How To Boost Cyber Resilience Amid Increasing Threats

STORMGuidance

Assured Service Provider

in association with National Cyber Security Centre

Cyber Incident Exercising

Using Cyber Incident Exercising (CIE) to determine coverage limits and much more

STORM Guidance

Full service offering

Assess

Lightweight cyber risk assessments to enable clients to learn and raise their levels of Cyber Risk Management Maturity. Supported with next-gen technology.

Plan

Helping insured clients to create, learn (through training) and exercise/test their plans in dealing with different types of cyber incidents in the context of their business.

Respond

Delivering a fully coordinated and Integrated Cyber Incident Response Team (I-CIRT).

ReSecure: full service offering for insured clients and CIR verification for insurers.

CyberCare: retainer and subscriber for cyber crisis response and proactive services.

The Problem

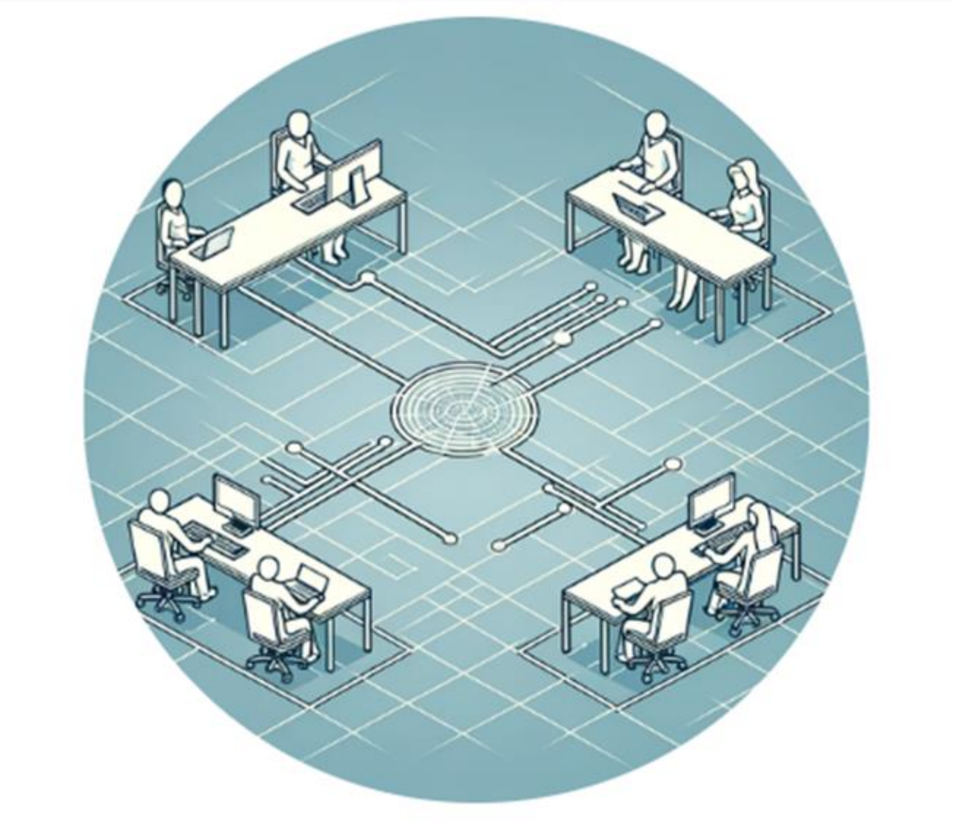
Is your CIR capability going to perform well when an incident occurs?

- ▶ **Uncertain Assessment of Liability, Impact and Risk**
- ▶ **Lack of Preparedness**
- ▶ **Inadequate Response Time**
- ▶ **Physical, Upstream and Downstream Impact**
- ▶ **Communication Breakdowns**
- ▶ **Technical Vulnerabilities**
- ▶ **Compliance Issues**
- ▶ **Lack of Awareness and Training**
- ▶ **Inefficient Incident Management and Recovery Processes**
- ▶ **Insufficient Collaboration with External Parties**
- ▶ **Lack of Internal Skills and Awareness**

Tabletop Exercises

Key elements of the Tabletop CIE experience are:

Our Tabletop CIE's are designed to be delivered in a time-efficient manner by simulating cyberattack scenarios in a controlled, discussion-based setting, it allows participants to think through the processes, procedures, and responsibilities required to effectively respond to and recover from cyber incidents.



