Program Best Practices > Resilience >

Measures and Metrics for Business Continuity Programs

By George Campbell, Emeritus Faculty, Security Executive Council

All security programs should be measured for performance. However, creating a truly effective and valuable measures and metrics process is not easy.

To that end we have gathered some presentation slides that successful security leaders have used in the past to demonstrate the value their Business Continuity programs are delivering to their organizations.

We are hopeful that this information will help generate ideas that you can use within your Business Continuity metrics program.

Example Presentation Slides

Business Continuity Dashboard

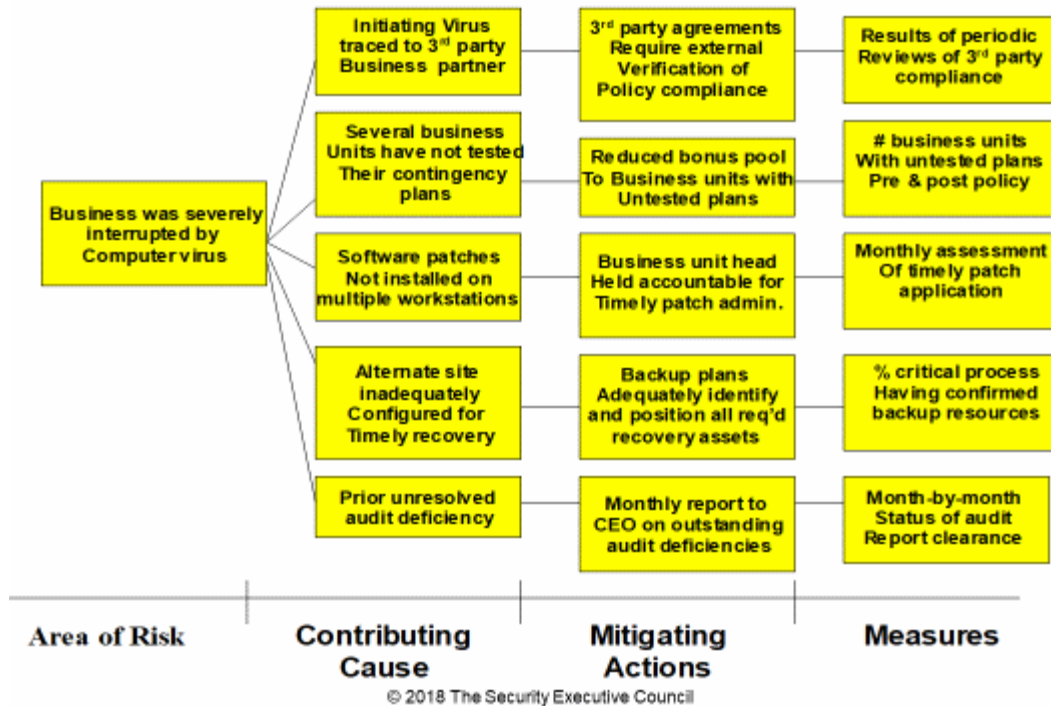|	
Updated and tested business continuity plans for all Level AAA business processes	○ 🟠 ○ ○ ○
Appointed and trained business continuity planning & response teams at all locations	○ ○ 🟡 ○ ○
Progress in reducing single points of failure in Level AAA & AA functions	○ ○ ○ 🟢 ○
Required service continuity plans at 3rd party vendors are tested and current.	○ 🔴 ○ ○ ○
Documented & current tested biohazard response plan for all facilities	○ ○ 🟡 ○ ○
Electronic sensing / early warning & all required crisis notification systems are 99.99% on-line	○ ○ ○ ○ 🟢
Public Safety First Responders demonstrate adequate response times over past 36 months	○ 🟠 ○ ○ ○

