

# Knowing and Applying Evidence Laws when Securing Computer Systems

By Wong Onn Chee – ISSA member, Singapore chapter

**Knowledge of local evidence laws is no longer optional to IT/IS managers. This article looks at Singapore evidence requirements.**

**I**f records from a computer system are not admissible in a court of law, the computer system is worthless.

A strong statement, but there are many truths behind the above statement.

Imagine this scenario: A business partner sent in a purchase order to a B2B procurement system via strong authentication. However, the order was disputed by the business partner for its authenticity and validity. The records of the B2B procurement system were presented to the court as evidence but were rejected as they did not comply with the local evidence act. The business partner was able to nullify the order, but your company had wasted significant resources fulfilling the order and pursuing the litigation.

If the above fictitious scenario were to happen, it would be very likely that some of IT/Information Security (IS) management were given a golden handshake.

As the above example shows, non-compliance with your local evidence laws directly and adversely impacts the return on any IT investment. Besides having information implications, lack of knowledge of your local evidence laws can result in huge financial losses from computer systems without a single hacker. From a Governance, Risk and Compliance (GRC) viewpoint, your local evidence laws impact both the *risk* and *compliance* areas, with the latter having a greater impact.

Knowledge of your local evidence laws is no longer optional to both IT and IS managers. It is not something an IS manager can view as a “lawyer’s problem.” Instead, it is a problem that an IS manager has to tackle together with legal counterparts. Despite the importance of knowing and understanding local evidence laws, often IS professionals lack knowledge and awareness in this area. Rare is the IS professional I have met who has read his local evidence laws.

A common mistake is to think that all commercial off-the-shelf (COTS) systems will comply with local evidence laws out-of-the-box. Compliance with specific evidence laws is usually not a requirement during the development of the COTS systems. Furthermore, with COTS systems being sold

around the world and across different legal jurisdictions, it is not realistic for the COTS principal to cater all the variants of evidence laws around the world.

Another common mistake is that an IS professional needs to pay attention to the local evidence laws only during a forensic investigation. To view that knowledge of evidence laws is something reserved for highly-specialized forensic investigators is very short-sighted. As I will explain, the impact on admissibility of evidence starts the moment a computer system becomes operational. How computer systems are operated and how computer records are handled during peacetime also affects the eventual admissibility to the court when the need arises.

Since I am based in Singapore, I will walk through the Singapore Evidence Act (Cap. 97) in this article. The relevant sections of the act will be shown in brackets [ ] and keywords are highlighted in bold for your easy reference. Key considerations when designing auditing or records collection systems will be further elaborated. Please consult your lawyers for application of local evidence laws to your computer systems.

## Singapore Evidence Act (Cap. 97)

The full name of the Singapore evidence act is Evidence Act (Cap 97, 1997 Rev Ed),<sup>1</sup> which means Evidence Act, Chapter 97, Revised on 1997. As the name shows, the Singapore evidence act was last revised in 1997. This act applies to all judicial proceedings in any court, but not to affidavits or arbitration [s 2(1)]. There are two sections, namely Section 35 (s 35) and Section 36 (s 36), in the Singapore Evidence Act which relates to computer evidence.

### Overview of Section 35

For any evidence to be admissible, it must first be relevant to the case in question. This is required in s 35(1) which states that the evidence must first be “relevant or otherwise admissible according to the other provisions of this Act or any other

<sup>1</sup> <http://agcvldb4.agc.gov.sg>.

