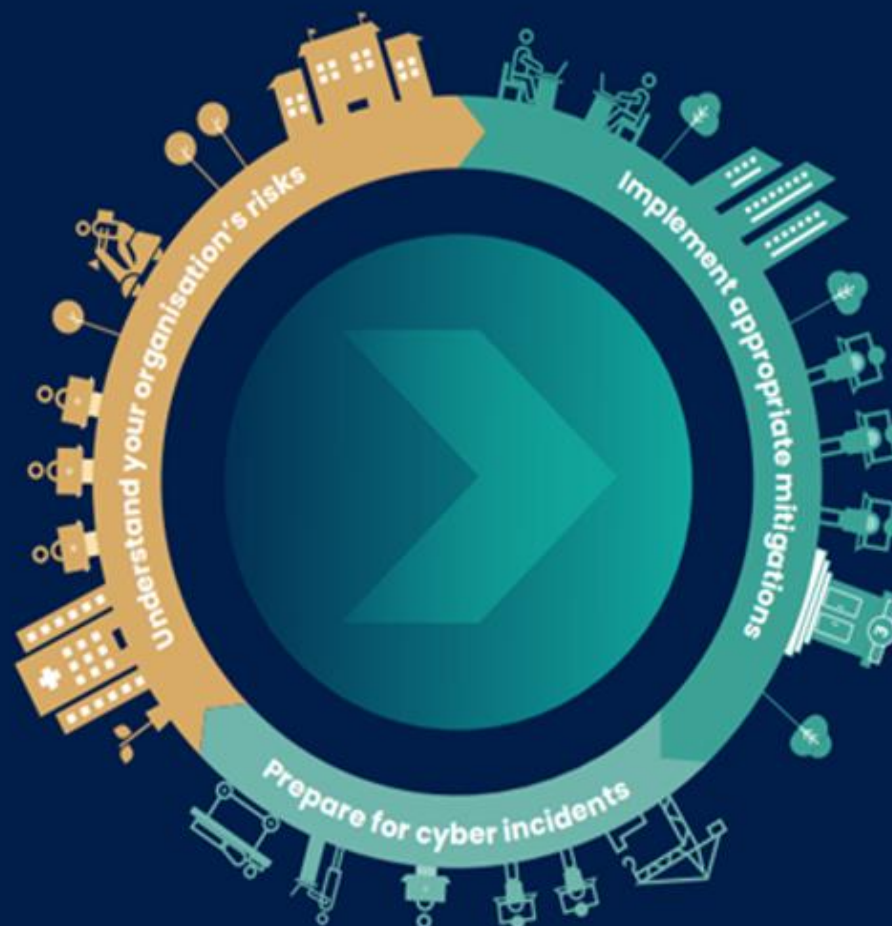
- **Risk management**  
Take a risk-based approach to securing your data and systems.

- **Engagement and training**  
Collaboratively build security that works for people in your organisation.

- **Asset management**  
Know what data and systems you have and what business need they support.

- **Architecture and configuration**  
Design, build, maintain and manage systems securely.

- **Vulnerability management**  
Keep your systems protected throughout their lifecycle.



- **Identity and access management**  
Control who and what can access your systems and data.

- **Data security**  
Protect data where it is vulnerable.

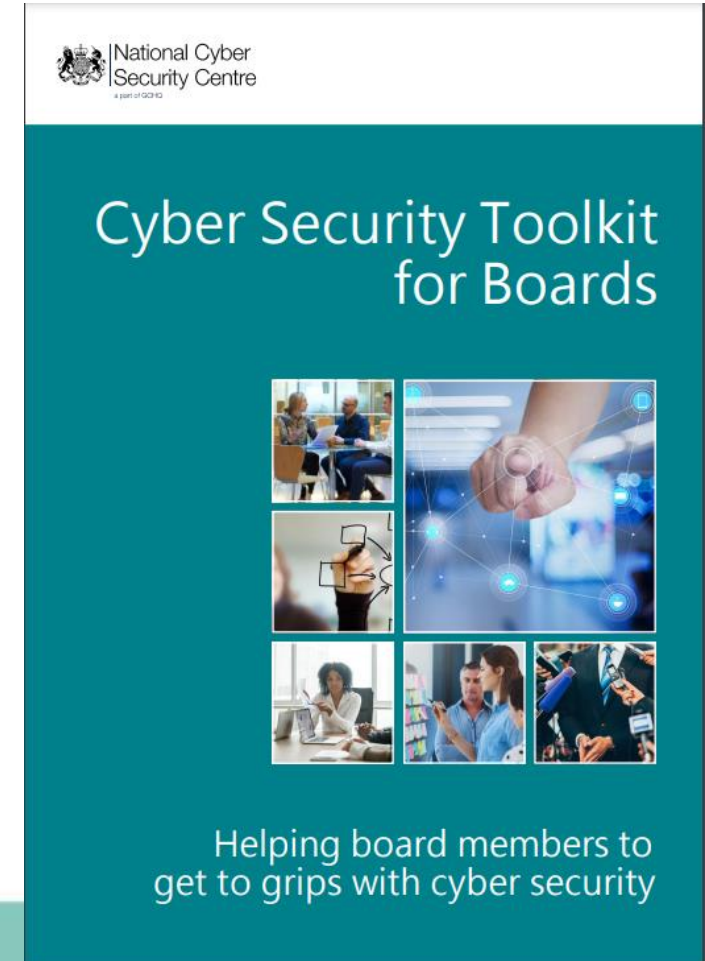
- **Logging and monitoring**  
Design your systems to be able to detect and investigate incidents.

