

## A FORSYTHE CASE STUDY

# Security Policy Review & Development

## A Major Media Company

### Business Challenge

Information security policies are required by auditors and regulators, expected by business partners and – in practice – ignored by most who read them. At many companies, they range from brief statements about acceptable employee behavior on the Internet to hundred-page tomes on dusty shelves. Forsythe worked with a major media company whose diverse and distributed business spanned traditional print media, radio, television and the Internet. A recent audit report had cited its IT department for the third year for out-dated or non-existent policies in key areas. The company's new security manager recognized that without a solid set of comprehensive policies, enforcement of his basic security objectives would be impossible.

The security manager's primary challenges were to:

- Review and update existing policies to meet current standards and audit requirements
- Develop new policies where short-falls existed
- Assemble a comprehensive set of policies that were appropriate for the business and aligned with ISO standards
- Work with company stakeholders to ensure acceptance and enforcement

When Forsythe examined the company's existing policies, we found that they had been created with a cohesive framework in mind, but had not evolved over time. The "Manage Assets" policy covered physical security and data classified as sensitive; "Manage Change" addressed configuration and software changes; "Manage Access" described overall network and application access; and so on. A few other policies had been created in response to specific tactical needs such as e-mail and wireless networking. New employees were directed to an Intranet site that contained these documents, but there was no company-wide mandate that they be acknowledged. Most of the policy documents were two or three years old.

The security manager had performed a gap analysis and had come up with a long list of topics and requirements for bringing the security policies up-to-date. To ensure

organization-side buy-in and consensus, he had assembled a team of stakeholders from the many divisions within the company who would need to comply. The security manager planned to divide up the policy topics and assign them to team members. The team members would then develop the policies, and when complete, he would incorporate them into the existing policy set. He asked Forsythe to validate his plan and to critique his overall approach.

### Solution

To meet audit expectations, security policies must be aligned with industry standards for information security management, such as the widely-referenced international standard, ISO 17799. Although most of the needed policy statements were represented in the company's existing documents, some topics, such as logging and monitoring, were not covered. Forsythe's gap analysis mapped the existing policies and the security manager's security requirements to the ISO standard, creating a Security Policy Framework. This framework would be used as a guide for new and updated policies.

From the outset, the security manager had planned to hand-off the writing of new policies and procedures to a team of company stakeholders. This team consisted of representatives from key departments like Human Resources and Facilities, and business areas like Circulation and Marketing.

The security manager had realized that without buy-in from the business, policy enforcement would be difficult, but Forsythe cautioned him against tasking such a diverse group with writing policies, especially on topics with which they had little or no prior experience.

The security manager decided to move forward with his plan, asking Forsythe to moderate and lead the Stakeholder Meeting where the new Framework would be distributed and policy assignments would be made. This was a successful meeting, where the team showed enthusiasm for the process and their assigned topics. At the conclusion of the meeting, Forsythe handed the project off to the client.

## Results

Two months later, Forsythe received a call from the security manager. He had the new policies, but needed our help "putting it all together". Because each policy had been written by a different author, there were different writing styles and different levels of granularity between policies. There was a lack of cohesiveness and many of the policies were missing key information and statements.

Forsythe conducted interviews with staff members to fill in missing information, rewrote the policies in a uniform style, and removed any redundancy. Finally, we selected the key policy statements from each individual document and created a single "high level" policy that referenced the more detailed policies.

The security manager said that, in hindsight, he should not have depended solely on his internal team to write the policies, because they did not have the expertise needed to create readable, enforceable policies. Forsythe's skilled security professionals provided this client with an audit-ready policy suite based on the ISO 17799 standard ready for communication throughout the organization.

