Dumpster diving is real

Reality is that your information is more susceptible to theft than ever

Consider your company's information—whether corporate information, employee records or other sensitive information—these are a valuable commodity in today's environment. Your security measures need to match that level of importance. Further, regulatory standards, including FACTA, HIPAA and GLB* legislation, demand heightened levels of protection in securing privacy.

Take steps to protect yourself; it doesn't take much time. Put together a security plan that includes the proper storage and destruction of the materials you no longer need. Once implemented, your plan will become routine and a manageable part of the workday.

Identity theft at the corporate level

Corporate identity theft is when someone steals a company's identity by:

- Using legitimate business information to obtain goods and services.
- Creating fake companies to scam real companies.
- Incorporating companies using the same name as a defunct or inactive publicly traded corporation.
- Corporate espionage.

Serious damage can be done if your corporate information gets into the wrong hands.

Did you know…

Dumpster diving is actually legal. Once you discard your company's materials, those materials are fair game. That's why it's imperative to properly manage all corporate information.**

*Fair and Accurate Credit Transaction Act , Health Insurance Portability and Accountability Act, and Gramm-Leach-Bliley Safeguards Rule

**Source: http://idtheft.about.com/od/identitytheft101/a/Dumpster_Diving.htm

ACCO Brands
300 Tower Parkway
Lincolnshire, IL 60069-3640
In USA call 800.541.0094
www.acco.com

www.gbc.com

4/2009

How to choose the right shredder

Frequency – Don't underestimate your organization's needs

- **Frequent usage – Typically more than 10 users who shred regularly; ideal for large offices or departments**

  Shredders in this category provide:

  - Maximum productivity and destroy a large number of sheets at a time
  - Continuous operation, no cool down needed and highest waste bin capacity

- **Moderate usage – Usually 5-10 users who shred often; ideal for medium departments**

  Shredders in this group offer:

  - Strong productivity and shred a standard number of sheets at a time
  - Non-continuous operation, some cool down needed and high waste bin capacity

- **Occasional usage – Normally 1-4 users; ideal for small or home offices**

  Shredders in this set give:

  - Lighter productivity and shred fewer sheets at a time
  - Intermittent operation, more cool down needed and average waste bin capacity

Shredding style

Choose your style based on the level of security and speed of shredding desired

	Security level	Shred speed
Strip-cut	Low – Internal documents with non-sensitive information	Fastest
Cross-cut	Moderate – Confidential documents with social security, employee ID and strategic information	Very fast
Micro-cut	High – Sensitive documents with financial, medical and proprietary information	Faster
Super micro-cut	Highest – Top secret government documents	Fast