- **Incident management**  
Plan your response to cyber incidents in advance.

- **Supply chain security**  
Collaborate with your suppliers and partners.

# Board Toolkit

- Introduction to cyber security for board members
- Understanding the threat
- Collaborating with suppliers and partners
- Planning a response to a cyber incident





# Cyber Essentials

- Cyber Essentials helps you to guard your organisation against cyber attack
- Cyber Essentials
- Cyber Essentials Plus
- Cyber Essentials Readiness Tool



**Build your  
online security.**

**Get **Cyber Essentials**  
for your business.**

Assured Service Provider

 in association with  
National Cyber  
Security Centre

 **CYBER  
ESSENTIALS**

# Supply Chain Security

A series of 12 principles, designed to help you establish effective control and oversight of your supply chain.

**The principles have been divided into four separate stages:**

1. Understand the risks
2. Establish control
3. Check your arrangements
4. Continuous improvement



# Active Cyber Defence (ACD)

---

## Email Security Check

Identifies vulnerabilities that could lead to email spoofing or email privacy being breached

## Logging Made Easy (LME)

Helps organisations to install a basic logging capability on their IT estate enabling routine end-to-end monitoring of Windows systems.

## Early Warning

Helps organisations investigate cyber attacks on their network by notifying them of malicious activity that has been detected in information feeds.



# Cyber Security Information Sharing Partnership – CiSP

---

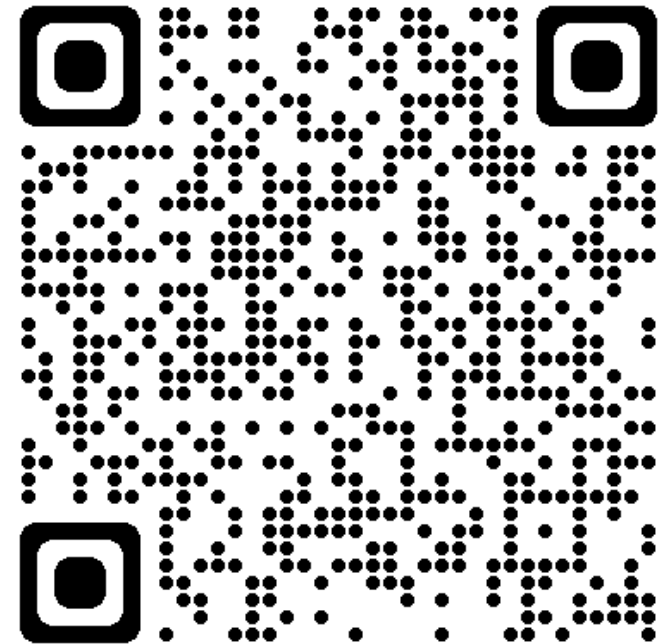
A joint industry and government initiative set up to allow UK organisations to share cyber threat information in a secure and confidential environment.



# NCSC Subscription Centre

---

- NCSC Small Organisations Newsletter
- Weekly Threat Reports
- NCSC Advisories
- Information about CyberUK
- NCSC Digital Lofts



# THE NEED FOR INCREASED CYBER SECURITY THROUGHOUT THE FOOD CHAIN



MARK BROWN, GLOBAL MANAGING  
DIRECTOR, DIGITAL TRUST  
CONSULTING, BSI

# PROTECT YOUR BUSINESS WITH THE RIGHT SOFTWARE



JAY TAHASILDAR, MANAGING  
DIRECTOR, MERCURIUS IT





# Cyber Security: The Hot topic in Cold storage Logistics



Gold Enterprise Resource Planning  
Gold Collaboration and Content  
Gold Application Development  
Gold Small and Midmarket Cloud Solutions  
Gold Cloud Platform