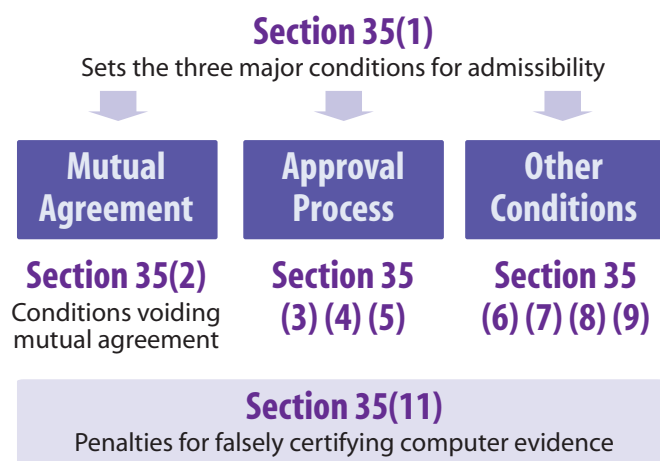


Figure 1 – Overview of Section 35 of Singapore Evidence Act

written law.” Usual evidential rules relating to the relevancy and admissibility of documents continue to govern computer outputs, for example s 9 of Evidence Act and s 380 of Criminal Procedure Code. [*Public Prosecutor v. Lim Mong Hong 2003*]

Figure 1 provides an overview of the major sub-sections within Section 35. There are three major conditions governing admissibility of computer evidence: mutual agreement, approved process and other conditions.

### Mutual agreement

Under s 35(1)(a), computer evidence is deemed to be admissible when both parties, plaintiff and the defendant, mutually accept and agree that the computer evidence in question is admissible. There are several additional conditions to which one must comply even if there is mutual agreement; hence, mutual agreement does not automatically guarantee that the computer evidence is admissible. These conditions are set out in s 35(2):

- In criminal proceedings on behalf of the prosecution if at the time the agreement was made, the accused person or any of the accused persons was not **represented by an advocate and solicitor**; or [s 35(2)(a)]
- In any proceedings, if the agreement was obtained by **means of fraud, duress, mistake or misrepresentation** [s 35(2)(b)]

What s 35(2) requires is that mutual agreement is made in presence of the defendant’s lawyer, and there is no fraud, duress, mistake or misrepresentation when the mutual agreement is made. Hence, “forced” agreements between plaintiffs and defendants are not allowed.

In times of dispute, mutual agreement on admissible computer evidence is least likely – one should not rely on this condition and depend on blind faith that the defendant will agree to incriminating computer evidence.

### Approved process

Under s 35(1)(b), computer evidence generated by an approved process is also deemed to be admissible.

A certificate is required to prove that the process by which the computer evidence is collected and handled is approved. The certificate can be signed by a person holding a responsible position in relation to the operation or the management of an appointed certifying authority. The certificate must identify the approved process, including that part of the process that is relevant to the proceedings.

As at June 2008, there are five recognized certification authorities here in Singapore.<sup>2</sup>

My recommendation is to engage an external certification authority to certify the process by which the computer evidence is generated. The certificate should be preferably issued by an external certification authority to provide greater weight to the computer evidence presented. We will talk more about weight of evidence in the later sections.

### Other conditions

Under s 35(1)(c), computer evidence can also be deemed as admissible if the following conditions are met:

- Is **accurate** and there is **no improper use of the computer** AND [s 35(1)(c)(i)]
- Is **true** and **reliable** AND [s 35(1)(c)(i)]
- The computer was **operating properly** AND [s 35(1)(c)(ii)]
- If **malfunction occurs, accuracy is not affected** [s 35(1)(c)(ii)]

First, the computer evidence must be **accurate**. To achieve accuracy, digitally-signed hash check sums can be used to verify integrity of computer evidence and to prevent authorized modification of the check sums.

Second, one must show that there is no **improper use of the computer** from which the evidence is collected or generated. The following controls are helpful in showing that the computer is properly used:

- Tight access controls: Who can use?
- Proper authorization levels: How it can be used?
- Audit logs for login and usage activities, e.g., executed commands, file/folder changes: What it had been used for?
- Audit logs for inbound and outbound network access
- Policy restrictions on removal or installation of software
- Audit logs for software changes, such as upgrades and patching

**Authenticity** or truthfulness and **reliability** of the presented computer evidence must also be shown. One can infer that completeness and timeliness are also required to fulfill the above two conditions.

