

Cyber East

Welcome to Adastral Park

Welcome to Cyber East

Cyber East is an industry body that works alongside the UK Government to develop the cyber security industry in the UK.

Our aim is to partner with cyber security businesses in the East of England and provide a platform for collaboration and growth within the Cyber Security industry.

Shaun Mary

Director



Agenda

12:45-13:00	Registration
13:00-13:10	Open & Welcome from Cyber East
13:10-13:40	Speaker #1 - Andy Compton
13:40-14:10	Speaker #2 - Stuart Golding
14:10-14:40	Speaker #3 - Mark Wrighton
14:40-15:00	Q&A Panel - all speakers plus guest from Sizewell C
15:00-15:10	Closing Thoughts & Prize Draw
15:10-16:00	Networking & Refreshments

CEO
Cortida

Andy Compton



1. Supply chain attacks are increasing

2. They can be deliberate or accidental

3. Attackers and motivations vary

4 Supply chains must be governed

Ripple affects



Availability attacks on supplier of seeds	Integrity attacks on ripeness sensors	Integrity attacks on packaging systems	Integrity attacks on forecasting or routing	Integrity attacks on refrigeration systems	Hunger
No crops	Food spoils	Food spoils	Empty shelves	Food spoils	

Definition



An attack that compromises a product, service, supplier, technology, or other trusted element within an organisation's supply chain, and then uses that compromise to access, disrupt, manipulate, or further attack the target organisation or its customers.

– National Cyber Security Centre (NCSC)

Are they always deliberate?



Yes	**Espionage, political and ideological objectives**
Yes	**Revenge, financial gain and commercial advantage**
No	**Human error, negligence and mistakes**
No	**Coding errors, insecure development, misconfigurations and inadequate security**

What is being attacked - CNI



Health services

2024 attack on laboratory services supplier to NHS, disrupted 10,000+ appointments



Food chain

2024 attack on Blue Yonder severely disrupted warehouse management, inventory tracking and fresh food distribution impacting major UK food retailers



Transportation

2025 - Collins Aerospace, the common system supporting airline check-in, boarding and baggage operations

Automated check-in, boarding and baggage processes were disrupted,



others

- Energy
- Water
- Finance
- Comm’s
- Defence

Dependency Attacks

What is being attacked – Non CNI



Retail

Attack M&S access through a third-party contractor's service desk leading to suspension of online order and Click & Collect

Est £300m impact



Automotive

Attack on Jaguar Land Rover halted production for 5 weeks impact impacted 5,000 organisations across its supply-chain

Est £1.9 billion



Luxury Goods

Attackers compromised credentials linked to a 3rd party system to gain access onto a public facing portal and then to probe internal network segments

Stopped at the last minute through monitoring



Leisure

Marriott International's reservation's database environment hacked exposing guest names, contacts, passport numbers, travel and reservation details.

Access through a third -party component of an acquired company

Third parties involved in

48%

of breaches in Verizon's 2026 dataset – a 60% year on year increase.

How big is the problem?

- **65%** Organisations surveyed reported experiencing a software supply chain incident in the previous 12 months. – **2025 Black Duck Research**
- **54%** More than half of surveyed organisations reported suffering a software supply chain attack in the previous 12 months.- **2024 – Synopsys and Ponemon Institute**

Why the growth?

- **Increased reliance on third parties** - Organisations increasingly depend on external suppliers to provide essential technology and services
- **Software dependencies** - Often contain code and components developed by multiple external organisations
- **Trust built in** - Attackers can exploit trust between suppliers and their customers
- **Fourth-party blindness** - Increasing use of multi-party solutions where the contractual obligations are limited to the 3rd party

What do the attacks look like?

Deliberate Attacks



Accidental Attacks



Who might an attacker be?



Criminal Groups

64%

Attributed to a criminal group



Nation States

13%

Attributed to state-sponsored or patriotic hacktivist groups

*where a threat actor was identified



Insider Actors

83%

Organisations experiences at least one insider threat incident in 2024

What motivates attackers?

Attacker	Financial gain	Espionage	Political / ideological	Disruption / sabotage	Personal gain / revenge
Cybercriminal groups	**High**	Low	Low	Medium	Low
Nation-state attackers	Medium	**High**	**High**	**High**	Low
Hacktivists	Low	Low	**High**	**High**	Low
Malicious insiders	Medium	Medium	Low	**High**	**High**
Industrial spies	**High**	**High**	Low	Medium	Low
Competitors	**High**	Low	Low	Medium	Low

A closer look at insider actors



Malicious actors

People with a grudge or reason to cause harm

e.g. disgruntled employees.

28%



Compromised individuals

Staff who are being pressured or coerced into helping a third party.

