



Federal Deposit Insurance Corporation
550 17th Street NW, Washington, D.C.

Financial Institutions Letter
FIL-55-2015
November 23, 2015

Cybersecurity Awareness Resources

Summary: As part of the FDIC's Community Banking Initiative, the agency is adding to its cybersecurity awareness resources for financial institutions. These include a Cybersecurity Awareness video and three new vignettes for the *Cyber Challenge*, which consists of exercises that are intended to encourage discussions of operational risk issues and the potential impact of information technology disruptions on common banking functions.

Statement of Applicability to Institutions with Total Assets under \$1 Billion: This Financial Institution Letter applies to all FDIC-supervised financial institutions.

Distribution:

FDIC-Supervised Banks

Suggested Routing:

Chief Executive Officer
Executive Officers
Chief Information Security Officer
Risk Officers

Related Topics:

FFIEC Cybersecurity Assessment Tool
<https://www.ffiec.gov/cyberassessmenttool.htm>

FFIEC Business Continuity Planning Booklet
<http://ithandbook.ffiec.gov/it-booklets/business-continuity-planning.aspx>

FFIEC Information Security Booklet
<http://ithandbook.ffiec.gov/it-booklets/information-security.aspx>

Contact:

Laura Lapin,
Chief, Information Technology Section
LaLapin@fdic.gov
(703) 254-0460

Marlene M. Roberts
Senior Specialist Critical Infrastructure Protection
MarRoberts@fdic.gov
(703)254-0465

Note:

FDIC Financial Institutions Letters (FILs) may be accessed from the FDIC's Web site at <https://www.fdic.gov/news/news/financial/index.html>.

To receive FILs electronically, please visit <https://www.fdic.gov/about/subscriptions/fil.html>.

Additional copies may be obtained through the FDIC's Public Information Center, 3501 Fairfax Drive, E-1002, Arlington, VA 22226 (1-877-275-3342 or 703-562-2200).

Highlights:

Community financial institutions may be exposed to operational risks through internal or external events ranging from cyber attacks to natural disasters. Operational risks can threaten an institution's ability to conduct basic business operations, impact its customer service, and tarnish its reputation. To help community financial institutions assess and prepare for these risks, the FDIC is incorporating new tools to its Directors' Resource Center at <https://fdic.gov/regulations/resources/director/>.

- The Cybersecurity Awareness Directors' College video provides an overview of the threat environment and steps community financial institutions can take to be better prepared should a cyber attack occur. This video is available at <https://fdic.gov/regulations/resources/director/technical/cybersecurity.html>.
- *Cyber Challenge* facilitates discussion between financial institution management and staff about operational risk issues. The exercises are designed to provide valuable information about an institution's current state of preparedness and identify opportunities to strengthen resilience to operational risk. The first four *Cyber Challenge* videos and supporting discussion materials were released in early 2014 and are available at the Directors' Resource Center. *Cyber Challenge* now consists of:
 - Seven scenarios presented through short video vignettes;
 - Associated challenge questions;
 - Reference materials; and
 - An instructional guide.
- *Cyber Challenge* is not a regulatory requirement; rather, it is an optional tool to assist financial institutions in strengthening their resilience to operational risk. *Cyber Challenge* is available at <https://www.fdic.gov/regulations/resources/director/technical/cyber/purpose.html>.