

TAXONOMY AND THE SECURITY OF DATABASES

[Roger L. Kaesler](#), [Jill W. Krebs](#), and [Douglas L. Miller](#)

ABSTRACT

Taxonomy is a complex, sometimes arcane subject that is marked by two distinctive characteristics: its historical perspective and its openness to all practitioners. The complexity of such historical taxonomic information as synonymies cries out for the development of electronic, relational databases. The need for openness implies that databases must be freely available.

In the flurry of activity to develop paleontological databases, insufficient attention has been paid to security. Three points underscore our concerns in this regard. First, data have value. Anything of value is subject to theft, misuse, or vandalism. Second, paleontologists who develop databases have a right to the first use of their data and a correlative obligation to share those data with the scientific community. These two aspects of the ownership of data—one a right and the other a responsibility—may lead to conflict. Third, sharing of information and the security of files may be incompatible. No system will ensure the security of data that are freely shared.

Ensuring the security of databases involves attention to ten kinds of risks: power outages and surges, natural disasters, turnover of staff, the year-2000 problem, buggy software, computer viruses, hackers and vandals, access by unwelcome users, and problems associated with copyright laws and abbreviations, acronyms, and other jargon. Effective security requires a team effort that involves developers, programmers, contributors, users, and security specialists associated with the central computer facility. The strategy should weigh security against performance, productivity, and accessibility. The goal of any security system should be to improve access to while maintaining the integrity of those data.

[Roger L. Kaesler](#), Paleontological Institute, The University of Kansas, 121 Lindley Hall, Lawrence, KS 66045-2911, USA.; Department of Geology, The University of Kansas, 120 Lindley Hall, Lawrence, KS 66045-2124, USA; and Division of Invertebrate Paleontology, Natural History Museum, The University of Kansas, 120 Lindley Hall, Lawrence, KS 66045-2124, USA

[Jill W. Krebs](#), Paleontological Institute, The University of Kansas, 121 Lindley Hall, Lawrence, KS 66045-2911, USA.

[Douglas L. Miller](#), Information Technology Center, The University of Kansas Computer Center, Lawrence, KS 66045, USA

KEY WORDS: paleontology, database, security, taxonomy

Copyright: Paleontological Society, 1 March 1999

Submission: 7 December 1998, Acceptance: 2 February 1999

INTRODUCTION

Electronic, relational databases are becoming increasingly important, and as their importance grows, there is a concomitant concern about database security. As specialists in every science turn increasingly to the use of databases in their research, each field makes unique demands on the technology that underlies database development. In turn, databases provide special opportunities for every field. Systematics and, for our purposes here, systematic or taxonomic paleontology are characterized by a focus on the historical development of ideas that is unprecedented in other fields. Thus, whereas papers in high-energy physics older than ten or fifteen years are likely to be permanently shelved, and papers on Internet and intranet security have a half-life measured in weeks, paleontologists may need to refer to taxonomic literature, irrespective of its quality, back to the times of [Clerck \(1758\)](#) and [Linnaeus \(1758\)](#).

Systematic paleontologists rely on the history of taxonomic ideas, and, because of the rules of priority, the information of taxonomic paleontology must also be made widely available to enhance communication among systematists. Nothing is gained by excessive secrecy on the taxonomic front; indeed, with secrecy all is lost, including the priority of names and the ideas they represent. It is essential, therefore, that any database prepared in support of taxonomic paleontology be available for a long period of time and be readily accessible to a wide range of potential users, many of whom are likely to be unknown to the owner of the database.

Both requirements spell trouble for the security of databases. Yet security is an aspect of the preparation of databases that has received little attention from the paleontological community. Our purposes here are to present reasons for securing the information in databases and to suggest means of wending one's way through the jargon-laden jumble of security-related matters.

Paying Attention to Security

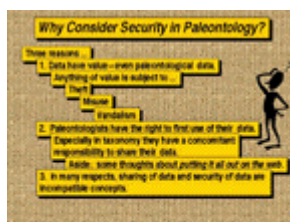


Figure 1.

Three points form the basis of our concerns regarding security ([Fig. 1](#)). First, data have value, and this is so even for paleontological data. Of late, our profession has experienced some difficulty convincing others of the truth of this notion.

Nevertheless, it is true, as several examples will make clear. (1) Petroleum companies often share geophysical data, but they tend to play their biostratigraphical cards rather close to the chest and typically regard such information as proprietary. (2) Paleontologists seeking grants from funding agencies in many instances find data from their previous studies to be of vital importance in establishing their qualifications.

(3) The business of publishing about fossils is booming—and here we mean not only

publishing books about dinosaurs—with the result that databases with illustrations of fossils are likely to be especially popular.

Second, anything of value is subject to theft, misuse, and, perhaps worst of all, vandalism. The threat to paleontological data is, of course, nowhere nearly so ominous as the threat to industrial, military, and financial investment data. By the same token, the impecunious paleontological community is ill-prepared fiscally to install security systems that are reliable and that provide effective security. Hackers have managed to break into the secret files of the U. S. Department of Defense, which are protected by an appreciable portion of a \$200 billion annual budget. Given this fact, how vulnerable do you suppose the data of paleontology are to similar invasion?

Paleontologists develop databases either through their personal research, from the cooperative work of close colleagues, or by extensive library work and **Treatise** grazing. Whatever the data source, the paleontologist who develops a database has the right to the first use of those data before broadcasting them to the general public. One often hears the plea to **just put it all out on the web**. Such pleas too often ignore the fact that data have value and that their supporting infrastructure are sometimes quite costly as well.

Third, in spite of all these concerns, paleontologists need to share information. Data may be shared among close colleagues in the early phases of a research project or at a later stage be made generally available through the Internet. Concomitant with the need to share information is the risk to those data. At the end of the day, sharing is incompatible with security. The issue of security—both Internet security and intranet security—is emphasized extensively by computer insiders, and a hefty literature on the subject is available. In industry, the principal concern is the access to data by unauthorized persons, especially the theft of economically or militarily valuable information. A secondary concern is vulnerability to vandalism, which can be an equally costly problem.

What is the situation in academia? Things are certainly different in paleontology from what they are in, say, the pharmaceutical or defense industry. If a colleague were to abscond with your data, whether electronically or otherwise, he would soon be found out and would no doubt suffer professional ostracism. Thus, the outright theft of data in paleontology, partly because of its low likelihood, is probably not as troubling as other aspects of the complete security picture.

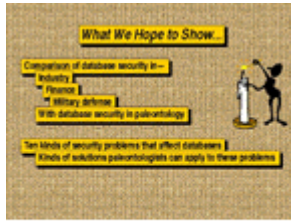


Figure 2.

Herein we compare the issues of database security in industry, finance, and the military with the issues facing paleontologists (Fig. 2). We identify ten problems of security that affect databases of every sort, and we propose some kinds of solutions that paleontologists can apply to help them address those problems.

Viewed **in toto**, the essence of the problem with security for databases is to weigh concerns about security against requirements for performance, productivity, and accessibility (Fig. 3; Hartley, 1998).



Figure 3.



Figure 4.

Adopting a thorough approach to security will help defray the costs of inadequate security: lost time, lost money, and unnecessary wear and tear on members of the staff, thereby curtailing their productivity (Fig. 4).

Security of Databases: Meanings, Advantages, and Disadvantages

What do we mean when we speak of the security of a database (Fig. 5)? Establishing a definition at the outset is important because the definition of security that one adopts will determine in large part the approach one takes to emplacing appropriate measures of security.

TechEncyclopedia has defined security as, "The protection of data against unauthorized access." This is quite a narrow definition, but we understand the reason for the emphasis on unauthorized users. The definition is geared to the kinds of security problems that are encountered by industry, wherein the primary concern is access by unwelcome users. It recognizes that persistent systems programmers and other technically competent individuals are likely to be able to gain access to the identification codes and passwords that protect nearly any system, enabling ingress to an otherwise secure database.

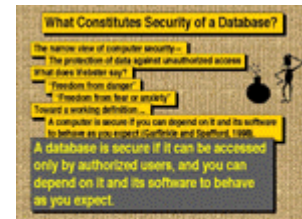


Figure 5.

The special needs facing paleontologists and their data cause us to favor a much broader definition of security. The dictionary definition (Mish 1995, p. 1056), always a good starting place, refers to security as "freedom from danger" or "freedom from fear or anxiety." An appealing working definition is that "a computer is secure if you can depend on it and its software to behave as you expect" (Garfinkel and Spafford 1996, p. 6). This definition ignores the problems that can result from the access by unauthorized individuals who use, but do not destroy, your database. Let us say that a database is secure if it can be accessed only by authorized users and you can depend on it and its

software to behave as you expect. Dealing with this broader definition of security has led us to identify the ten areas of concern ([Table 1](#)).

The Downside of Security. Paranoia is stressful. It consumes energy and, where security of data systems is the issue, can devolve into a dreadful time sink. Of greater importance for our profession, excessive attention to matters of security will necessarily diminish communication to the detriment of paleontology as a whole. For this reason, although we must pay careful attention to matters of security, we must do so with an eye to our other goal, fulfilling the obligation of taxonomic paleontologists to communicate freely with each other.

The Upside of Security. The obvious advantage to having in place an effective system of security is that you and your data will be free from danger, fear, and anxiety. In addition, a very thin silver lining is that something good sometimes comes from examining and reexamining computer systems. Given the threats to databases, prudence requires a well-formulated, comprehensive, and appropriate security policy and the performance of all necessary security protocols on a daily or weekly basis. In the long run, systems designed with security in mind are more cost-effective than those that are not, especially if a major breach of security can be avoided.

