JCSC
Jersey Cyber Security Centre

What Can Cybersecurity Incident Responders Learn from Real-World Crises?

Matt Palmer, FIRST Annual Conference, Copenhagen 2025

TLP: CLEAR

Welcome to Jersey

Welcome to JCSC

Founded in 2021 as Jersey Cyber Emergency Response Team (CERT.JE)

Became Jersey Cyber Security Centre (JCSC) in 2023

New Cyber Security Law due 2025/6

Our aim is for Jersey to be internationally recognised as a safe place to live and do business online

Welcome to JCSC

Founded in 2021 as Jersey Cyber Emergency Response Team (CERT.JE)

Became Jersey Cyber Security Centre (JCSC) in 2023

New Cyber Security Law due 2025/6

Our aim is for Jersey to be internationally recognised as a safe place to live and do business online

MEMBERS OF FIRST: JUNE 2025!!

What Can Cybersecurity Incident Responders Learn from Real-World Crises?

Paul Dutot
Head of Cyber Defence, JCSC

Building a National CSIRT at Nano Scale

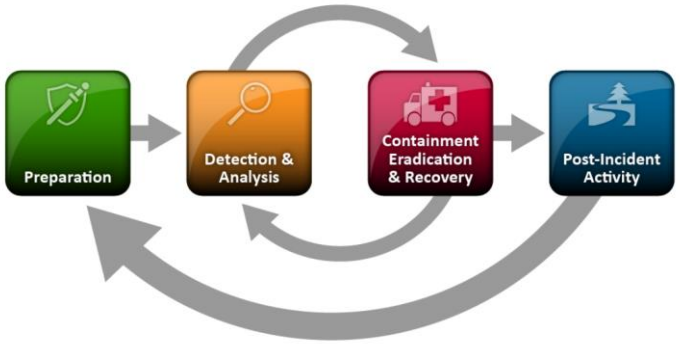
James McLaren
Senior Analyst, JCSC

Aligning Incident Response with Emergency Response Using JESIP

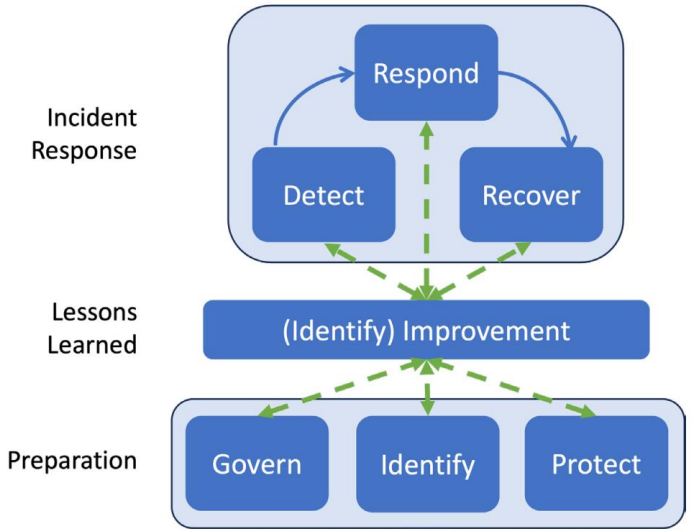
Matt Palmer
Director, JCSC

What Can Cybersecurity Incident Responders Learn from Real-World Crises?

Using Internationally Recognised Cyber Incident Response Models



NIST SP800-61 R2



NIST SP800-61 R3

Using Internationally Recognised Cyber Incident Response Models

ISO27035 3.1.6
information security incident management: collaborative activities to handle *information security incidents* (3.1.5) in a consistent and effective way

NIST SP800-61 R2
Coordinating Team: An incident response team provides advice to other teams without having authority over those teams—for example, a departmentwide team may assist individual agencies' teams. This model can be thought of as a CSIRT for CSIRTs. *Because the focus of this document is central and distributed CSIRTs, the coordinating team model is not addressed in detail in this document.*

Carnegie Mellon IM Maturity Assessment (2018)
4.3.3 IR Coordination: *This capability focuses on the enterprise-wide and external coordination that an organization performs among the various staff or groups that have roles and responsibilities in incident response activities. These can include internal and external groups such as other CSIRTs or external experts. Coordination with these groups occurs to share information and response actions on intrusions, attacks, and suspicious activities…*

