How to Maximize Evidential Weight of Electronically Stored Information
Recommendations of BS 10008

Enhancing cybersecurity and protecting critical information infrastructures are essential to each nation’s security and economic well-being. Deterring cybercrime is an integral component of a national cybersecurity and critical information infrastructure protection strategy. In particular, this includes the adoption of appropriate legislation against the misuse of information and communications technologies (ICTs) for criminal or other purposes and activities intended to affect the integrity of national critical infrastructures.1

Apart from substantive criminal law provisions, law enforcement agencies need the necessary tools and instruments to investigate cybercrime. Such investigations present a number of challenges. Perpetrators can act from nearly any location in the world and take measures to mask their identity. The tools and instruments needed to investigate cybercrime can be quite different from those used to investigate ordinary crimes.2 Furthermore, as stated by Jerker Danielsson and Ingvar Tjøstheim:

In many jurisdictions, it is unclear to organizations which requirements and constraints the legislation sets on collection and preservation of potential digital evidence. Often it’s also unclear how the responsibility is shared between law enforcement organizations and organizations affected by criminal activity leaving digital traces. It can be argued that organizations have to take a greater responsibility in the cyber-world than they currently do in the physical world. This is due to the complexity of the environment and consequently the complexity of investigations of crimes in this environment. Law enforcement needs support in getting an overview of affected systems. Additionally, law enforcement can only collect evidence post mortem and is consequently dependent on the fact that organizations affected by crime have collected and preserved potential digital evidence in a way that guarantees that it is authentic, accurate and complete.3

In most jurisdictions and organizations, digital evidence is governed by three fundamental principles: relevance, reliability and sufficiency. These three principles are important for the digital evidence to be admissible in a court of law, as stated in ISO/IEC DIS 27037. Digital evidence is relevant when it goes toward proving or disproving an element of the specific case being investigated. The meaning of reliability varies between jurisdictions; however, a general principle of it is to ensure that the digital evidence is what it purports to be and has not been spoiled. The concept of sufficiency means that digital investigators need only to collect enough evidence to prove or disprove the elements of the matter (ensuring that no exculpatory material has been overlooked).4

There has been much discussion about the value of information stored electronically when required as evidence in a court of law or for other purposes. British Standard BS 10008 specifies the requirements for the implementation and operation of electronic information management systems, where the issues of authenticity, integrity and availability, as required by legal admissibility and evidential weight, are important.5 This article introduces the basic recommendations, based on BS 10008, for improving the reliability of, and confidence in, electronically stored information.

PRINCIPLES OF GOOD PRACTICE FOR INFORMATION MANAGEMENT

Code of Practice for the Implementation of BS 10008 is structured according to a set of five principles of good practice, which are defined
The principles of good practice for information management. The five principles (figure 1), as defined in PD 0010, are:  
1. Recognize and understand all types of information.  
2. Understand the legal issues and execute duty-of-care responsibilities.  
3. Identify and specify business processes and procedures.  
4. Identify enabling technologies to support business processes and procedures.  
5. Monitor and audit business processes and procedures.  

“The ordering of the five principles also reflects a cascade from the high-level classification of information streams to responsibilities, and then on to operational, technological and system monitoring considerations.”7

The following sections outline some of the most important processes and procedures that need to be established to ensure compliance with this code.

**DUTY OF CARE**
The board of directors (or other equivalent group) of an organization is responsible for the conduct of that organization in every way—financially, operationally, legally and ethically. Specifically, it has responsibility for the organization’s assets and their use. One such asset is information—not information systems, but stored information itself. It is essential that organizations be aware of the value of information that they store.

**DESIGN FOR EVIDENCE**
Traditionally, corporations have considered the evidentiary implications of electronic documents only when it is required for litigation, or forensic practitioners have focused on collecting IT evidence as artifacts of an investigation. Unlike latent evidence that is inadvertently produced when a person contacts something (e.g., fingerprints, DNA), computer systems must be specifically designed to generate electronic records in a manner that maximizes their potential evidentiary value. Once electronic records are created, they must be carefully handled to maximize their evidentiary weight.8

**SECURITY MEASURES**
All information, irrespective of the media on which it is stored, is vulnerable to loss or change, whether accidental or malicious. To protect information stored electronically, security measures need to be developed and implemented to reduce the risk of a successful challenge to its authenticity.

