# NWSMART5.0

Strengthening North West UK Manufacturing
Through Industry 5.0 Innovation

## WELCOME TO THE WORKSHOP

We will begin shortly

University of Salford MANCHESTER

Greater Manchester Chamber of Commerce

GREATER MANCHESTER IOT

UKRI Engineering and Physical Sciences Research Council

CyberFocus

CENTRE FOR SUSTAINABLE INNOVATION

NWSMART5.0

# WHEN CYBER ATTACKS DISRUPT PRODUCTION

## Building Resilient Manufacturing Operations

**University of Salford**
NWSmart5.0 Workshop Series

# Dr Sadaf Hina

Lecturer in Cyber Security
University of Salford

## Additional Roles

- Strategy, People and Research Environment Lead
- Cybersecurity Consultant – Greater Manchester

s.hina@salford.ac.uk

https://www.salford.ac.uk/our-staff/sadaf-hina

NWSMART5.0

# Our Journey Today

Exploring how we can build resilience and protect productivity in manufacturing.

## 1. Challenges

Understanding the growing cybersecurity challenges facing manufacturing.

## 2. Shift

Adapting to a new reality where cyber and operations are deeply connected.

## 3. Guardrails

Establishing practical safeguards and best practices to protect people, systems and processes.

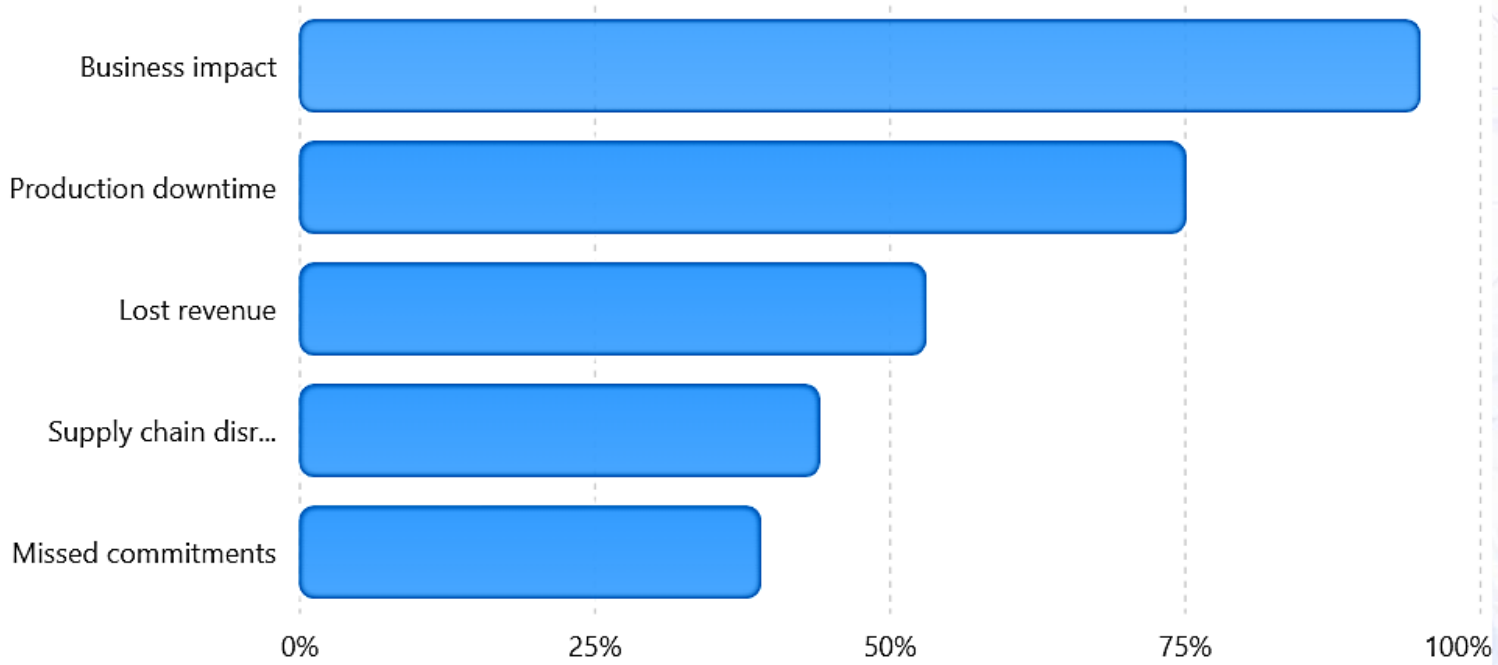
## 4. Road Ahead

Building a more resilient future for productivity and sustainable manufacturing.

# Challenges

## Business impacts reported by UK manufacturers after cyber incidents

Based on a survey of 500 UK manufacturing decision-makers.



NWSMART5.0