TIP

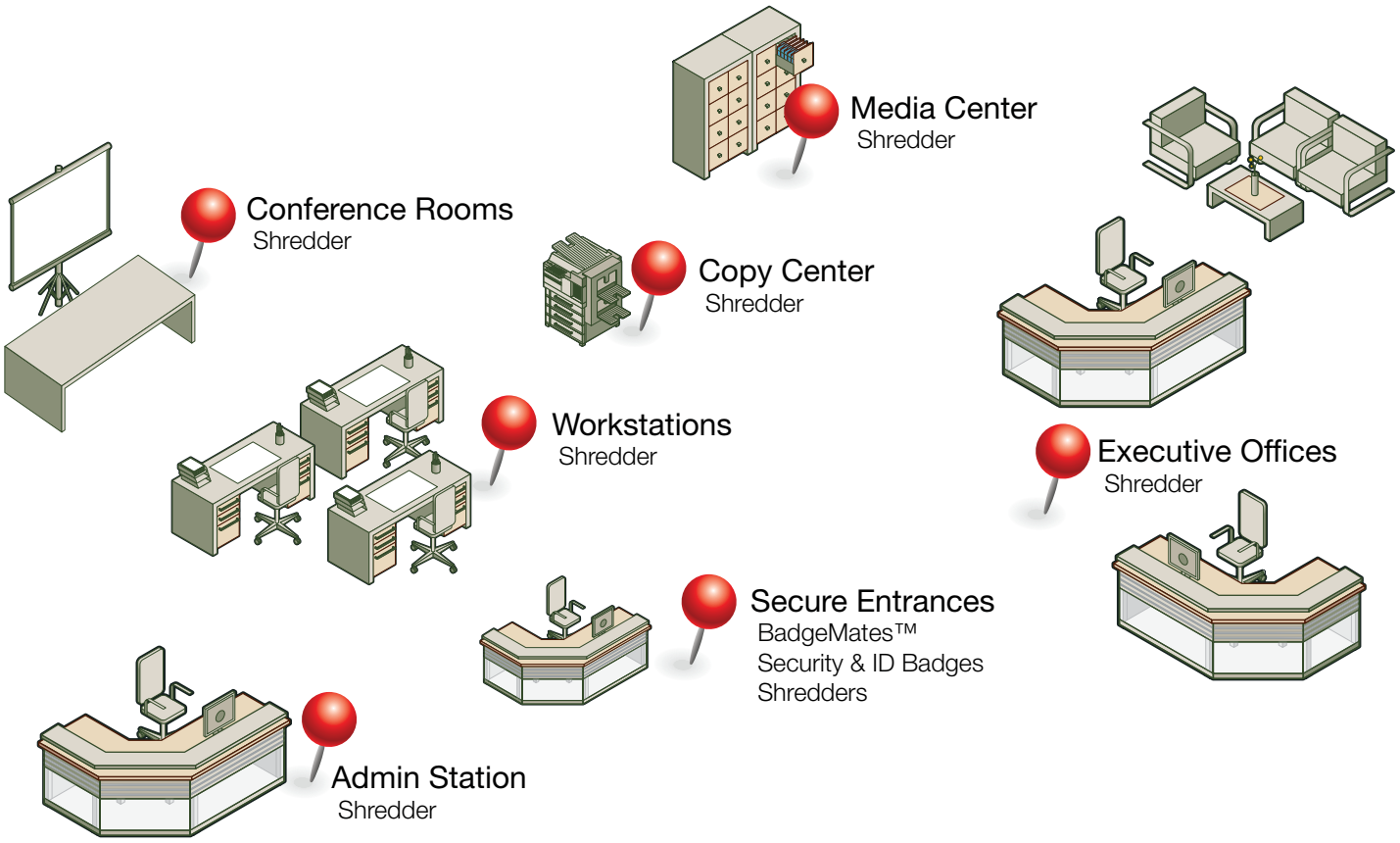
Use a GBC® ShredMaster® Jam Free Series shredder to prevent paper jams before they happen.

Did you know…

Nearly two-thirds of businesses replace shredders within three years due to purchasing lower capacity shredders incapable of handling thier shredder needs.*

Plan shredder coverage wisely
The pay-off is worth millions

Consider different needs accross your business. Is an individual using the shredder or is it for departmental use? Will more than one department utilize a centralized shredder? Do certain departments, such as human resources and finance, have a higher shredding propensity and would benefit from desk-side and centrally located shredders?



TIP

Environmental concerns and maintaining security aren't mutually exclusive. You can shred and then recycle the shredded material. Many GBC® shredders offer the option of recyclable paper bags.

Did you know…

More than one-third of individuals don't put confidential material in a secure place when a shredder is not accessible**

*Source: GBC primary research.

**Source: IAM Survey.

ACCO Brands
300 Tower Parkway
Lincolnshire, IL 60069-3640
In USA call 800.541.0094
www.acco.com

www.gbc.com

4/2009

Shredding internally is the best option

By the rules

By shredding internally, you'll meet government document destruction requirements. Regulatory standards, such as FACTA, HIPAA and GLB* demand new levels of protection in securing sensitive information. Shredding on-site helps you meet those requirements. For instance, documents won't be made vulnerable while awaiting the shredding service.

Shredding services

Using an outside source is better than simply throwing away documents; but keep in mind that shredding companies take material and shred it off-site, opening the door to possible theft. If your business will be using a shred service, make sure a trusted company does the shredding; and that they do so on-site.

The big picture

With a comprehensive information security policy that includes a deskDefense Program for sensitive materials, you're employing a strategy to save time, money and integrity. Whether your concern is regulatory compliance or maintaining a healthy business, you'll be secure when confidential information is properly destroyed.

TIP

CDs, DVDs, flash drives and other media often contain sensitive information that should be shredded.

Did you know…

A large office shredder could pay for itself in a few months versus a third party shredding service.

