

BOARDROOM

Info Security Policy Tips

Kelly Dowell, president of Garrison Technologies Inc., Austin, Texas, and founder of the new Credit Union Information Security Professionals Association (CUISPA), recently shared his thoughts about information security with *Credit Union Magazine*.

Q What should CUs consider when developing an information security policy?

Consider the written policies' fundamental structure or layout. Policies are ineffective when employees dread reading them, can't understand them, or can't easily reference them. Information security policies, by nature, require periodic updating due to changes in regulatory requirements, technology, and business environments. The problem many organizations experience is that their policies evolve over time into complex, disorganized documents.

The policy's structure should allow users to find the requirements for a specific subject by perusing the table of contents. Categorize related policies appropriately so users don't have to search for information. Proper layout also allows the policy administrator to accurately modify policies. The

policy's primary goal is to educate staff on the guidelines you establish. If the document isn't legible and is poorly organized, contradictions and confusion can result.

Q What should CUs include in the policy?

Some common policy components are setting data classifications, roles and responsibilities, acceptable use of the Internet and e-mail, remote access, protection measures, and response procedures. Policies are legal documents, so include nondisclosure rules and an employee acceptance agreement.

Don't write precise rules for every possible scenario. Doing so can create loopholes that can work against the credit union. Instead, write policies in a general manner. For example, remote access rules should apply to any form of remote access. This accounts for future technology. When you authorize access, you further can define in a policy how it's controlled.

Boards and management regularly should review policies and procedures to ensure their completeness and effectiveness. Mergers; changes in technology, business models, and staff roles; and new regulations are key instigators of the review process. As events occur, review existing policies to ensure proper modifica-

tions.

Policies involve compliance, business process, technology, and employee awareness, so include all managers in policy reviews. Review policy considerations at each management meeting. Assign a policy manager to facilitate policy review, approval, and writing, and employee awareness. Make policy review a component of your credit union's third-party security assessment process that should be performed annually.

Q How do you monitor compliance?

Monitoring requires periodic testing. If you don't test, there's no way to know if your policies are being adhered to. With information technology (IT), seemingly minor procedural mistakes can go undetected until an incident occurs. A basic example is an e-mail policy. It's hard to know if a user routinely opens unsolicited e-mail attachments until a worm cripples the network.

You can perform testing in creative and educational ways. You could have an outside firm perform a social engineering-based penetration test, where a mock attack is performed using techniques that exploit existing policy rules. Or you could implement a more direct policy test, using a Q&A exam sent via e-mail, hard copy, or intranet. Remember, the

testing's intent is to educate staff on their role in security, not to identify a guilty party. Make education fun to maximize retention. Make monitoring policy compliance an integral part of a more encompassing employee awareness program.

Q How will CUISPA help CUs?

CUISPA's mission is to facilitate collaboration between security specialists, vendors, regulatory bodies, and credit union IT professionals to improve security throughout the movement. CUISPA's Web site will give members direct access to quality education, relevant information, confidential knowledge sharing, and services.

Policy development is one example. CUISPA and one of its affiliate members has initiated a security policy collaboration project members can access through www.cuispa.org.

The policy project will provide standardized, credit union-specific templates, policies, and management tools to help members maintain comprehensive policies.

CUISPA's Web site will consolidate relevant security information, updates, and news to eliminate the need for IT administrators to visit multiple sites to find what they need.

Q What led to CUISPA's formation?

Securing information is a complex challenge. The threats and risks are in a constant state of change, and the culprits' sophistication continues to advance along with the sophistication of hacking software. In addition, security vendors are getting increasingly competitive.

Despite a tremendous amount of security information that's available through the Internet, finding relevant information and impartial advice has become a real challenge. ©