

Loose lips sink ships

The convenience of modern communication methods puts information at risk, writes Kevin Fitzgerald.



Privacy and confidentiality, integrity, and availability of information are all under constant threat through today's open communications systems — notably the Internet, email, and SMS.

Web sites and email are stolen (copied or simply read), interfered with (changed), and prevented (denied service or destroyed). SMS is expected to suffer similar problems in the next few years.

Email in particular has become an essential part of our business communications to such an extent that many companies have now classified it as a core mission-critical system. In 2001, IDC calculated that globally 31 billion emails were sent each day. And this was expected to rise to 60 billion by 2006. Today we are about halfway there at an estimated 45 billion a day. How much of this material is mission-critical or in some way sensitive is not known, but there is a healthy proportion of business people who take a security risk for the

sake of the tremendous convenience of email.

Twenty years ago sensitive business communications were done through what we now call 'snail mail'. However, despite being 'slow' or 'not instant', this mail was:

- In a sealed envelope (tampering was evident) so confidentiality could be reasonably assumed.
- On a letterhead (providing indication of genuine mail), so identity could be reasonably assumed.
- Often typewritten (any changes were evident), so integrity (i.e. no unauthorised changes) could be reasonably assumed.
- Personally signed by the author (providing legal proof), so authenticity of the author could be reasonably assumed and enforced in a court of law.

Unfortunately the assumptions we made about the security of our communications have tended to persist in the new version of mail despite it having significant weaknesses:

- There are no sealed envelopes and encrypted messages are not widely used.
- There is usually no letterhead.
- The magic of word processing leaves no audit trail of any unauthorised changes so we should not assume integrity of the contents.
- Genuine signatures are rarely used in practice (digital signatures are yet to be widely accepted).

As a result, we communicate today with an unhealthy dose of blind trust in email. It is true that most of the time this trust works. Yet sensitive information is at risk.

The quickest way to address these problems is by considering the way in which we protect access to our systems — usually using passwords. It is by breaking our password controls that the problems arise. If access to emails and their attached files can be tightly controlled, information will not be copied or changed.

Where do we start? Firstly, it is sensible to analyse the information that we communicate. What information is highly secret to ourselves and/or our business? By identifying it we can treat it accordingly. Perhaps we will never send such information by email. It must revert to the benefits of snail mail. Less important information may be communicated by email but it must be encrypted and perhaps signed using a digital certificate. Other emails may utilise double-factor authentication, perhaps a password plus a smartcard. The remaining emails can operate as usual, open and insecure.

The good news for most of us on a personal level is that the majority of our communications, often as high as 90 percent, are in the latter category. The remainder, those contracts that need to be sent to the solicitor, the agreement with the bank, and the X-rays we

'We communicate today with an unhealthy dose of blind trust in email.'

picked up from the radiologist, are always delivered by hand.

Businesses that analyse their information communicated over the Net also have a high percentage of 'open and insecure' mail, perhaps 70 to 80 percent. However, they will need to be aware of the other categories and apply effective solutions well above the current reliance on a password.

In any case, businesses must be conscious that passwords, as they are currently used in most organisations, are really a false sense of security. If passwords are persisted with, personnel must adopt secure password principles.

These principles include: forced regular changing of passwords; no password repetition; not less than seven characters; using representatives from the full keyboard character set in each password (e.g. 5add!3 but memorised as Saddle); no passwords related to partners, pets or cities; memorised not written down; and never lent to another.

Any access tool must be considered as a key which each user is accountable for. An access tool policy must be signed off by each user, including agreed penalties for failing to maintain control of the tool.

Email is a new mailing system. We must manage it with new levels of security or its marvellous convenience will be tainted. □

KEVIN FITZGERALD
 is an information security consultant with more than 25 years experience in designing and executing security solutions for large organisations.
kevinfitzgerald@ozemail.com.au