

By C. Warren Axelrod

## Introduction

Recent events, including the loss of backup computer tapes by Bank of America, Ameritrade and Time Warner, have pointed to the vulnerability of decidedly low-tech activities, such as the packaging, shipping and storage of physical computer media, such as tapes, disks, and memory devices. Such high-profile events have quickly made the front pages of major national and international newspapers and are being examined by the computer press.<sup>1</sup>

## In-Depth Data Protection

A basic tenet of information security is "defense in depth," meaning that an organization should not secure its infrastructure using only one or two tools, such as firewalls and antivirus software. A security portfolio should, as a matter of good practice, include a number of means to avoid, deter or prevent the occurrence of damaging security breaches. These methods might include intrusion detection systems (in the network, at the host and on the desktop), intrusion prevention systems, enterprise security management tools, data aggregation, correlation and reporting tools, multi-factor authentication products, effective access control systems and procedures, encryption, monitoring and auditing capabilities, and so on.

The decision as to how much should be implemented depends upon the incremental cost-benefit ratio of each additional security tool and the risk posture of the organization's management.

Likewise, the handling of data, particularly sensitive data (such as customer personal information, intellectual property, and other confidential corporate information), should follow a philosophy of "data protection in depth." That is to say, it is the aggregation of protection methods, rather than any one, which might be called upon to provide the desired level of protection.

As an example for media shipping, a decision-maker may consider it adequate to ship paper-based company confidential reports in a sealed cardboard box by Federal Express, DHL, UPS, or similar service. On the other hand, a computer tape containing customer personal information might contain encrypted data and be shipped in a padlocked metal case by bonded courier.

Additionally, the method for disposing of data will depend on the sensitivity of the data, the type of media containing the data, the security of the locations through which the data or media might travel, the cost of disposal, and so forth.

To summarize, the determination of the most appropriate handling and disposal methods depends upon a number of factors. As alluded to above, these include:

1. the nature of the information contained on the media
2. the type of media (e.g., paper, magnetic disk)
3. whether or not the media are shipped out of house
4. who might have access to the media in transit and when stored
5. the ease and cost of cleansing the data from the media, and
6. the ease and cost of destroying the media properly

## Goals of Media Handling and Data Disposal Functions

The ultimate objective of developing media handling and data disposal policy, standards and procedures is the protection of sensitive data, specifically, personal information about customers and employees. This can be achieved by:

1. Developing and implementing policy and standards for the protection of customer personal information and company confidential data at every step in its lifecycle on whatever medium it resides, with a degree of protection commensurate with the sensitivity and value of the data. This will generally include a combination of methods that, in total, will provide appropriate protection from misappropriation, damage and misuse.
2. Developing and implementing procedures to monitor and report the status of the data; including knowing the whereabouts, condition, and current handling of the media containing the data, and the status and use of the data.
3. Developing procedures to handle or respond to actual or suspected breaches that might lead to the compromise of sensitive data during its lifecycle and however it is being handled.
4. Encouraging the transition from high-risk media and media handling methods to lower risk media and handling methods, such as moving from the physical shipment of magnetic tape to electronic transmissions over dedicated and/or protected lines or transmission protocols.
5. Making everyone coming in contact with sensitive information and the media containing it aware of the appropriate handling and disposal of such data and media.

## Overarching Principle

The overarching principle is to protect customer, corporate and other sensitive data using a combination of methods appropriate to the classification and use of the data, of converting the data and/or media to less risky options, where feasible and cost-effective, and incorporating mechanisms such as data encryption, data disguise, or masking in order to avoid making data available when there is not a definite need to know.

## Levels of Risk by Type of Media and Form of Data

### Paper

Paper documents generally represent the riskiest form of media, since information written on paper is generally immediately readable or recognizable and understood by a human subject usually without the need for additional transformation equipment.<sup>2</sup> While it is possible to encrypt data on paper, it is not commonly done in modern times.<sup>3</sup> More usual is the physical protection of paper documents and similar physical substrates, such as putting them in locked rooms, safes, cabinets, drawers and cases.

On the other hand, paper is bulky and has much lower data density than do most other forms of media, such as magnetic tape. The data contained in a single magnetic tape, when printed, might be equivalent to a truckload of paper reports. Thus the exposure, when tapes, disks, or similar media are lost and compromised is orders of magnitude greater than for paper, assuming that the contents media can be easily "read."

