Most backup software, including the built-in Windows backup software, lets you select down to the individual file that you want backed up. You can also choose to backup things like the "system state".

Incremental
When you schedule an incremental backup, you are in essence instructing the software to only backup files that have been changed, or files that have their flag up. After the incremental backup of that file has occured, that flag will go back down. If you perform a normal backup on Monday, then an incremental backup on Wednesday, the only files that will be backed up are those that have changed since Monday. If on Thursday someone deletes a file by accident, in order to get it back you will have to restore the full backup from Monday, followed by the Incremental backup from Wednesday.

Differential
Differential backups are similar to incremental backups in that they only backup files with their archive bit, or flag, up. However, when a differential backup occurs it does not reset those archive bits which means, if the following day, another differential backup occurs, it will back up that file again regardless of whether that file has been changed or not.

Source: KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 69.

And: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter 9: Disaster Recovery and Business continuity (pages 617-619). And: http://www.brighthub.com/computing/windows-platform/articles/24531.aspx

QUESTION 571
Which one of the following is NOT one of the outcomes of a vulnerability assessment?

A. Quantative loss assessment
B. Qualitative loss assessment
C. Formal approval of BCP scope and initiation document
D. Defining critical support areas

Correct Answer: C
Explanation:
When seeking to determine the security position of an organization, the security professional will eventually turn to a vulnerability assessment to help identify specific areas of weakness that need to be addressed. A vulnerability assessment is the use of various tools and analysis methodologies to determine where a particular system or process may be susceptible to attack or misuse. Most vulnerability assessments concentrate on technical vulnerabilities in systems or applications, but the assessment process is equally as effective when examining physical or administrative business processes.

The vulnerability assessment is often part of a BIA. It is similar to a Risk Assessment in that there is a quantitative (financial) section and a qualitative (operational) section. It differs in that i t is smaller than a full risk assessment and is focused on providing information that is used solely for the business continuity plan or disaster recovery plan.

A function of a vulnerability assessment is to conduct a loss impact analysis. Because there will be two parts to the assessment, a financial assessment and an operational assessment, it will be necessary to define loss criteria both quantitatively and qualitatively.

Quantitative loss criteria may be defined as follows:

Incurring financial losses from loss of revenue, capital expenditure, or personal liability resolution. The additional operational expenses incurred due to the disruptive event Incurring financial loss from resolution of violation of contract agreements Incurring financial loss from resolution of violation of regulatory or compliance requirements

Qualitative loss criteria may consist of the following:

The loss of competitive advantage or market share
The loss of public confidence or credibility, or incurring public mbarrassment

During the vulnerability assessment, critical support areas must be defined in order to assess the impact of a disruptive event. A critical support area is defined as a business unit or function that must be present to sustain continuity of the business processes, maintain life safety, or avoid public relations embarrassment.

Critical support areas could include the following:

Telecommunications, data communications, or information technology areas Physical infrastructure or plant facilities, transportation services Accounting, payroll, transaction processing, customer service, purchasing

The granular elements of these critical support areas will also need to be identified. By granular elements we mean the personnel, resources, and services the critical support areas need to maintain business continuity

Reference(s) used for this question:

Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 4628-4632). Auerbach Publications. Kindle Edition.
KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Page 277.

QUESTION 572
Controls are implemented to:

A. eliminate risk and reduce the potential for loss
B. mitigate risk and eliminate the potential for loss
C. mitigate risk and reduce the potential for loss
D. eliminate risk and eliminate the potential for loss

Correct Answer: C
Explanation:
Controls are implemented to mitigate risk and reduce the potential for loss. Preventive controls are put in place to inhibit harmful occurrences; detective controls are established to discover harmful occurrences; corrective controls are used to restore systems that are victims of harmful attacks.
It is not feasible and possible to eliminate all risks and the potential for loss as risk/threats are constantly changing.
Source: KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 32.
QUESTION 573
Which of the following statements pertaining to disaster recovery planning is incorrect?