*Fair and Accurate Credit Transaction Act , Health Insurance Portability and Accountability Act, and Gramm-Leach-Bliley Safeguards Rule

ACCO Brands
300 Tower Parkway
Lincolnshire, IL 60069-3640
In USA call 800.541.0094
www.acco.com

www.gbc.com

4/2009

Follow the rules

The following regulations may affect your business. This is for informational purposes only and is not all-inclusive; other regulations may apply to your particular industry or state. Entities regulated by any of these laws are obligated to comply with all their applicable requirements and should not rely on this summary as a source of legal information or advice. Contact your legal advisor for further information and direction.

Rules and the law

- Fair and Accurate Credit Transaction Act (FACTA)
- Disposal Rule for Consumer Reports Information
- Gramm-Leach-Bliley (GLB) Safeguards Rule
- Family Educational Rights and Privacy Act (FERPA)
- The Health Insurance Portability & Accountability Act (HIPAA)
- The Economic Espionage Act of 1996
- Anti-Cybersquatting Consumer Protection Act

Fair and Accurate Credit Transaction Act (FACTA)

This act stipulates requirements for information privacy, accuracy and disposal and limits the ways consumer information can be shared. FACTA was created to require financial institutions provide consumers with improved protection against fraud and identity theft by implementing certain safeguards to monitor suspicious activity.

Who must comply?

Financial institutions and creditors must have in place a written program to detect, prevent and mitigate identity theft.

For more information, go to: http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci801871,00.html

Disposal rules for consumer reports information

The Disposal Rule requires companies to take appropriate measures to dispose of all sensitive information derived from consumer reports. The Federal Trade Commission enforces the Disposal Rule.

Although the Disposal Rule applies to consumer reports, the FTC encourages those who dispose of any records containing a consumer's personal or financial information to take similar protective measures.

The Disposal Rule requires disposal practices that are reasonable and appropriate to prevent the unauthorized access to—or use of—information in a consumer report.

For example:

- Shred papers containing consumer report information so that the information cannot be read or reconstructed.
- Destroy or erase electronic files or media containing consumer report information so that the information cannot be read or reconstructed.

Who must comply?

The Disposal Rule applies to people and organizations that use consumer reports. Among those who must comply are:

- Consumer reporting companies
- Lenders
- Insurers
- Employers
- Landlords
- Government agencies
- Mortgage brokers
- Automobile dealers
- Attorneys or private investigators
- Debt collectors
- Individuals who obtain a credit report on prospective contractors or tenants
- Entities that maintain information in consumer reports as part of their role as service providers to other organizations

For more information, go to www.ftc.gov/opa/2005/06/disposal.shtm

Gramm-Leach-Bliley (GLB) Act

The Gramm-Leach-Bliley (GLB) Act requires companies defined under the law as "financial institutions" to ensure the security and confidentiality of the following information. The definition of "financial institution" under the Act is broad, and includes many businesses that may not normally describe themselves that way.

- Names, addresses and phone numbers
- Bank and credit card account numbers
- Income and credit histories
- Social Security numbers

GLB requires each financial institution to develop a written information security plan to protect customer information. The plan must be appropriate to the company's size and complexity, the nature and scope of its activities, and the sensitivity of the customer information it handles.

For more information visit: www.ftc.gov

Who must comply?

The Safeguards Rule applies to all businesses, regardless of size, that are "significantly engaged" in providing financial products or services including:

- Check-cashing businesses
- Payday lenders
- Mortgage brokers
- Non-bank lenders
- Real estate appraisers
- Professional tax preparers
- Credit reporting agencies
- ATM operators that receive information about customers of other financial institutions

Family Educational Rights and Privacy Act (FERPA)

The Family Educational Rights and Privacy Act is a federal law that protects the privacy of student education records. FERPA gives parents certain rights with respect to their children's education records. These rights transfer to the student when he or she reaches the age of 18 or attends a school beyond the high school level.

- Parents or eligible students have the right to review the student's education records maintained by the school.
- Parents or eligible students have the right to request that a school correct records which they believe to be inaccurate or misleading.
- Generally, schools must have written permission from a parent or eligible student in order to release any information from a student's education record with some exceptions like other schools to which a student is transferring or to comply with a judicial order.