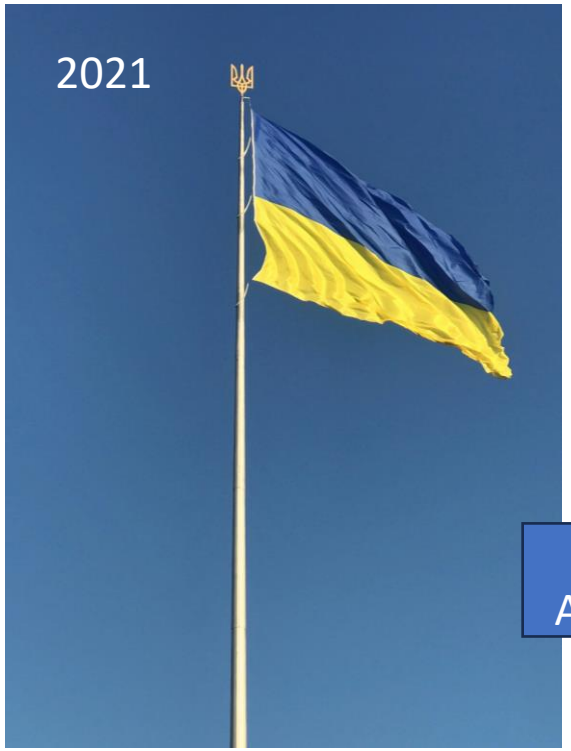
Discovering Cyber Incident Response Models are Not Enough: Part 1

Recognised international standards and frameworks are great where there is a natural hierarchy of authority for responding within an organisation…

And even for information sharing in the CSIRT community or upwards to public authorities….

but are not as much help when you need to co-operate and make decisions in real time across multiple organisations.

Learning to collaborate in real time with industry, gov & emergency services



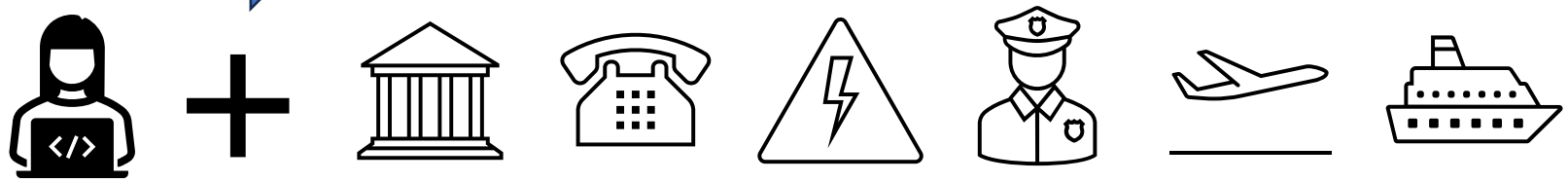
Cyber Technical Advice Cell (C-TAC)

Emergencies Council → Political oversight and direction

Strategic Coordination Group → Gold → Sets the Strategy

Tactical Coordination Group → Silver → Develops the tactics

Functional Cells → Manage impacts



TLP: CLEAR

Learning to collaborate in real time with industry, gov & emergency services

29 October 2023
Storm Ciaran named by UK Met Office

31 October 2023
Met with Emergency Services for Strategic Emergency Management Training

31 October 2023
Storm expected to hit Jersey; training becomes a Co-ordinating Group

1 November 2023
Storm hits. 8.5cm hailstones recorded are largest in British Isles since 1950s; most powerful Tornado recorded in Jersey, - T6/7, previous worst T3

TLP: CLEAR

Why did it work?

JESIP
Working Together – Saving Lives

Principles for Joint Working + Joint Decision Model + Shared Situational Awareness + Standardised Record Keeping

Interoperability is defined as...
the extent to which organisations can work together coherently as a matter of routine.

TLP: CLEAR

Principles for Joint Working

JESIP
Working Together – Saving Lives

CO-LOCATE

Co-locate with other responders as soon as practicably possible at a single, safe and easily identified location.

