AN A.S. PRATT PUBLICATION
OCTOBER 2015
VOL. 1 • NO. 2

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

Pratt's Privacy & Cybersecurity Law Report

VOLUME 1 | NUMBER 2 | OCTOBER 2015

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please contact:
Deneil C. Targowski at 908-673-3380
Email: ..... Deneil.C.Targowski@lexisnexis.com
For assistance with replacement pages, shipments, billing or other customer service matters, please call:

Customer Services Department at ..... (800) 833-9844
Outside the United States and Canada, please call ..... (518) 487-3000
Fax Number .... (518) 487-3584
Customer Service Web site ..... http://www.lexisnexis.com/custserv/
For information on other Matthew Bender publications, please call

Your account manager or ..... (800) 223-1940
Outside the United States and Canada, please call ..... (518) 487-3000

ISBN: 978-1-6328-3362-4 (print)
ISBN: 978-1-6328-3363-1 (eBook)

ISSN: 2380-4785 (Print)
ISSN: 2380-4823 (Online)

Cite this publication as:
[author name], [*article title*], [vol. no.] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [page number] (LexisNexis A.S. Pratt);
Aaron P. Simpson and Adam H. Solomon, *Dealmakers Ignore Cyber Risks at Their Own Peril*, [1] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [46] (LexisNexis A.S. Pratt)

An A.S. Pratt™ Publication
Editorial

Editorial Offices
630 Central Ave., New Providence, NJ 07974 (908) 464-6800
201 Mission St., San Francisco, CA 94105-1831 (415) 908-3200
www.lexisnexis.com

MATTHEW BENDER

(2015–Pub. 4939)

Editor-in-Chief, Editor & Board of Editors

Pratt's Privacy & Cybersecurity Law Report is published nine times a year by Matthew Bender & Company, Inc. Periodicals Postage Paid at Washington, D.C., and at additional mailing offices. For customer support, please contact LexisNexis Matthew Bender, 1275 Broadway, Albany, NY 12204 or e-mail Customer.Support@lexisnexis.com. Direct any editorial inquires and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway Suite 18R, Floral Park, New York 11005, smeyerowitz@meyerowitzcommunications.com, 718.224.2258. Material for publication is welcomed—articles, decisions, or other items of interest to lawyers and law firms, in-house counsel, government lawyers, senior business executives, and anyone interested in privacy and cybersecurity related issues and legal developments. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

POSTMASTER: Send address changes to *Pratt's Privacy & Cybersecurity Law Report,* LexisNexis Matthew Bender, 630 Central Ave., New Providence, NJ 07974.

FFIEC Releases Voluntary Cybersecurity Assessment Tool

By James S. Talbot and Cristina Vasile

The Federal Financial Institutions Examination Council has issued a voluntary Cybersecurity Assessment Tool to help institutions assess their cybersecurity exposures and processes for addressing known risks. The authors of this article discuss the assessment tool.

The Federal Financial Institutions Examination Council ("FFIEC") recently released a voluntary Cybersecurity Assessment Tool to assist financial institutions in evaluating their cybersecurity risks and preparedness and determining whether their existing cybersecurity controls and practices are aligned with their inherent risk profile.[1]

BACKGROUND

The assessment tool is the product of the FFIEC's 2014 pilot assessment of cybersecurity preparedness at more than 500 community financial institutions, which found significant variances in inherent risks across the institutions. Following the pilot assessment, the FFIEC identified several cybersecurity action items, including creating the assessment tool, improving incident analysis, crisis management, training, policy development, and collaboration with law enforcement and intelligence agencies.

CYBERSECURITY ASSESSMENT TOOL

The assessment tool is a methodology for conducting a self-assessment of an institution's cyber risk. Financial institutions are provided with a matrix and instructed to evaluate which description of the organization best matches the institution's cybersecurity risk and preparedness across various categories. The tool consists of two parts — Inherent Risk Profile and Cybersecurity Maturity — and is ultimately designed to help senior management determine whether the institution's level of cybersecurity preparedness is appropriate given its internal risk profile. The user guide provides targeted guidance for senior management and the board of directors, emphasizing the goal of making cybersecurity an executive-level responsibility rather than just an IT function.

