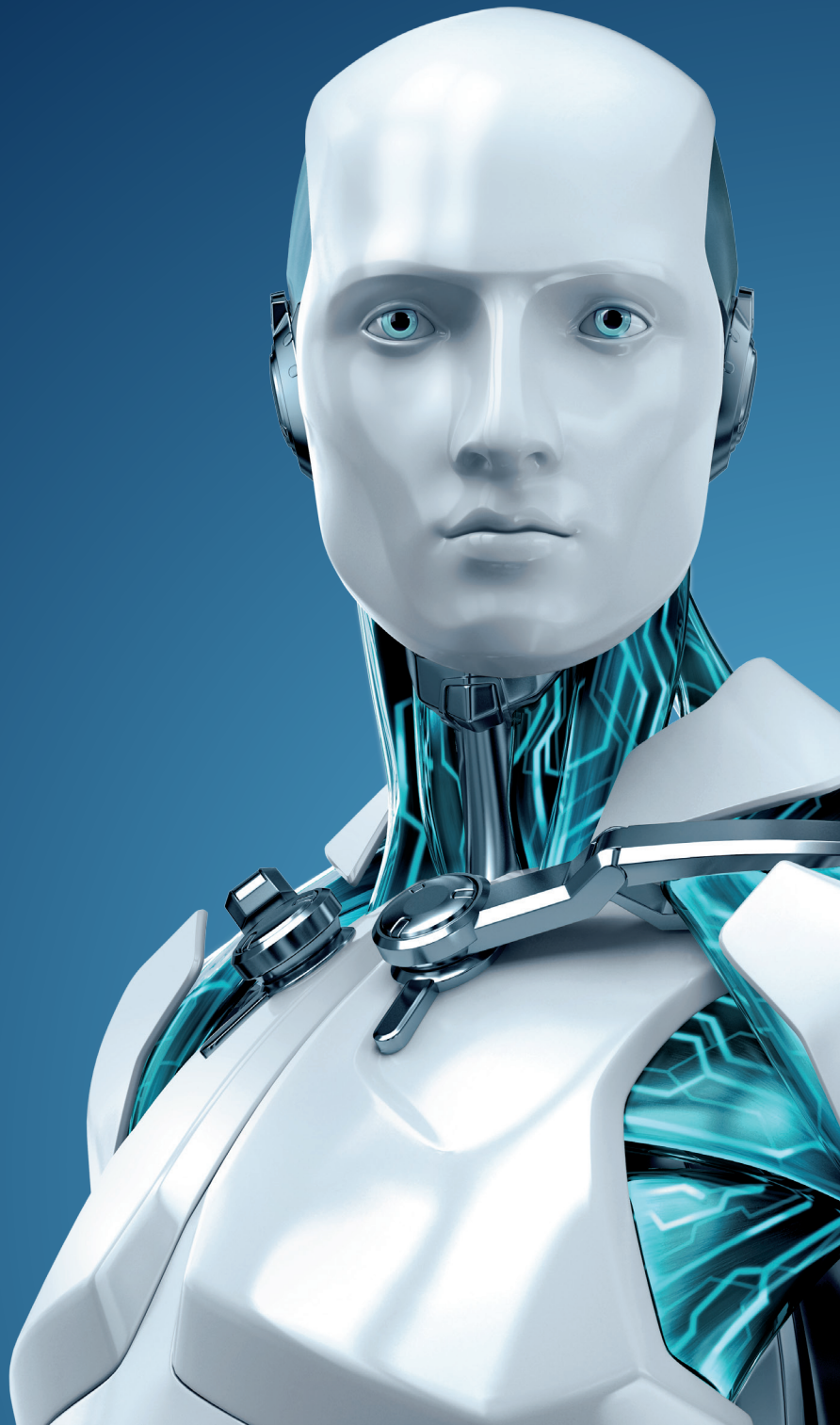
TECH BRIEF

Business continuity management: Key to securing your digital future



ENJOY SAFER TECHNOLOGY™

BUSINESS CONTINUITY MANAGEMENT: KEY TO SECURING YOUR DIGITAL FUTURE

By Stephen Cobb, ESET Security Researcher

Business continuity is all about surviving the bad things that can impact your business, from a computer virus outbreak to a biological virus outbreak, and all the other perils in between, like fires, floods, tornadoes, hurricanes, earthquakes, and tsunamis. The international standard for business continuity, ISO 22301, defines it as an organization's "capability to continue to deliver its products and services at acceptable predefined levels after disruptive incidents have occurred."