© 2018 The Security Executive Council

Select your several measures of effectiveness of your organization's business continuity program and monitor them monthly. This dashboard may be prepared for a specific business unit to keep them apprised of strengths and weaknesses and to hold the business continuity specialists in that unit more accountable.
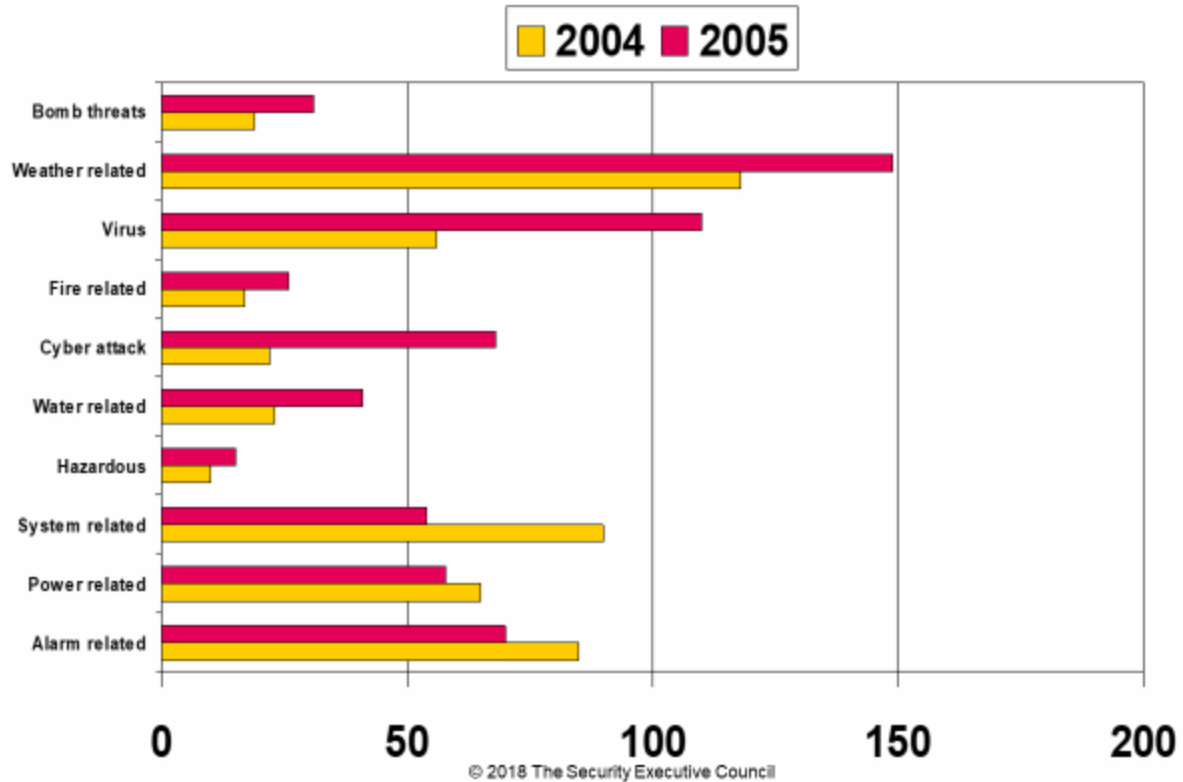
Charts like this need to be backed up by specific risk assessment and reporting results so that plans to fix problem areas may be appropriately focused and resource requirements obtained.

Lessons from Severe Virus Incident

Area of Risk	Contributing Cause	Mitigating Actions	Measures
Business was severely interrupted by Computer virus	Initiating Virus traced to 3rd party Business partner	3rd party agreements Require external Verification of Policy compliance	Results of periodic Reviews of 3rd party compliance
	Several business Units have not tested Their contingency plans	Reduced bonus pool To Business units with Untested plans	# business units With untested plans Pre & post policy
	Software patches Not installed on multiple workstations	Business unit head Held accountable for Timely patch admin.	Monthly assessment Of timely patch application
	Alternate site inadequately Configured for Timely recovery	Backup plans Adequately identify and position all req'd recovery assets	% critical process Having confirmed backup resources
	Prior unresolved audit deficiency	Monthly report to CEO on outstanding audit deficiencies	Month-by-month Status of audit Report clearance