### Displays

CRTs, LCD or similar screens display data in directly readable form and therefore are considered high risk. Data on screen is considered volatile since, if the screen is turned off or if a particular screen is replaced with a different one, the data image, which was formerly displayed in the screen, is no longer visible.<sup>4</sup> Also, the operator is usually aware whenever someone is trying to read the screen, unless it has been left unattended, which usually infringes upon an organizations' security policy.<sup>5</sup>

Protection of data on screens might involve a number of methods, such as installing special screen covers or shields to restrict the angle of view, keeping displays in secured areas, facing displays away from others, and requiring that screens be locked by the operator when left unattended. Here it is beneficial to have an automatic screen lock triggered after a specific idle time, to compensate for users' inattention. Particular care must be taken with portable devices, such as laptop computers, PDAs, and so on, since they are generally not secured physically or by location. Furthermore, portable devices are often used in public places, where a passing stranger might catch a glimpse of the screen.

### Film Media

Microfilm and microfiche cannot be read directly; they require some form of magnification and illumination in order to be fully legible (except for the title bars, which are in large print). However, microfiche and microfilm readers are readily available, such as in public libraries, and are easy to use, so that the protection requirements are similar to paper.

However, the data density on microfilm or microfiche is orders of magnitude greater than for paper documents. For example, a typical microfiche may contain some 200 or more pages. Consequently, the physical removal or loss of a box of microfiche would have that much more impact.

### Magnetic Tapes and Disks and Optical Media

These forms of media contain data that is machine-readable only and cannot be read directly by humans. Some media, such as CDs and diskettes, may be read using commonly available equipment, such as PCs or CD players, with common software, such as Microsoft Office, or built-in software or firmware. Other media, such as tape cartridges, will require specialized equipment and retrieval programs not commonly available to the individual. If data on such media is password protected, compressed and/or encrypted, then either knowledge of the password or access to decryption tools is needed in addition to specialized programs and equipment. However, cracking software is available for those wanting to decrypt encrypted data. The ease of decryption is directly related to the strength of the encryption, although the bar keeps getting higher as more powerful machines and programs become available.

### Consideration of Data Volatility

It should be noted that for the above-mentioned media, data remains on the media after the tape or disk, for example, has been removed from the writing and reading equipment. Such media forms are termed "non-volatile." However, there are other forms of media, so-called "volatile"

media, which carry the data only when there is a power supply operating. For example, computer memory is often volatile, meaning that the data contained in it disappears when the power is shut off.

### Transmission over Copper, Fiber, Ether (Wireless)

The difference between most other media and transmission media is that transmission media are volatile or transient and do not retain an image of the data transmitted over it. Therefore the risk is not related to commandeering the physical copper cable or fiber, but in intercepting the data when it is in transit. Transmitting data in the clear is, however, considered somewhat risky, so that highly sensitive data, such as passwords and customer and confidential information, are generally required to be encrypted during transmission. Public networks, such as the Internet, are generally considered more risky than dedicated or private lines, which are more difficult to “sniff.” It is also easier to intercept wireless transmissions than it is physical cable.

While data items transmitted over lines or air are transient or volatile, if the data stream is sniffed, the data can be directed to a storage device where it will remain in non-volatile form for future use.

## Levels of Risk by Lifecycle Step and Handling Method

### Data Origin and Creation

All data has to be originating from some source. Often it is information:

- ▲ divulged in a telephone conversation with a person, or through a telephone key recognition system or voice recognition system
- ▲ obtained from data contained on a handwritten document or form or on a printed form or report received through the mail, by messenger, or similar conveyance, or
- ▲ taken from a document that was scanned and faxed or conveyed by another method.

The information may then be keyed into a computer, or scanned and converted into text and entered into a database, or the like. It may also be entered or keyed into a system by someone who knows the information innately or obtains it from another source.

During this transformation stage,<sup>6</sup> wherein the data is entered somehow into a file or database, the data may change classification and therefore risk level. For example, isolated pieces of data about an individual may be insufficient to enable compromise of any particular source to be used in identity theft, whereas the combined data from several sources could well represent sensitive personal information from which someone might gain sufficient personal information to conduct fraud in that person’s name. The risk at this stage may well hinge on who has access to the source data at a particular point in time, and what degree of data aggregation an operator might see. Thus, if there is a separation of duties so that any one operator cannot see enough data to identify a subject, then the risk is lower. However, it is much more likely that operators will be able to construct identities if they wished to do so.