COMMUNICATE

Communicate using language which is clear, and free from technical jargon and abbreviations.

CO-ORDINATE

Co-ordinate by agreeing the lead organisation. Identify priorities, resources, capabilities and limitations for an effective response, including the timing of further meetings.

JOINTLY UNDERSTAND RISK

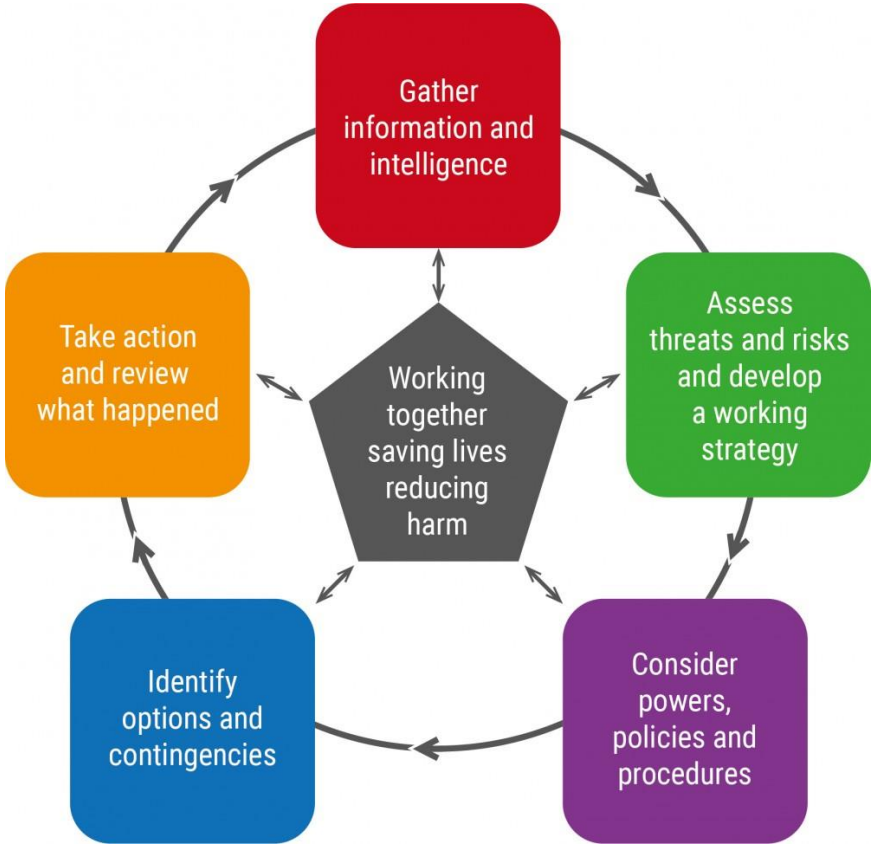
Jointly understand risk by sharing information about the likelihood and potential impact of threats and hazards, to agree appropriate control measures.

SHARED SITUATIONAL AWARENESS

Establish shared situational awareness by using M/ETHANE and the Joint Decision Model.

