

ASSURING DATA SECURITY CALLS for both high-tech and high-touch

By Jeff Thompson

Consider this hypothetical but plausible scenario: Production Agency Inc. sends Service Provider Inc. an unencrypted file listing all current Credit Card Corp. customers and account numbers to be used for a promotional mailing.

The file is transmitted electronically for merging with creative content the same day. A terminated employee of Production Agency Inc. remembers the username and password on the Service Provider Inc. server and waits for the file to be uploaded before making a copy. He then uses the information to post thousands of fraudulent transactions on behalf of those Credit Card Corp. customers.

Service Provider Inc. obviously must react to this breach of security, but over-reaction can be costly and ineffective. One customer wants more cameras, another wants bigger firewalls, and both want encryption. Service bureau providers that have thrown technology at security holes can attest to its impact on their bottom lines.

Security basics. Data security is a maturing field of information technology that uses risk management to guide responsible IT operations. Business owners must find and identify confidential data. Social Security numbers, birth dates, credit card numbers and bank account information are protected by law and must be secured at the highest level. Names and addresses are not legally protected, but must be

guarded against competitors.

Ultimately, security is the result of rational decision-making. Transmitting unencrypted information via e-mail is tantamount to using postcards instead of sealed envelopes. Because there is no expectation of security, whoever sees the information can read it.

Failure to deploy sufficient firewalls, essential to modern security, can be likened to leaving open your front door. And failure to employ cameras and intrusion detection is like leaving a house without an alarm system. The level of security must be commensurate with the value of the information at risk.

Legal compliance. Besides satisfying customers' security requirements, those who store or transfer sensitive information must comply with laws governing the protection of this information. The table provides relevant privacy laws and standards.

Security challenges. Because service providers, especially smaller ones, face daunting data security challenges, some may cut corners to save money, a huge risk when financial statements and personal information are at stake. Indeed, many may not even be aware of the regulations. Production managers are therefore advised to confirm compliance with internal standards and regulations. When selecting a services provider, they are further advised to require a comprehensive security framework that includes written security policies, reliable infrastructure and continuous security awareness.

Security at the highest levels presents challenges of its own. Creating a security-conscious enterprise requires significant resources and vigilance.

Investing in firewalls, security appliances and software cannot preclude unencrypted data from being sent via e-mail. Even when dealing with aggressive production schedules, service providers must never lose sight of security concerns, but must balance them against customer demands.

Winning the security game. So how can mailers and their service providers win at the security game? Here are some general guidelines:

1. Don't ignore security holes. Think of security as business insurance.
2. Identify at-risk data. General marketing information can be low-risk. Personal financial or medical data are high-risk.
3. Prioritize threats. All security threats have some merit, but not all require equal attention.
4. Act in all parties' best interest. Anyone willing to look the other way to speed the supply chain will not have the same perspective after a security breach.
5. Don't reinvent the wheel. Look to security standards for answers. For financial and credit card mailers, the PCI standard is a comprehensive framework for security.

In the final analysis, a winning security strategy calls for investment in both infrastructure and the education it requires to establish and maintain a pervasive security culture. ☒



Jeff Thompson

NORTH AMERICA.....

Gramm-Leach-Bliley Act (GLBA)(U.S.)

Security and privacy of personal financial information.

Health Insurance Portability and Accountability Act (HIPAA) (U.S.)

Security and privacy of health data.

Family Education Rights and Privacy Act (FERPA) (U.S.)

Privacy of student education records.

State Security Breach Notification Laws (U.S.)

34 states require notification if unencrypted personal information of residents is compromised.

Sarbanes Oxley Act (SOX) (U.S.)

Bill 198 (Canada)

Security, accuracy and reliability of financial data systems.

EUROPE.....

UK Data Protection Act

Obtaining, storing and disclosing personal information.

GLOBAL STANDARDS.....

Payment Card Industry – Data Security Standard (PCI-DSS)

Data security measures for protection of cardholder data.

Jeff Thompson is senior security engineer at Transcontinental Direct, Warminster, PA. Reach him at jthompson@transcontinentaldirect.com.