ASPECTS OF SECURITY



Figure 6.

We envisage ten kinds of problems that may compromise access or prevent a database or its software from behaving in the expected manner ([Table 1](#); [Fig. 6](#)). We shall consider these and some possible solutions more-or-less in the order of the ease with which they may be addressed and solved ([Fig. 7](#)).

What we regard as the most likely possible solutions to the ten categories of problems are ranked in the matrix of [Figure 8](#) as essential, prudent, or useful. [Figure 9](#) further categorizes security problems into assaults from the outside, people problems, and problems that are beyond one's direct control.



Figure 7.

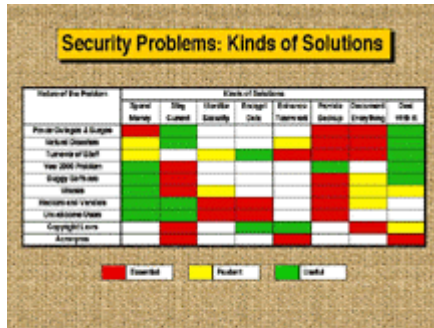


Figure 8.

Power Outages and Surges

As nearly everyone has learned from bitter experience, when the electricity goes off, your computer is likely to lose any documents with which you are working at the time. A more serious problem may occur as a result of a power surge and especially a lightning strike. [Cobb \(1998a\)](#) has estimated that power surges and lightning are responsible for more loss of data than any other cause except theft. In paleontology, therefore, where theft is not yet a major concern, it seems likely that

power surges are the major factor in the loss of data.

Any such power outage or surge can result not only in the loss of data, however, but also in the corruption of data and software, the misconfiguration of files, or the frying of logic boards. Such corruption or misconfiguration may go undetected until a later computation produces some sort of unintelligible gibberish or otherwise obviously erroneous result. Any problems of this sort are expensive and time consuming to correct.

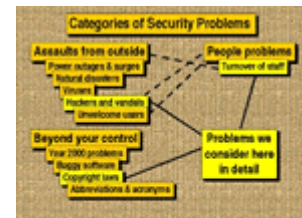


Figure 9.

What to Do? Solutions to the problems caused by power outages and surges are suggested in Figure 8. Most problems associated with both power outages and power surges can be averted by spending money and, fortunately, by spending only a modest sum. The destructive effects of power outages can be prevented by installing a device called a UPS (uninterruptible power source). A variety are available, ranging from units that provide fairly long-term battery power to those that provide power only for enough time to allow users to shut down the computer.

Problems from power surges can be averted as well, and some surge protectors also filter out electronic noise. As is true of uninterruptible power sources, many kinds of surge protectors are available. The most common of these is a simple strip of receptacles that shuts itself off in the event of a power surge. At the Paleontological Institute we use a different kind of surge protector, one that is alleged to be able to take a direct hit from lightning and actually to melt before it lets a power surge through to the computer. We hope never to test its full capabilities. It is important to remember that lightning strikes can send power surges through telephone lines as well as power lines. Therefore, protection for modems should be considered as well when purchasing a UPS.

In addition to uninterruptible power sources and surge protectors, an essential means of protecting databases from such electrical instability is to back up everything thoroughly and often. For example, at the Paleontological Institute we back up daily the changes we have entered into our computers, and once a week we make backups of everything

on our hard drives. Software is available that operates in the background to provide this sort of backup routinely and efficiently.

The worst-case instance of unstable electrical power is one in which the database management system is destroyed—including files of data and all the code that allows operation of the database. Proper backup will enable you to reconstruct things, but there is no substitute for proper, thorough documentation of the system in the event that the backup system fails. Preparing proper documentation is very time consuming and, hence, expensive. It is guaranteed to slow progress in the development of a database, but one has to believe that in the long run such attention to detail will be of great benefit to the project.

A useful course of action in anticipation of unstable electrical power is to stay current. New kinds of hardware that provide protection are devised regularly, and one should stay abreast of these developments. Nevertheless, you can be sure that both power outages and power surges will occur, and you should make every effort to be so well prepared for them that when they come you are able to take them in stride.

Natural Disasters

The cable television Weather Channel reminds us daily of the devastation that can be wrought by natural disasters. It reports tornadoes, hurricanes, and, for some reason, even earthquakes. In addition, one is always faced by the danger of fires, both local and regional; and although the threat of a nuclear holocaust, a most unnatural kind of disaster, may have subsided somewhat in recent years, the possibilities of an attack by terrorists or the failure of a nuclear power plant remain—both with horrendous implications for electronic data. Most recently, the impact of cosmic rays on storage media has been recognized as a rare but distinct and largely unavoidable threat to the integrity of data.

What to Do? To prepare for natural disasters, two courses of action are essential: implement backup procedures and document everything. In addition to the backup of systems that we described above, we keep copies of all electronic files and paper copies of all documentation of PaleoBank in a fire-retardant, waterproof safe. We also store a second copy away from the Paleontological Institute at my home, which is about three miles away. We judge that anything in the safe will survive a tornado, if we can find the safe afterward. Moreover, if a disaster were to strike Kansas of such magnitude as to destroy both the Paleontological Institute's building and my home, all of us would probably be thinking about a lot of things other than paleontological data.

A prudent course of action in anticipation of a natural disaster is to foster a team spirit among colleagues. Each person should know his responsibility, which may range from being the one to close the safe at the end of each workday to being the person whom emergency-management personnel should contact.

A modest expenditure may be required to be prepared for a natural disaster, including the purchase of fireproof safes, CD-ROM writers for backup, and other means of

providing electronic backup. In addition, if one is committed fully to proper documentation, one has to accept the resultant slower pace of progress.

Project managers should conduct periodic training exercises and foster a spirit of awareness to keep staff members up to date. Above all, as discussed above under the power outages and surges topic, one needs to play the pessimist. Assume that natural disasters will occur, and be ready for them.

Staff Turnover

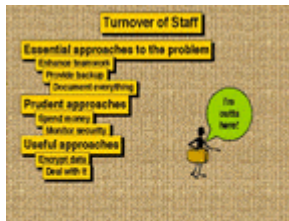


Figure 10.

Few episodes are more threatening to the security of a database than staff turnover (Fig. 10). Turnover results from a number of causes including the firing of an incompetent employee, normal attrition due to retirement, relocation of other family members of the employee, the employee's quitting to take a higher-paying position, and interpersonal conflicts. In the university environment, a computer-literate employee's quitting to take a higher-paying position in the private sector is a problem of epidemic proportions and can leave development of a database high and dry with very

short notice. When the employee leaves as a result of interpersonal conflicts, an added hazard exists because a disgruntled employee can administer electronically a great deal of damage in a very short time. In the long term, moreover, the actions of such an employee can be detrimental if he programs a means of entry—the jargon is *back door*—that bypasses security measures and allows later access to vital records in the database.

What to Do? The first line of defense against problems that may result from turnover of staff is to enhance teamwork. Although making all staff members feel that they are vital members of a team will not help much if employees have a chance to double their salaries elsewhere, it will go a long way toward defusing problems that may arise from having a disgruntled employee. Nevertheless, the problem with personnel management is that it involves people, and no matter how much attention is paid to team building, anyone who has first-hand experience as a project manager knows that interpersonal relationships can sometimes disintegrate almost overnight.

In this regard, other essential activities that we have discussed previously are to provide in-depth backup of all files and to document everything. Make certain that the departing employee is debriefed and, above all, leaves behind copies of all documentation.

Although spending money to retain key staff members and avert problems is prudent, in many instances it is not as easy as it sounds, even in the unlikely event that you have the money to spend. Salaries in governmental agencies are likely to be specified by a predetermined salary scale. In any event, in the university environment expenditure of funds to begin anew is likely to be easier than to raise salaries to retain good employees. Spending money is not limited to raising salaries, of course. Providing a

pleasant working environment and state-of-the-art equipment goes a long way toward keeping good employees contented and on the job.

When faced with staff turnover, it is prudent to initiate security measures that restrict access to valid users and to monitor routinely the effectiveness of the security measures. We discuss below the security issues that pertain to unwelcome users. When employees leave, one must make sure that their access to the database is terminated with their employment.

In fields where unauthorized access is likely to have profound economic or military implications, the computer security personnel rely on data encryption of data and on elaborate means to authenticate users including passwords, tokens, and such various biometrics as finger imaging, facial recognition, speech identification, retinal scanning, hand geometry, and signature recognition ([Tilton 1998](#)). We deal with encryption in a later section because, although it might be a useful approach when faced with the turnover of staff, it is somewhat peripheral to the present issue. Tokens, such as electronic ID cards, are a widely used means of security—one sees them in hospitals, airports, and computer centers—but they can be lost or stolen, and their use somehow does not seem to be very academic or collegial.

We have difficulty envisaging a time when the users of a taxonomic paleontological database will be authenticated by the use of biometrics. Can you imagine asking your graduate students to submit to a retinal scan before they can access information about crinoid stems on your database? [Tilton \(1998, p. 40\)](#) has discussed the use of biometrics, the most common of which is finger-image authentication, and listed the four steps in the authentication process:

1. Capture an image of the user's fingertip with a scanner.
2. Digitize the image and evaluate it for quality.
3. Calculate a finger-image identifier by mapping the minutiae—the points where individual ridges in the friction-ridge pattern bifurcate . . . or end.
4. PPerform an enrollment or verification.