Live Play Exercises

Key elements of the Live Play CIE experience are:

Our Live Play CIE's are best suited to mature organisations looking for detailed validation of plans. The exercises immerse participants in a realistic, hands-on scenario where they must respond to simulated cyberattacks with real-time adaptation called 'injects’. This dynamic approach tests the organisation's strategic and operational response capabilities.

CIE Enhanced Experience

We can add a range of media and supporting artefacts to add to the realism and immersive experience of our CIEs

- Digital Media
- Sample Artefacts
- Welcome Packs
- Integrated real-time intrusion test
- Additional Facilitators
- Separate de-briefing session
- Integrated CIR Training

Types of CIE

Hybrid & customised incident scenarios.
We 'walk-the-walk' so we can 'talk-the-talk'

Your selected scenario will be designed around your business. Here are some examples from our library:

- Ransomware & Extortion
- Data Breach & Extortion
- Business Email Compromise (BEC)
- Threat Actor Engagement (TAE)
- Website defacement, Doxing & Disinformation
- Technology-related Fraud
- Denial of Service Attack
- Malware & Network Intrusion Attack incl. Advanced Persistent Threat (APT)
- Operational Technology (OT) and/or Industrial Control Systems (ICS) Attack
- Physical Technology & Information Theft
- Natural Disaster & Information Systems Outage

Focus and Delivery

Our experts have extensive working knowledge of every aspect of cyber incident response

To coin a phrase, "*There really isn't much we have not seen*".

Board-level
Strategic business impact assessment and decision making; reporting to legal and regulatory bodies; threat actor engagement; and external facing communications.

Managerial
Assistance with incident coordination including translation from operational detail to business risks, tracking strategic objectives, tactical decision-making, and wider stakeholder engagement.

Operational
Operational activities carried out as part of an incident response plan including initial triage and escalation as well as technical support for the investigation and systems & data recovery.

Optional CIR Training

Leverage our long experience to understand the blockers and enablers for effective cyber incident response in strategy, tactics and operations.

Training techniques taken from our book on the subject.

- Workshop-based training session
- Pre-or Post CIE delivery
- **Strategic: Board-level/Senior Management considerations**
  - Rolling impact assessment
  - Legal and regulatory considerations
  - Crisis PR considerations
  - Operational funding for CIR activities
  - Insurance considerations
  - Ransom negotiation
  - Coordinator interaction
- **Tactical: CIR Coordination**
  - Establishing secure comms
  - Strategy & Operations Group interaction
  - Update cadence
  - Record keeping
  - Reporting
- **Operational: Technical specialist activities**
  - Best-practice frameworks (NIST/SANS)
  - Detection, Containment & Eradication
  - Evidence preservation
  - Digital Investigations
  - IT Recovery
  - Coordinator interaction

CIR Training activity includes techniques described on the book '*Information Security Incident Management - A Methodology*', written by STORM's Neil Hare-Brown and published by the British Standards Institution (BSi).

Prepare your CIR Team ready for optimal response!