A common mistake is to wrongly assume that a lack of graphical interface to modify records means the records cannot be

<sup>2</sup> [http://notesapp.internet.gov.sg/\\_48256DF20015A167.nsf/LookupContentDocsByKey/DEVT-5UCA4U?OpenDocument](http://notesapp.internet.gov.sg/_48256DF20015A167.nsf/LookupContentDocsByKey/DEVT-5UCA4U?OpenDocument).

modified. To really show the computer records are authentic, the use of digitally-signed records, multiple-factor authentication and server-client digital certificates for network communications will help. Consistency of records from multiple sources, e.g., between firewall and NIDS logs, between operating system and HIDS logs, can provide further assurance that the computer evidence is authentic. One must also ensure that all computer systems and devices are time-synchronized to correlate records from multiple sources. Timeliness of the evidence has a bearing on its weight as stated in s 36(4)(a), elaborated later.

In addition, security loopholes such as SQL injections must be closed at the application level to prevent any spoofing of log records. See OWASP for a more detailed description of log injection vulnerability.<sup>3</sup>

To show completeness, one has to configure the computer system correctly such that all events, failed or successful, are logged. This is different from doing verbose or debug logging. The volume of details per event should be sufficient for investigation and not more.

Next, I believe our fellow business continuity specialists will agree that to ensure **zero malfunction** of a computer system is a tall (and costly) order, and to prove that a computer system never malfunctions is even more difficult.

A better option is to focus on protecting the **accuracy of the computer evidence even when malfunction occurs**. Routine backups of the computer records must be performed with backup encryption enabled. With latest technologies, such as CDP (continuous data protection), one can provide better protection of the computer records during times of malfunction. As mentioned above, use of digitally-signed records helps to detect any tampering of records during times of malfunction. In addition, the computer application must not be prone to SQL injections which can be used to spoof the records when other protection mechanisms are down.

### Certificate for other conditions

To show that all the conditions in s 35(1)(c) are met, a certificate signed by a person holding a responsible position in relation to the operation or management of the relevant computer system is required [s 35(6)]. The certificate must “identify such output and describing the manner in which it was produced” [s 35(6)(a)]; “give particulars of any device involved in the processing and storage of such output” [s 35(6)(b)]; and “deal with the matters mentioned in s 35(1)(c)” [s 35(6)(c)].

Section 35(6) provides a good checklist for IT management, which is usually the party to issue the certificate, to show that conditions in s 35(1)(c) are met. However, the defense can attempt to prove otherwise to void the certificate. If this happens, s 35(11), which states the penalty for the person signing the void certificate is a fine or imprisonment not exceeding two years or both, may apply.

Section 35(9) states that “it shall be sufficient for a matter to be stated to the best of the knowledge and belief of the person stating it”; hence, the person signing the certificate must “KNOW” and “BELIEVE” that the computer satisfies the conditions in s 35 are met.

Even so, it is reasonable to expect a manager to hesitate to put his or her signature down, considering the potential penalties if the manager is proved to be wrong. The law permits a supplementary certificate signed by another person to be submitted, provided that the person had relevant control or access to the computer system and made in accordance with s 35(6)(a), (b) and (c) [s 35(7)]. This allows delegation. In addition, s 35(8) permits submission of a signed certificate by an independent person who had “obtained or been given control or access to the relevant records and facts in relation to the production by the computer of the computer output and made in accordance with subsection (6) (a), (b) and (c)” [s 35(8)]. This allows the organization to outsource the assessment of the computer system to an external entity, preferably a certification authority. The second option is usually preferred by IT management as it transfers risks away from internal members, but this option may be costly.