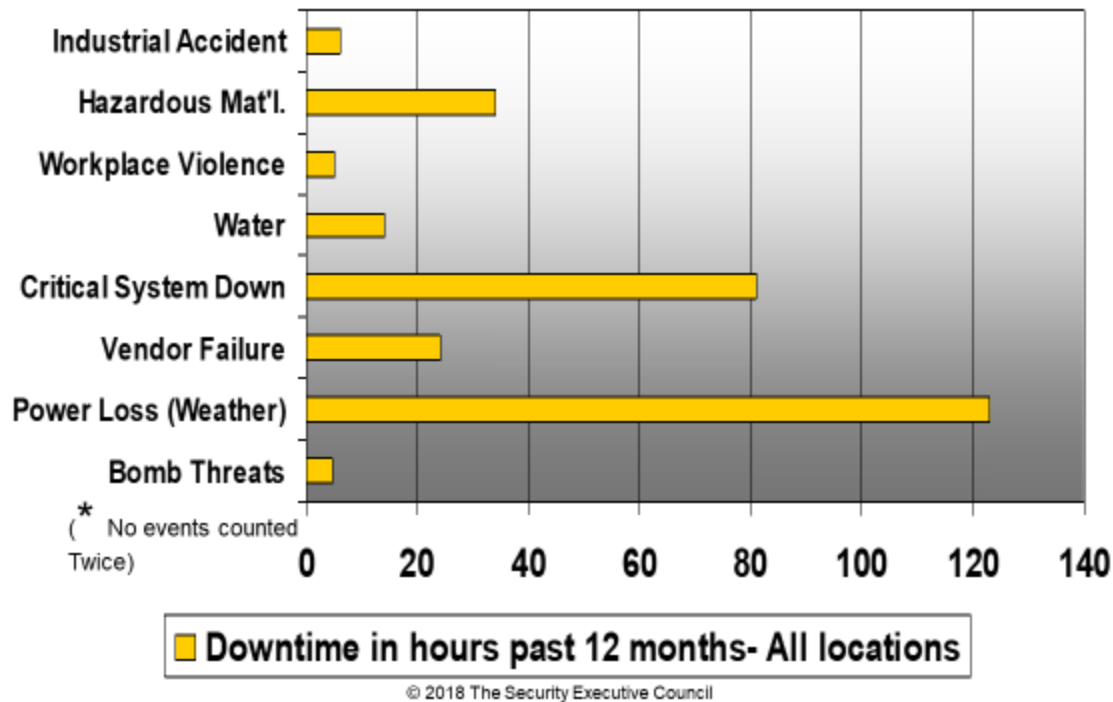© 2018 The Security Executive Council

Post-incident lessons-learned are essential processes in contingency planning. Here, vulnerabilities enabled a virus where adequate risk assessment and follow-up mitigation tactics would otherwise have prevented or minimized the impact. New viruses seeking to capitalize on safeguard weaknesses are always a risk. But having a resilient and proactive risk management strategy, directly aided by incident postmortems, will enable you to do better than the competition.

Business Interruption Incidents

2004 (yellow) / 2005 (red)

Categories (top to bottom): Bomb threats, Weather related, Virus, Fire related, Cyber attack, Water related, Hazardous, System related, Power related, Alarm related

X-axis: 0, 50, 100, 150, 200

© 2018 The Security Executive Council

Here is a simple informational chart that may be part of an overall "state of security" briefing. Breaking this type of information out for an individual site with more extensive incident details can help in the awareness area as well as cause rethinking on the adequacy of the backup strategy or the location of particular assets there.

291.5 Hours* of Critical Business Processes Lost to Risk Events

Chart categories (Downtime in hours past 12 months - All locations):
- Industrial Accident
- Hazardous Mat'l.
- Workplace Violence
- Water
- Critical System Down
- Vendor Failure
- Power Loss (Weather)
- Bomb Threats

(* No events counted Twice)

Legend: ☐ Downtime in hours past 12 months- All locations

© 2018 The Security Executive Council

What would 291.5 hours of critical business process downtime cost in your company? This slide should be in a presentation on contingency planning to emphasize the need for a strong offsite strategy, increased redundancy and perhaps more in-depth planning in specific sites with higher probabilities of outages.

In addition, this slide should drive a companion on lessons learned from several of the higher impact events. Likely there are common denominators that contribute to more extended downtimes.

**Business Continuity: Annual Evacuation Drill**
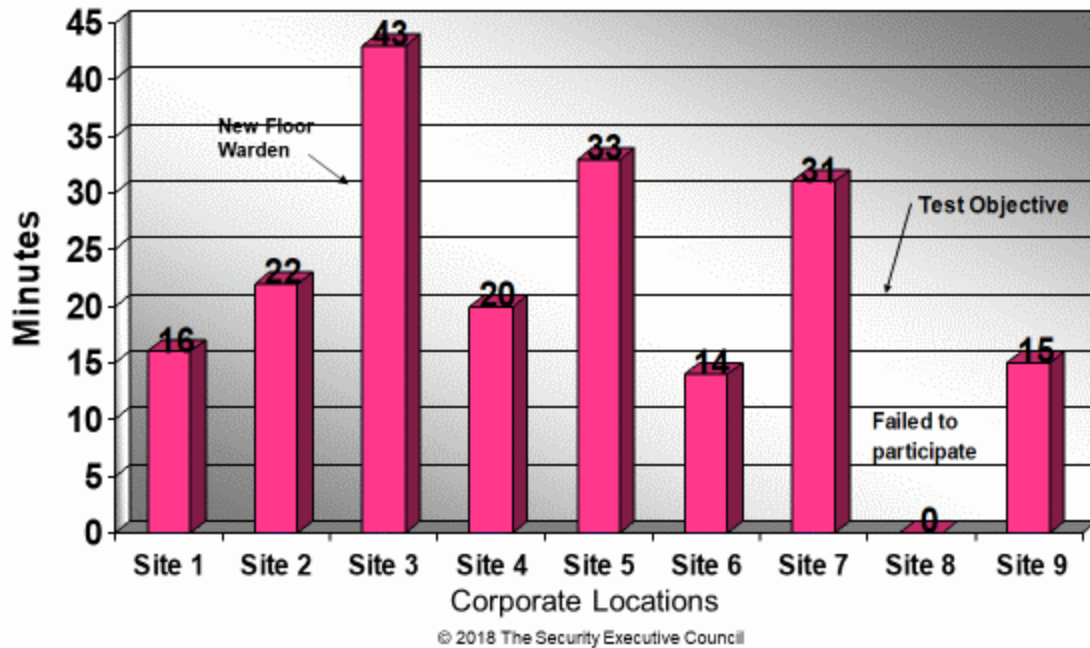
This is a very revealing display that highlights those who are paying attention to a serious employee safety objective and those who should attract management's attention during performance reviews. Note the test objective that obviously must be adjusted for each set of sites where the logistics of reasonable evacuation timelines dictate. The new Floor Warden is noted to give slack to this individual but also to highlight the focus on the next exercise.

