Encryption technologies may not be optional

No, this article is not about NCR Building 26, at least not directly. We know the history of Building 26 and the efforts there to decipher the encrypted communications created by the German Navy's Enigma machine in World War II. No, what I am talking about relates to electronic information and the growing obligation of companies to take reasonable steps to make it more difficult for criminals to understand and use personal information of customers, consumers and employees.

So why mention Building 26? The Enigma machine provides a good example to understand modern computer encryption technologies and the need to protect data. Think of the e-mails you send and the documents you generate like a letter generated by a typewriter. In other words, if a person can read the e-mails and documents, then nothing prevents that person from learning the contents of the letter. However, with the Enigma machine, a letter could be understood only if the recipient had the key to the Enigma code.

Encryption technology behaves in many respects just like the Enigma machine. Without the Enigma machine (encryption), documents and data that reside on computers and e-mail move about the Internet appear in what is basically human readable clear text. Anyone who intercepts the e-mail or accesses the computer can read the contents of the document with little effort. Encryption converts the data so that only someone with the key can read the document. In other words, if a criminal intercepts an encrypted e-mail (in transit) or steals a laptop (at rest) with encrypted data, then he will need the encryption key before the data can be viewed and the information used for improper purposes.

Expert Advice

Companies operating in regulated industries, such as banks and hospitals, have heard about encryption, and probably discussed employing this technology in their security programs. For example, the "Security Rule," found in the Health Insurance Portability and Accountability Act, requires covered entities to ensure the confidentiality of electronic protected health information, and to protect against reasonably anticipated threats or hazards (45 C.F.R. § 164.306[a]). The Gramm-Leach-Bliley Act places similar requirements on financial institutions via the Safeguard Rule (16 C.F.R. Part 314). However, the employment of encryption was not mandatory; it was just a good practice.

More recently, encryption has received attention because of data breaches at DSW, TJ Maxx and other notable companies. This attention is due to state laws that require companies to provide notice when criminals have obtained unauthorized access to data (in fact there is not an industry unaffected by a data breach and the notice laws). The epicenter for these laws was California's Senate Bill 1386 effective in 2003. After 2005 when the legislation gained notoriety, 48 states, including Ohio (Ohio Rev. Code §§ 1347.12, 1349.19), followed California's lead and passed nearly identical legislation. Importantly, most of these notice statutes provide that if the data was encrypted, then notice is not required under the law.

So what is the big deal about having to provide notice? It is more than just the cost of a letter and stamp. The most obvious response is captured by a simple question: what company wants to tell its customer that the personal information they provided to the company may now be in the hands of identity theft as costs associated with investigations, class action litigation, public relations and media plans, and developing processes in the midst of a crisis. For TJ Maxx, the costs resulted in it reporting a reserve of $107 million in its second quarter 2008 10Q. The simple use of encryption technologies might have prevented these losses.

But use of encryption may no longer be optional. It certainly is now required for companies doing business in Nevada, which enacted NRS 597.970. Effective Oct. 1, 2008, the statute requires "encryption" if personal information about a customer that is transmitted to a person outside of the secure system. The definition of a customer is not limited to residents of Nevada, but any person a company does business with in Nevada.

Similarly, on May 1, 2009, companies handling the data of residents of Massachusetts will be faced with a similar encryption requirement and even broader requirements as to data security (201 CMR 17.03). In sum, the Massachusetts regulation requires every business handling Massachusetts residents' personal data to (1) build firewalls and encrypt data whenever it is transmitted or stored on portable devices; (2) develop a security program, designate an employee to manage it, and discipline employee violators, and (3) train employees regarding security.

As the proverb says: "A good plan today is better than a perfect plan tomorrow." As with the breach notice law in California, it is likely that other states will follow the lead of Nevada and Massachusetts and pass similar legislation and develop comparable regulations. Regardless, the cards are lining up behind the use of encryption as not only a good data security tool, but also as a legal requirement. Assessing where this technology could be useful, and incorporating it into a general data security regime protects your customers, and the future success of your business.

Ronald Raether *is a lawyer with Faruki Ireland & Cox P.L.L. in Dayton. Reach him at rraether@ficlaw.com.*