Automated face recognition is one of the best means of authentication. The TrueFace system from Miros uses neural-network technology to distinguish a face even when the appearance is different, due, for example, to wearing or not wearing glasses and to changing hair styles. We paleontologists do not yet have funds to emplace such elaborate systems as these to identify our fossils, let alone use them to identify our graduate students and other colleagues who might seek access to our databases.

For this reason, in the foreseeable future, access to paleontological databases is likely to be determined by one's having a valid password—or, if data are as valuable as we have suggested, by having a valid credit card. Passwords are convenient, but can be compromised in a number of ways. Software for hacking is available on the Internet that

will electronically test the contents of dictionaries as possible passwords until a word is found that will allow ingress. To forestall this sort of behavior, one should, at the very least, insert a nonalphanumeric character into the middle of a password. The operating system can be programmed to prevent users from logging onto the system without the proper password. Each application program can also be designed to check for passwords, thereby providing access to a specific database or fields within a database, while restricting access to other information in the computer. Keep the list of passwords in a fire-retardant safe, not in the computer, and make sure that the validity of the password of a departing employee is terminated.

Turnover of staff is reality. We think of the small staff of the Paleontological Institute as being quite stable, yet in the past ten years we have had three members of the professional staff depart, each of whom had full access to our computer systems and databases. Every manager of a database project should expect turnover of staff and be prepared for its possible consequences.

The Year-2000 (Y2K) Problem

The Y2K problem is a vestige of the 1960s, a time when programmers in the business world used COBOL, all information had to fit into the 80 columns of a keypunched card, and 19 went without saying when talking about the date. Of course it was 1967 and not 1867 or 1767. [Grossman \(1998, p. 48\)](#) has put the Y2K problem neatly into perspective, pointing out that opinion about it ranges from its being a fraud, to being something that can be fixed in a long weekend, to engendering TEOTWAWKI (that is, **the end of the world as we know it**).

Systematic paleontology's concern with the history of names has saved the day for us. No paleontologist would think of restricting reference to years to two digits when 58 could refer to [Linnaeus \(1758\)](#), [Wallace \(1858\)](#), or any of a host of more recent taxonomic literature. This means that our principal concern is to make sure that the operating systems in our computers and the software packages we use have addressed the Y2K problem.

What to Do? Solving or avoiding altogether the Y2K problem may be straightforward for paleontologists, but nevertheless it is essential that managers of databases stay current. The closer we get to January 1, 2000, the greater will be the hubbub about the problem in general. Some of what is said is likely to apply to your operating system, your software, and your database.

Useful courses of action will be to spend money to purchase updated software that addresses specifically the Y2K problem. If by mid-1999 it appears that the new millennium will present more problems than we anticipate, routinely backing up all your files will become even more important. Above all, recognize that the year 2000 is coming. Stay flexible and informed in order to deal with problems that may arise.

Buggy Software

Software with bugs can certainly prevent a computer's operating in the manner we expect. A former student, who now works as a project manager for a major producer of computer software, recently told me that he worries that computer software has become so complicated that it is sometimes almost impossible for an individual user to cope. He speculated that if the growth of complexity continues, personal computers will become significantly less personal, requiring frequent servicing by paraprofessionals. Compare some of the early versions of point, click, and drag software for the Apple Macintosh to the present versions that provide dictionaries in seven or eight languages, can be made to check grammar and spelling as you write, and perhaps as a consequence trigger systems errors with disconcerting frequency.

Software is written by people, so one must expect software to have bugs. As everything about computers becomes more complex, bugs in software and other quirks that cause incompatibilities between software packages will become increasingly common and harder to detect. Version 8.0.1 of the Macintosh operating system (OS) had been available for only a few months when software vendors received advanced versions of OS 8.5, so they could reprogram their wares, and OS 10 is racing toward us at breakneck speed. Vendors scarcely have time to update one version of their software for compatibility before another is demanded.

What to Do? One must stay current and, as always, provide backup of all files. The consequences of not staying current can be catastrophic. One of us recently inflicted severe damage on some files in his computer, presumably by using an old version of virus-detection software. The version, it turned out, was not compatible with Mac OS 8.0.1. Software vendors eliminate bugs when they find them. Moreover, many software companies issue service packs to correct bugs. You should be sure to obtain and install them. If you do not install the latest available version of the software that you use, you can scarcely expect to take advantage of the vendors' efforts to eliminate bugs.

As we have stressed repeatedly, if you are preparing code for your database, be sure to document every step you take. Doing so will slow your progress now, but it provides the means of avoiding catastrophic failure at a later date by enabling you to trace incompatibilities and other subtle bugs within the software package you are using.

Staying current by providing staff members with the latest, most recently debugged software costs money. Managers of database projects need simply to recognize that bugs will occur and to deal with the problem by budgeting funds to buy their way out of trouble.

Viruses

What gets into these people who devise computer viruses? In antiquity these sorts of people knocked the heads off marble statues. More recently they have tipped over tombstones on Halloween. Now they develop and distribute computer viruses—equally mischievous but potentially far more costly. In the not-too-distant past, the world of

Macintosh users was comparatively free of viruses, whereas PC users faced a plethora of viruses of all degrees of destructiveness. More recently, viruses have become more ecumenical, infecting any kind of computer that comes along. [Cobb \(1998b, p. 28\)](#) has estimated that some 12,000 viruses are known and 200 to 300 new viruses appear each month, some of which are polymorphic and change their appearance with each infection. That is the equivalent of a lot of heads off a lot of statues. The recent ado concerning infection by viruses transmitted as a part of an e-mail message has subsided, but the danger has not ([Levy 1998](#)). Providers of Internet and electronic mail software are scurrying to fix the problems their earlier, equally hasty programming has engendered.

What to Do? Staying current and, of course, providing backup of all files are essential activities to combat viruses. Vendors who provide software to inoculate computers against viruses update their products regularly, and some offer updates on the Internet. [Cobb \(1998a, p. 12\)](#) listed five types of antiviral software: "scanner, integrity checker, behavior blocker, heuristic analysis, and access control—each with a different approach to the problem of identifying and removing viruses." Refer also to [Cobb's \(1998b\)](#) paper for a description of the most popular antiviral software packages, their capabilities, and how they work. [Cobb \(1998b\)](#) also provided guidance for the use of the EICAR test file ([European Institute of Computer Anti-Virus Research](#)) to ascertain if antiviral software is properly installed and how it functions when it encounters a virus.

Monitoring security is a prudent course of action. Here the monitoring entails ascertaining that all members of the staff are aware of the problems that viruses can cause and are using current antiviral software. Make sure programmers document every step they take and, above all, recognize that the virus-designing mentality dates to antiquity and is apparently here to stay. Invest enough funding to make sure you and your database are protected from viruses.

Hackers and Vandals

As we have pointed out previously, most of the literature about security of computer systems, the Internet and local intranets, and electronic databases deals with controlling access by unauthorized users, an aspect of security that is the principal concern of industrial, financial, and military agencies.

We prefer to divide unauthorized users into three categories that we consider separately: disgruntled and vengeful former employees (above), hackers and vandals, and nondestructive data thieves. Means of coping with unauthorized users are dealt with in a fast-growing, short-lived literature scattered in trade journals; the popular, periodical literature, and thick, quickly prepared, jargon-laden books. All the pertinent literature is dated 1998, and in six months much of it will be obsolete. The best a paleontologist-manager can hope for is, first, to convince himself that he needs to exclude unauthorized users of his system and, second, to rely on specialists. Most university computer centers have at least one security guru on staff; private companies that do not have security officers court disaster. [Note: The relevant terms are Chief

Information Officer (CIO), or Computer Security Officer (CSO).] Four convenient ways in which paleontologists can begin to understand the problems that unauthorized users cause in industry and government are by referring to [Linda McCarthy's \(1998\)](#) book of true, breach-of-security anecdotes and her solutions to them, [Carolyn Meinel's \(1998a\)](#) book **The Happy Hacker**, articles in the October 1998 issue of **Scientific American** ([Cheswick and Bellovin 1998](#), [Ford 1998](#), [Gosling 1998](#), [Meinel 1998b](#), [Rivest 1998](#), and [Zimmermann 1998](#)), and the pages of **Security Advisor** magazine.

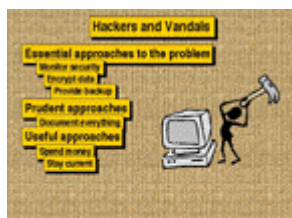


Figure 11.

Hackers and vandals include unauthorized users who cause problems, either inadvertently or maliciously ([Fig. 11](#)). Some of the problems they cause include revealing confidential information, destroying data files or altering the information in them, and sabotaging research. Hackers can be malicious outsiders or even members of your own organization who access files without proper authorization. In the university setting, this category of unauthorized user includes immature mischief makers and students who change their grades electronically or who cheat by

gaining access to tests.

Although precautions can be taken to detect an unauthorized user, determining if a valid user is performing unauthorized tasks is much more difficult. Effective security measures involve a balance of technology and personnel management.

What to Do? If faced with the potential of attack by hackers and vandals—that is, if any of your computers are connected to the Internet—you should, of course, back-up every file and monitor security carefully and routinely. (See also the section above on turnover of staff.) At the very least you should initiate a system of passwords to restrict access to authorized users. We have difficulty imagining the day when paleontologists will employ biometric devices to restrict access, but stranger things have happened in the unfolding information age.