## Overview of s 36

### More evidence

The court may call for further evidence in the form of affidavits or oral evidence. Section 36(2) outlines the list of persons whom the court may call for affidavits. They include:

- A person occupying a responsible position in relation to the operation or management of the certifying authority appointed under s 35(5) [s 36(2)(a)]
- Any other person occupying a responsible position in relation to the operation of the computer at the relevant time [s 36(2)(b)]
- The person who had control or access over any relevant records and facts in relation to the production of the computer output [s 36(2)(c)]; a person occupying a responsible position in relation to the operation or management of the certifying authority appointed under section 35(5) [s 36(2)(a)]
- Any other person occupying a responsible position in relation to the operation of the computer at the relevant time [s 36(2)(b)]
- The person who had control or access over any relevant records and facts in relation to the production of the computer output [s 36(2)(c)]
- The person who had obtained or been given control or access over any relevant records and facts in relation to the production of the computer output [s 36(2)(d)]
- An expert appointed or accepted by the court [s 36(2)(e)]

Oral evidence may be called by the court to be given by the person making the affidavit under s 36(2) or the person signing the certificate under s 35 [s 36(3)].

<sup>3</sup> [http://www.owasp.org/index.php/Log\\_injection](http://www.owasp.org/index.php/Log_injection).

### Weight of computer evidence

Even when a piece of computer evidence is admissible, different weight may be applied to it. Section 36(4) states that “all the circumstances from which any inference can reasonably be drawn as to the accuracy or otherwise of the output” should be considered when estimating the weight of any computer evidence.

In addition, s 36(4) lists three criteria when evaluating the weight of computer evidence:

- Whether or not the information which the output reproduces or is derived from was supplied to the relevant computer [s 36(4)(a)]
- Contemporaneously with the occurrence or existence of the facts dealt with in that information, if such contemporaneity is relevant [s 36(4)(a)]
- Whether the supplier of the information or any person involved in the processing of such information had any incentive or motive to conceal or misrepresent the information so supplied [s 36(4)(b)]

In s 36(4)(a), the court will evaluate the accuracy of the computer evidence, with specific focus on whether the output (i.e., evidence) matches the inputs of the computer system. To demonstrate accurate input-output relationship, controls such as hash totals can be used. In addition, the output can be matched against digitally-signed checksums to ensure that it has not been modified in post-production.

Besides accuracy, the court will evaluate the timeliness of the evidence with regards to the facts that the computer evidence proves. To achieve this, ensure all computer systems' clocks are synchronized to allow depiction of facts in accurate and consistent timing.

Lastly, the court will evaluate independence of personnel involved in the generation of the computer evidence. In this case, the value of external personnel as compared to internal personnel is higher, as the likelihood of personal motives affecting independence is lower for external personnel. In addition, presence of disincentives can help to convince the court that the personnel involved are independent. Disincentives

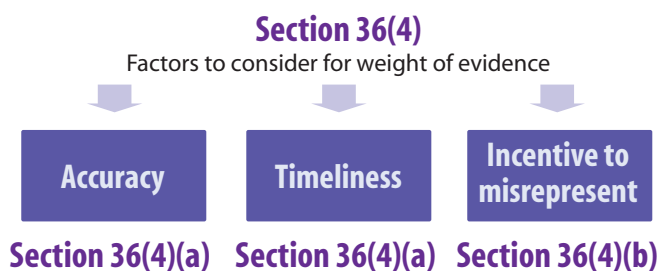


Figure 2 – Overview of Section 36(4) of Singapore Evidence Act

can be added to employment contracts for relevant personnel, such as penalties for any misrepresentation of computer evidence and rewards for ensuring accuracy and integrity during evidence handling.

### CAMPACT

An easy way to remember what key areas one has to observe when designing or building a computer system to ensure compliance with Evidence Act (Cap 97) is to remember CAMPACT.

Completeness  
Authenticity and accuracy  
Resilience against malfunction  
Proper use of auditing systems  
Certification by an external certification authority  
Timeliness

### About the Author

Wong Onn Chee, CISSP, CISA, is CTO at Resolvo Systems, a leading information security firm in Singapore. His areas of expertise include IT infrastructure and security strategy, IS management, identity management and network security. Onn Chee is a founding member of ISSA Singapore chapter and is currently the first vice president. Onn Chee is also the current Singapore chapter leader of Open Web Application Security Project (OWASP). He may be reached at [ocwong@usa.net](mailto:ocwong@usa.net).