The data origination phase, wherein information is converted from human-readable to machine-readable form, should be considered to be one of the riskier stages in the data lifecycle and precautions commensurate with such risk need to be taken. While data entry operators are usually low-paid personnel, they might have access to highly sensitive information, which data could have significant market value if purloined. This emphasizes the need for thorough background checks on such staff, stringent security procedures in regard to copying and handling the orig-

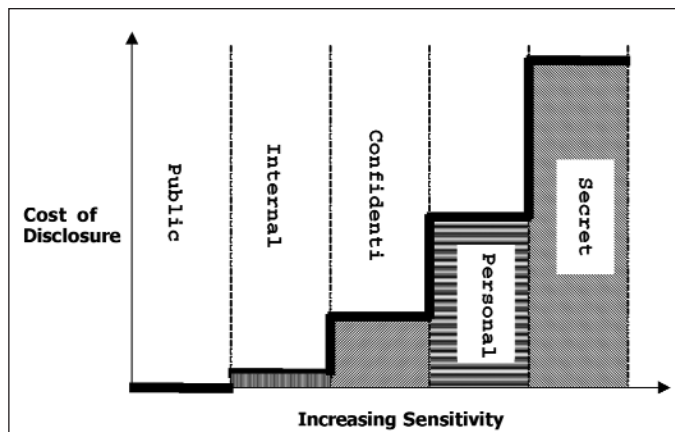


Figure 1: Cost of Unintentional Disclosure vs. Data Sensitivity

Mitigation Expenditure	Expected Loss from Disclosure	Aggregate Cost
\$0	\$200,000	\$200,000
\$50,000	\$130,000	\$180,000
\$100,000	\$60,000	\$160,000
\$120,000	\$30,000	\$150,000*
\$150,000	\$20,000	\$170,000
\$200,000	\$10,000	\$210,000
\$250,000	\$6,000	\$256,000
\$300,000	\$3,000	\$303,000

\*Approximate minimum cost

Figure 2: Relationship between Expenditures on Risk Mitigation and Losses from Disclosure

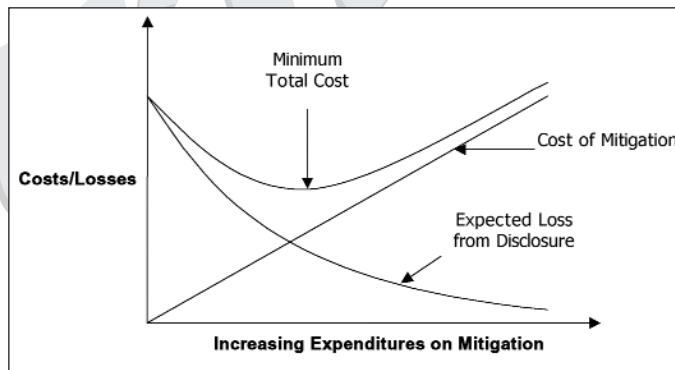


Figure 3: Minimization of Total Cost of Disclosure and Mitigation

inal source documents, effective deterrents to discourage misappropriation and misuse of data due to serious personal consequences in the event of discovery, and effective oversight monitoring and reporting systems to enable management to recognize any aberrant behavior.

### Storage

Once created, data are almost invariably stored on some medium for future access and use.<sup>7</sup> The decision as to whether or not the data will need to be protected by a password (or other key) and/or encrypted while stored will depend upon factors such as:

1. the sensitivity of the data
2. how valuable the information might be for a thief
3. how painful the loss of such data will be for the organization (e.g., regulatory or reputation impact)
4. the medium used for storage (particularly if removable media)
5. who is likely to have authorized access to the information

6. how restrictive the authentication process will be
7. for what length of time the data will be maintained on the storage medium, and
8. to what use the data will or could be put

These factors need to be balanced against available protective measures. Encryption, for example, will require more powerful processors and probably additional network bandwidth and data storage requirements, and will likely introduce overhead and delays, all of which increase costs. Also, the strength and form of the authentication methods need to be considered. Data may have to be retrieved years after it was originally stored, meaning that procedures must be in place to manage and maintain encryption keys over long periods of time.

On the other hand, many (particularly lawmakers and regulators, as well as the public) consider encryption of data to be highly secure and do not necessarily require reporting the loss or theft of data, if it is encrypted.

## Access

Data may be accessed directly, usually by database administrators for maintenance and repair purposes, or more usually through applications. Access is managed through two methods: authentication and authorization.