# Cybersecurity is no longer just an IT problem.

NWSMART5.0

# WHAT IS IT AND OT?

Business systems and production systems are now more connected than ever.

## IT (INFORMATION TECHNOLOGY)

- Email & Collaboration
- Cloud Services
- Business & ERP Systems
- Data Storage
- Employee Devices

SUPPORTS BUSINESS OPERATIONS

## CONNECTED MANUFACTURING


Shared Networks | Data Exchange | Integration | Visibility

## OT (OPERATIONAL TECHNOLOGY)

- Production Lines
- Industrial Robots
- PLC Controllers
- Sensors & Monitoring
- SCADA Systems

CONTROLS PHYSICAL OPERATIONS

As IT and OT become increasingly connected,
cyber incidents can quickly spread from business systems into manufacturing operations.

NWSMART5.0

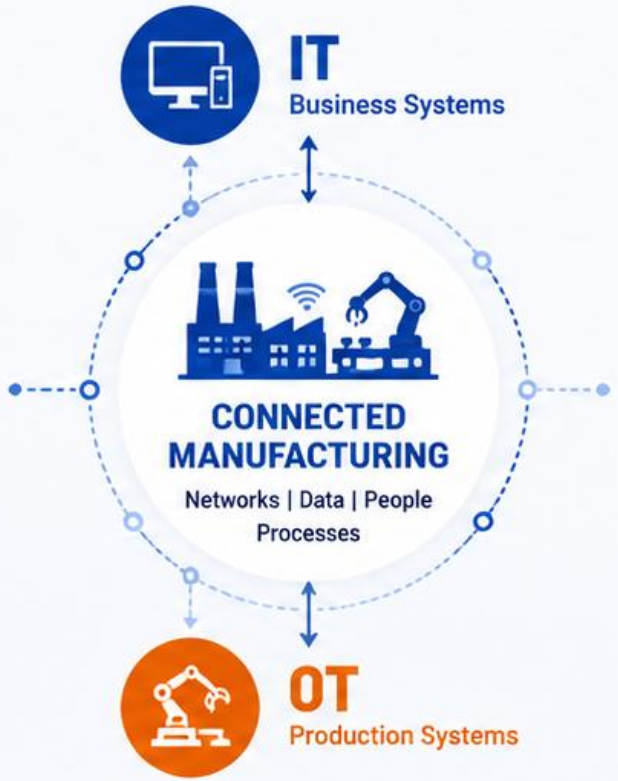
# THREATS TO IT AND OT

Different targets. Shared consequences.

## IT THREATS

- Phishing & Email Attacks
- Stolen Credentials
- Malware & Ransomware
- Cloud & Data Breaches
- Insider Threats

**IMPACT:**
Data loss | Financial loss | Business disruption




## OT THREATS

- Production Downtime
- Compromised Controllers
- Unsecured Legacy Systems
- Third-Party Access Risks
- Safety & Operational Disruption

**IMPACT:**
Production stoppages | Equipment disruption | Supply chain delays

**Cyber attackers increasingly target IT systems as a pathway into operational environments and manufacturing processes.**

NWSMART5.0

# MANUFACTURING IS UNDER ATTACK

Top target. Fast moves. Real impact.