# Today's speaker



**Jay Tahasildar: Founder & Managing Director**  
E-mail: [jay.t@mercuriusit.com](mailto:jay.t@mercuriusit.com)

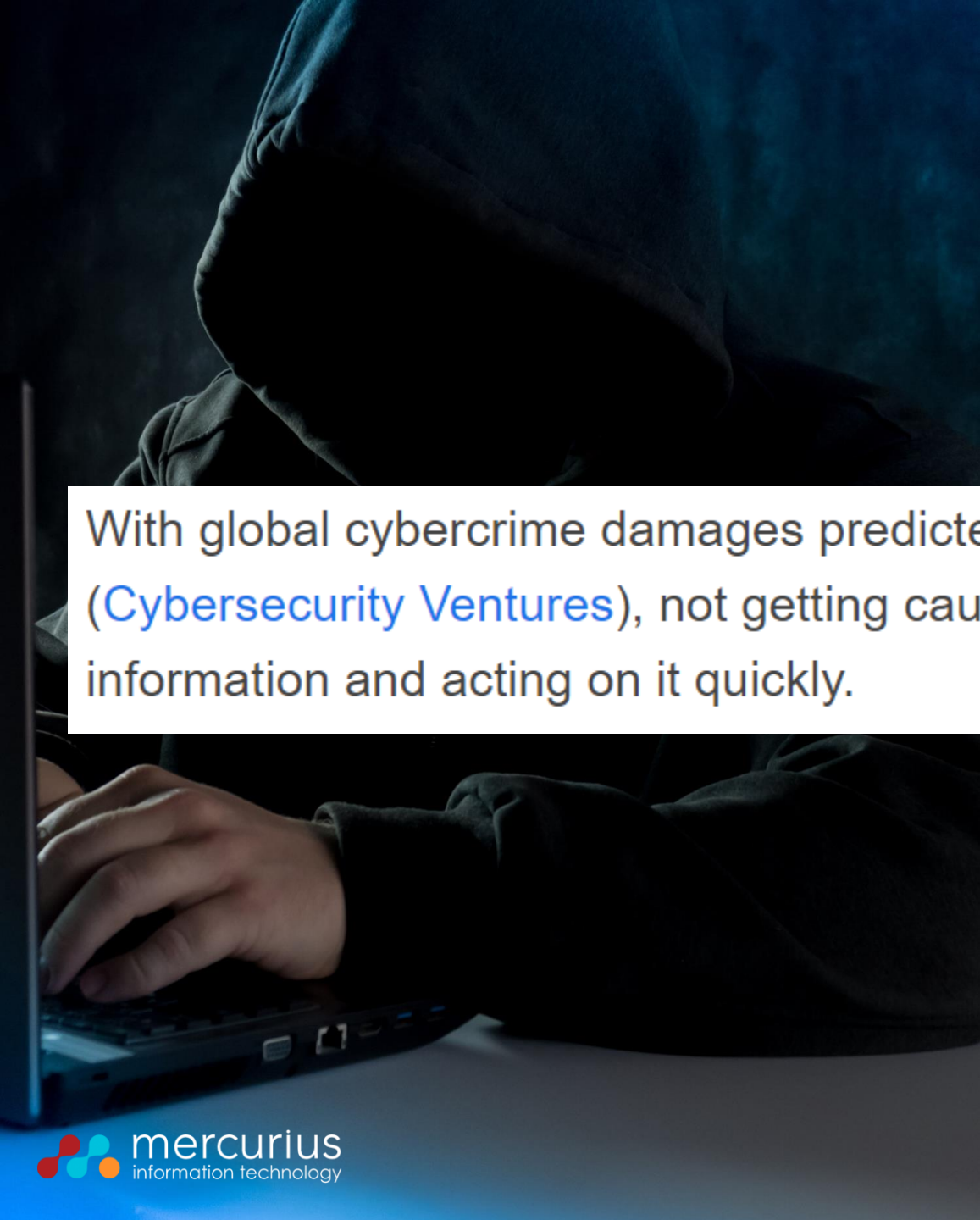
## Microsoft Gold Partner

- Gold Enterprise Resource Planning
- Gold Collaboration & Content
- Gold Cloud Platform
- Gold Cloud Productivity
- Gold Application Development
- Gold Small & Midmarket Cloud Solutions
- Gold Project & Portfolio Management
- Gold Windows & Devices
- **UK Partner for Boltrics 3PL Solution, powered by Microsoft Dynamics 365 Business Central**



# Why do we talk about Cyber Security?

- Worldwide shift towards cyber crime
- Prime targets

A person wearing a dark hoodie is shown from the chest down, sitting at a desk and typing on a laptop. The scene is dimly lit, with a blue light source visible on the left, creating a moody atmosphere. The person's hands are positioned on the laptop keyboard.

With global cybercrime damages predicted to cost up to \$10.5 trillion annually by 2025 ([Cybersecurity Ventures](#)), not getting caught in the landslide is a matter of taking in the right information and acting on it quickly.

# The numbers



**39% of businesses reported cyber security breach or attack**

**21% of businesses that reported a cyber breach or attack experienced a negative outcome**

**The average cost of cyber security breaches is estimated to be £8,460**

**83% of cyber breaches or attacks on businesses were phishing attacks**



# Prime targets in Food Supply Chain

- Temperature controlled goods
- High cost of a systems outage
- Old systems
- Pressure on Supply chain
- Limited attention to Cyber Security





# How to prevent cyber attacks?



# Can we prevent cyber attacks?

Well, we can't stop them completely!