One of the most basic Internet security measures is the use of a firewall, software that recognizes and excludes unauthorized users. More elaborate procedures involve the use of software that routes hackers to an electronic limbo or software that detects and warns against multiple attempts to gain entrance by using computer-generated guessing of passwords. Most elaborate of all is use of retaliatory software that transmits vast files of nonsense to the hacker, thereby overloading his system and causing it to lock. Software is also available that assesses security, detects intrusions, and identifies and reports weaknesses in the system (e.g., [Internet Security Systems](#)).

As we have mentioned previously, we cannot envisage the day when paleontological data will be encrypted, but pressure on the government to deregulate encryption technology suggests that elaborate methods of high-tech encryption are likely to be readily available in the near future. Of course, similarly elaborate decryption software

will follow on its heels in a never-ending escalation of the computer cold war.

A prudent course of action is to require programmers and those who enter data to document everything they do. It is useful to spend enough money to enable you to implement the latest security measures. To know what those latest measures are, one must stay abreast of the latest developments.

Unwelcome Users

For want of a better term, we refer to unauthorized users, who access files but do not damage them or publicize their contents, simply as unwelcome users. The greatest concern in general is the theft of data. It is inconceivable that one professional paleontologist would steal the data of another, but similar theft of data has taken place in other fields of science where the pressure to receive awards and large research grants is greater than in paleontology. At present, being aware of the possibility of theft is the best course of action. Perhaps of greater concern is the potential for theft of illustrations of fossils, but even this seems to be a distant threat given the present climate in paleontology.

What to Do? An essential step to avert this kind of problem is to monitor security and implement the use of passwords as discussed earlier. One could encrypt data, and the extent to which this kind of procedure will be employed will depend on the development of inexpensive, easy-to-use encryption and decryption software. As always, backing up files is essential because the data thief may inadvertently damage files. Finally, it is useful to stay current and to budget enough money to keep security measures up to date.

Copyright Laws

Copyright laws are expected to change dramatically as lawmakers attempt to accommodate the existing body of law to the digital age ([Washington Post 1998](#)). Indeed, changes are already afoot, and no one can be certain what will emerge from the current international deliberations [[Association of Research Libraries \(ARL\) 1998](#)]. The [ARL \(1998\)](#) has summarized the role of one of the bills that has been proposed, H.R. 2652: ". . . rather than protecting the creative organization or selection of the information, as copyright law does, this new right would, in effect, allow control of the facts themselves." They quoted Adam Eisgrau of the American Library Association, who described the proposed legislation: "This would put simple facts under potential lock and key for the first time in our history. This 'sea change' in American intellectual property law will have been made despite the principled opposition of a 'Who's Who' in the public and private sectors and without benefit of a single minute of formal scrutiny by the Senate."

[Gardner and Rosenbaum \(1998, p. 786\)](#) have described the difficult straits through which the proposed legislation must navigate, faced on the one hand with the Scylla of protecting information and, on the other, with the Charybdis of restricting the flow of information. From the point of view of the academic paleontologist, the situation is

especially fraught with perplexing difficulties. The proposed legislation provides penalties for harming, either actually or potentially, the market for goods or services. Not-for-profit educational and scientific institutions, however, are to be exempted from liability so long as they do not harm marketability. This exemption seems to imply, in effect, that a paleontologist who has prepared a database that is not to be marketed has no protection under the law from raiders so long as they are associated with a not-for-profit institution.

A complex issue related to copyright with which we shall not deal in detail is the matter of ownership. In many instances, programming of a database management system is a drawn-out process that involves a number of staff members over an appreciable period of time. Sometimes the programmers have used code developed elsewhere, and in the past they have typically not signed an invention agreement that clearly assigns title to the code to the employer. Most universities have begun to address the question of ownership of intellectual property in all its aspects, but if your organization has not done so, you should consult a copyright and patent attorney for clarification of the issues involved.

What to Do? Faced with the uncertainty in copyright law, one must, above all, stay current, perhaps by referring to the ARL web page ([Fig. 12](#)). In addition it is essential to document every activity to provide a paper trail of attempts to obey the copyright laws. The key words for academic institutions seem to be **good-faith effort**. If you have inadvertently disobeyed a law pertaining to copyright but are seen as having made a good-faith effort to do the right thing, you are unlikely to be penalized severely in the courts. This is especially true if the economic impact of your error is small. A cavalier attitude toward such things, however, can cost you dearly.



Figure 12.

One needs to be ready to deal with copyright law because one aspect of this situation is certain: as the information age unfolds, copyright law is going to become increasingly complex. If you are concerned that your own copyrighted material will be pirated, encrypt it. Otherwise, you can help alleviate problems by encouraging your team of staff members to think about copyright laws routinely.

The U. S. Congress has apparently decided to postpone for a year any ruling about copyrighting databases. Perhaps the passage of time will allow legal wording that protects ownership of ideas while not allowing the copyrighting of such facts as the geological time scale or that **Olenellus** is a Cambrian trilobite.

Abbreviations, Acronyms, and Jargon

Use of such acronyms as **SNAFU**; such abbreviations as **GSA, NSF, and ROM**; and such jargon as **firewall, Trojan horse, and sandboxed environment** are not actually matters of security. That is, they do not pertain to the operation and functioning of

computer systems and certainly not to a taxonomic paleontological database. Nevertheless, the use of such terms impedes communications in the same ways as our paleontological use of infraradial, gongylodont, and avicularium. As readers encounter unfamiliar terms when delving for the first time into the literature on security of computer systems, they will have difficulty understanding that literature, profiting from what it has to say, and applying it to ensure the security of his own database.

In our very first foray into the literature on security we were overwhelmed by the sheer number of abbreviations and acronyms and the welter of jargon: **NIS vulnerability, IT support desk, CM, Discretionary Access Controls, firewall, IRT, CIO, ISP, and POC**. Wading through this morass involved appreciable agony, and we spent an inordinate amount of time in the search for definitions.

What to Do? Coping with encrypted English of this sort will be facilitated by teamwork. If possible, enlist a fully computer-literate person who knows the meanings of these terms and is willing to teach them to others. A useful resource is the encyclopedia of terms located at [TechWeb, The Technology News Site](#). Once you have caught up with the jargon makers, stay current and add vocabulary as they invent it. Above all, resolve simply to deal with it. Jargon and encrypted English are unfortunately here to stay. We suspect that if their use were to cease tomorrow, the result would be, mercifully, TEOTWAWKI.

PUTTING SECURITY INTO PERSPECTIVE

Managing the security of any database must involve weighing matters of security against performance, productivity, and accessibility ([Fig. 13](#)).

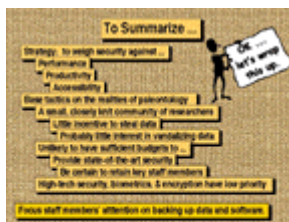


Figure 13.

Tactics to accomplish effective security must be based on the realities of paleontology. Specifically, we are a small, rather closely knit community of researchers. We have little incentive to steal each other's data, even less incentive to vandalize them, and a great deal of professional and social pressure weighing in against either sort of activity. On the other hand, paleontology is unlikely ever to have sufficient fiscal resources to provide state-of-the-art security or to pay key computer-related staff members sufficient salaries to ensure that we retain them. Finally, such high-tech

security means as biometrics and encryption are likely to retain their low priority among paleontologists, at least until security becomes much more of a problem than it is at present.

For the foreseeable future, the key to security of paleontological databases is likely to remain backup. One needs to develop protocols that ensure that data files and database management systems are frequently backed up. Copies of files should be stored off line so that they are electronically inaccessible. Furthermore, they should be

stored off site as a hedge against natural disasters.

ACKNOWLEDGMENTS

We are grateful to Bruce S. Lieberman and Jill Hardesty for evaluation of an earlier version of our manuscript. Our research was made possible by grants from the National Science Foundation to The University of Kansas (BSR-9024567 and DEB-9505100), a bridging-fund grant from The University of Kansas, the R. C. and Lillian B. Moore funds administered by the Kansas University Endowment Association, and the generous support of Russell M. Jeffords.

REFERENCES

- Association of Research Libraries (ARL). 1998. (<http://arl.cni.org/>).
- Cheswick, W., and Bellovin, S. M. Firewalls. **Scientific American**, October 1998:106-107.
- Clerck, C. A. 1758. **Aranei Svecici descriptionibus et figuris** Stockholm.
- Cobb, M. 1998a. Security solution. **Security Advisor**, Premiere 1998:12-14.
- Cobb, M. 1998b. What to look for in an enterprise anti-virus product. **Security Advisor**, Premiere 1998:28-33.
- Ford, W. 1998. Digital certificates. **Scientific American**, October 1998:108.
- Gardner, W., and Rosenbaum, J. 1998. Intellectual property. Database protection and access to information. **Science** 281:786-787.
- Garfinkel, S., and Spafford, G. 1996. **Practical UNIX & Internet Security** (second edition). O'Reilly & Associates, Inc., Sebastopol, California.
- Gosling, J. 1998. The Java sandbox. **Scientific American**, October 1998:109.
- Grossman, W. M. 1998. Cyber View. Y2K: the end of the world as we know it. **Scientific American**, October 1998:48.
- Hartley, B. V. 1998. Get your network ready for e-business. **Security Advisor**, Premiere 1998:16-18.
- Levy, S. 1998. Living with the bugs. **Newsweek**, August 17, 1998:68.
- Linnaeus, C. 1758. **Systemae naturae per regna tria naturae, secundum classes, ordines, genera, species cum characteribus, differentiis, synonymis, locis, Editio decima, reformatra, Tomus I** (tenth edition). Laurentii Salvii, Holmiae.
- McCarthy, L. 1998. **Intranet Security: Stories from the Trenches**. Sun Microsystems Press, Prentice Hall, Mountain View, California.
- Meinel, C. P. 1998a. **The Happy Hacker: A Guide to (Mostly) Harmless Computer Hacking**. American Eagle Publications, Show Low, Arizona.
- Meinel, C. P. 1998b. How hackers break in ... and how they are caught. **Scientific American**, October 1998:98-105.
- Mish, F. C. 1995. **Merriam-Webster's Collegiate Dictionary** (tenth edition). Merriam-Webster, Incorporated, Springfield, Massachusetts.
- Rivest, R. L. 1998. The case against regulating encryption technology. **Scientific**

American, October 1998:116-117.

