ONTIC

TOOL

Business Continuity for Corporate Security

HOW RESILIENT IS YOUR ORGANIZATION?

Organizations face greater risk exposure than at any other time in recent history. It is well understood that threats from cybercrime, fraud, activism and workplace violence are the source of significant financial loss. But the impact is not limited to business operations – many of these threats also have the potential to impact employees, customers and business relationships directly.

88% of organizations are experiencing a dramatic increase in physical threat activity compared to early 2021, with more than 41% of security practitioners expecting to miss more than half of these upcoming threats.

To meet these risks head on, today's business leaders must widen the aperture with more comprehensive threat monitoring to help ensure business continuity despite an ever-growing set of risks and threats. Taking an "all-hazards" approach is one way to determine what areas to include or enhance within a risk monitoring program.

"There are many different threats or hazards. The probability that a specific hazard will impact your business is hard to determine. That's why it's important to consider many different threats and hazards and the likelihood they will occur."

US GOVERNMENT'S READY.GOV

Here are some to consider:

EXTREME WEATHER / CLIMATE / NATURAL DISASTER

- Earthquake
- Extreme weather (hurricane, flood, snow)
- Wildfire
- Climate risk

HEALTH & SAFETY

- Epidemic pandemic
- Food-borne illness
- Infectious disease
- Duty of care

WORKPLACE VIOLENCE

- Any act or threat of violence or abuse against employees, clients, customers, or visitors to the worksite including targeted attacks on corporate leadership

ACTIVISM / UNREST

- Acts of war/terrorism
- Activism demonstrations
- Civil disorder
- Political instabilities
- Labor

INSIDER THREATS

- Breach or incident
- Theft
- Fraud
- Sabotage
- Espionage

CYBERCRIME

- Cyberattacks against internal or supply chain systems by malicious outsiders

OPERATIONAL

- Power or water outage
- IT failure
- Supply interruption
- Data corruption
- Production loss
- Market trends

COMPLIANCE

- Regulations
- Background checks
- Policy enforcement

Threats have many kinds of costs...


Financial


Reputational


Operational


Human Capital


Legal & Regulatory

Just because you have a business continuity plan doesn't mean you are tactically prepared for today's threat landscape—not only to identify risks before they cause disruptions, but to become more agile and resilient when those risks do occur.

The below outlines the optimal path from reactive, siloed response activities after a threat occurs to a more real-time, collaborative approach to business continuity across the entire organization.

How mature is your corporate security program?

While most organizations focus on improving their reaction to threats, a complete business continuity plan involves creating a digitally-supported, collaborative, and strategic team better able to identify, understand, and actively manage risks in all areas of operations.

LEVEL 1

REACTIVE RESILIENCE

Responsive, siloed approach occurs after a crisis to help minimize disruption.

- Manual threat tracking
- Lack of common understanding of threats between physical security, cybersecurity, HR, legal and compliance
- Delays in investigating and managing active threats

LEVEL 2

QUANTIFIED RISK

Threats quantified, resilience systems developed to help recover operations faster.

- Threats identified and quantified for risk to business operations
- Emergency response playbooks created
- Investment in threat monitoring tools (LPR cameras, VMS, cybersecurity)
- Disjointed effort leads to delays in identifying connected events

LEVEL 3

PROACTIVE RESILIENCE

Gaining proactive resilience and agility to better anticipate and mitigate risks.

- Automated alerting solutions for high risk threats (insider threats, fraud, cyber attack)
- Gaining proactive resilience for highest-risk threats
- Better team agility when risks do arise

LEVEL 4

COMPLETE BUSINESS CONTINUITY

Real-time protective intelligence used collaboratively to support strategic decision-making.

- Cross-functional collaboration
- Adoption of an organization-wide protective intelligence system to identify, score, and rank threats
- Proactive resilience applied to all threat categories
- Every stage of threat management actionable