Schools may disclose without consent "directory" information such as a student's name, address, telephone number, date and place of birth, honors and awards and dates of attendance. However, schools must tell parents and eligible students about directory information and allow parents and eligible students a reasonable amount of time to request that the school not disclose directory information about them.

Who must comply?

The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education.

For more information visit: www.ed.gov

TIP | *The laws help protect your business only when you fully comply.*

Did you know…

The average loss to business due to employee fraud and theft is $2000 per employee per year.

The Economic Espionage Act Of 1996

The Economic Espionage Act of 1996 made it a federal offense to steal trade-secret information.

The term "trade secret" refers to all forms and types of financial, business, scientific, technical, economic or engineering information—whether tangible or intangible, and whether stored, compiled or memorialized physically, electronically, graphically, photographically or in writing, including:

- Patterns
- Plans
- Compilations
- Program devices
- Formulas
- Designs
- Methods
- Techniques
- Processes
- Procedures
- Programs or codes
- Prototypes

Who must comply?

The law protects the owner who has taken reasonable measures to keep their information secret, and the information must obtain independent economic value—actual or potential—from not being generally known and not being accessible to the public.

For more information visit:
www.usdoj.gov

The Health Insurance Portability & Accountability Act (HIPPA)

HIPAA aims to guarantee the security and privacy of patients' health information. Individuals have privacy rights under this federal law. Health care providers and insurers must comply with a patient's right to:

- Ask to see and get a copy of his or her health records.
- Make corrections to his or her health information.
- Receive a notice to describing how his or her health information is used and shared.
- Decide to give permission before his or her health information can be used or shared.

Who must comply?

- Doctors, nurses, pharmacies, hospitals, clinics, nursing homes and other health care providers.
- Health insurance companies, HMOs, employer group health plans.
- Government programs that pay for health care, such as Medicare and Medicaid.

For more information visit: www.cms.hhs.gov

Anti-Cybersquatting Consumer Protection Act (ACPA)

The Truth in Domain Names Act

This federal law targets people who register a domain name that is either a trademark or an individual's name with the sole intent of selling the rights of the domain name for financial gain. To bring a claim under this law, the owner must establish that:

- The trademark owner's mark is distinctive or famous.
- The domain name owner acted in bad faith to profit from the mark.
- The domain name and the trademark are either identical or confusingly similar.

The act is meant to reduce consumers confusion about the source and sponsorship of web pages. It provides customers with a measure of reliability so that when they visit a website using a brand's name, they will find that brand's services and products, not something different. It also protects trademark owners from loss of customer goodwill that may occur if others used the trademark to market disreputable goods or services.

Who must comply?

- Everyone

For more information visit:
www.uspto.gov/web/offices/dcom/olia/tmcybpiracy/repcongress.pdf

*Source: https://promo-manager.server-secure.com/download/files/04904/72865/0710-The_average_loss_to_business_due_to_employee_fraud.pdf

ACCO Brands
300 Tower Parkway
Lincolnshire, IL 60069-3640
In USA call 800.541.0094
www.acco.com

www.gbc.com

4/2009

Act fast when your security is breached

Determine the scope of the problem, investigate it, create a plan of action and respond aggressively.

Notify key business units including public relations, IT, HR and facilities management with the following:

- Business continuity plans
- Back-up arrangements
- Staffing solutions
- Internal and external communications
- Liaison for insurance and law enforcement

Notify your customers including:

- A general description of the breach
- What information was stolen
- What your business has done to protect the individual's information from further unauthorized access
- How your business is helping affected individuals
- How to protect themselves from identity theft

Prepare for the future by:

- Having a response plan ready in advance
- Dealing with identified vulnerabilities immediately
- Staying up-to-date with security issues
- Improving your information-handling processes
- Being consistent when carrying out procedures
- Conducting regular data security audits
- Reassessing your strategies annually

TIP

If costumer information is stolen, follow the regulations for security breeches in your state

Did you know…

Lost Information costs $182 per compromised record and companies sacrificed $2.5 million in lost business as a result.*

*Source: Ponemon institute October 2006 study

4/2009

ACCO Brands
300 Tower Parkway
Lincolnshire, IL 60069-3640
In USA call 800.541.0094
www.acco.com

www.gbc.com

Protect against online scams

Phishing

Phishing is an e-mail or instant message attempting to acquire sensitive information such as usernames, passwords and credit card details masquerading as a trustworthy entity. These messages look like they come from trusted sources such as banks or legitimate companies.