TechEncyclopedia. <http://www.techweb.com/>.

Tilton, C. 1998. Put a finger on your security. **Security Advisor**, Premiere 1998:40-43.

Wallace, A. R. 1858. On the tendency of varieties to depart indefinitely from the original type. **Journal and Proceedings of the Linnaean Society (Zoology)** 3:53-62.

Washington Post. 1998. October 5, 1998:A20.

Zimmermann, P. R. 1998. Cryptography on the Internet. **Scientific American**, October 1998:110-115.

Figure 1. Reasons to consider security of paleontological databases.

Why Consider Security in Paleontology?

Three reasons ...

1. Data have value—even paleontological data.
Anything of value is subject to ...
 - Theft
 - Misuse
 - Vandalism
2. Paleontologists have the right to first use of their data.
Especially in taxonomy they have a concomitant responsibility to share their data.
Aside: some thoughts about *putting it all out on the web*.
3. In many respects, sharing of data and security of data are incompatible concepts.

Figure 2. Goals of this study.

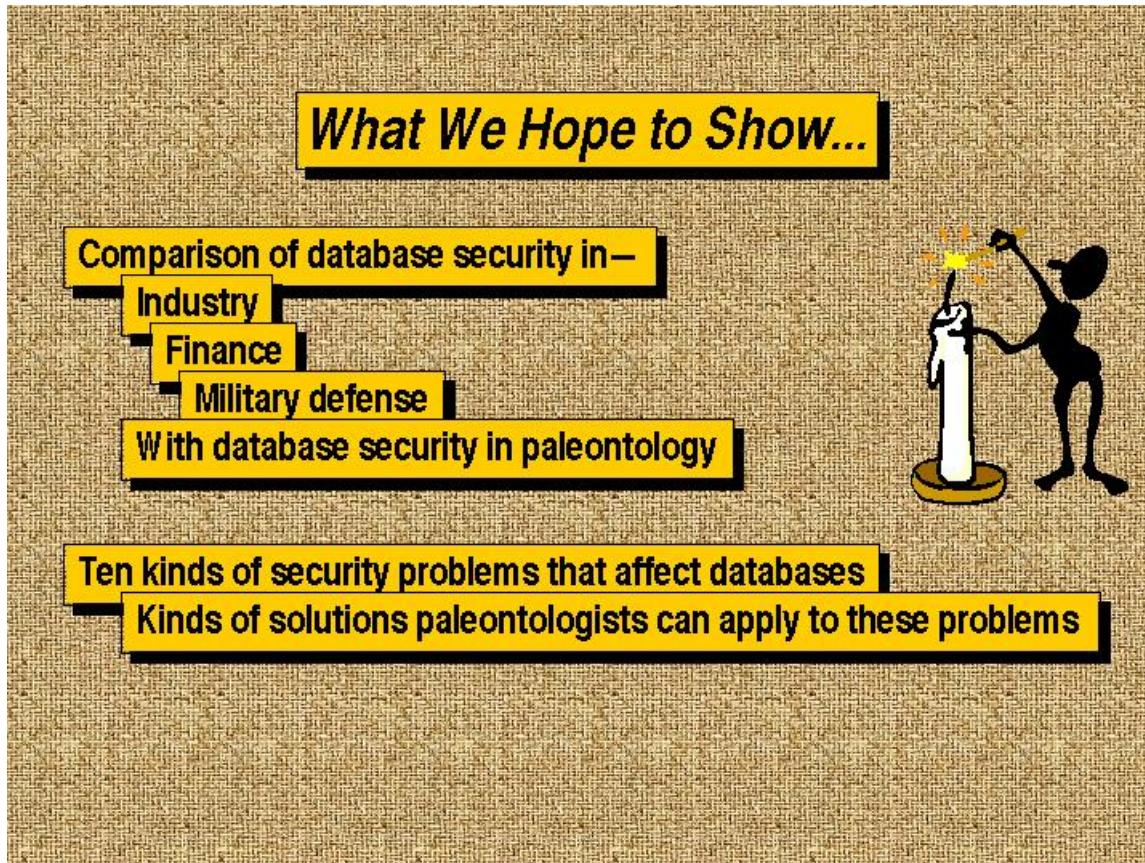


Figure 3. The essence of the security problem: to weigh concerns about security against requirements for performance, productivity, and accessibility.

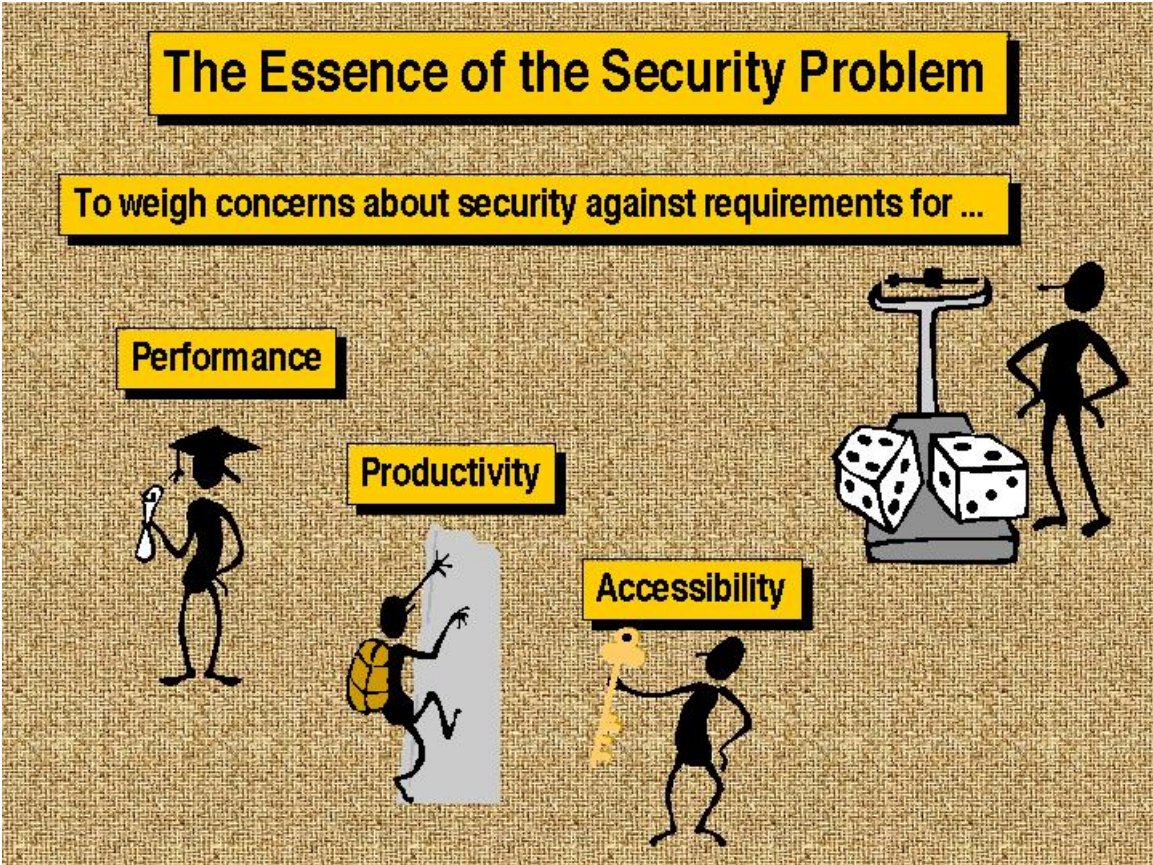


Figure 4. Some costs of inadequate security of databases.