In order to be authenticated, a user must have gone through a registration or enrollment process to establish identity credentials against which the authentication software can check the proffered credentials at the time access is requested. There is a risk that someone is falsely enrolled as well as a risk that the credentials of another valid user might have been stolen.

Authorization or entitlement is given from previously determined rules which permit certain individuals to have specific access rights to predetermined functions and information. Here, the risk is that if someone is given access inappropriately or imprecisely, then that person may be able to access information to which they are not entitled. This can result in theft, compromise and fraud. Therefore inappropriate access can be obtained by someone defeating the authentication system and masquerading as a legitimate user, and/or from poorly managed entitlements.

## Use

Along with access rights comes a series of capabilities specific to a user's role and application being accessed. Simple use parameters involve reading, writing and modifying data. More complex access controls restrict use within

a certain facility, such as writing to only certain files or data elements, for example.

Access implies minimally the ability to view or read data. The danger here is giving access to data that a user should not be able to see. Inappropriate access along with the ability to print or write the data to another medium, particularly removable medium, or to transmit to another location, opens the door to significant data theft opportunities. If someone can change data, then there is a threat to data integrity and accuracy.

Similarly for data stored on removable media, even when it is in encrypted form, there remains the risk that someone might abscond with the medium and be able to access and decrypt the contents, given enough time and computer resources.

## Movement

When data are sitting on volatile and non-volatile media, protection usually focuses on physical controls over access and use, along with a variety of logical restrictions as noted above. However, once it is decided to move the data or a copy of the data from one physical location to another, a series of new risks arise.<sup>8</sup> These risks relate to the transferring of the data to removable (and movable) media or over transmission facilities (physical or wireless).

The transfer process itself, between one medium and another, or between one location and another, usually occurs at both source and destination. The transfer process is also subject to risks, particularly if, during it, data are decrypted and then re-encrypted. Data might exist in the clear for a specific instant during the transition.

The movement process is also considered to be very risky, particularly when physical media are involved. Encrypting the data reduces the risk but does not eliminate it. Movement of data and media within internal facilities of an organization is considered less risky than shipments or transmissions out of house, although the former is still subject to compromise.

## Destruction and Disposal

At the end of the useful life of data and/or media, and subject to legal and regulatory requirements, data are generally erased and/or the media on which the data sits are discarded and physically destroyed.

Being a physical process, it is particularly subject to human error. The process begins with the determination that the data and/or media need to be destroyed and/or the data made unreadable. This requires some sorting process in which media destined for destruction are separated out from other items. This step, which

might involve putting some items in one kind of waste container for destruction (e.g., shredding) and another type of container for media that is just garbage. It is surprising how difficult it is to get everyone to comply.

If there is a reasonable chance of reusing the media, the data erasure method should be non-destructive. The latter is often accomplished by repeatedly overwriting useless data over good data, so that the latter can no longer be read. This is the most likely way to preserve the integrity and reusability of the media. Another means of erasure is the passing of a strong magnetic field across the media, thereby aligning all the magnetic particles in one direction. This is known as "degaussing." Some degaussed media can be reused, with varying degrees of difficulty, through re-initializing or re-manufacturing the media. In other cases, the media are destroyed if degaussed and cannot be reused.

The main idea here is to render the data and/or media into such a form that, when discarded, the original sensitive data residing on the media cannot be retrieved and read.<sup>9</sup>

## Tracking Mechanisms and Controls

No amount of data encryption and other data protection methods can fully succeed unless adequate tracking mechanisms and controls are in place.

### Tracking Mechanisms

The goal of a tracking mechanism is to ensure that there is full knowledge as to the whereabouts of any particular item of personal and confidential information at any point in time. Ideally this translates into the use of an integrated real-time tracking system, preferably automated, although manual procedures can be used. In order to accomplish this, current tracking systems, which may be home-grown, commercial, in-house and/or at the service providers, need to be integrated at some level. The system should report on the location of all media, including when they are in containers holding a number of media items, in which case, the container must be tracked.

### Procedural Controls

It is important to have policy and procedures, including supervisory procedures, in place which specify unambiguously all sensitive (personal, confidential, secret) data and the media on which it resides. The controls must include source and destination information, media type, contents, reporting and validation

processes, mode of transportation (when applicable) and appropriate management approvals. Preferably this information is carried on the tracking system.