But we can **Prepare** and

**Protect** our business from any potential damage!

**Stay one step ahead!**



# A Microsoft way...

- **Start with a secure foundation**
- **Simplify security with built in controls**
- **Detect threats early with unique intelligence**

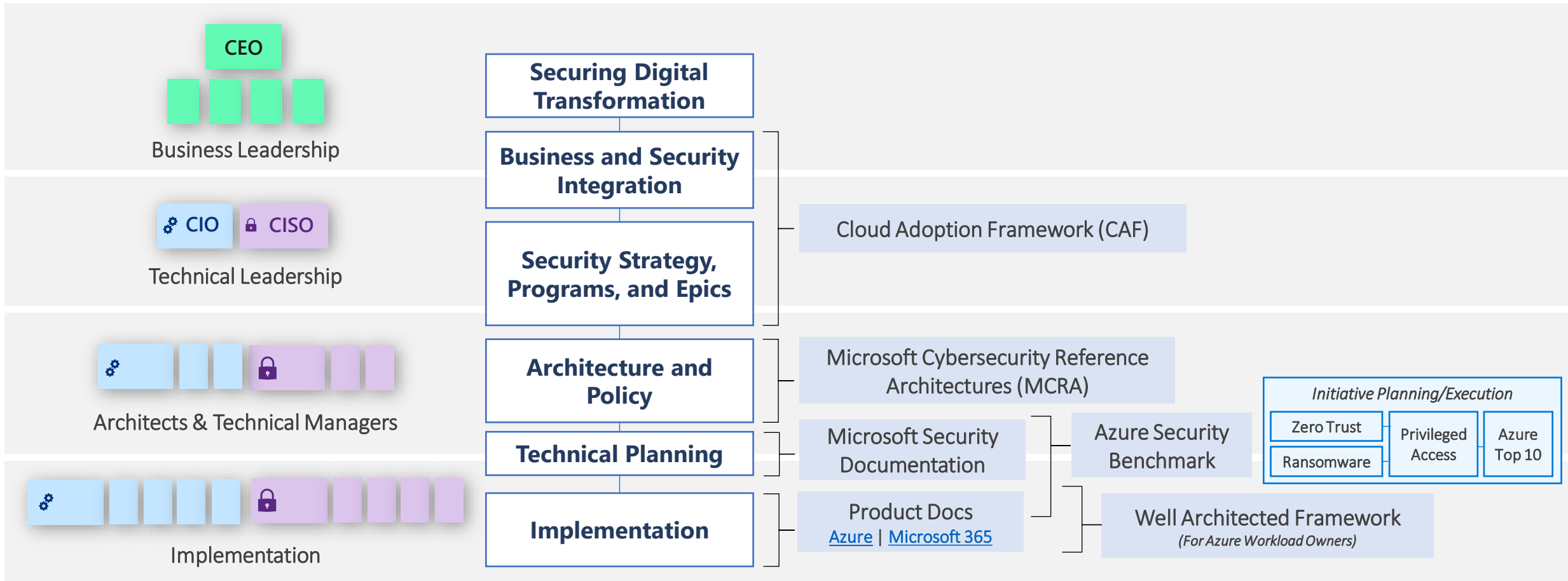


Microsoft

- Source: <https://azure.microsoft.com/en-gb/overview/security/>



# Security Guidance

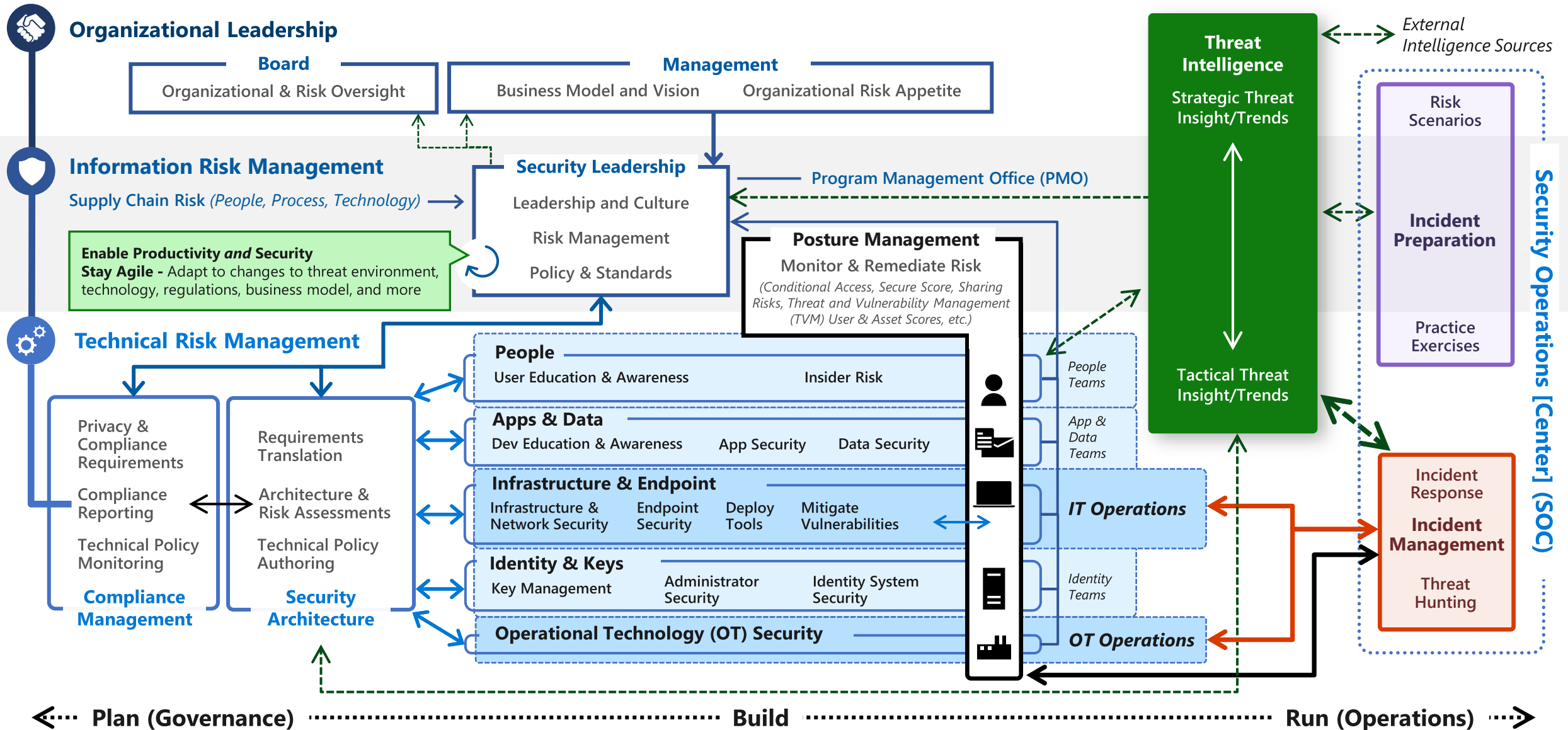


# Managing Information\Cyber Risk

Security responsibilities or “jobs to be done”

December 2021 -

<https://aka.ms/SecurityRoles>



## Security Operations / SOC

Threat Experts | Detection and Response Team (DART) | MSSP/MDR

**Microsoft Sentinel** – Cloud Native SIEM, SOAR, and UEBA for IT, OT, and IoT

### Microsoft Defender – Extended Detection and Response (XDR)

Advanced Detection & Remediation | Automated Investigation & Remediation | Advanced Threat Hunting

#### Cloud

Azure, AWS, GCP,  
On Premises &  
other 3<sup>rd</sup> party  
clouds

#### Endpoint & Server/VM

#### Office 365 Email and Apps

#### Identity Cloud & On-Premises

#### SaaS Cloud Apps

#### + More OT, IoT, SQL, and more

Other Tools,  
Logs, & Data  
Sources



# Cybersecurity Reference Architecture

Security modernization with Zero Trust Principles

December 2021 – <https://aka.ms/MCRA>

This is interactive!

1. Present Slide
2. Hover for Description
3. Click for more information

Security Guidance

1. [Security Documentation](#)
2. [Microsoft Best Practices](#)
3. Azure Security [Top 10 | Benchmarks](#) | [CAF](#) | [WAF](#)

## Software as a Service (SaaS)

### Microsoft Defender for Cloud Apps

- App Discovery & Risk Scoring (Shadow IT)
- Threat Detection & Response
- Policy Audit & Enforcement
- Session monitoring & control
- Information Protection & Data Loss Prevention (DLP)



## Identity & Access

**Conditional Access** – Zero Trust Access Control decisions based on explicit validation of user trust and endpoint integrity

## Endpoints & Devices

### Microsoft Endpoint Manager

Unified Endpoint Management (UEM)

Intune | Configuration Manager



### Microsoft Defender for Endpoint

Unified Endpoint Security

Endpoint Detection & Response (EDR)

Web Content Filtering

Threat & Vuln Management

Endpoint Data Loss Protection (DLP)