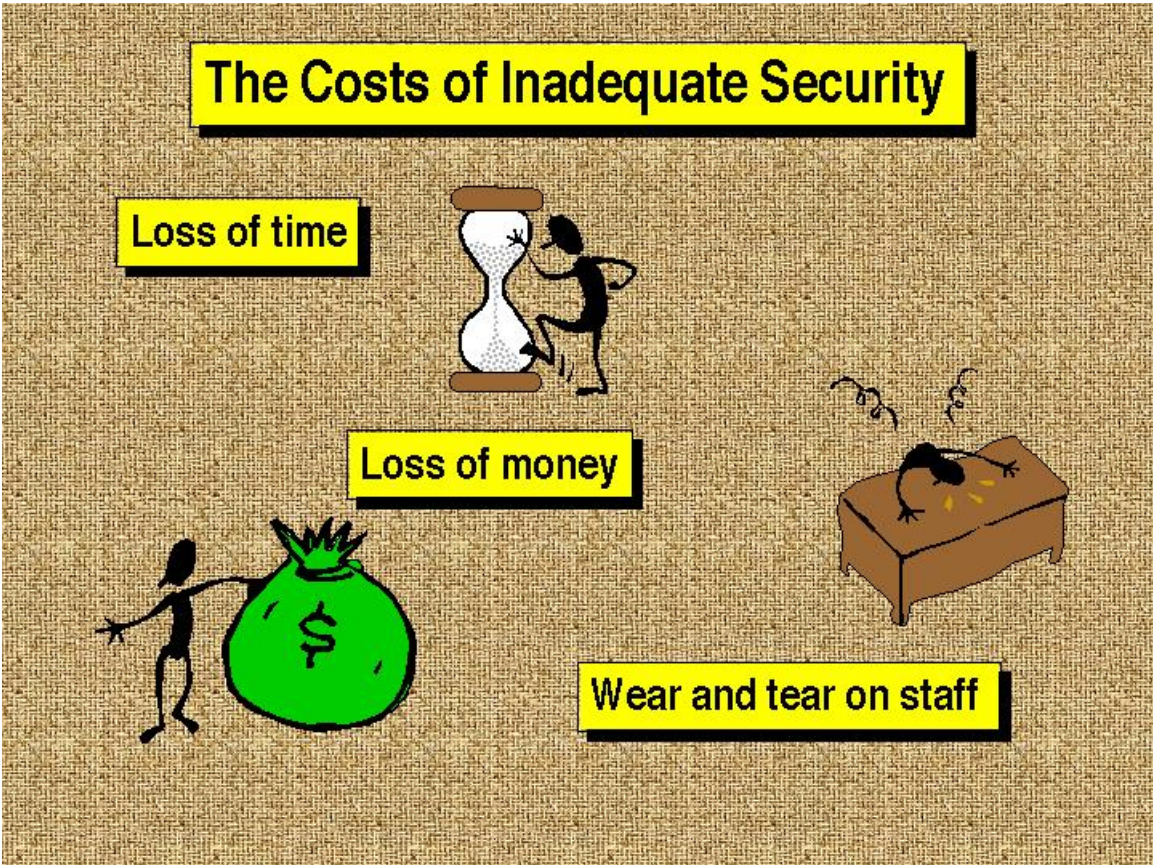
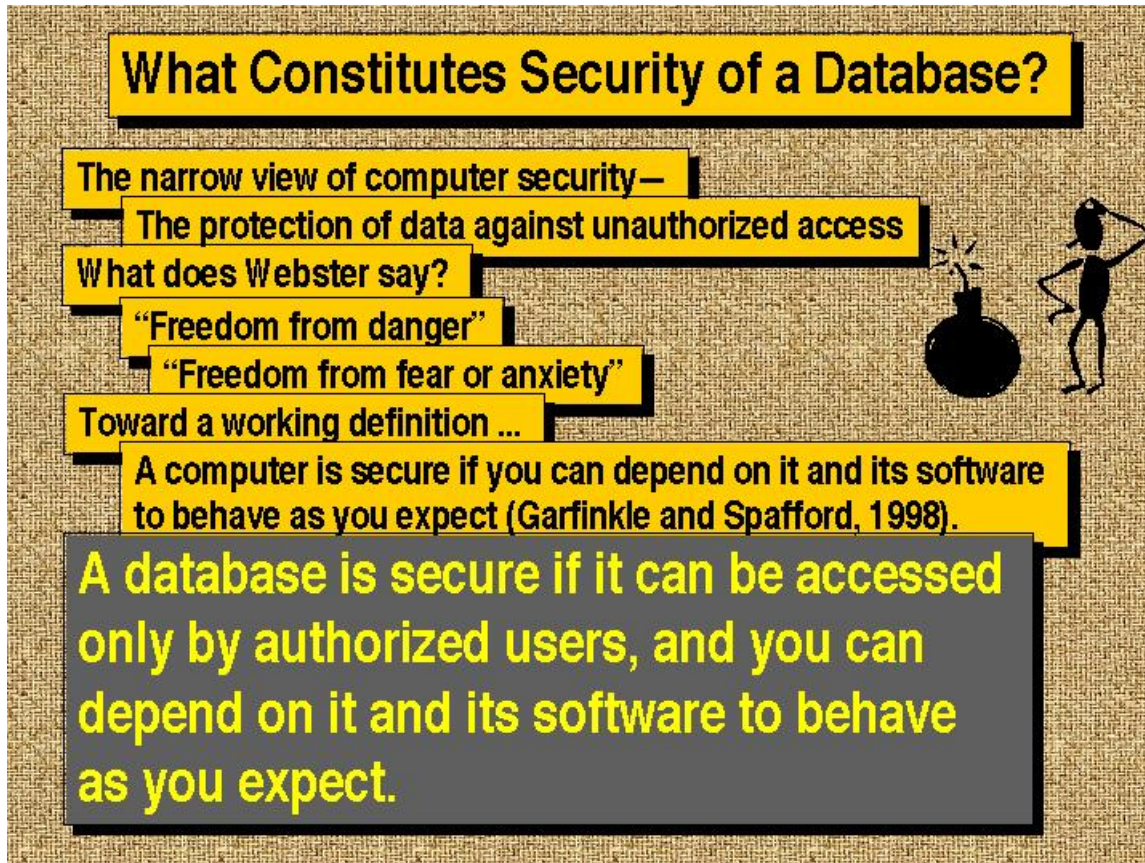


Figure 5. Definitions of the security of databases.



What Constitutes Security of a Database?

The narrow view of computer security –

The protection of data against unauthorized access

What does Webster say?

“Freedom from danger”

“Freedom from fear or anxiety”

Toward a working definition ...

A computer is secure if you can depend on it and its software to behave as you expect (Garfinkle and Spafford, 1998).

A database is secure if it can be accessed only by authorized users, and you can depend on it and its software to behave as you expect.

The slide features a cartoon illustration of a stick figure looking at a bomb with a lit fuse.

Figure 6. Ten security problems, some of which apply directly to paleontological databases and some of which are not yet a problem for paleontologists.

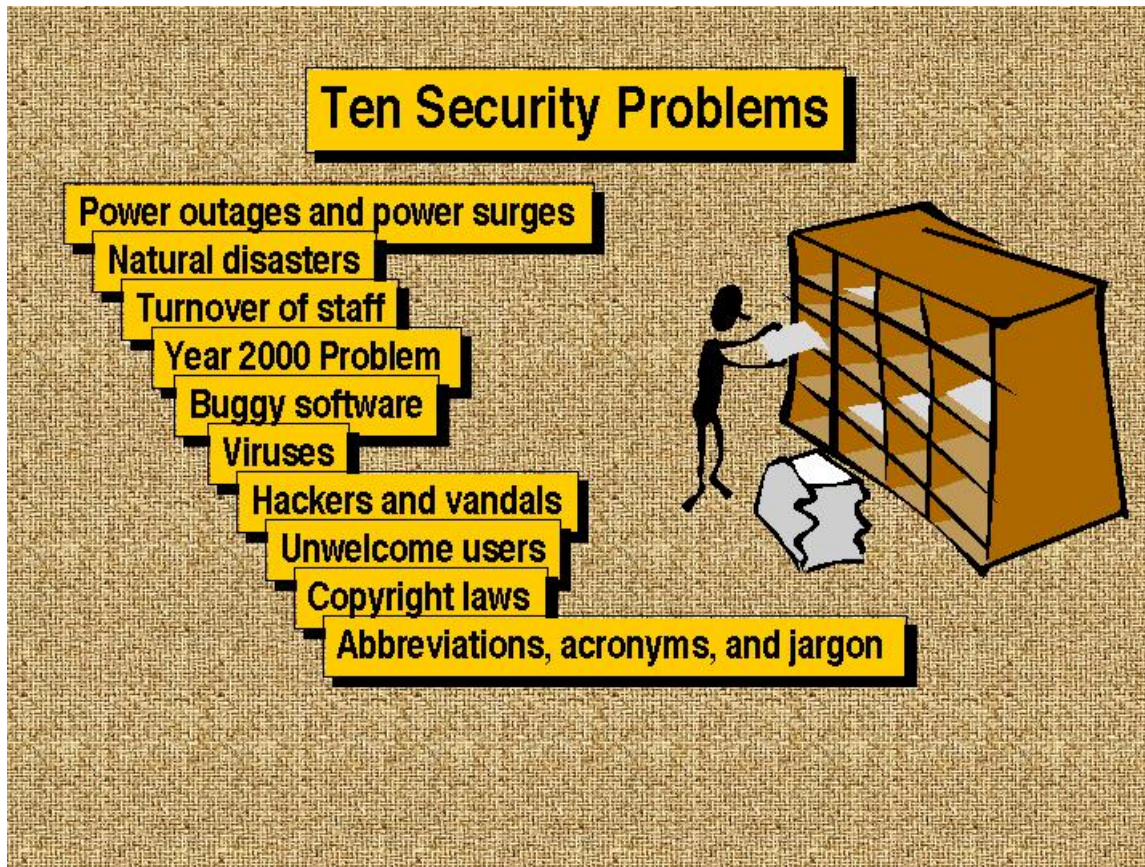


Figure 7. Eight categories of solutions to security problems with databases.

