

Incident Response Program: Before & After a Data Breach

WEBINAR – ON DEMAND WEB LINK & FREE CD ROM

Tuesday, April 27, 2010

12 - 1:30 pm PT
1 - 2:30 pm MT
2 - 3:30 pm CT
3 - 4:30 pm ET

Incident response planning, recovery, and testing are receiving strong focus by regulators and banks. Management's goal is to minimize damage to the institution and its customers, through containment and restoration. How is management required to address unauthorized access or use of customer information? Learn the process banks should use to identify, manage, remediate, and test security incidents. Understand how to assess the nature and scope of the incident; how to identify what customer information has been accessed or misused; the importance of promptly notifying your primary federal regulator and appropriate law enforcement authorities; and filing a timely SAR. National and state data-breach laws that your bank must comply with will be outlined and a step-by-step roadmap to prepare an efficient incident response program will be provided.

Continuing Education: Attendance verification for CE credits provided upon request.



HIGHLIGHTS

- What is a data breach?
- Define unauthorized access to customer data
- When do I need to notify law enforcement or my customer of a data breach?
- Incident response program – What do the regulators want?
- Develop an incident response process
- Incident response testing and policy
- SAR's – When to file?
- Breach laws – How will they affect you?
- How do I preserve evidence during a data breach?
- How does a penetration test assess my incident response program?

WHO SHOULD ATTEND?

This informative session is directed to bank presidents, directors, operations managers, IT personnel, Information Security Officers, and IT Committee members.

MEET THE PRESENTER

**Dr. Kevin F. Streff,
Secure Banking Solutions**



[CLICK HERE TO LEARN MORE ABOUT YOUR REGISTRATION OPTIONS](#)