### Requirements for Moving and Storing Data

The table in Figure 4 indicates various suggestions for protecting data during their physical or electronic movement and storage. It should be noted that, as the classification category becomes more stringent (i.e., tends towards “secret”), all prior standards apply in addition to the standards specific to that category.

It is generally held that the more sensitive the information, the greater the precautions against compromise of the information. Therefore we will begin by defining different data classifications and what they mean in general.<sup>10</sup> Organizations tend to have their own definitions.

First, we have “public information,” which is generally available to the public and does not require special protective treatment in regard to confidentiality. Care should be taken in differentiating that which is meant to be public and confidential information that has somehow been leaked to the public.<sup>11</sup> It is not always obvious what is actually in the public domain, so it is wiser to be conservative on this issue and not distribute copyrighted or confidential information belonging to others, since the consequences of infringement can be considerable.

Then there is “internal information,” which is generally held to be information for the use of only internal staff, which might include permanent employees, part-timers, consultants, and the like. If such internal information were to become available to someone outside the organization, it would not be considered serious, only inappropriate. There would not usually be any negative impact on the organization. However, to an outsider, it might be considered indicative of a lack of adequate controls that would also affect more sensitive data.

What is left is the broad category of “sensitive information” with its various levels of restrictions as to availability and use, and the harm done were it to be disclosed and compromised. Whereas the disclosure of “confidential information” might inflict significant harm or damage to an organization, if the information is “restricted” or “secret,” the damage could be severe.

It is difficult to place “personal information” along the information risk spectrum, except that the consequences of inappropriate disclosure of such information are becoming more serious

Data Classification >	Publicly Available	Internal Use	Sensitive, e.g., Personal, Confidential	Secret, i.e., Highly Restricted
<b>Type of Media v</b>				
Internal volatile, e.g. memory, and nonvolatile, e.g. hard disk	No specific data protection requirements.	Restrict general access by weak authentication.	Require strong access authentication. Secure physical devices and environment.	Require very strong authentication. Isolate machines, networks, etc.
Removable magnetic, e.g. disk, tape, electronic; e.g. flash memory cards, USB thumb drives; optical, e.g., CD-ROM.	No specific data protection requirements.	No specific data protection requirements.	Media should be labeled appropriately. Media should be placed in appropriately labeled sealed boxes or envelopes for in-house distribution. Media shipped externally should be in locked tamper-resistant boxes or cases. Effective end-to-end tracking of containers and media should be in place. Data should be encrypted and/or password protected.	Media should be labeled appropriately. Media should be placed in appropriately labeled sealed boxes or envelopes for in-house distribution. Media shipped externally should be in locked tamper-resistant boxes or cases and be accompanied by a courier at all times. Effective end-to-end real-time tracking of containers and media should be in place, during which media should not be left alone.
Paper, film, etc.	No specific data protection requirements.	No specific data protection requirements.	Media should be labeled appropriately. Media should be placed in appropriately labeled sealed boxes or envelopes for in-house distribution. Media shipped externally should be in locked tamper-resistant boxes or cases. Effective end-to-end tracking of containers and media should be in place.	Media should be labeled appropriately. Media should be placed in appropriately labeled sealed boxes or envelopes for in-house distribution. Media shipped externally should be in locked tamper-resistant boxes or cases and be accompanied by a courier at all times. Effective end-to-end real-time tracking of containers and media should be in place, during which media should not be left alone.
Transmissions	No specific data protection requirements.	No specific data protection requirements.	Data must be encrypted if it passes over public networks.	Data cannot be transmitted over public networks,
Storage	No specific data protection requirements.	No specific data protection requirements.	Data should be encrypted or protect via strong authentication.	Data cannot be stored in shared facilities.

Figure 4: Protecting different data classes by media type

Media	Clear	Sanitize
Magnetic tape	Degauss	Degauss or destroy
Magnetic disk – non-rigid, removable	Degauss or overwrite	Destroy
Magnetic disk – rigid	Overwrite, degauss if removable	Degauss, overwrite or destroy
Optical disk	Overwrite if “write many”	Destroy if information is classified
Memory – Dynamic random access	Overwrite or remove power, including batteries	Overwrite, remove power or destroy
Memory – Programmable read only	Full chip erase or overwrite as feasible	Various overwrite methods, then destroy
Magnetic memory	Overwrite	Various overwrite methods, then destroy
Memory – Nonvolatile, static	Overwrite or remove power, including batteries	Overwrite, remove power or destroy
Memory – Read only		Destroy
Cathode ray tubes	Remove power, including batteries	Destroy if information burned-into surface
Printers – Impact	Remove power, including batteries	Destroy ribbons, clean platen
Printers – Laser	Remove power, including batteries	Run through 5 pages of unclassified text