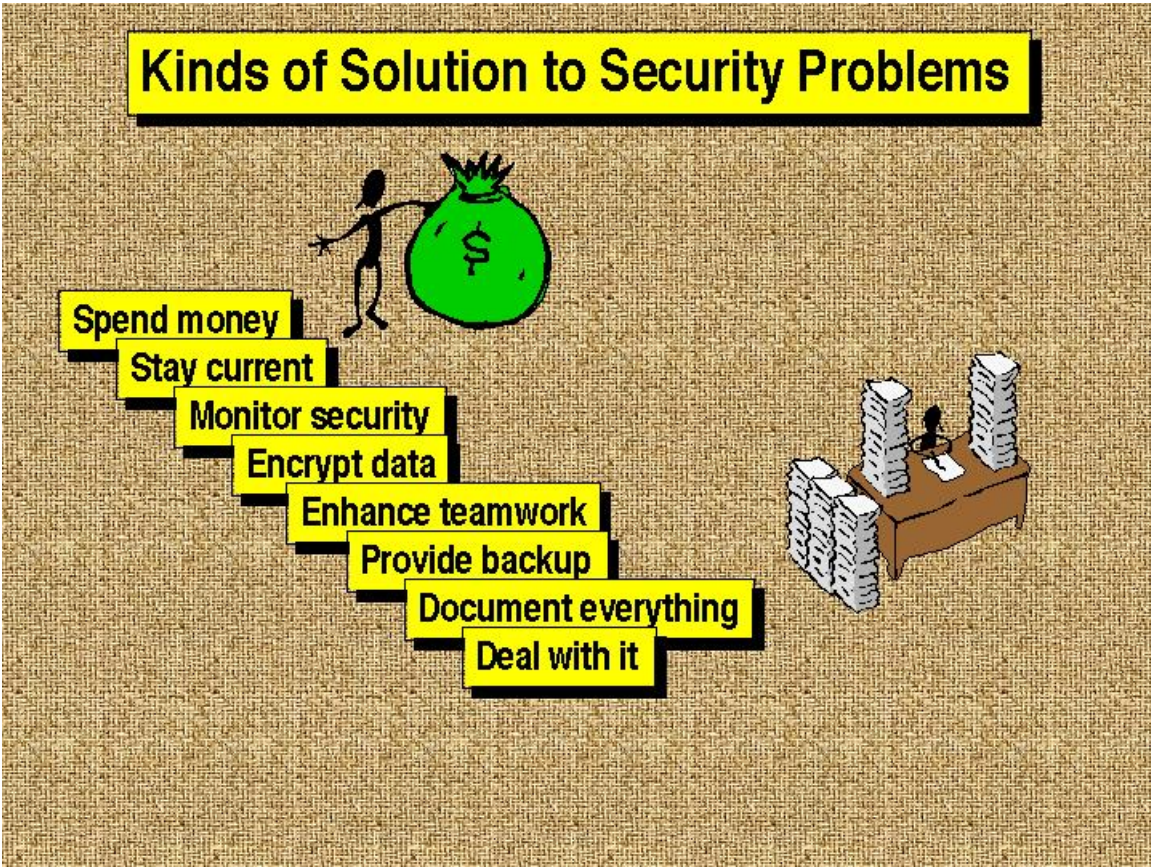


Figure 8. A matrix showing the degree of importance of the eight kinds of solutions (Fig. 8) to the ten problems (Fig. 7).

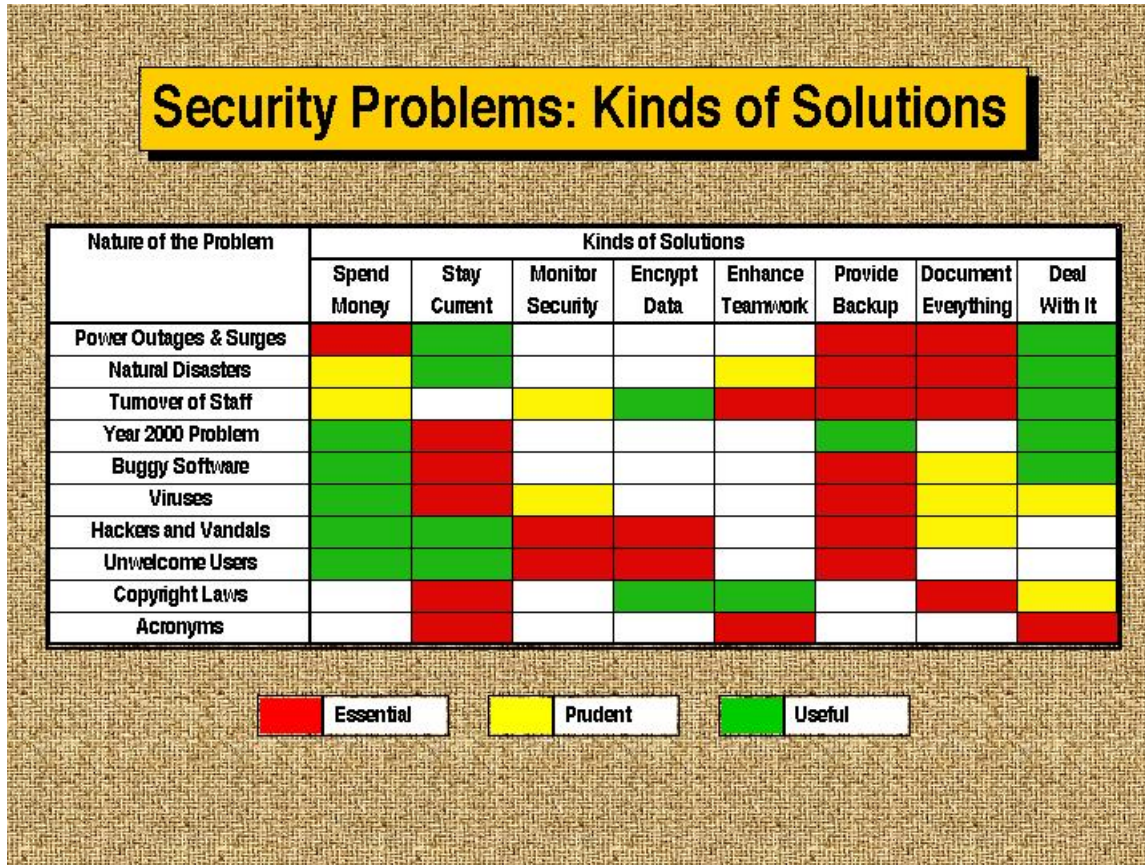


Figure 9. Three categories into which security problems may be considered showing three examples that are dealt with in Figures 10, 11, and 12.

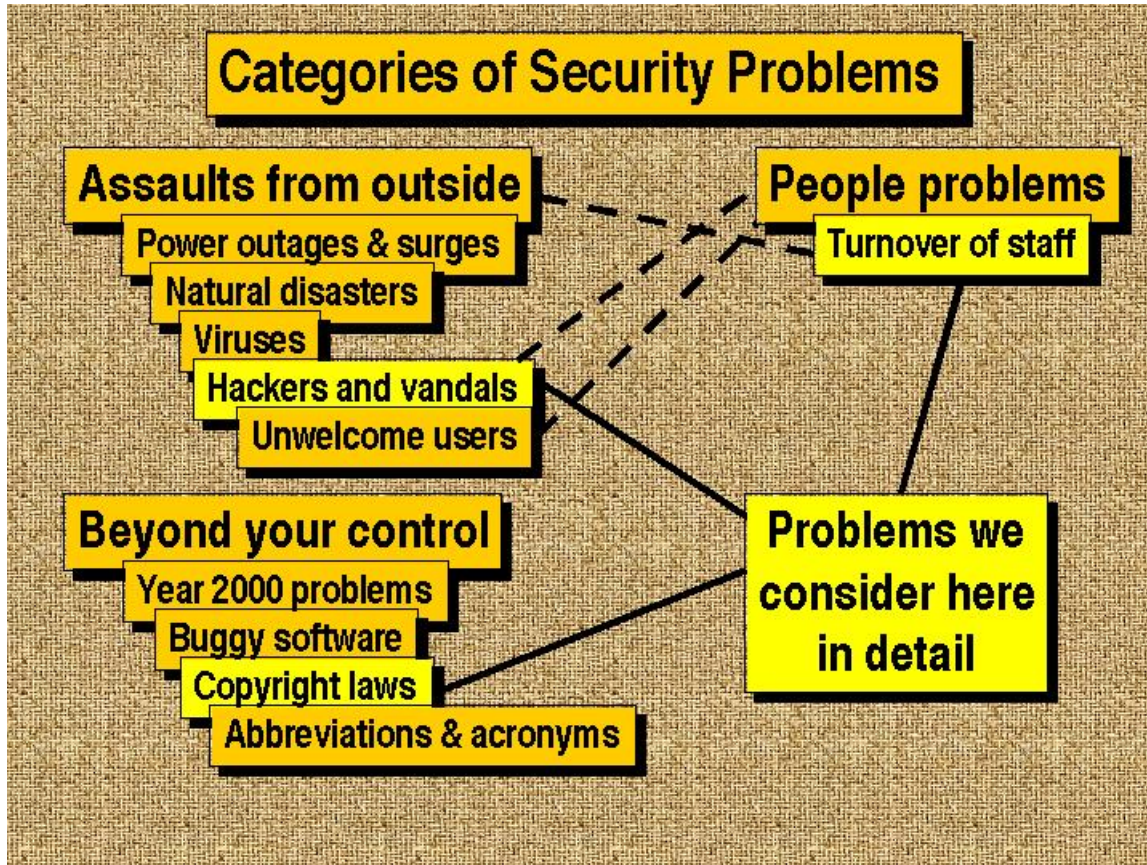


Figure 10. The broad nature of security problems that result from the turnover of staff members.

