SECURITY FORUM 2025

Cyber security crisis: recovery business case

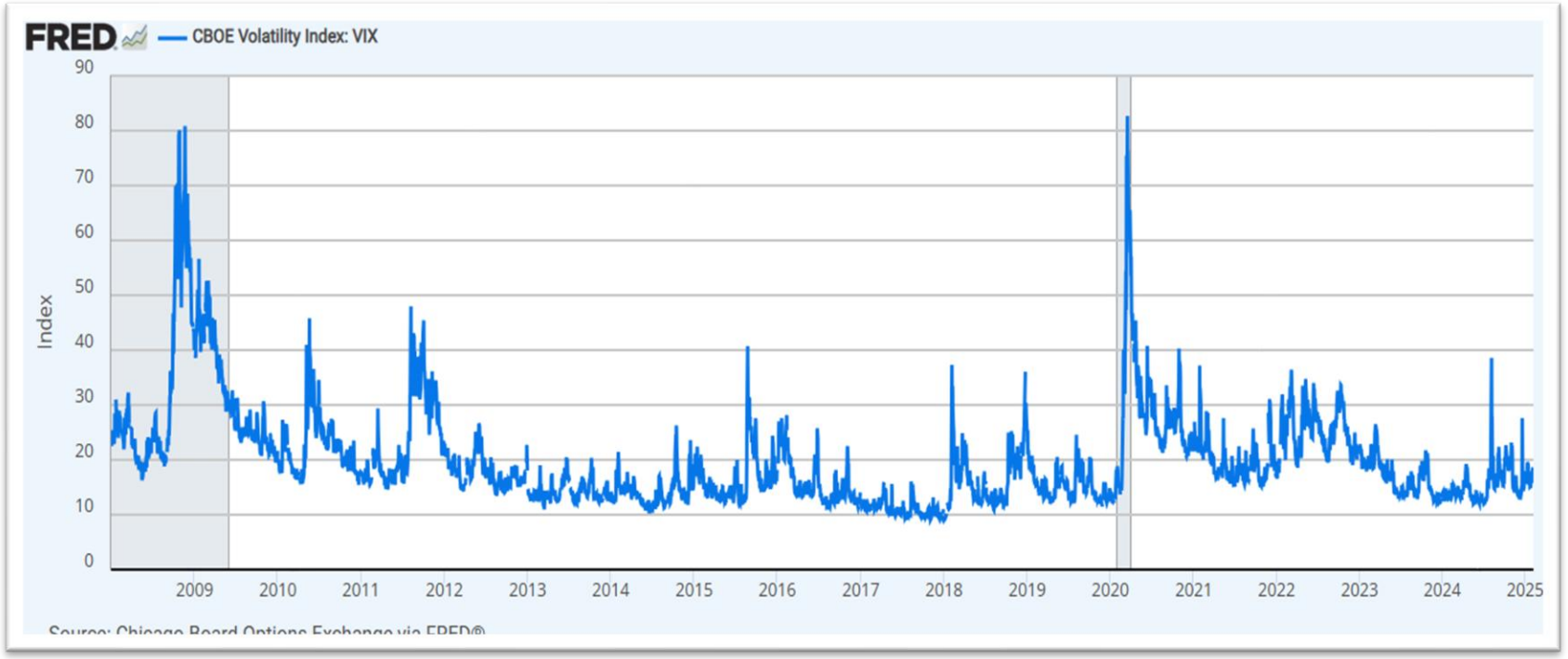
Last update: 02/2025

GRACE CONNECT

"ALL-ROUNDED" PREPARATION TO FACE HIGH VOLATILITY SITUATIONS

READINESS

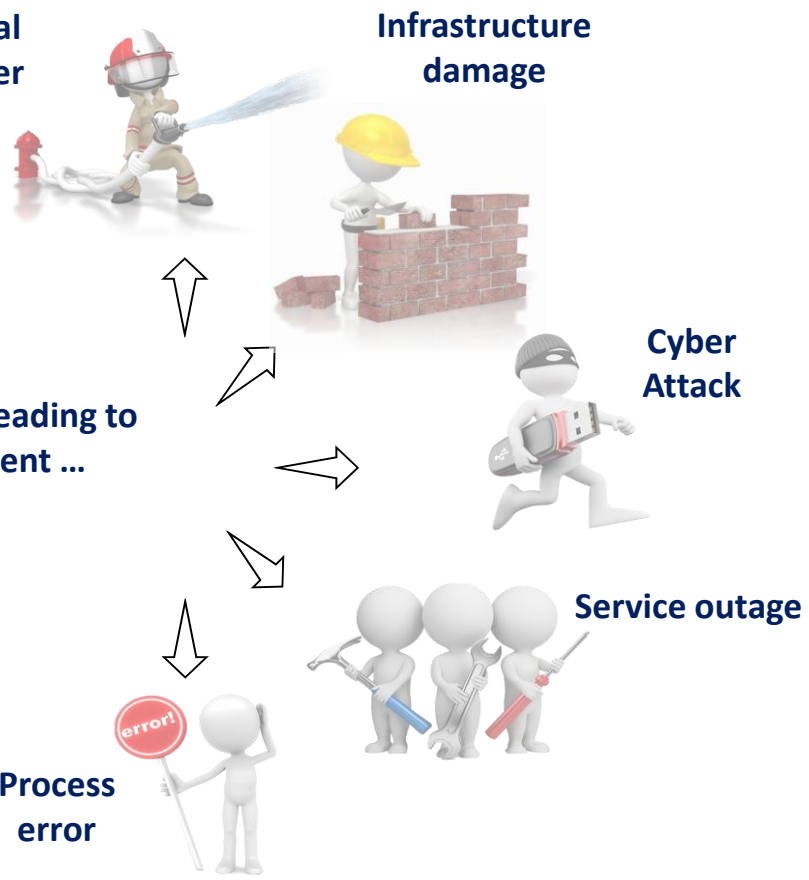
- All rounded preparation means **preparatory activities performed with internal stakeholders to update procedures (CIRP), adjust policies, update contact lists (call trees), adjust the list of critial IT assets (RTO/RPO), organize tabletops exercise, align with external IT suppliers.**
- Preparation phase (readiness) vs incident response phase.: from theory to practice.



