ONSOLVE®

Organizational Resilience in 2022

A Checklist for Security Professionals

In an era of rising risk and uncertainty, security professionals are all but guaranteed to face one or more critical events at some point—from severe weather and civil unrest to power outages and cybersecurity incidents.

A proactive, focused strategy to mitigate and manage risk is essential, but it doesn't happen by accident.

Here's a handy checklist to help ensure you're ready:

1 Identify gaps in your current security and risk management strategy.

- [ ] How reliable is the information you receive about potential risks?
- [ ] Is your strategy proactive or reactive?
- [ ] What have been the downstream implications of recent events that impacted your organization?

Only 38 percent *of respondents indicated their current risk management strategies are effectively measured or optimized.*

— "Failing To Plan Is Planning To Fail," Forrester Consulting, October 2021

2 Clearly define your team's role in supporting overall organizational resilience and employee safety.

- [ ] Can you communicate with stakeholders quickly and via multiple channels?
- [ ] Are there systems and processes that have failed to protect your employees during an event?
- [ ] Have you incorporated practice exercises or drills into your response plans?

Two of the most common impacts *of incidents on organizations are operational disruption and impact to employee safety and morale.*

— "Failing To Plan Is Planning To Fail," Forrester Consulting, October 2021

3 Embrace the power of digital transformation.

- [ ] Have you collected data to help you create a business impact analysis or a digital model of your organization?
- [ ] Have you identified areas of unnecessary complexity in your processes?
- [ ] Where are areas you could leverage technology to detect, assess and respond to an incident?

It's not a matter of having a crisis management capability that lasts for a few days. ***We must build a competency to look ahead and ask: "What If"?***

— **Brian Zawada**, Chief Operating Officer at Castellan, a firm specializing in business continuity and operational resilience

4 Recognize the convergence of cyber and physical security roles.

- [ ] Where do you think your organization is most vulnerable?
- [ ] Have you asked for input from both IT and physical security stakeholders within your organization?
- [ ] Are remote and/or traveling workers incorporated into your security strategy?

If you're not connecting the dots, you're going to see the physical repercussions of ***digital vulnerability.***

— **Stefanie Drysdale**, Vice President of Cyber at Prescient, a global risk management and intelligence services firm

5 Learn the language of executives and become a trusted security advisor.

- [ ] Are you keeping the organizational "big picture" at the forefront of your strategy?
- [ ] Do you incorporate appropriate metrics, where possible, to strengthen your security plan?
- [ ] Is your recommended approach to protect the organization clear, with concise language and a realistic timeline?

It's less about what it takes for your organization to be resilient...and more about asking ***"What heartbeats do you need to protect?"***

— **Ann Pickren**, Chief Customer Officer, OnSolve

Learn more strategies for keeping your organization's people, places and property safe in this ebook. **Download Ebook**

ONSOLVE®