STORMGuidance

Assured Service Provider

in association with National Cyber Security Centre

Cyber Incident Exercising

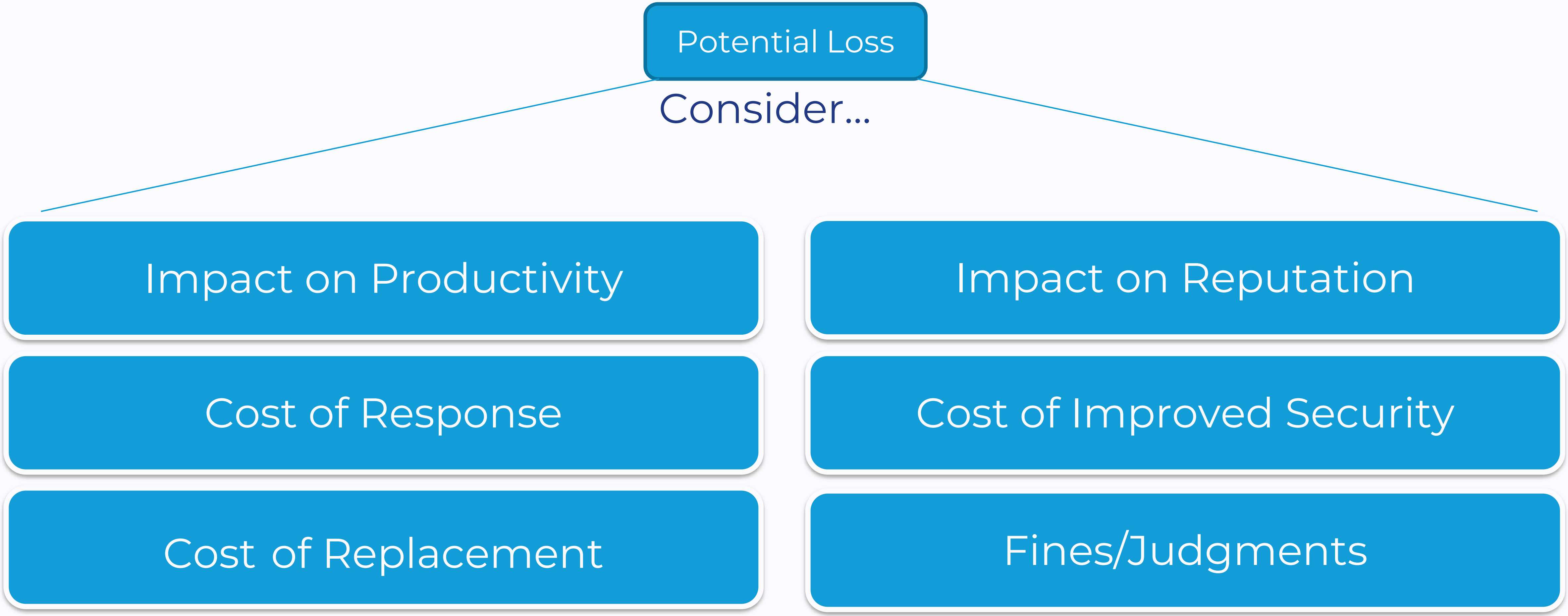
Determining coverage limits during a CIE

Drivers for lost revenue

- Type of incident/trigger
  - **Data breach: with or without extortion**
  - **Unauthorised access & malware: with or without systems outage**
  - **3rd party involvement (upstream/downstream)**
- Primary Loss vs Secondary Risk
  - **Primary Loss**
    - **Cyber Incident Response (CIR), Legal, Increased Costs Of Working (ICOW), Credit Monitoring, TAE/Ransom/Stolen Funds, Systems Recovery, BI (timing in biz schedule)**
  - **Secondary Risk**
    - **Ransom settlement, fraud losses, fines & judgements, data rebuild**
- Readiness for recording BI losses has big effect on actual losses
  - Extensive record keeping during incidents is recommended

Impact Assessment: Key Factors

How Bad?



Potential Loss

Consider…

- Impact on Productivity
- Cost of Response
- Cost of Replacement
- Impact on Reputation
- Cost of Improved Security
- Fines/Judgments

Impact Assessment: Key Factors

Example: ‘1 week outage of due to a ransomware incident affecting the whole network would result in a worst-case cost of £n

Worst Case Cost (£000)

System	Productivity	Response	Replacement	Reputation	Improved Security	Fines & Judgements	Time critical?	Totals
Payroll	0	50	180	200	25	200	Y	655
CRM	120	25	450	200	15	100	N	910
Prod Line A	350	50	800	500	200	350	Y	2250
Prod Line B	250	25	400	250	100	200	N	1225
BMS	100	50	250	125	25	50	N	600
Telecoms	400	50	200	300	50	200	Y	1200
Core servers	500	100	200	300	250	200	Y	1550
Email	250	50	50	200	50	200	Y	800
								9190

Analysis Example

Payroll

- **Productivity**: Time Critical?, Where hosted?, Data unrecoverable?
- **Response**: Technical?, Legal?, Other?
- **Replacement**: Legacy software? On-prem vs cloud?, data re-creation?
- **Reputation**: Staff legal action?, Public Impact on brand? Other Stakeholders?
- **Improved Security**: Time Critical?, Expertise? Hardware/Software?, Physical?
- **Fines & Judgements**: Regulatory penalties, Legal defence? Stakeholder, supplier or customer action?

Patterns of Loss

- Higher Losses - Sector specific
  - **Industrial more likely to have extensive BI losses**
  - **Transactional orgs (time critical)**
  - **CNI Orgs**
  - **Other Regulated orgs (incl. Gambling, Healthcare, Legal)**
  - **Larger organisations IF:**
    - **They are running legacy systems**
    - **Complexity of the data exchanges between systems**
    - **They are highly federated**
    - **They have no board strategy – they assess poorly on CyberSeven (www.cyberseven.global)**
- Cloud dependency – double-edged sword
  - **Heavily reliant on the type of cloud services used**
  - **May be more, or less exposed to BI losses. Is true resilience achieved?**

STORMGuidance