12%



Unintended outcomes

Accidental or careless disclosure of credentials, documents or secrets.

60%

Why might someone be open to coercion



Personal Predispositions

- Maladaptive coping mechanisms
- Anxiety
- Depression
- Personality or social skills issues

Stressors

- Personal lives
- Workplace
- Financial

Multipliers

- Unsettling planned or unplanned workplace change
- Formal HR processes
- External coercion

Concerning behaviors

- Interpersonal relationships
- Misuse of tech
- Disregarding security rules
- Unusual financial decisions
- Social Media use
- Excessive or unusual travel or time off



Predispositions, stressors and **multipliers** can make individuals fragile and precarious, much like a house of cards.

Supply chain security principles

1. Understand the risks	Understand what need to be protected and why, know your suppliers and their own security.
2. Establish control	Communicate your needs to suppliers, build needs into your processes and contracts.
3. Check your arrangements	Build assurance into your approach to manage your supply chain.
4. Continuous improvement	Encourage continuous improvement within your supply chain and build trust with suppliers.

National Cyber Security Centre
a part of GCHQ

How to proceed - Understand risk

Tier suppliers into categories based on the risk they present

High Risk

- Stores, processes, transmits or shares personal, sensitive or special category data. Examples of sensitive data are: information about vulnerable data subjects such as children or vulnerable adults. Examples of Special category data such an individual's race, ethnicity, politics, religion, trade union membership, genetics, biometrics, health, sex life or sexual orientation
- Stores, processes, transmits or shares confidential or sensitive business data
- Provides a communication mechanism through which organisation data or that of its employees, customers, partners or supplier data could be transferred or shared
- Provides, manages, configures, develops or personalises systems or applications that involve connecting to or interacting with organisation systems or data or that of data subjects contained within them
- Has trusted access to a physical building in which information systems or records are stored
- Tracks individuals online or off-line location or behaviour or process personal data on a large scale
- Applies profiling or automated decision-making to make decisions about people, e.g. profiling of individuals to make decisions concerning employees performance at work
- Provide organisation with services for the destruction or disposal of paper records or systems and devices containing information

How to proceed - Understand risk

Assess suppliers against and appropriate baseline of infosec and data protection measures

Identify baseline needs

Based on understanding of risk or risk category, determine a controls baseline requirement for infosec and data protection measures.

Assess in-place controls

Asses against baseline, typically, through questionnaires or for extremely high-risk suppliers through validation exercise such as audits or other external validation.

Decision

Issue approval, conditional approval or rejection, albeit it, subject to completion of diligent selection process

Diligent selection & contracts

Assess suppliers against non-technical requirements and build safety into supplier contracts

Selection

- Supplier history
- Qualifications
- Business references from previous engagements
- Financial
- Reputation
- Legal and regulatory compliance history
- Use or 4th parties
- Insurance coverage
- disaster recovery/ business continuity capability
- Values alignment
- Value for Money

Contractual

- Comply with all legal, regulatory requirements
- Flow down agreements to 4th parties
- Confidentiality agreements
- Indent reporting requirement and right to audit
- Return/destruction of confidential information on termination
- Deliver services with skill and competency
- Maintain adequate insurance

Continuous oversight

Risk Level	Checks & Triggers	Frequency	Who
High	Performance levels	12 months or on significant change or falling standards or incidents	Supplier owner supported by: InfoSec? Data Protection? Procurement?
	Questionnaires & audits		
	Incidents		
	Changes to org, tech or locations		
	4th Party checks		
	Insurance & Viability		

Thank you

Andy Compton
Cortida Limited

Linkedin

Cortida

Direct Dial :
+44 (0) 796 969 7217

Email:
acompton@cortida.com

Web:
www.cortida.com

Offices:
Jersey | Guernsey | London

CEO
UK Data Secure

Stuart Golding



KEEP SUPPLIER RISK MANAGEMENT LIVE

Turn an established process into everyday business practice

Stuart Golding – CISM | CIS LI | PCIP

CEO – UKDataSecure - www.ukdatasecure.com

07824 445375

info@ukdatasecure.com

ukdatasecure

The Third-Party Service Provider (TPSP) process exists; now make it useful.

Make better supplier decisions, spot early warnings, fewer surprises and less forms.

Use it in decisions

Bring supplier risk into renewals, changes, projects, incidents and management meetings.

Keep evidence current

Replace annual chasing with scheduled and event-driven checks.

Act on findings

Give every gap an owner, due date, treatment and escalation route.

Change the effort

Use different evidence and controls for different supplier types and levels of risk.

Management should be able to name the highest supplier risks and show what is being done about them.

Run it as a business rhythm

Build supplier risk into work that already happens, rather than creating a separate annual exercise.