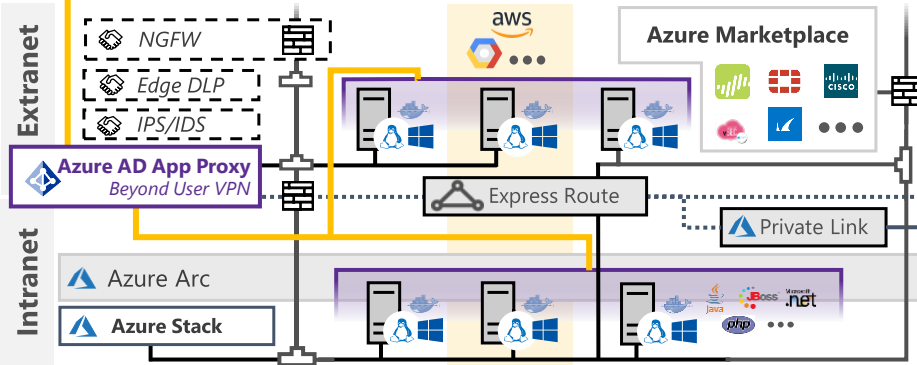
## Hybrid Infrastructure – IaaS, PaaS, On-Premises

### Defender for Cloud – Cross-Platform Cloud Security Posture Management (CSPM)

Secure Score

Compliance Dashboard

On Premises Datacenter(s) | 3rd party IaaS & PaaS | Microsoft Azure



## Information Protection

### Azure Purview

### Microsoft Information Protection (MIP)

Monitor | Discover | Classify | Protect

### File Scanner (on-premises and cloud)



Data Governance

Advanced eDiscovery

Compliance Manager

## Azure Active Directory

### Passwordless & MFA

Hello for Business  
Authenticator App  
FIDO2 Keys

Identity Protection  
Leaked cred protection  
Behavioral Analytics

Azure AD PIM

Identity Governance

Azure AD [B2B](#) & [B2C](#)

Defender for Identity

Active Directory

**Securing Privileged Access** – Secure Accounts, Devices, Intermediaries, and interfaces to enable and protect privileged users

**Privileged Access Workstations (PAWs)** – Secure workstations for administrators, developers, and other sensitive users

**Microsoft Secure Score** – Measure your security posture, and plan/prioritize rapid improvement with included guidance

**Microsoft Compliance Score** – Prioritize, measure, and plan improvement actions against controls

## Windows 10 & 11 Security

Network protection  
Credential protection  
Full Disk Encryption  
Attack surface reduction  
App control  
Exploit protection  
Behavior monitoring  
Next-generation protection

## IoT and Operational Technology (OT)



Azure Sphere

### Microsoft Defender for IoT

- ICS, SCADA, OT
- Internet of Things (IoT)
- Industrial IoT (IIoT)
- Asset & Vulnerability management
- Threat Detection & Response

### Defender for Cloud – Cross-Platform, Cross-Cloud XDR

Multi-asset detection and response for infrastructure and platform as a service (IaaS & PaaS), Proactive Threat defenses



## People Security

Attack Simulator

Insider Risk Management

Communication Compliance

**GitHub Advanced Security** – Secure development and software supply chain

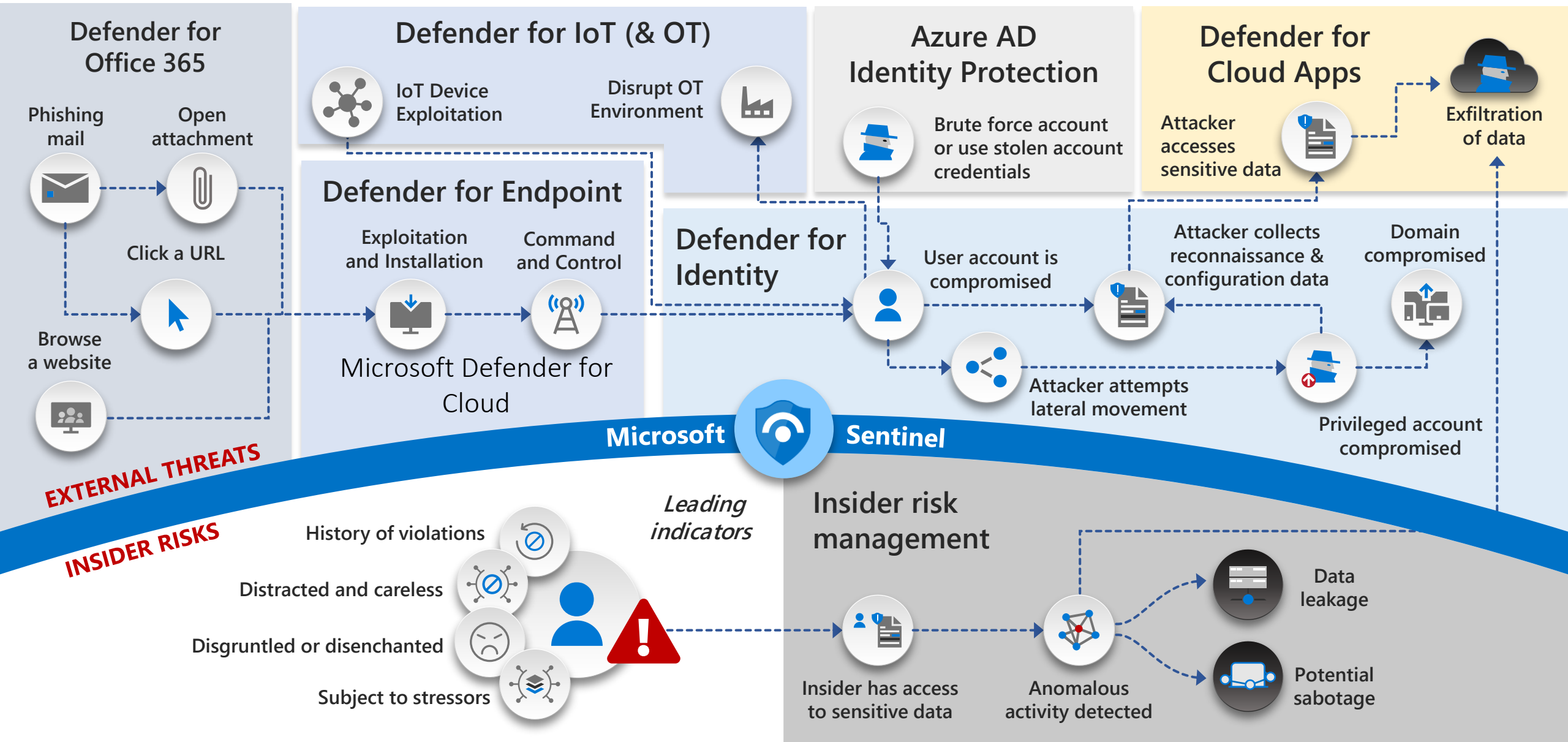
**Threat Intelligence** – 8+ Trillion signals per day of security context