Phish e-mails usually ask recipients to click on a link in the e-mail to verify or update contact details or credit card information. Phishing links in e-mail messages, websites or instant messages may contain all or part of a real company's name and usually lead to an illegitimate website. The Internet address often resembles the name of a well-known company, but is slightly altered by adding, omitting or transposing letters.

Ways phish e-mail gets private information

Verify your account

Businesses do not ask you to send passwords, login names, Social Security numbers or other personal information through e-mail. If you receive an e-mail message from a company asking you to update your credit card information, do not respond.

You have won the lottery

The lottery scam is a common Phishing scam. This is a message that claims that you have won a large sum of money or that a person will pay you a large sum of money for little or no work.

If you don't respond within 48 hours, your account will be closed

These messages convey a sense of urgency so that you'll respond immediately and without thinking. A phishing e-mail message might even claim that your response is required because your account may have been compromised.

Click the link below to gain access to your account

Copycat websites are designed to look like the legitimate site, sometimes using graphics or fonts from the legitimate site. They might even have an Internet address that's similar to the legitimate site. Once you're at the fake site, you might unsuspectingly send personal information. If you enter your login name, password or other sensitive information, a criminal could use it to steal your identity.

Spear phishing

Spear phishing is highly targeted phishing. The e-mail goes out to members of a company and appears to be genuine. The message might look like it's from your employer or from a colleague who would plausibly send an e-mail message to everyone in the company and that message could include a request for user names or passwords (e.g., from an IT or HR department head).

TIP

Online criminals gain access to a company computer by manipulating employees into revealing confidential information.

Did you know…

Losses from phising was $2.8 billion in 2006. The per victim loss increased five-fold from $257 in 2004 to $1,244 in 2006.*

Pretexting

Pretexting is where someone assumes the identity of another person in order to establish trust and get private information either over the phone or on the Internet. The scammer not only pretends to be someone they're not, but they also create a credible "pretext" for why the confidential information is needed.

Baiting

In this scheme, the con artist leaves a disk, CD or USB flash drive in a public location (elevator, bathroom, parking lot, company lobby). The material is labeled with an intriguing title, one that will pique the curiosity of the person who finds it. When the storage unit is inserted into the computer, malware is surreptitiously installed on it, likely giving the criminal complete access to the victim's PC and perhaps the company's internal computer network.

Quid pro quo

The definition of quid pro quo is "something for something." In this scheme, an attacker calls a random number at a company claiming to be calling from technical support. Eventually they hit someone with a legitimate problem, grateful that someone is calling back to help. The attacker will "help" solve the problem and in the process have the user type commands that give the attacker access or to launch malware. Take note: in a 2003 survey, 90% of office workers gave researchers what they claimed was their password in answer to a survey question in exchange for a cheap prize.

Brandjacking

Brandjacking encompasses a variety of online threats to brand names. One form of this corporate identity theft is to mislead a consumer by advertising on a major search engine using one company name and when the consumer clicks on the ad, they go to a competitor site.

Cybersquatting

Cybersquatting is registering, trafficking in, or using a domain name with bad faith intent to profit from the goodwill of a trademark belonging to someone else. The cybersquatter then offers to sell the domain to the person or company who owns a trademark contained within the name, and to do so at an inflated price.

Corporate hijacking

The thieves incorporate companies using the same name as a defunct or inactive publicly-traded corporation, thereby hijacking that corporation and stealing its identity.

Stealing a shelf corporation

It's easy to change a corporation's information—who the president is, who manages it, where it's located. Simply file some paperwork via mail, fax or online. The government is not in the business of overseeing who files what or discovering scam artists. They simply collect the records; so it's relatively easy to pull this particular switch-a-roo.

Corporate espionage

This ploy involves accessing the location where the company information is actually stored and seeking out the company's methods and tactics or gaining unauthorized access to a company computer. It includes contacting people who know the desired information and trying to get them to divulge it.

TIP

Never share passwords online unless the source is trustworthy

*Source: 2006 Gartner research study

ACCO Brands
300 Tower Parkway
Lincolnshire, IL 60069-3640
In USA call 800.541.0094
www.acco.com

www.gbc.com

4/2009