Every month	New suppliers, material changes, incidents, overdue actions and expiring evidence.
Every year minimum	Critical-supplier health, service performance, security issues, exposure and exit readiness.
At renewal	Reconfirm need, owner, tier, evidence, contract position, value and alternatives.
Something Changes	Reassess after acquisition, new sub-processor, new integration, AI feature, data change, outage or breach.

Keep one live register and link it to contract dates, service owners, incidents, actions and evidence.

Give ownership to the people using the service

Supplier risk cannot sit only with security, IT or procurement.

Business owner

Owns the need, impact, performance, fallback and risk acceptance.

IT / security / privacy

Checks access, data, technical risk, incidents and assurance evidence.

Finance / procurement / legal

Tracks spend, renewal, viability, terms, insurance and commercial options.

Management

Challenges overdue critical risks, weak exceptions and over-dependence.

Minimum operating rule

No critical supplier without a named business owner and a named deputy.

The supplier owner provides the judgement, specialists provide evidence and challenge.

Identify the different types of supplier

One-person consultant

Managed Service Provider (MSP) / IT provider



Physical service provider

Large Software-as-a-Service (SaaS) provider

Use different methods for different suppliers

One questionnaire does not fit everybody. Match the review to the risk and the supplier's reality.

One-person consultant

Identity, confidentiality, device security, backups, availability and substitute arrangements.



Physical service provider

Site access, staff screening, keys/cards, safety, supervision, disposal and incident reporting.



Managed Service Provider (MSP) / IT provider

Privileged access, remote tools, logging, patching, backup, subcontractors, rapid containment.



Large Software-as-a-Service (SaaS) provider – including AI models and tools

Trust centre, audit reports, service status, terms, sub-processors, configuration and exit plan.



One-person consultants: manage dependency as well as security



A sole consultant may be low-tech but still business-critical.

Practical controls

- Confirm exactly what data, systems and premises can be accessed
- Use a simple confidentiality and data-handling schedule
- Require MFA, supported devices, encryption and secure transfer
- Agree backup contact, handover notes and return of information

Business continuity controls

- Record illness, holiday and key-person dependency
- Avoid shared accounts and permanent admin access
- Check professional indemnity and cyber cover where relevant
- Review access at least quarterly and remove it immediately on exit

Do not demand compliance certification (eg. CE / ISO 27001) from a sole trader. Demand clear, realistic controls for the actual risk.

Physical service providers: focus on people, places and access



Cleaning, maintenance, security, waste and facilities firms can reach places and information that systems cannot.

Before access

Named staff, induction, screening where justified, badges/keys, restricted areas and supervision.

During service

Sign-in/out, visible identification, secure storage, no photography, reporting of lost access items.

Information handling

Secure disposal, no papers left exposed, controlled use of USB/mobile devices and confidentiality.

When the service ends

Return keys/cards, remove accounts, collect equipment and confirm deletion or return of records.

Check delivery on site; a perfect policy at head office does not prove that local staff follow it.

Managed Service Providers (MSP): privileged access is critical



An MSP can administer identity, devices, backups and security tools. That access can spread an incident quickly.

Access

Named accounts, MFA, separate admin roles, least privilege, approval for high-risk work.

Visibility

Logs available to the customer, alerts for admin activity, asset and software records.

Resilience

Tested backups, recovery priorities, alternate contacts, customer-owned emergency access.

Supplier chain

Know remote-management tools, cloud platforms, subcontractors and offshore support.

Response

Immediate containment rights, agreed notification, evidence preservation and joint exercises.

Exit

Credential rotation, documentation handover, data export and clean removal of tools/agents.

Large Software-as-a-Service (SaaS): work with the evidence you can get

When terms are non-negotiable and questionnaires are refused, make a deliberate risk decision instead of pretending assurance happened.

Read the public evidence	Trust centre, Cyber Essentials, ISO certificate, SOC report, PCI DSS, privacy terms, sub-processors, status history and security notices.
Check scope and dates	Confirm the product and locations are covered; record issue date, expiry date and audit period.
Configure your side	MFA, Single Sign On (SSO), roles, logging, retention, sharing, export controls and approved integrations.
Record gaps	Unacceptable terms, unclear deletion, weak incident wording, no audit report or poor portability.
Decide treatment	Assess risk, accept, limit use/data, add compensating controls, choose another product or obtain management approval.



A click-through contract is still a contract.
Save the terms and privacy notice that applied when you signed up.

Make trust-centre review perpetual

Use the supplier's own assurance hub as a live source, not a document downloaded once and forgotten.



