Schneider Electric Business and Operations Resiliency Framework

Resiliency allows Schneider Electric to provide reliable products and services
Our commitment: keep our services and operations running smoothly, so that we can provide our customers with the best service possible and a peace of mind to their customers and business.

Our priorities: identify and manage the technological, environmental, process, geo-political, and health risks that could disrupt business.

Schneider Electric is the most local of global companies. As such, decisions are made at the very beginning of a crisis to triage an incident to the right leadership team for maximum efficiency.
Here is the risk-centric framework that lays out our approach for a reduced risk exposure and preparedness for any hazards.

Legend
- Reduced risk exposure
- Preparedness

Identify & Assess
- Risk register definition & update
- Risk owner identification & animation
- Intelligence

Protect
- Mitigation actions (policies, training, capabilities, tools)
- Coverage (insurance, hedging, provisions)
- Influencing
- Action prioritizations & resource allocation

Detect / Monitor
- Reality check (audit, controls, simulation)
- Automatic & manual systematic controls

Respond
- Crisis management plan

Recover
- Business Continuity Plan
- Disaster recovery plan
Crisis management preparedness plans, disaster recovery plans and business continuity plans prepare us to respond and recover efficiently when our operations are affected. They all serve a different purpose.

We take an “All Hazards” approach to our resiliency planning; ready to respond to all types of challenges.

**Natural disasters**
E.g. hurricanes, floods, fires, earthquakes

**Terrorist/man-made disasters**
E.g. Active shooter, protests

**Technology crisis**
E.g. Software failure, industrial accidents, cyber attacks

**Organizational misdeeds**
E.g. Management misconducts, product misinformation and recalls
The purpose of **preparedness planning at Schneider Electric** is to protect employees and business operations by providing actionable guidance and tools to effectively manage a crisis.

Schneider Electric prescribes the tools, responsibilities and roles to ensure immediate and effective management of a crisis.

It includes the definition of triggers for escalation of an incident to a crisis, the composition of the crisis team and communications/media handling.

This preparedness planning ensures Schneider Electric is ready to:

- ensure safety and security,
- assess the situation and damages quickly,
- provide internal & external communication for full transparency.
Based on our risk assessment and business impact analysis, Schneider Electric business continuity plans are developed to sustain or restore our critical operations after a crisis.

When there is an unplanned event that affects Schneider Electric, our continuity plan kicks in to provide a quick response and recovery.

To withstand and thrive during challenging times, we developed holistic business continuity plans that can keep our business up and running, protect data, safeguard the brand, retain customers – and ultimately help reduce total operating costs over the long term. Having a business continuity plan in place can minimize downtime and achieve sustainable improvements in business continuity, IT disaster recovery, corporate crisis management capabilities and regulatory compliance.
IT Resilience requires proper planning to be ready in the face of disaster.

Schneider Electric policies require Disaster Recovery planning for key assets, routine maintenance of plans, and regular testing frequency to ensure readiness.

Plans are standardized and centrally available, globally.

Team and leadership involvement is critical, roles and responsibilities are identified.

Infrastructure and application configurations are documented and standards in place.

Our digital suppliers are monitored for DR Readiness.
Continuous improvement is at the core of our business resiliency framework. We test our plans and draw conclusions from simulations and the real crises.

- Incorporation of revisions into plans
- Communication of changes

Revise

Review

Exercise or Real Crisis

- Test plans
- Simulation exercise
- Scenario planning
- Tabletop exercise
- Lessons learnt

- Periodic review of Schneider Electric plans by various stakeholders
Our framework is designed for flexibility so we can answer to a crisis of any type, scope, or complexity. Our local leaders are empowered to handle any type of hazard for rapid and effective response.

- **When experiencing a crisis**, there are 3 key steps to take quickly:
  - Ensure safety and security of people
  - Assess situation and damages
  - Communicate
- We refer to the crisis preparedness plan known by the leadership team and readily accessible.
- Once the above is taken care of, we enter a business continuity phase. There are 2 key aspects:
  - Customer experience continuity: Customer interaction lifecycle (e.g. selecting offers, get quotations, get delivered, get technical support)
  - Key internal processes continuity: Managing payroll and cash, paying suppliers, invoicing customers
- To allow our employees to perform, we must ensure the digital continuity of our business. It includes our communication infrastructure; Schneider Electric IT team has policies and disaster recovery plans in place.
- Even in a crisis, our values guide us:
  - People culture and values: **we do the right thing**
  - Compliance with our policies: **we always abide by local rules and regulations**
Our process and procedures support the **prompt and consistent management of security incidents** to minimize any harm to Schneider Electric’s customer and their operations, employees, partners, physical and digital assets and to reduce the risk of future breaches of security.

Our **Cyber Incident Response process** follows 5 stages summarized below:

**Identify**

We identify Cyber risks, vulnerabilities and threats throughout the company, by robust **risk assessment, threat intelligence, detection & hunting** capabilities and focusing on high value (crown-jewel) assets. Also, we protect the company through initiatives implementing cyber capabilities and **digital locks**.

**Detect**

Our extended ecosystem is connected to efficiently **detect anomalies** and **prevent cyber events**, via people and technology sensors. Lawful and proportionate measures complemented with a **modern technology stack** is in place to protect the information in **monitored networks and systems**.

**Analyze**

We are leveraging our **correlation technology & tools** and Security Operations Center to assess and triage incident types, define severity and assign adequate escalation paths.

**Respond**

With a **risk-based approach** we define **clear incident ownership** enforced by our internal policies and procedures, among which is a strong Incident Response Plan and Privacy Breach Response Procedure. We respond to incidents through an organization of **Security Officers** across regions.

**Recover**

As a learning organization, we systematically conduct **root cause analysis** and **mitigation actions** are implemented. Business continuity plans are developed, as well as IT Disaster Recovery Plans, with regular testing and exercises.