A. Every organization must have a disaster recovery plan
B. A disaster recovery plan contains actions to be taken before, during and after a disruptive event.
C. The major goal of disaster recovery planning is to provide an organized way to make decisions if a disruptive event occurs.
D. A disaster recovery plan should cover return from alternate facilities to primary facilities.

Correct Answer: A
Explanation:
It is possible that an organization may not need a disaster recovery plan. An organization may not have any critical processing areas or system and they would be able to withstand lengthy interruptions.

Remember that DRP is related to systems needed to support your most critical business functions.

The DRP plan covers actions to be taken when a disaster occur but DRP PLANNING which is the keywork in the question would also include steps that happen before you use the plan such as development of the plan, training, drills, logistics, and a lot more.

To be effective, the plan would certainly cover before, during, and after the disaster actions.

It may take you a couple years to develop a plan for a medium size company, there is a lot that has to happen before the plan would be actually used in a real disaster scenario. Plan for the worst and hope for the best.

All other statements are true.

NOTE FROM CLEMENT:
Below is a great article on who legally needs a plan which is very much in line with this question. Does EVERY company needs a plan? The legal answer is NO. Some companies, industries, will be required according to laws or regulations to have a plan. A blank statement saying: All companies MUST have a plan would not be accurate. The article below is specific to the USA but similar laws will exist in many other countries.

Some companies such as utilities, power, etc... might also need plan if they have been defined as Critical Infrastructure by the government. The legal side of IT is always very complex and varies in different countries. Always talk to your lawyer to ensure you follow the law of the land :-)

Read the details below:

So Who, Legally, MUST Plan?
With the caveats above, let's cover a few of the common laws where there is a duty to have a disaster recovery plan. I will try to include the basis for that requirement, where there is an implied mandate to do so, and what the difference is between the two Banks and Financial Institutions MUST Have a Plan

The Federal Financial Institutions Examination Council (Council) was established on March 10, 1979, pursuant to Title X of the Financial Institutions Regulatory and Interest Rate Control Act of 1978 (FIRA), Public Law 95-630. In 1989, Title XI of the Financial Institutions Reform, Recovery and Enforcement Act of 1989 (FIRREA) established the Examination Council (the Council).

The Council is a formal interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions by the Board of Governors of the Federal Reserve System (FRB), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency

(OCC), and the Office of Thrift Supervision (OTS); and to make recommendations to promote uniformity in the supervision of financial institutions. In other words, every bank, savings and loan, credit union, and other financial institution is governed by the principles adopted by the Council.

In March of 2003, the Council released its Business Continuity Planning handbook designed to provide guidance and examination procedures for examiners in evaluating financial institution and service provider risk-management processes.

Stockbrokers MUST Have a Plan
The National Association of Securities Dealers (NASD) has adopted rules that require all its members to have business continuity plans. The NASD oversees the activities of more than 5,100 brokerage firms, approximately 130,800 branch offices and more than 658,770 registered securities representatives.

As of June 14, 2004, the rules apply to all NASD member firms. The requirements, which are specified in Rule 3510, begin with the following:

3510. Business Continuity Plans. (a) Each member must create and maintain a written business continuity plan identifying procedures relating to an emergency or significant business disruption. Such procedures must be reasonably designed to enable the member to meet its existing obligations to customers. In addition, such procedures must address the member's existing relationships with other broker-dealers and counter-parties. The business continuity plan must be made available promptly upon request to NASD staff.