Business continuity management, often referred to as BCM, is the process of achieving and sustaining this capability, and it is a vital part of information system security management, commonly known these days as cybersecurity. This article describes the basics of BCM and provides a list of resources that you and your organization can use to improve your ability to survive any unexpected and undesirable turn of events.

Business continuity is IT and more

Most organizations today are heavily dependent on information technology — from laptops to servers, desktops to tablets and smartphones — but it is clear that this technology can be disrupted by a wide range of potentially disastrous incidents. These range from power outages caused by storms to data loss caused by misguided employees or criminal hackers. From the earliest days of IT it was clear that organizations needed strategies to prepare for, respond to, and recover from such incidents. For that reason, a lot of early work on how to handle disruptive incidents came out of the IT community; however, over time the discipline of "disaster recovery" evolved into "a holistic management process," one that:

> "Identifies potential threats to an organization and the impacts to business operations those threats, if realized, might cause, and which provides a framework for building organizational resilience with the capability of an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities."

Again, that's ISO 22301 language. Note that, while your company doesn't have to get ISO 22301 certified to survive a disaster, some enterprises may want to pursue this certification to improve their BCM program and also to win business. For example, I foresee companies that are critical to the supply chain in some industries getting more requests for business continuity assurances in contract negotiations, and adhering to ISO 22301 certainly addresses that.

A basic four-step BCM program

Sadly, some companies do go out of business when they are hit with a disaster for which they have not adequately prepared. This is unfortunate because the path to preparedness is well-documented. Any company of any size can improve its chances of coming through a disruptive event in one piece – with its brand intact and its revenue undiminished – by following some tried and trusted strategies, whether they are going for ISO 22301 or not. I have outlined the four

main steps here and provided links to more resources on the web, including templates for a Business Continuity Plan.

1. Identify and rank the threats

List potentially disruptive incidents that are most likely to threaten your business. Don't use someone else's list because threats vary according to location. For example, here in San Diego where I live, there is a relatively high level of earthquake and wildfire awareness, and many organizations have undertaken a basic level of disaster preparedness planning with those events in mind. But what about where your firm is located? And what about a data breach or IT outage that can happen anywhere? What if a toxic chemical spill puts your premises off limits for several days? Are you located near a rail line? Major highway? How reliant on foreign suppliers are you?

A good technique at this stage is to include people from all departments in a brainstorming session. The goal is a list of scenarios ranked by probability of occurrence and potential for negative impact. You can find a basic list of threats in OFB-EZ, the first resource on our list at the end of the article.

2. Perform a business impact analysis

You need to figure out which parts of your business are most critical to its survival. One way is to begin by detailing the functions, processes, personnel, places, and systems that are critical to the functioning of your organization. The BCM project leader can do this by interviewing employees in each department and laying the results out in a table that lists functions and key person(s) and alternate person(s).

You then determine the number of Survival Days for each function. How long can your business endure without that function causing serious impact? Next you rank the impact of each function not being available. For example, disaster recovery expert Michael Miora suggests using a scale of 1 to 4, where 1 = critical operational impact or fiscal loss, and 4 = no short term impacts. If you then multiply Impact by Survival Days you can see which functions are most critical. At the top of the table will be functions with major impact and just one survival day.

3. Create the response and recovery plan

This is where you catalog key data about the assets involved in performing critical functions, including IT systems, personnel, facilities, suppliers, and customers. You'll want equipment serial numbers, licensing agreements, leases, warranties, and contact details. You will need to determine "who to call" for each category of incident and create a calling tree so that the right calls get made, in the right order. You also need a "who can say what" list to control interaction with the media during an incident. (Consider going to a "CEO-only" strategy if the incident is a delicate one.)