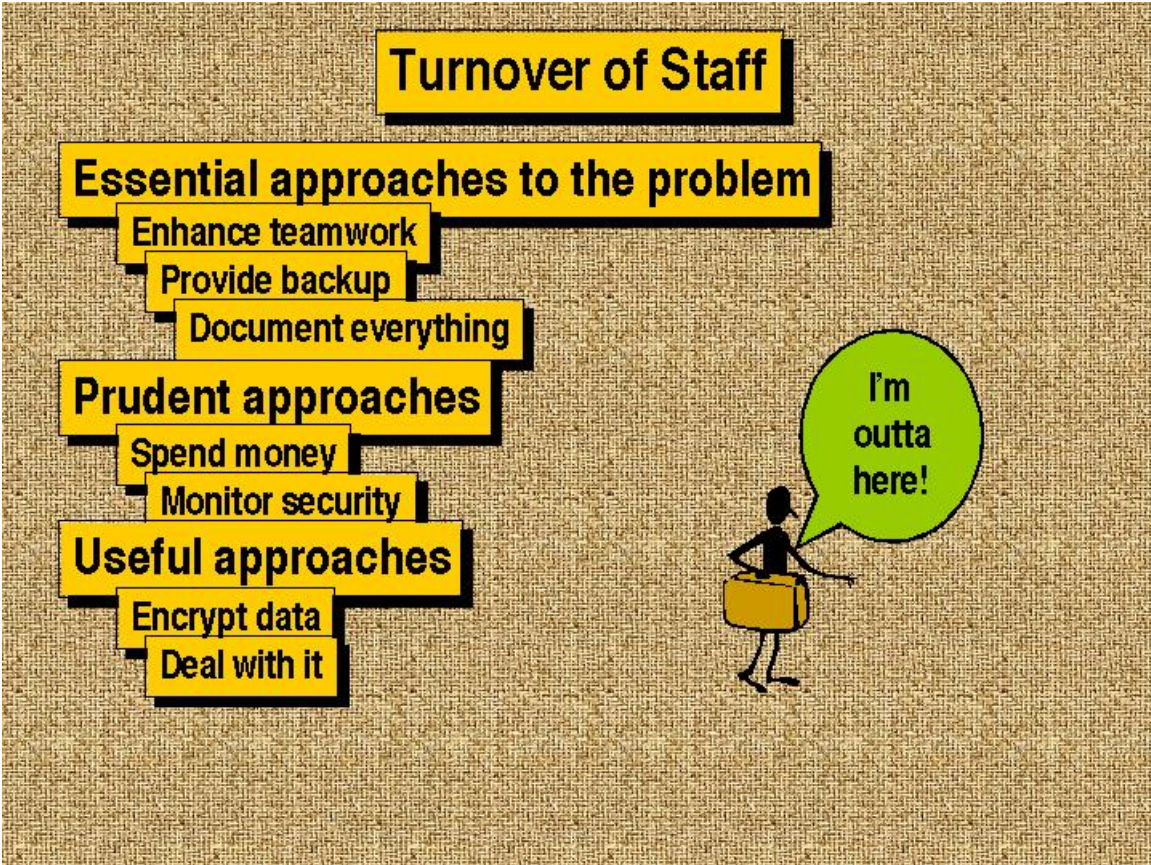


Figure 11. Hackers and vandals are a source of security problems that have not yet become a problem for paleontology, but this favorable situation could change at any time.

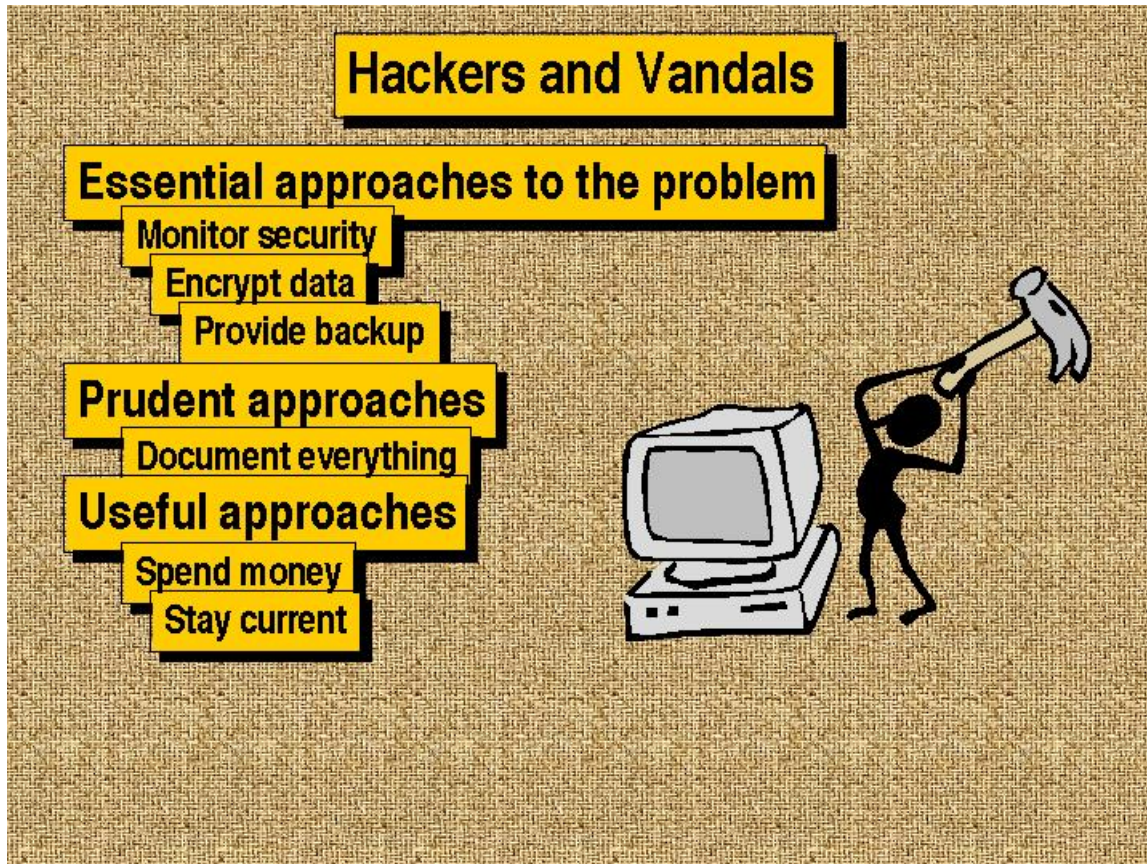


Figure 12. Copyright laws are becoming increasingly complex as the information age unfolds. Not understanding the laws and their implications can seriously impair security of a paleontological database.

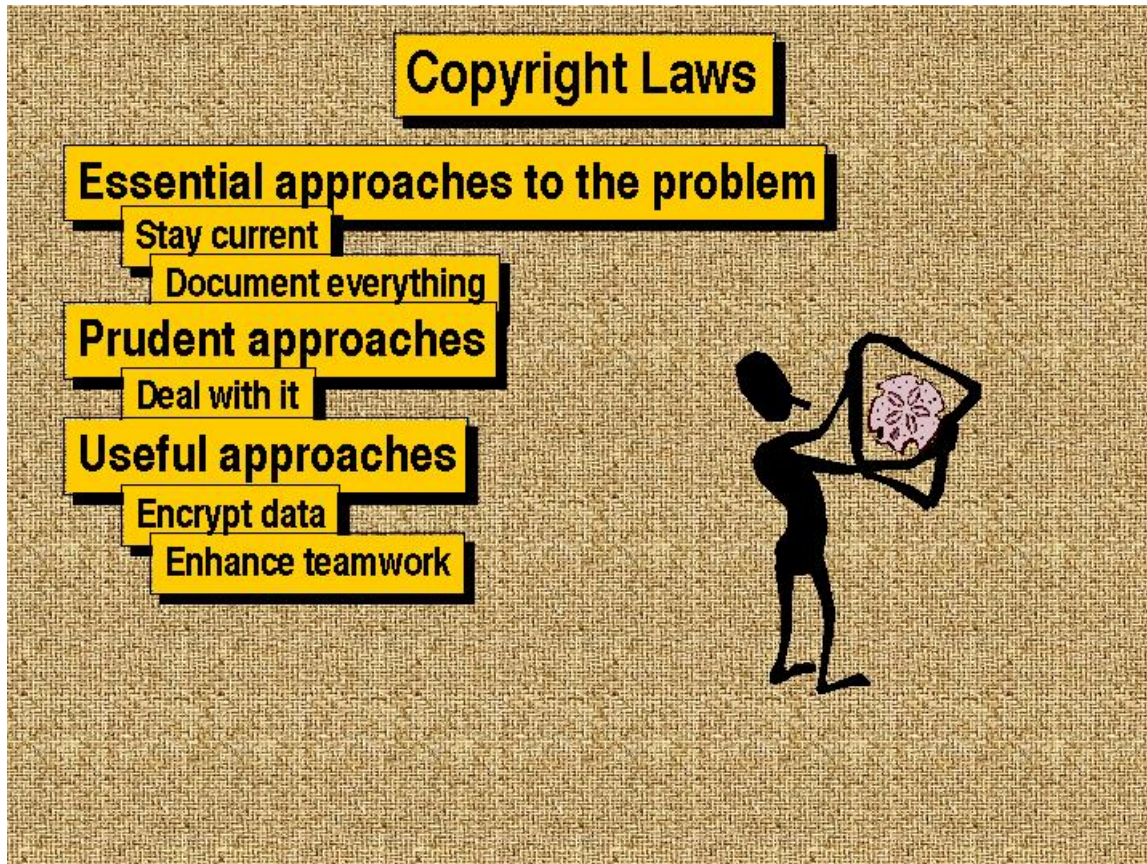


Figure 13. Summary.