**Service Trust Portal** – How Microsoft secures cloud services

**Security Development Lifecycle (SDL)**

# Defend across attack chains

Insider and external threats



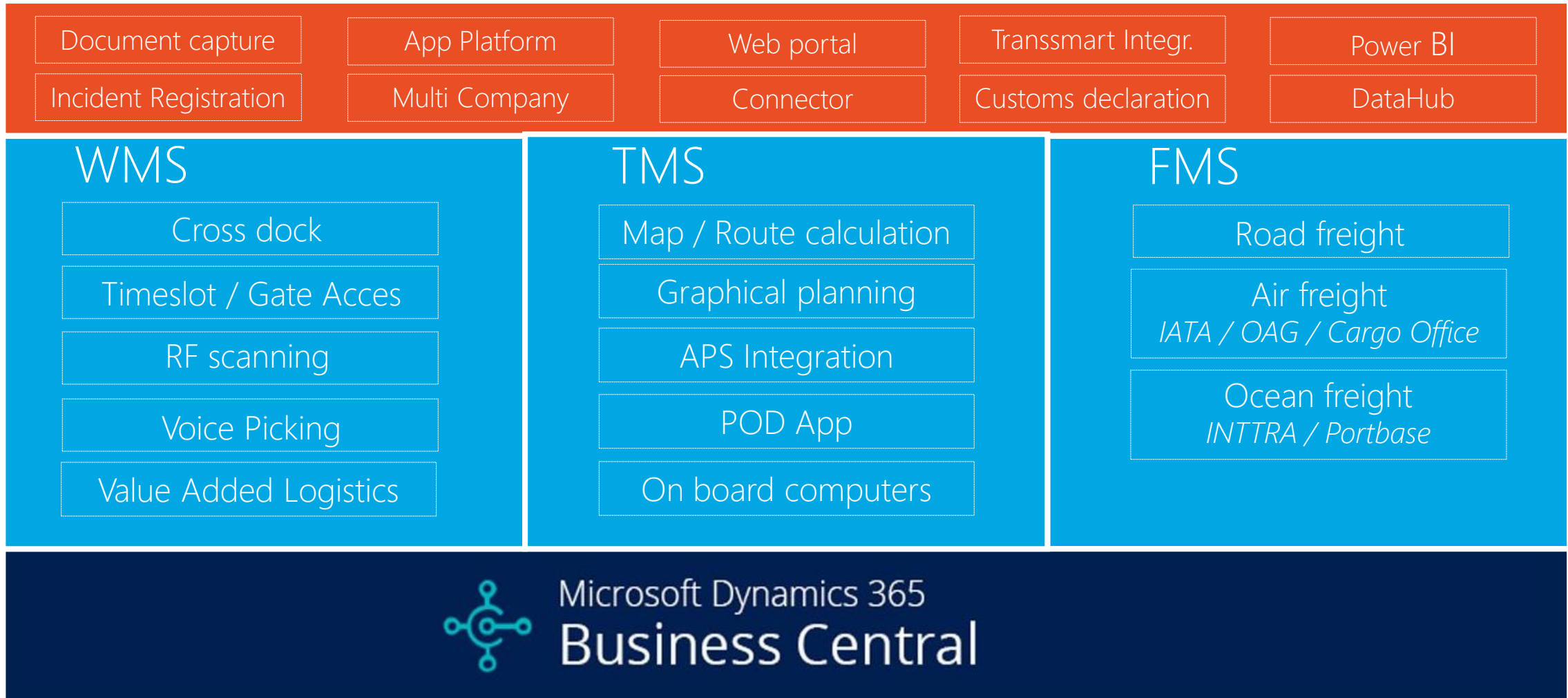


# 7 Practical Cyber Security tips from Microsoft

1. Maintain antivirus and security software
2. Manage identities and access
3. Protect devices
4. Lock unattended machines
5. Consider a VPN for Remote Access
6. Provide security training and reminders
7. **Use secure tools built for business**



# Software Solution for 3PL Cold Stores: Boltrics 3PL Solution Business Solution delivered on Cyber Secured Microsoft Azure Platoform!





# Customer Story



Mercurius IT

2,143 followers

3mo • Edited • 

As the world's largest temperature-controlled logistics service provider, [Lineage Logistics](#) decided that 3PL Dynamics is and will be the standard WMS for all sites in Europe. After a successful go-live, Lineage Logistics Peterborough is the first site in the UK to streamline its cold storage processes with the new future-proof WMS after implementation with Mercurius IT.

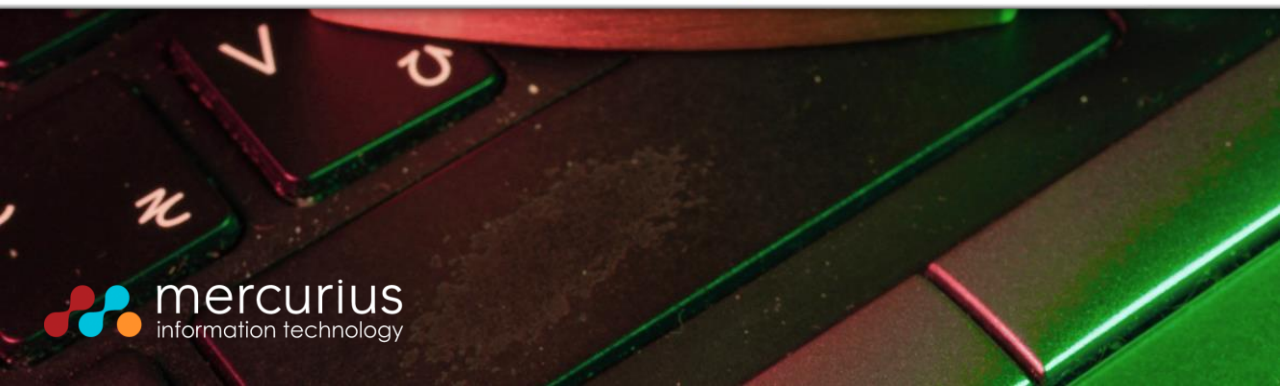
[Elise Ramsden](#), Lineage Project Manager: 'After this successful implementation, we do not only follow the path of Lineage Europe. We can also trust on functionalities from the cold storage industry. Now, we can easily trace all goods in our warehouse and match all of our customer requirements.'

Read the complete article here: <https://lnkd.in/e-PqVxsc>