- Bookmark the trust centre, status page and sub-processor page
- Subscribe to updates and security advisories where offered
- Track CE, ISO, SOC, PCI DSS and penetration-test dates
- Recheck scope, exclusions and audit findings, not only the badge
- Compare changes in terms, regions, features and sub-processors
- Store evidence with review date, reviewer and decision

Treat certification and audit evidence as time-limited

Independent assurance is valuable, but only if it is current, relevant and followed up.

ISO 27001 certificate

Check legal entity, locations, services, scope, issue and expiry. Ask for the Statement of Applicability if risk justifies it.

SOC 2 Type II report

Check the audit period, exceptions, subservice organisations and customer responsibilities.

Cyber Essentials (Plus) / PCI DSS

Check expiry and whether the certified organisation and scope match the service.

Penetration-test summary

Check date, scope, severity of findings, retest and remaining high-risk issues.

Set evidence expiry alerts 90, 60 and 30 days before renewal.
Escalate if critical evidence lapses.

Keep tiers current: criticality changes with use

Tiering is not a label for life. Re-tier when dependency, access, data, reach or alternatives change.

Move up a tier

New sensitive data; privileged access; more users; integration with core systems; no practical replacement; repeated outage.

Move down a tier

Service retired or reduced; access removed; data minimised; effective substitute tested; dependency genuinely reduced.

Mandatory reassessment

Material incident; acquisition; hosting move; new sub-processor; major AI feature; contract change; financial concern.

Five questions to retest

- How long can the business operate without it?
- What data or access does it now have?
- How many services depend on it?
- How quickly can it be replaced or worked around?
- Would failure cause customer, legal or safety harm?

Any “yes, this is worse” answer should trigger re-tiering and a fresh treatment decision.

Keep the Third-Party Service Provider (TPSP) Policy alive

The policy should direct everyday decisions and change when the operating model changes.

Review triggers

Annual policy review plus major incident, audit finding, acquisition, new law or material sourcing change.

Coverage

Consultants, physical services, MSPs, SaaS, software, data sources, AI models, APIs and fourth parties.

Clear rules

When review is needed, who owns it, evidence expected by tier, approvals, exceptions and exit.

Usable records

One register, standard evidence folder, actions log, decision record and expiry dates.

Exceptions

Named approver, reason, compensating controls, review date and automatic expiry.

Measures

Critical reviews on time, overdue actions, expired evidence, unowned suppliers and tested fallbacks.

Where the process commonly goes wrong

Most failures are operating failures, not missing paperwork.



Register becomes stale	No owner, no link to joiners/leavers, projects, finance or renewals.
Everyone gets the same review	Small suppliers are overwhelmed while critical suppliers receive shallow checks.
Evidence is collected but not read	Expired certificates, audit exceptions and out-of-scope services are missed.
Problems have no consequence	Actions remain overdue and non-compliance is repeatedly accepted.
SaaS is waved through	Click-through terms and lack of questionnaire response become excuses for no decision.

When a supplier will not comply

Use a consistent decision ladder and avoid endless chasing with no decision.

Confirm the gap

State the unmet requirement, evidence requested and business risk in plain English.

Ask for an alternative

Trust centre evidence, management attestation, limited report, meeting or independent certificate.

Reduce exposure

Limit data, access, users, integrations or duration; strengthen monitoring and backup.

Set a deadline

Agree an action owner and realistic date. Escalate before renewal or expansion.

Decide

Accept formally, pause onboarding, restrict use, replace the supplier and exit.

Risk acceptance is a decision with an owner and expiry date, not the absence of a reply.

Five actions to keep the process effective

Make these part of normal operations from the next working day.

1. **Add supplier risk to monthly operations and quarterly management reviews.**
2. **Apply supplier-specific due-diligence instead of one universal questionnaire.**
3. **Subscribe to critical suppliers' trust centres, status pages and assurance updates.**
4. **Re-tier immediately when use, access, dependency, ownership or service changes.**
5. **Escalate expired evidence, overdue actions and non-compliance before renewal.**

Keep the process short, visible, owned and tied to real business decisions.

KEEP SUPPLIER RISK MANAGEMENT LIVE

Turn an established process into everyday business practice

Stuart Golding – CISM | CIS LI | PCIP

CEO – UKDataSecure - www.ukdatasecure.com

07824 445375

info@ukdatasecure.com

ukdatasecure

Founder
Supply Guard

Mark
Wrighton



https://supply-brand.co.uk/experience/cyber-east-ecosystem

Q&A Panel Discussion

Cyber East MEETS...

BECOME A CYBER AMBASSADOR IN YOUR LOCAL CITY



Why become a Cyber Ambassador?

- Share your skills and knowledge with our community
- Be at the heart of your local peer events
- Help us grow and engage our local communities
- Be part of a growing cyber cluster supporting the East region
- Represent Cyber East at events and trade shows

Contact info@cybereast.co.uk for more details

Thank you for joining us today.