## 27.7%

**#1 MOST TARGETED INDUSTRY GLOBALLY**

27.7% of all cyberattacks

## 29 MINUTES

**AVERAGE BREAKOUT TIME**

Attackers move fast inside compromised environments

## 27 SECONDS

**FASTEST OBSERVED BREAKOUT TIME**

Some attackers move in seconds

Cyber threats to manufacturing are increasing **in frequency, speed, and sophistication.**



Sources: IBM X-Force Threat Intelligence Index 2026 | CrowdStrike Global Threat Report 2026

NWSMART5.0

# How Cyber Attacks Move Through Industrial Environments

The **Purdue Model** illustrates how attackers can move from business systems into operational technology.

## ATTACK PROGRESSION

- Reconnaissance
- Initial Access
- Unpatched Systems
- Lateral Movement
- Command and Control
- Operational Impact

## PURDUE MODEL LEVELS

| | |
|---|---|
| Level 5 | Enterprise IT |
| Level 4 | Business Systems |
| Level 3 | Operations Management |
| Level 2 | SCADA / HMI |
| Level 1 | PLCs |
| Level 0 | Physical Process |

A weakness in one layer can enable attackers to move across multiple layers and ultimately impact production operations.

NWSMART5.0

# REAL-WORLD IMPACT


**JLR (2025)**
Production halted for weeks

**HUNDREDS OF MILLIONS**
**IN BUSINESS LOSSES**

**ESTIMATED IMPACT OF**
**NEARLY £2 BILLION**
**TO THE UK ECONOMY**

**A CYBERATTACK ON ONE SUPPLIER CAN STOP PRODUCTION ACROSS AN ENTIRE MANUFACTURING ECOSYSTEM.**

NWSMART5.0

# Which of these challenges feels most relevant to your organisation?

1. **Legacy OT systems (hard to patch/secure)**
   Outdated systems that are difficult to update and secure
2. **Lack of visibility into production networks**
   Limited visibility across IT and OT environments
3. **Cybersecurity skills shortages**
   Limited internal expertise and resources
4. **Vishing / social engineering attacks**
   People-focused attacks that bypass technical controls
5. **Access brokers & stolen credentials**
   Stolen usernames/passwords sold on the dark web

NWSMART5.0

# Which would have the BIGGEST impact on your production?

Lost output / halted production lines

Missed customer deadlines

Supply chain disruption

Safety or regulatory risks

Other

NWSMART5.0

# SHIFT

NWSMART5.0

# Evolution of Cybersecurity

Cybersecurity has evolved from a necessary cost to a strategic enabler that drives productivity, resilience and safe innovation.

| OLD THINKING | | NEW THINKING |
|---|---|---|
| **Cost & Compliance**<br>Viewed as a necessary expense and compliance requirement | → | **Productivity Enabler**<br>Drives efficiency, uptime and business performance |
| **Reactive Fixes**<br>Responding to incidents after they happen | → | **Continuous Resilience**<br>Anticipates threats and adapts to protect what matters |
| **Security Slows Change**<br>Seen as a barrier to innovation and transformation | → | **Secure Industry 5.0 Transformation**<br>Builds on Industry 4.0 connectivity with resilience, trust and human-centred innovation |

**Cybersecurity is no longer just about protection — it enables innovation, productivity and growth.**

NWSMART5.0

# Which of these shifts is your organisation currently making or planning?

1. Moving to continuous monitoring & real-time visibility
2. Adopting Zero Trust principles
3. Implementing network segmentation (IT/OT)
4. Rolling out MFA more widely
5. Treating cybersecurity as a productivity/ resilience enabler
6. Other

NWSMART5.0

# Quick Wins for Manufacturing SMEs

High-impact actions that can begin this month.