Lineage Logistics Peterborough successfully live with new future-proof WMS

mercuriusit.com • 2 min read







**Smithfield**

Food company secures data in a hybrid cloud

"Microsoft has a great commitment to the problems of the enterprise. The security built into Azure is huge for us and ensures the safety of our data wherever it is."

Julia Anderson, Global Chief Information Officer



# Contact us for “Cyber Security Readiness”!



**Jay Tahasildar:** Founder & Managing Director

E-mail: [jay.t@mercuriusit.com](mailto:jay.t@mercuriusit.com)



**Scott McKenzie:** Marketing Manager

E-mail: [scott.m@mercuriusit.com](mailto:scott.m@mercuriusit.com)

A close-up, slightly blurred photograph of a large pile of fresh raspberries, filling the background of the slide.

Thank you for joining.

[www.mercurius.com](http://www.mercurius.com)



# FOOD SECURITY WEEK



## ENSURING FOOD SAFETY & TACKLING MODERN SLAVERY IN AN INCREASINGLY UNCERTAIN WORLD

THURSDAY 19 MAY 2022 @ 10:30

What are the key risks to businesses and the wider supply chain following Brexit and other recent world events? How to protect against the risks, remain vigilant and report suspicious activity?

[www.coldchainfederation.org.uk/events/](http://www.coldchainfederation.org.uk/events/)

SUPPORTED BY



Sean Daly  
Relationship Manager  
National Food Crime Unit



Rachel Ward  
Managing Scientist  
Exponent International Ltd



Hannah Lerigo-Stephens  
Business Liaison Officer  
Stronger2gether