NOTE:
The rules apply to every company that deals in securities, such as brokers, dealers, and their representatives, it does NOT apply to the listed companies themselves.
Electric Utilities WILL Need a Plan

The disaster recovery function relating to the electric utility grid is presently undergoing a change. Prior to 2005, the Federal Energy Regulatory Commission (FERC) could only coordinate volunteer efforts between utilities. This has changed with the adoption of Title XII of the Energy Policy Act of 2005 (16 U.S.C.824o). That new law authorizes the FERC to create an Electric Reliability Organization (ERO). The ERO will have the capability to adopt and enforce reliability standards for "all users, owners, and operators of the bulk power system" in the United States. At this time, FERC is in the process of finalizing the rules for the creation of the ERO. Once the ERO is created, it will begin the process of establishing reliability standards.

It is very safe to assume that the ERO will adopt standards for service restoration and disaster recovery, particularly after such widespread disasters as Hurricane Katrina. Telecommunications Utilities SHOULD Have Plans, but MIGHT NOT

Telecommunications utilities are governed on the federal level by the Federal Communications Commission (FCC) for interstate services and by state Public Utility Commissions (PUCs) for services within the state.

The FCC has created the Network Reliability and Interoperability Council (NRIC). The role of the NRIC is to develop recommendations for the FCC and the telecommunications industry to "insure [sic] optimal reliability, security, interoperability and interconnectivity of, and accessibility to, public communications networks and the internet." The NRIC members are senior representatives of providers and users of telecommunications services and products, including telecommunications carriers, the satellite, cable television, wireless and computer industries, trade associations, labor and consumer representatives, manufacturers, research organizations, and government-related organizations.

There is no explicit provision that we could find that says telecommunications carriers must have a Disaster Recovery Plan. As I have stated frequently in this series of articles on disaster recovery, however, telecommunications facilities are tempting targets for terrorism. I have not changed my mind in that regard and urge caution.

You might also want to consider what the liability of a telephone company is if it does have a disaster that causes loss to your organization. In three words: It's not much. The following is the statement used in most telephone company tariffs with regard to its liability:

The Telephone Company's liability, if any, for its gross negligence or willful misconduct is not limited by this tariff. With respect to any other claim or suit, by a customer or any others, for damages arising out of mistakes, omissions, interruptions, delays or errors, or defects in transmission occurring in the course of furnishing services hereunder, the Telephone Company's liability, if any, shall not exceed an amount equivalent to the proportionate charge to the customer for the period of service during which such mistake, omission, interruption, delay, error or defect in transmission or service occurs and continues. (Source, General Exchange Tariff for major carrier)

All Health Care Providers WILL Need a Disaster Recovery Plan HIPAA is an acronym for the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, which amended the Internal Revenue Service Code of 1986. Also known as the Kennedy-Kassebaum Act, the Act includes a section, Title II, entitled Administrative Simplification, requiring "Improved efficiency in healthcare delivery by standardizing electronic data interchange, and protection of confidentiality and security of health data through setting and enforcing standards."

The legislation called upon the Department of Health and Human Services (HHS) to publish new rules that will ensure security standards protecting the confidentiality and integrity of "individually identifiable health information," past, present, or future.

The final Security Rule was published by HHS on February 20, 2003 and provides for a uniform level of protection of all health information that is housed or transmitted electronically and that pertains to an individual.

The Security Rule requires covered entities to ensure the confidentiality, integrity, and availability of all electronic protected health information (ePHI) that the covered entity creates, receives, maintains, or transmits. It also requires entities to protect against any reasonably anticipated threats or hazards to the security or integrity of ePHI, protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required by the Privacy Rule, and ensure compliance by their workforce.

Required safeguards include application of appropriate policies and procedures, safeguarding physical access to ePHI, and ensuring that technical security measures are in place to protect networks, computers and other electronic devices.
Companies with More than 10 Employees

The United States Department of Labor has adopted numerous rules and regulations in regard to workplace safety as part of the Occupational Safety and Health Act. For example, 29 USC 654 specifically requires:

(a) Each employer:

(1) shall furnish to each of his employees employment and a place of employment which are free from recognized hazards that are causing or are likely to cause death or serious physical harm to his employees;
(2) shall comply with occupational safety and health standards promulgated under this Act.