### 1. Adopt Zero Trust Principles

Verify every user and device

### 2. Patch Critical Systems

Including OT gateways

### 3. Staff Awareness Training

Phishing & deepfakes

### 4. Map Critical Assets

Know what matters most

### 5. Test Backups

And recovery procedures

### 6. Review Third-Party Access

Suppliers & contractors

### 7. Network Segmentation

Separate IT and OT to contain threats

**Start small. Build momentum. Strengthen resilience.**

NWSMART5.0

# Where Would You Start?

If you could implement one improvement tomorrow, where would you begin?

1. **Security by Design**
   Build security into systems from the start
2. **Network Segmentation**
   Protect production by separating IT and OT
3. **Access Controls that Support Operator Workflows**
   Give people the right access at the right time
4. **I'm not sure**
5. **Other**

Your priorities today shape a more secure, productive tomorrow.

NWSMART5.0

# GUARDRAILS

Practical controls that protect your operations and enable recovery.

NWSMART5.0

# CYBERSECURITY STANDARDS & FRAMEWORKS FOR MANUFACTURING

Use proven frameworks and standards to protect OT, IT and your extended supply chain.

## NIST CSF 2.0

Cyber risk management framework

GOVERN | IDENTIFY | PROTECT | RESPOND | RECOVER

Comprehensive, flexible and widely adopted for managing cyber risk.

## ISO/IEC 27001:2022

Information Security Management System (ISMS)

ESTABLISH | IMPLEMENT | IMPROVE | ASSURE

Internationally recognised standard for managing information security.

MOST RELEVANT FOR MANUFACTURING

## IEC 62443 SERIES

Industrial Automation & Control Systems Security

POLICY & PROCEDURES | SYSTEM DESIGN | SYSTEM INTEGRATION | OPERATIONS & MAINTENANCE

The global standard for securing industrial automation and control systems (IACS).

## NIST SP 800-82 REV. 3

Guide to OT Security

ARCHITECTURE & ENGINEERING | SECURITY CONTROLS | OPERATIONS | RISK MANAGEMENT

Practical guidance for securing OT systems and industrial control environments.

## WHY IT MATTERS

- Reduce cyber risk across IT, OT and IIoT
- Protect production uptime and safety
- Meet regulatory & contractual obligations
- Strengthen supply chain resilience
- Enable secure digital transformation

## KEY MESSAGE

**Start with a risk-based approach.**
**Adopt the right frameworks, implement consistently, and continually improve.**

**Sources:** NIST Cybersecurity Framework (CSF) 2.0 | ISO/IEC 27001:2022 | IEC 62443 Series | NIST SP 800-82 Rev. 3

NWSMART5.0

# Basic Cyber Hygiene for Manufacturing

## The foundations of cyber resilience

1

### Firewalls & Secure Internet

Protect networks from unauthorised access.

2

### Secure Configuration

Remove default settings and disable unnecessary services.

3

### User Access Control

Only give users access to what they need.

4

### Malware Protection

Prevent malicious software from compromising systems.

5

### Security Updates

Patch vulnerabilities before attackers exploit them.

**Good cyber hygiene significantly reduces the likelihood of successful attacks and forms the foundation for more advanced security measures.**