Figure 5: Standard for Clearing Data and Sanitizing Media. This is a simplified version of the U.S. Department of Defense 5220.22-M clearing and sanitization matrix. For details, refer to full standard.

with each passing day as lawmakers and regulators are clamping down on reporting and customer assistance requirements and are making the corporate and personal consequences of such breaches much more serious than before. Personal information, that at one time was merely considered confidential, is now well into the restricted/secret realm, where the unauthorized revelation and use of "secret information" might prove disastrous to an organization.

There is yet another category called "sensitive personal information," which relates to the private lives of individuals and which should only be collected for a specific authorized purpose at a particular point in time, if it can be collected at all.

As we march through the categories of data from public through internal and confidential and on to highly restricted data, the sum of the costs of disclosure and misuse of the data increases markedly in an almost exponential fashion, as shown in Figure 1. At the same time, the return on investing in proper handling, storage and disposal mechanisms might well increase at an even faster rate.

As mentioned, the costs of unintentional disclosures might include financial losses (e.g., due to fraud), costs of response (e.g., assisting customers in reestablishing their credit ratings, paying fines to regulators, involvement in lawsuits), losses of revenues (e.g., due to losing customers), opportunity costs (e.g., from new customers not signing on, or existing customers not expanding their business), and loss of reputation (which, apart from the embarrassment, can lead to many of the other costs and losses).

## **Risk Versus Cost of Mitigation**

The determination of the most appropriate forms of data/media handling, storage and disposal is very much based upon the sensitivity of the data, the potential aggregate cost if the data is lost or stolen and then compromised, and the cost of increasing the security of handling, storage and disposal.

In Figure 4, we show generally available options for data/media handling and storage for data of various sensitivities. These are just suggestions. There is a broader range of possibilities, including eliminating physical media to the greatest extent possible, and converting where possible to transmissions and electronic delivery, thereby avoiding many of the issues.

Figure 5 shows the generally acceptable standards for clearing and sanitizing data and media for a whole range of media types.

The choice of method and possible combination of methods (such as degaussing magnetic tapes and locking them in transit) needs to be assessed in terms of the estimated costs of lost or stolen media and the likelihood that a compromise will happen, versus the cost of the extra measures. It appears that, within reason, the expected losses far outweigh the costs, so that there is little excuse not to implement secure handling, storage and disposal mechanisms.

It would appear that a very large component of the costs revolve around the tracking mechanisms. For physical media these can be very elaborate and costly, involving bar-coding, GPS, RFID, and the like. The major package shipment services (such as UPS, FedEx and DHL) have very elaborate and sophisticated tracking systems. This may in fact become the de facto standard for organizations generally.

## **Cost of an Event**

As more events are widely publicized and the items included in a typical response are better defined, there are better measures of the cost. For example, if credit card numbers are stolen, the company must

account for the cost of reissuing the card, cost of fraud, cost of additional customer service, and cost of providing credit tracking assistance, if that is offered. These are more tangible and more measurable costs. Other less tangible costs, such as loss of customers, not getting new customers, and the like, are fuzziest and must be estimated as best as possible. There are then the indirect costs, such as the potential for more stringent costly laws.

The costs can be scaled to the size of the event (e.g., number of identities stolen), where the relationship may not be linear. That is to say, the bigger events may require much more effort to shore up customer confidence.

## **Probability of an Event and Expected Loss**

It would seem that the likelihood of media being lost or stolen and data stored on computer systems being hacked has increased significantly of late. This may be the case, but the more stringent reporting requirements, as dictated by California SB 1386 in particular, may have resulted in a greater percentage of events being made public, rather than an actual increase in events. That being said, there may also be an increase in the absolute number and size of events.

This doesn't help in estimating the probability of an event of a certain magnitude. However, most businesses, particularly in financial services, are assuming a high likelihood of an event within a specified period of time, say one year.

## **Acceptable Cost of Risk Mitigation**

It is then a relatively simple matter to estimate the cost of measures available and to compare them to related losses to determine what a reasonable level of protection might be.

