WESTERN BANKERS ASSOCIATION

WBA INCIDENT RESEPONSE PROGRAM: FAQ

Q: Is the program and the customized incident response plan reviewed by the bank examiners?

A. Yes. The IRP is favorably received by the bank examiners.

Q. What is the entire cost of the IRP (i.e., insurance, legal, technical, communication review, training session and the customized incident response plan)?

A. $7,500, plus any necessary, reasonable travel expenses. An annual review of the plan and training session (optional) is $4,500.

Q. What is the value of the IRP if outsourced outside the WBA?

A. If a bank were to outsource each element of the program (legal, insurance, PR, IT), the cost would be significantly more than $7,500. For example, a tailored incident response plan itself would cost more than $7,500.

Q. What exactly is involved with the insurance review?

A. Each bank's insurance contract is unique and is thoroughly reviewed by the IRP insurance expert (Peter Marchel). Specifically, both the cyber and bond components of the insurance policies are examined, as well as a review of the professional liability. The IRP insurance expert will also review the limits, the policy terms and conditions, as well as the endorsements. In addition, the bank's policy may have specific exclusions, or conditions precedent in order to trigger coverage—all of which will be examined.

Q. What exactly is involved with the legal review?

A. The legal review is provided from both an information security and regulatory perspective. This involves a review of current online threats affecting banks, and a review of consumer and regulatory obligations in the event of an incident. It also involves a step-by-step review of the incident response process.

Q. What exactly is involved with the technical review?

A. A thorough review of the bank's IT process, vulnerabilities and an information security incident table-top test.

Q. What exactly is involved with the communications/crisis plan review?

A. A comprehensive review of the bank's existing crisis plan (if available), followed by a development of the bank's communications task force to ensure the right department leads and spokespersons (e.g., executives, HR, customer service, IT, community relations) are assembled to immediately address incidents. Communication policies and procedures are also drafted, including a step-by-step process to identify—and the decision-making process to respond to—an incident. How to immediately respond to media inquiries and social media posts are also included.

Q. What is contained in the customized incident response plan?

A. The IRP plan is a comprehensive framework established by the National Institute of Standards and Technology and involves four major breach response phases; 1) preparation, 2) detection and analysis, 3) containment, eradication and recovery and 4) post-incident activity. The IRP plan includes incident response policies and procedures, an incident response checklist, a communications plan, evidence collection guidelines, legal and regulatory incident response guidelines, internal and external communication guidelines and an information technology incident notification form.