Any arrangements you have in place for transitioning your operations to temporary locations and IT facilities should be documented. Don't forget to document an "all-hands" notification process and a customer advisory procedure.

The steps to recover key operations should be laid out in a sequence that accounts for functional inter-dependencies. When the plan is ready, make sure you train managers and their reports on the details relevant to each department and the importance of the overall plan to surviving an incident.

4. Test the plan and refine the analysis

Most BCM experts recommend testing your plan at least once a year, with exercises, walk-throughs, or simulations. Testing enables you to make the most of your investment in creating the plan. Testing not only enables you to find gaps and account for changes in the business over time, it can also impress management.

Clearly, these four steps encompass a huge undertaking, but one that companies ignore at their peril. If the task seems too daunting to undertake on a company-wide basis, consider beginning with a few departments, or one office if you have several. Everything you learn in the process can then be applied more broadly as you progress. At all costs avoid thinking bad things won't happen, because they do. And don't pretend that if something does happen it won't be so bad, because it just might be.

Want to learn more? We will be taking a closer look at these four steps in future articles. In the meantime, check out these additional resources, including a free set of templates for a business continuity program.

Business continuity resources:

- OFB-EZ: Stay open for business. This is a streamlined disaster protection and recovery planning toolkit for the small to mid-sized business, with lists, forms, and templates. A great place for your SMB to start the BCM process

  https://www.disastersafety.org/disastersafety/open-for-business-ez

- BCI Horizon Scan 2014: the definitive annual report on the state of play in BCM, free from the Business Continuity Institute (light registration required)

  http://www.thebci.org/index.php/the-2014-bci-horizon-scan

- Disaster Preparedness Planning: Maintaining Business Continuity During Crisis, Disruption and Recovery is a good introduction to the subject (from Chase he noted with some surprise)

  https://www.chase.com/online/commercial-bank/document/Perspective_DisasterPreparedness.pdf

- BCI Good Practice Guidelines: considered by many to be the bible of BCM, free with annual membership of BCI (Affiliate membership is a good investment for your organization at about $135 for the year)

  http://www.thebci.org

- NFPA 1600 Standard on Disaster/Emergency Management and Business Continuity Programs: free from the National Fire Protection Association (with registration), this document lists all the things you need to cover in a full BCM program

  https://www.nfpa.org

- Disaster Recovery Journal: one of the top websites to know if you are working on BCM

  http://www.drj.com

- TechTarget Business Impact Analysis Template: one of several free templates to help you tackle the crucial BIA that is part of every good BC program

http://searchdisasterrecovery.techtarget.com/feature/Using-a-business-impact-analysis-BIA-template-A-free-BIA-template-and-guide

- ISACA Business Impact Analysis Template: helps you tackle the crucial BIA that is part of every good BC program

  http://www.isaca.org/Groups/Professional-English/business-continuity-disaster-recovery-planning/GroupDocuments/Business_Impact_Analysis_blank.doc

- Continuity Central US: another good website to know if you're doing BCM

  http://www.continuitycentral.com/namerica.htm

- Continuity Central UK: another good website to know if you're doing BCM

  http://www.continuitycentral.com

- NIST Business Impact Analysis Template

  http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_bia_template.docx

- Contingency Planning Guide for Federal Information Systems: because government agencies need BCP too

  http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf

- MIT Business Continuity Plan: because schools need BCP too

  http://web.mit.edu/security/www/pubplan.htm

- Business Continuity Planning Booklet, Federal Financial Institutions Examination Council (FFIEC)

  http://ithandbook.ffiec.gov/it-booklets/business-continuity-planning.aspx

- Latest Business Continuity Testing and Exercising News Headlines, Continuity Central

  http://www.continuitycentral.com/bctenews.htm

- Principles and Practice of Business Continuity, Tools & Techniques: if you're going to buy a book on BCP, this is the one, by Jim Burtles

  http://www.amazon.com/gp/product/1931332398