The **Volatility Index (VIX)**, often called the **"Fear Index,"** reflects market uncertainty.
Peaks in the VIX correspond to global crises (e.g., 2008 Financial Crisis, 2020 COVID-19 market crash).

WHICH ARE THE RISKS AND THREATS RELEVANT FOR BUSINESS OPERATIONS?

INCIDENT



Different scenarios leading to a disruptive incident …

Attention points:

- Link between business operations , IT assets, IT components, and data.
- Escalation flow:
  - (new) reporting criteria
  - Notification from external IT suppliers
  - Notification from SOC / NOC and severity evaluation
- Concept of Critical or Important functions.

Major impact related to:

- **Building and facilities**
- **Employee's safety**
- **Business interruption**
- **Customer services**
- **Company reputation**
- **Regulatory requirements**

UNDERSTANDING EXTERNAL CYBER THREATS AND IMPACT ON YOUR ORGANIZATION

READINESS

Which are my cyber threats?

Understanding potential cyber security threats which may impact your organizatio is KEY to your business continuity.
Cyber Security attacks could materiailze trough multiple ways:

1. Data breach, Information compromise
2. Espionage
3. Phishing
4. Identity theft
5. Money fraud
6. C-Level fraud (E-mail/phone)
7. Malware breakout
8. Ransomware
9. (D)DOS
10. Sabotage
11. IT / Cyber Vulnerability (Vulnerability scanning)
12. Supply chain attacks
13. (Business) User error
14. Physical loss
15. System failure (HW/SW)
16. Essential services network outage (non – technical)
17. External ICT service provider outage (technical)
18. Copyright violation
19. Legislation changes
20. Crypto-Mining/-Jacking

Effective cyber security management

Combining external source of information (cyber security threats landscape, CTI feeds) with internal information related to your assest and applications, allows to **quantify the potential impact from cyber threats** and **identify the prioritized actions and scope for cyber security monitoring and management**

Which are my Crown Jewels?

Knowing your critical applications and information assets classified in terms of Confidenciality, Integrity, Availability (CIA Classification) allows you to define the scope of your monitoring

CALL TREE ACTIVATION
WHO IS DOING WHAT? WHEN AND HOW?

Who?

- **First responders:** IT security team, SOC (Security Operations Center).
- **Decision-makers:** Risk management, compliance, legal, and executive leadership.
- **Operational teams:** Business continuity, public relations (if external impact), customer service (if client-facing systems are affected)

When?

- **Immediate activation** upon detecting a critical security event (e.g., ransomware attack, major breach).
- **Within predefined escalation thresholds**—severity levels determine if the crisis team is fully engaged

How?

- **SMS/email notifications** ensure real-time alerts.
- Escalation must be **predefined** (who gets called first, escalation triggers).
- **Automated workflows** (e.g., SIEM integrations) help optimize activation timing