Joint Decision Model

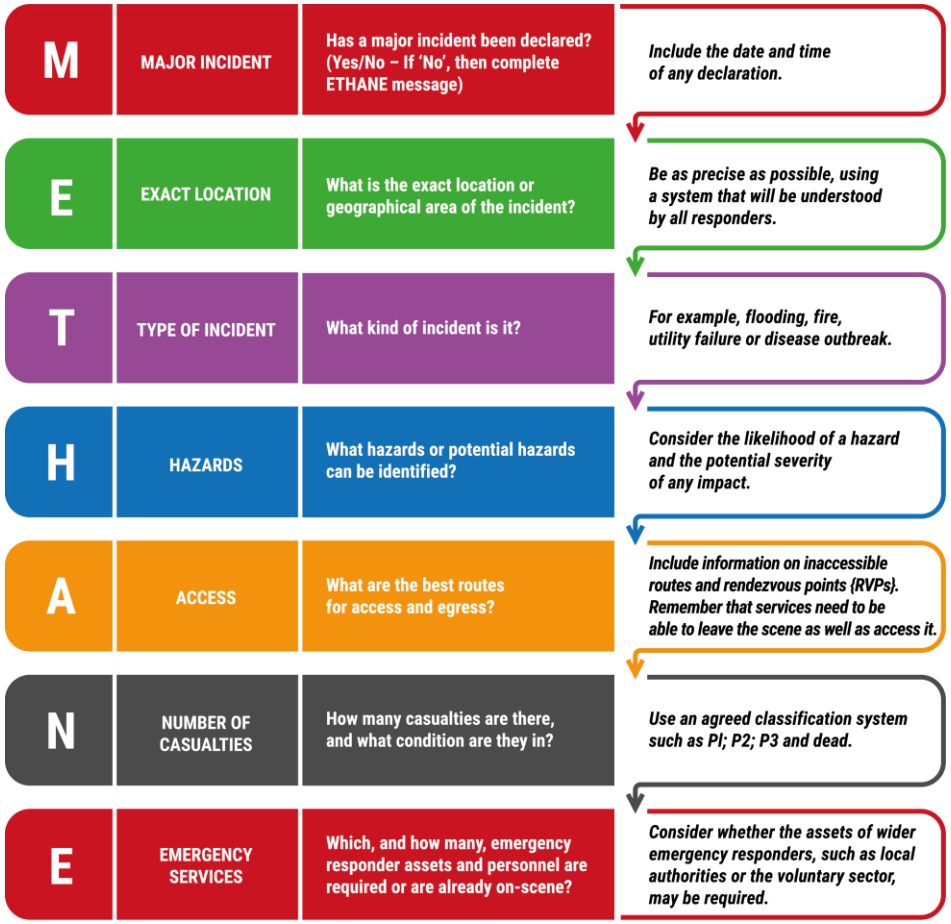
JESIP
Working Together – Saving Lives



TLP: CLEAR

Shared Situational Awareness

JESIP
Working Together – Saving Lives



Standardised Record Keeping

JESIP
Working Together – Saving Lives

TLP: CLEAR

Discovering Cyber Incident Response Models are Not Enough: Part 2

Cyber incident response protocols generally work well during **pure cyber incidents** and for asynchronous information sharing with customers and suppliers to protect technical and financial assets….

*But not as well for **hybrid incidents** when we need to collaborate in real time or implement shared command / coordination structures across industry and the public sector to minimise risk to life or wellbeing.*

However, the lessons we need to apply are well known.

Pollock Report

4 key themes present in all incidents:

- **Doctrine & organisation** – provision of clear and easily understood guidance that ensures everyone is aware of their own and others roles and responsibilities
- **Operational Communications** – the need for a common system used by all stakeholders with the capacity to deal with surges of activity associated with major incidents
- **Shared Situational Awareness** – the ability to quickly access and share information between stakeholders
- **Training & Exercising** – the need for continuous development of stakeholders to ensure sufficient capacity to cope with a prolonged event

1980s	1990s	2000s
1986 Crowd Safety at Football Grounds	1994 Texaco Refinery Explosion	2000 UK Fuel Disputes
1987 King's Cross Underground Fire	1996 Dunblane Shooting	2000 Harold Shipman & 'the 3 Inquiries'
1987 Herald of Free Enterprise	1996 BSE Outbreak Inquiry	2001/2007 Foot & Mouth Disease
1987 Hungerford Shooting	1997 Southall Rail Crash	2001 Victoria Climbie Murder
1988 Piper Alpha Explosion	1997 Stephen Lawrence Murder Inquiry	2003 Failures in NHS Report
1988 Clapham Rail Crash	1999 Ladbroke Grove Rail Inquiry	2003 Bichard Inquiry (Soham Murders)
1988 Lockerbie Bombing		2004 ICL Factory Explosion
1989 Hillsborough Stadium		2004 Boscastle Floods
1989 Kegworth Air Crash		2005 Buncefield Oil Depot Explosion
1989 Marchioness-Bowbelle Sinking		2005 London Terrorist Attacks
		2005 Stockwell Shooting
		2005 Carlisle Floods
		2007 Hull Floods
		2007 Pitt Review (UK Floods)
		2009 Influenza Pandemic
		2010 Derrick Bird Shootings