NWSMART5.0

# Which cyber control do you think delivers the greatest return on investment?

Multi-Factor Authentication

1

Network Segmentation

2

Asset Monitoring

3

Tested Backups

4

Incident Response Planning

5

Other

6

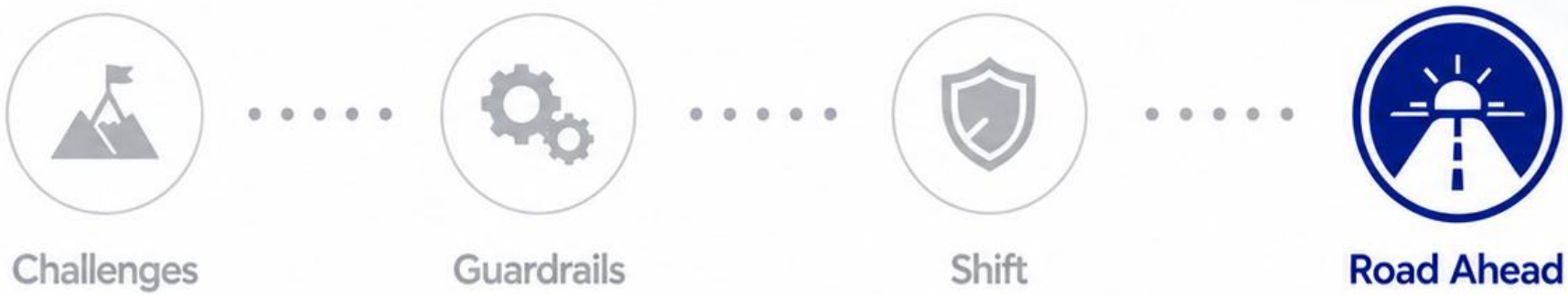
Every organisation faces unique challenges and trade-offs.

Which control do you believe offers the most value for your organisation, and why?

NWSMART5.0

# Road Ahead

Building resilient, productive and secure manufacturing operations



NWSMART5.0

# Cyber Resilience is a Continuous Process

Cybersecurity is not a project with an end date — it is an ongoing business capability.

NWSMART5.0

# Preparing for Industry 5.0

The future of manufacturing is **human-centric, sustainable, and resilient.**

## HUMAN-CENTRED

Empowering people with technology that enhances skills, safety, and well-being.

## SUSTAINABLE

Building responsible operations that reduce environmental impact and support a better future.

## RESILIENT

Creating secure, adaptable, and reliable operations that can withstand disruption and change.

**Resilience is becoming a competitive advantage.**

Organisations that build trust and resilience today will lead the industries of tomorrow.

NWSMART5.0

# Things to Remember

Simple principles that drive meaningful impact.

1

## Security supports productivity

Strong security reduces risk and disruption, enabling people and operations to perform at their best.

2

## Small improvements create momentum

Practical, incremental steps build capability over time and lead to strong, lasting results.

3

## Resilience enables innovation

When you can adapt and recover with confidence, you can innovate, grow and seize new opportunities.

**Secure today. Strong tomorrow. Ready for what's next.**

NWSMART 5.0

# FREE CONSULTATIONS

*Tailored support for your organisation*

Get practical advice and guidance from our team to strengthen your **cybersecurity**, **safe AI** and **digital transformation** journey.

**BOOK YOUR FREE CONSULTATION TODAY!**

**SCAN TO BOOK YOUR CONSULTATION**

## HOW WE CAN HELP

- Cybersecurity assessments and guidance
- Safe AI adoption advice
- Digital transformation support
- Risk management and resilience planning
- Practical solutions tailored to your business

One-to-one support, focused on your needs and challenges.

Let's build a more secure, smart and resilient future together.