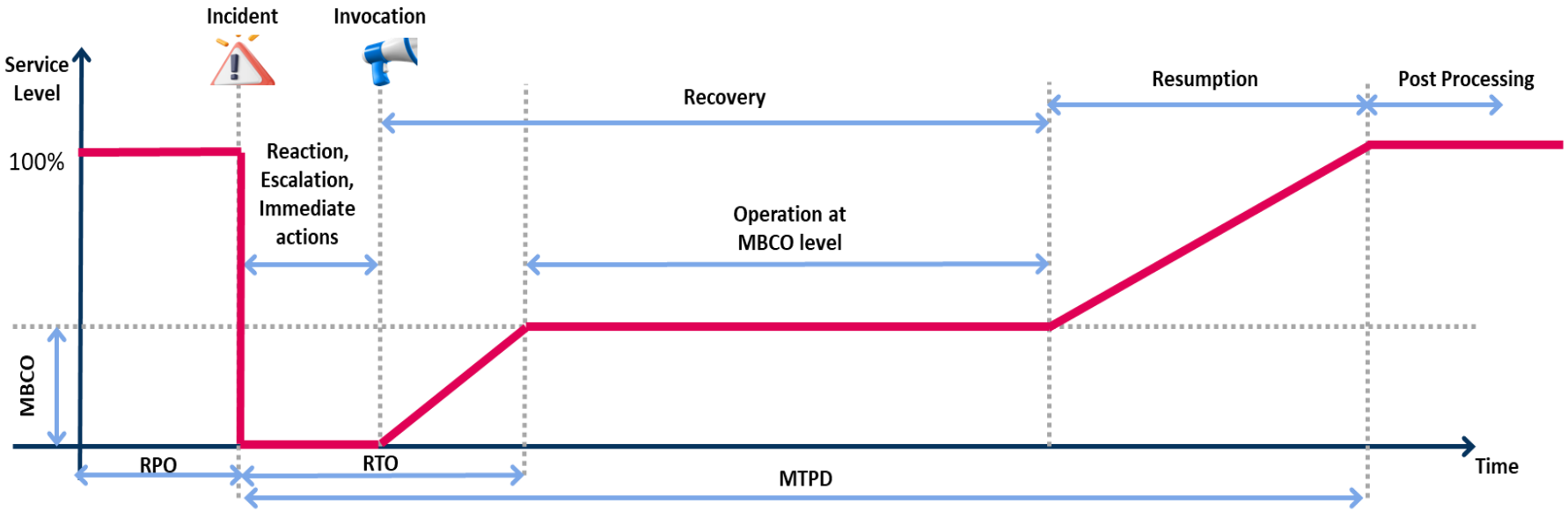
Objective: Ensure a structured, rapid response to incidents by notifying key personnel in the correct sequence

RECOVERY PHASE: JOINT EFFORT BETWEEN ALL STAKEHOLDERS TO RETURN IN BUSINESS AS USUAL

RECOVER

Key elements of emergency response

1. Clear and tested procedure to follow (escalation process, updated contact lists, post reporting communication) until incident/crisis resolution;
2. Link between all decision bodies involved in incident/crisis resolution. (decision making and action implementation);
3. Updated and tested Cyber Incident Response Plan;
4. Effective communication with key external stakeholders (e.g., Customers, Regulator, Regular/Social media).



FOCAL POINT: MANAGING THIRD-PARTY DEPENDENCIES

TPRM

Objective

Address **third-party risk management (TPRM)** in crisis scenarios, especially when **a critical supplier is the root cause** of a cyber incident.

Key Challenges:

- **E2E Supply chain vulnerabilities** – Many cyber incidents originate from **compromised third parties** (e.g., SolarWinds, Kaseya attacks).
- **Data & service dependencies** – What if a key cloud provider, payment processor, or vendor is disrupted?
- **Shared responsibility model** – Who is accountable for mitigation and reporting?

Frequently evaluate **third-party risk exposure** to preempt supply chain vulnerabilities.

STEP 1

- 1. Identify (all) IT suppliers: critical and non-critical.
- 2. Identify their co-tenants.

STEP 2

- Ensure that contractual documentation is present and up-to-date (ideally centralized).

STEP 3

- Perform regular risk assessment on third parties (document system and data integration, exposed APIs).
- Perform an assessment of the suitability of IT services (focus on substitutability, exit strategies, multi-vendor strategy).

STEP 4

- Enter into contractual negotiation to explicitly formalize resilience contributions

STEP 5

- Engage into joint testing activities (incl. notification, joint incident resolution).

KPI TRACKING: MEASURING RESPONSE EFFECTIVENESS

MONITORING

Objective 1

Define **key performance indicators (KPIs)** to assess incident handling efficiency and continuously improve response times.

Critical Cyber Incident KPIs

How long from initial compromise to detection?

Time to detect (MTTD - Mean Time to Detect)

How fast can the organization isolate the threat?

Time to contain (MTTC - Mean Time to Contain)

How quickly are systems restored to full operations?

Time to resolve (MTTR - Mean Time to Respond/Recover)

Objective 2

Define **continuous improvement targets**

Incident recurrence rate - Have similar incidents occurred in the past?

Regulatory compliance response time - Was the required notification timeline met (e.g., 72-hour GDPR/ 4hr DORA requirements)?

Best practice: track KPIs through automated dashboards for real-time visibility

MAIN TAKE AWAYS

WHY

- To safeguard the interest of the company and its stakeholders.
- To comply with legal and customer requirements.

WHAT

- Management requirements/business objectives or strategies (e.g. move to cloud)
- Contractual commitment (SLA, contracts with customers, audits…)

HOW

- Market best practices (ISO standards, NIST CSF)
- Policies and procedures (Pyramid of applicability).
- Security Policy, Third Party Risk Management.
- Cyber Incident Response Plans: update call trees (contact lists), check-lists.
- Business Continuity Plans
- Disaster Recovery Plans
- Crisis Management Plans
- Practicing (Testing, Exercises, Training, Lessons learned…)

YOU?

- Know your role & responsibilities: in quiet times and crisis mode (Panic button is on).

BCM

- Hope for the best, but prepare for the worst

APPENDIX

GRACE CONNECT

Holistic approach towards Cyber Security Risk Management

OVERVIEW