Example: If the expected probability of an event, leading to the compromise of one million identities, occurring in the next year is 0.1 percent, and the direct cost of responding to the event is \$100 per customer, then the expected direct cost is \$100,000. Additional, less tangible opportunity and indirect costs may come to \$200,000. Therefore, the organization should be willing to spend up to \$300,000 per year to reduce the probability of occurrence of this type of event to almost zero.

However, the cost of eliminating risk altogether, if attainable, is usually extremely onerous as to make it infeasible. Some acceptable calculated risk generally has to be assumed. The key is to find a degree of mitigation that makes the risk tolerable. Thus, for example, management may be willing to pay (say) \$100,000 to bring the risk down to .005 percent.


In Figure 2, we give a hypothetical example as to how the expected cost or losses due to unintentional disclosure might relate to the amount spent on mitigation. The cost of disclosure is in turn related to the sensitivity of the data. Here let us assume that we are dealing with customer personal information as in the above case.

The third column, which is the sum of the first two columns, shows the aggregate of the mitigation costs and disclosure losses. This is illustrated graphically in Figure 3. It is clear from the graph that there is a point at which the total estimated cost is a minimum, which is at \$150,000 in mitigation expenditures in this case.

## **Summary and Conclusions**

With major exposés of the loss and/or theft of personal and confidential data hitting the newspapers, it is clear that organizations must greatly improve how they handle, store and dispose of sensitive data.

Here, we have looked at the issue, its risks, costs and remedies, and we have suggested standard approaches which should mitigate those risks and reduce the total cost of media management to a company.

The bottom line is that the methods of data protection must meet the business needs and satisfy the legal and regulatory environment by suitably mitigating the risks. 

---

*C. Warren Axelrod, PhD, CISSP, CISM, is Director, Global Information Security, for Pershing LLC, a BNY Securities Group Co. He is the author of Outsourcing Information Security (Artech House, October 2004), which has received excellent reviews. He is chair of the GAISP Information Security Policy Principles Working Group and a member of the Editorial Advisory Board of The ISSA Journal.*

<sup>1</sup> Gary H. Anthes, "Lost, Stolen or Strayed", Computerworld, August 1, 2005, pages 31-32.  
<sup>2</sup> For example, if some finds a \$20 bill, it is immediately obvious what it is and what its value is. On the other hand, if one were to find a prepaid subway card, on which the remaining value is encoded on a magnetic strip, its residual value would not be known unless the finder had access to a card reader.  
<sup>3</sup> It is noteworthy that the use of foreign languages (particularly when colloquialisms are used) is tantamount to encryption if there are few or no translators available.  
<sup>4</sup> Older CRT designs have the characteristic that if the screen is left on for a long period of time with a constant image, the image will burn into the phosphors on the screen and will therefore be visible even when the CRT is turned off. More modern CRTs and other displays do not exhibit this characteristic.  
<sup>5</sup> In a piece by Mike Fratto, editor of Secure Enterprise Magazine, with the title "Security Holes in Plain Sight," he describes how easy it was for him to overhear cell phone conversations or read sensitive information on laptop computers during his air travels.  
<sup>6</sup> Interestingly, some financial regulators are differentiating between data in text form, whether physical, electronic or magnetic, and not text, such as voice telephone conversations.  
<sup>7</sup> It is feasible that the data is held temporarily in some volatile medium, such as the computer memory, and then worked on and transformed into other information, which is then stored, or transmitted to another location where it is stored. Note that if it is merely printed, the printed page is a form of storage medium.  
<sup>8</sup> To quote Dan Geer, CTO of Verdasys: "... threats to [data] value are at the point of use where a state change between at-rest and in-motion occurs ..."  
<sup>9</sup> Even seemingly effective methods of destruction can be foiled. For example, cross-cut shredding of paper is generally considered to be highly effective. However, in his article "Secure Your Shredding" in the June 20, 2005 edition of eWeek, Ben Rothke describes how there exist services, which can piece together the "confetti" that the shredder produces, using sophisticated pattern-matching software.  
<sup>10</sup> For greater detail, see my book, Outsourcing Information Security, Artech House, Norwood, MA, pages 142 and 143.  
<sup>11</sup> In a recent search of the public Internet in regard to another topic, I came across a document that was clearly labeled "Private and Confidential" and another couple of copyrighted documents that were actually for sale by another organization but had been posted for the internal use of employees of a different organization. None of these documents could be considered public, but had clearly been made available, probably unintentionally, to anyone browsing the Web.