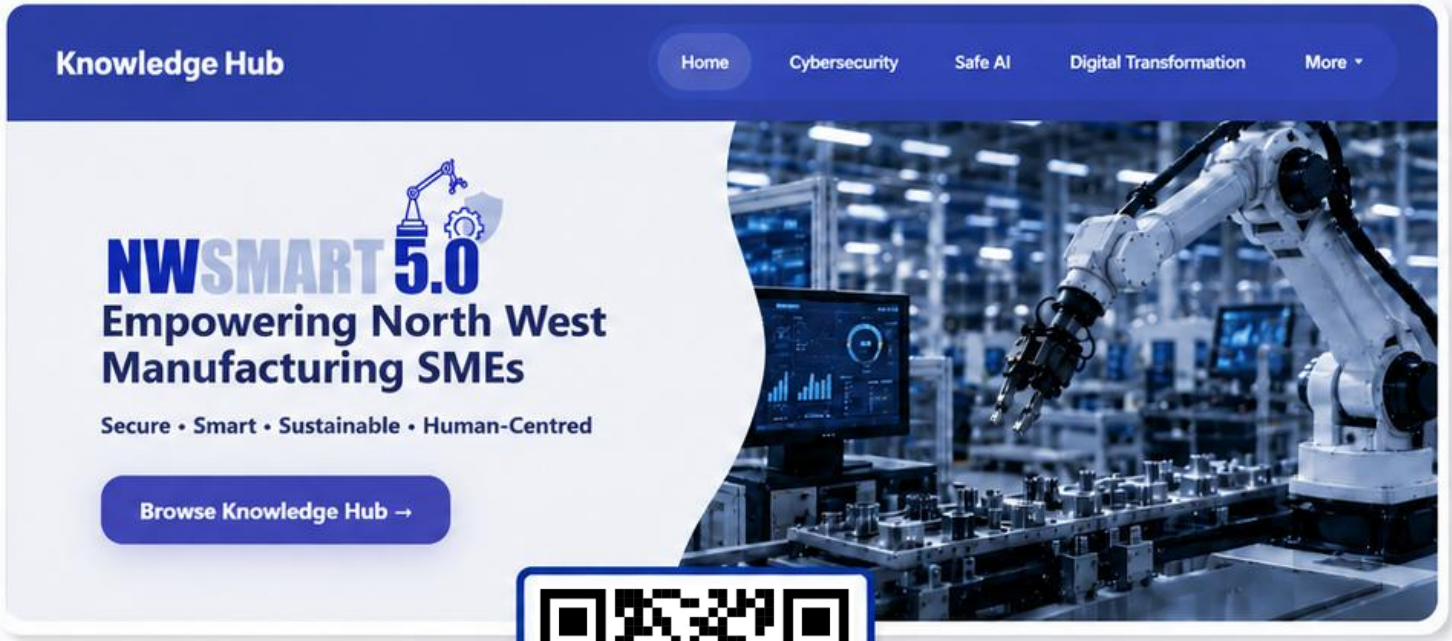
NWSMART5.0

# EXPLORE THE NWSMART5.0 KNOWLEDGE HUB

Your gateway to free, practical resources and expert guidance

## WHAT'S AVAILABLE?

- Cybersecurity Resources
- Safe AI Guidance
- Digital Transformation Tools
- Knowledge Library
- News & Insights
- Workshop Materials




SCAN TO VISIT THE KNOWLEDGE HUB

OR VISIT

nwsmart.secureailab.co.uk

## DESIGNED FOR NORTH WEST MANUFACTURING SMEs

- Manufacturing-focused resources
- Practical cybersecurity guidance
- Support for safe AI adoption
- Digital transformation support
- Free access to tools and resources

**Secure • Smart • Sustainable • Human-Centred**

Supporting North West Manufacturing SMEs through cybersecurity, safe AI and digital transformation.

NWSMART5.0

# THANK YOU

## Any Questions?

**Thank you for your participation!**

Together, let's build secure, productive and future-ready manufacturing operations.

# Sources & References

## Reports & Surveys

### ESET UK Manufacturing Cybersecurity Survey 2026
Used for manufacturing cybersecurity statistics.

### CrowdStrike Global Threat Report 2025
Used for vishing, access broker and threat actor statistics.

These sources have been used to inform the statistics, insights and recommendations shared in this workshop. All sources are publicly available.

## Guidance & Frameworks

### NCSC – Logging and Monitoring
Used for monitoring and visibility recommendations.

### NCSC – Planning Your Response to Cyber Incidents
Used for incident response and recovery guidance.

### NCSC – Operational Technology Security Guidance
Used for OT/ICS security best practices.

### NIST SP 800-82 Rev. 3
Used for ICS/OT security guidance and principles.

### CISA – ICS Security Guidance
Used for industrial control systems security best practices.