Post 9/11, these drills are increasingly high on the risk management agenda and in this hypothetical example the responsible manager at site 8 may be updating a resume in an organization that takes this aspect of risk management seriously.

Master Control System Uptime Reliability

(Most recent 30 day rolling average with trend line- 99.9% uptime objective)

© 2018 The Security Executive Council
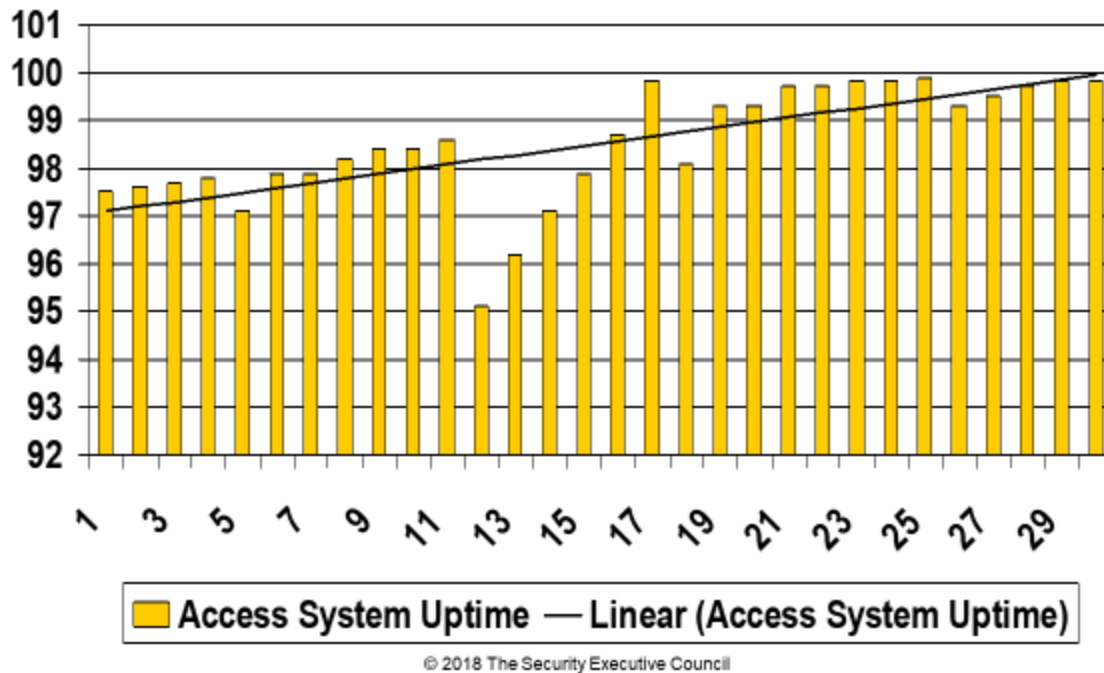
Tracking critical systems for reliability is an imperative. Mean time between failures for systems, subsystems and components drives your back-up strategy and contractual relationships with key vendors.

In this example, a 99.9% uptime goal has been set and is measured in minutes or hours. IT departments maintain rigorous records on uptime reliability. For critical components or systems, a reliability measure should be incorporated in RFPs and contractual documents.

Visit the Security Executive Council web site to view more resources in the Program Best Practices: Resilience series.

About the Security Executive Council

The SEC is the leading research and advisory firm focused on corporate security risk mitigation solutions. Having worked with hundreds of companies and organizations we have witnessed the proven practices that produce the most positive transformation. Our subject matter experts have deep expertise in all aspects of security risk mitigation strategy; they collaborate with security leaders to transform security programs into more capable and valued centers of excellence. Watch our 3-minute video to learn more.

Contact us at: contact@secleader.com
Website: https://www.securityexecutivecouncil.com/