---

**Figure 1—The Principles of Good Practice for Information Management**

<table>
<thead>
<tr>
<th>The Principles of Good Practice for Information Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recognize and understand all types of information.</td>
</tr>
<tr>
<td>Understand the legal issues and execute duty-of-care responsibilities.</td>
</tr>
<tr>
<td>Identify and specify business processes and procedures.</td>
</tr>
<tr>
<td>Identify enabling technologies to support business processes and procedures.</td>
</tr>
<tr>
<td>Monitor and audit business processes and procedures.</td>
</tr>
</tbody>
</table>

Source: BSI Group, PD 0010:1997
However, security is not a concern with computer systems only. Security and availability of the operating environment (e.g., buildings, temperature controls, network links, physical media) and the auditable implementation of procedures by all staff are key elements.

Security measures are often developed in an unstructured way, by reacting to security incidents and/or to available computer software tools. This approach on its own can easily leave gaps in security, which are filled only at some later date, typically after a security breach. A more structured approach is to review the information assets of the organization, and then assign risk factors based on asset value, potential threats, system vulnerability and likelihood of attack. These should be assigned on the basis of which appropriate, cost-effective security measures can be identified.9

**ACCESS RIGHTS**

“The segregation of roles is a fundamental aspect of duty of care,” according to the *Code of Practice for the Implementation of BS 10008*. It provides a check on errors and on the deliberate falsification of records. In this respect, segregation of roles is particularly important in systems where there is risk of fraud or other malicious action.

*Code of Practice for the Implementation of BS 10008* further suggests that it is also important to ensure that the physical and managerial segregation that exists around a system is mirrored by the logic access control within it, via the implementation of an access control system. Only staff with relevant access rights should be permitted to enter data or amend stored data. It is also important to ensure that a suitably granular level of automatic logging is applied to the process to record the activities performed, times and dates.10 System access rights should be granted only after the members of staff have successfully proved their competence.

Some of the electronic data files can have a nonhuman author. A computer-generated record is the output of a computer program untouched by human hands, thus the author can be considered to be a particular computer program or programs executing on a particular computer or multiple computers. One computer program may author many records, and many computer programs may author elements of a single record. Each computer program generating elements of the electronic record must be identified clearly in the record. The key evidentiary issue is demonstrating that the computer program generating the record is functioning properly.11

Further, some data files, particularly those generated by word processor or spreadsheet programs, may contain automatically executable code (often referred to as *macros*), which can have the effect of modifying the file each time it is retrieved, viewed or printed out. It may be difficult to assess what evidential weight is attached to such files.12

**RELIABLE AND TRUSTWORTHY SYSTEMS**

It is important to be able to demonstrate that the computer system has been functioning properly (i.e., according to agreed-upon procedures) in order to authenticate data stored on the system. Arguments over admissibility of information as evidence can lead to an investigation into the system from which the information came, the method of storage, operation and access control, and even into computer programs and source code. It may be necessary to satisfy the court that the information is stored in a proper manner. This could be a tactic used to try to discredit the evidence and to make inadmissible, or reduce the evidential weight of, that evidence and any similarly stored information that is produced.

Questionable hardware reliability, for example, could be used to discredit the information management system. This could call the whole system into question and cause information stored within it to be ruled inadmissible.13

It is important to utilize reliable and trustworthy technology to store electronic information over a long period of time. Each part of the system needs to be chosen with care, taking into account the possible need to demonstrate the proper and appropriate working of the system some time in the future. This demonstration may need to encompass both technology itself and the methods by which it was configured and used.14

The information management system should be maintained and corrective maintenance should be carried out only by qualified personnel to ensure that its performance does not deteriorate to such an extent that the integrity of the data captured, created by or stored within it is affected. A maintenance log should be kept, stating the preventive and corrective maintenance procedures completed. The log should include information regarding system downtime and details of action taken. Where system access control can be bypassed during maintenance of hardware and/or software, personnel performing such processes should be strictly controlled, monitored and audited.15
BUSINESS CONTINUITY PLANNING

From time to time, problems arise with information management systems that require emergency procedures to be implemented in order for recovery. Such procedures may involve the temporary use of additional or third-party resources. To ensure that the integrity of information is not compromised during these operations, an agreed-upon and approved business continuity plan (sometimes known as a disaster recovery plan) may be implemented.