Manchester Arena

22:30, Monday 22 May 2017

22 lives lost

Some of the lessons learned:

- **Command** – those expected to take command did not do so
- **Communications** – telecoms infrastructure did not work as expected
- **Shared Situational Awareness** – fire service left out of the loop
- **Training & Exercising** – activation of prepared response plan for a suspected Marauding Terrorist Firearms Attack (Plato) not clearly communicated and understood

"we heard heartbreaking evidence of the injured and rescuers … hearing the sirens of ambulances, knowing paramedics were close by, expecting their imminent arrival, only for them not to arrive in the sort of numbers that were needed."

Sir John Saunders, Manchester Arena Enquiry, Volume 2

Some challenges

- ✓ We already have some great tools and frameworks
- ✓ Many organisations already learn from emergency services, for example IR command structures…. *but*
- ➢ Real-time coordination and shared decision making across organisations is hard; clear operational governance and a shared understanding are essential
- ➢ Cyber IR frameworks are better suited to single entity working than to real time multi-entity collaboration. They also don't consistently meet the challenges raised in the Pollock report.
- ➢ We often lack the structured implementation of JESIP tools, with little or no standardised supporting templates, tools and guidance available
- ➢ The language and approaches we use are very different to emergency services – and a need for translation means delays and mistakes

"Had JESIP worked on the 22nd of May [2017], things could and should have been very different"

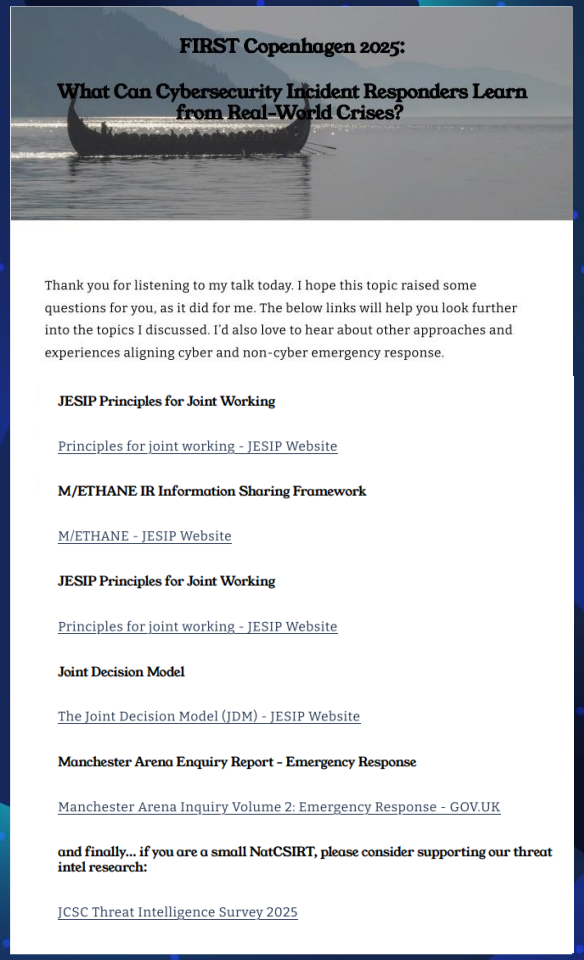
Sir John Saunders, Manchester Arena Enquiry, Volume 2

Some solutions?

- The four key themes from the Pollock report provide good guidance for IR teams in improving practices and integrating with their organisations and communities.
- JESIP principles and tools could be applied to cyber incident management to enhance co-operation and improve outcomes, both within organisations and externally.
- Developing an international approach to **Cyber Incident Interoperability** - aligning cyber incident management with 'real world' emergency response - would help find a common language and raise the ability of cyber IR to support wider goals
- Cyber security functions in organisations could benefit from JESIP style standardised document templates and approaches - to provide better alignment of governance, record keeping and communication.

References & Resources

reference links from this presentation
mattpalmer.net/first-Copenhagen



TLP: CLEAR

Thank you

reference links from this presentation
mattpalmer.net/first-Copenhagen

connect on linkedin
linkedin.com/in/mattpalmercyber

TLP: CLEAR