Procedures to be used in cases of major equipment, environmental or personnel failure should be developed, tested, maintained and implemented. Such procedures should ensure that the integrity of stored information is not compromised during implementation. Issues surrounding the security of backup data may be important in the event of a dispute over authenticity. It may be argued that backup media had been compromised, and then used to recover from an information loss, thus affecting the authenticity of stored information. In some cases, the availability of backup data that have been in secure storage, to be used only in the event of a challenge to the authenticity of the live data, can be used to enhance the evidential weight of the stored information.

DATE AND TIME STAMPS

Being able to determine the date and/or time of an event can be an important piece of evidence. Thus, all appropriate events should be date- and/or time-stamped. Where accuracy of date and/or time stamps is important, regular checking of system clocks should be carried out. Any errors should be corrected and any actions taken should be documented. Only authorized personnel should be able to change system clocks.

AUDIT TRAILS

Code of Practice for the Implementation of BS 10008 further suggests that when preparing information for use as evidence, it is often necessary to provide further supporting information. This information may include details such as date of storage of the information, details of movement of the information from a medium, and evidence of the controlled operation of the system. These details are known as audit trail information. This audit trail information is needed to demonstrate that the system is working as well as the progress of information through the system. Audit trails need to be comprehensive and properly looked after, because without them, the integrity and authenticity and, thus, the evidential weight of the information stored in the system could be called into question.

The audit trail consists of the aggregate of the information necessary to provide a historical record of all significant events associated with stored information and the information management system. As such, it covers the answers to all classic questions concerning the provenance of any piece of information stored within the information management system:

- Who?
- What?
- Where?
- When?
- Why?
- How?

Access to the audit trail information needs to be controlled. In some applications, access may be needed only infrequently, so it is important that the interpretation procedures be documented. As audit trail data may be inspected by authorized external personnel (such as auditors) who have little or no familiarity with the system, interpretation procedures should be understandable to nontechnical users. The storage of audit trail data is a topic often not included in an organization’s information management policies. As they are frequently created automatically and infrequently accessed, they are forgotten and, thus, not subject to adequate control.

Some systems control the size of audit trail data files by the use of looping. Looping sets the maximum size for the data file, and when the size is reached, new data overwrite the oldest data in the file. Thus, old audit trail data are lost. This process may not be in compliance with required retention policy. This should not be the case with audit trail data from information management systems, which should be stored for the same period as that of the data to which they relate.

In a general sense, if an attacker gains unlimited access to a system, if the audit trail is not protected by write-only or write-once technology, and if no physical means are used or are effective in determining authenticity of audit trails, it is possible to create a forged audit trail that is not differentiable from a legitimate audit trail.

When attackers try to cover up attacks, they tend to do one of three things:

1. Attempt to delete all files on a system to remove all traces of their entry.
2. Try to modify selected audit trails to remove any indication of their use.
3. Try to prevent their attack from being audited by avoiding the use of audited events.

If they prevent their attacks from being audited by avoiding the use of audited events, there is little that can be done to detect their tampering within the system.\(^\text{20}\)

**CONCLUSION**

ICT brings potentially increased, or at least different, risk in terms of civil or criminal wrongdoing, and organizations must be able to protect themselves against such risk. Failure to do so raises governance and accountability issues for which management of the organization could be held responsible.

When information is used as evidence in the event of a dispute, the maximum weight of evidence is not affected by the size or shape of the organization and its own view of security risk. It frequently depends on the opinion of an independent arbiter. That view may well be affected by the opposing party in the dispute attempting to discredit evidential value.

Legal admissibility concerns whether a piece of evidence would be accepted by a court of law. To ensure the admissibility, information must be managed by a secure system throughout its lifetime (which can be for many years). Where doubt can be placed on the information, the evidential weight may well be reduced, potentially harming the legal case.

BS 10008 can provide assurance that any electronic information required as evidence of a business transaction is afforded the maximum evidential weight. Compliance with this standard does not guarantee legal admissibility. It defines best practice. The standard pays particular attention to setting up authorized procedures and subsequently being able to demonstrate, in a court of law, that these procedures have been followed.

Information security is key when discussing legal admissibility issues. The main discussion on this topic is likely to be the authenticity of the stored information. When the electronic information was captured by the storage system, was the process secure? Was the correct information captured, and was it complete and accurate? During storage, was the information changed in any way, either accidentally or maliciously? When responding to these questions, information security implementation and monitoring are central to demonstrating authenticity.

**ENDNOTES**

2. Ibid.
10. Ibid.
15. Ibid.
16. Ibid.
17. Ibid.
18. Ibid.
19. Ibid.