---

* James S. Talbot is a counsel at Skadden, Arps, Slate, Meagher & Flom LLP in the Intellectual Property and Technology Group, with a practice focused on transactional matters. Cristina Vasile was a summer associate at the firm. Mr. Talbot may be contacted at james.talbot@skadden.com.

[1] The Cybersecurity Assessment Tool is available at: http://www.ffiec.gov/cybersecurity.htm.risk.

Inherent Risk Profile

The first part of the assessment, the Inherent Risk Profile, considers the institution-specific cybersecurity risks across five categories, for which the user guide provides the following descriptions:

1) Technologies and Connection Types

Certain types of connections and technologies may pose a higher inherent depending on the complexity and maturity, type of connections and nature of the specific technology products or services. This category includes number of Internet service provider and third-party connections, whether systems are hosted internally or outsourced, number of unsecured connections, use of wireless access, volume of network devices, use of end-of-life systems, extent of cloud services and use of personal devices.

2) Delivery Channels

Various delivery channels for products and services may pose a higher inherent risk depending on the nature of the specific product or service offered. Inherent risk increases as the variety and number of delivery channels increases. This category addresses whether products and services are available through online and mobile delivery channels and the extent of ATM operations.

3) Online/Mobile Products and Technology Services

Different products and technology services offered by institutions may pose a higher inherent risk depending on the nature of the specific product or service offered. This category includes various payment services, such as debit and credit cards, person-to-person payments, merchant remote deposit capture, treasury services and clients and trust services, global remittances, correspondent banking, and merchant-acquiring activities. This category also includes consideration of whether the institution provides technology services to other organizations.

4) Organizational Characteristics

This category considers organizational characteristics, such as mergers and acquisitions, number of direct employees and cybersecurity contractors, changes in security staffing, number of users with privileged access, changes in IT environment, locations of business presence, and locations of operations and data centers.

5) External Threats

The volume and type of attacks (attempted or successful) affect an institution's inherent risk exposure. This category considers the volume and sophistication of the attacks targeting the institution.

Institutions should use these criteria to rate their risk level for each category as: least, minimal, moderate, significant or most, without considering any mitigating controls the institution may have in place.

Cybersecurity Maturity

The second part of the assessment, Cybersecurity Maturity, evaluates the existing cybersecurity controls and practices of the institution across five domains, ranking each as: baseline, evolving, intermediate, advanced or innovative. The FFIEC notes that the baseline level of cybersecurity maturity is consistent with legally required minimum risk management and control expectations. Each category provides several assessment factors and subfactors to guide this analysis. The user guide provides the following descriptions:

1) Cyber Risk Management and Oversight

Addresses the board of directors' oversight and management's development and implementation of an effective enterprise-wide cybersecurity program with comprehensive policies and procedures for establishing appropriate accountability and oversight.

- Assessment factors: governance, risk management, resources, and training and culture.

2) Threat Intelligence and Collaboration

Includes processes to effectively discover, analyze and understand cyber threats, with the capability to share information internally and with appropriate third parties.

- Assessment factors: threat intelligence, monitoring and analyzing, and information sharing.

3) Cybersecurity Controls

The practices and processes used to protect assets, infrastructure and information by strengthening the institution's defensive posture through continuous, automated protection and monitoring.

- Assessment factors: preventative controls, detective controls and corrective controls.

4) External Dependency Management

Involves establishing and maintaining a comprehensive program to oversee and manage external connections and third-party relationships with access to the institution's technology assets and information.

- Assessment factors: connections and relationship management.

5) Cyber Incident Management and Resilience

Includes establishing, identifying, and analyzing cyber events; prioritizing the institution's containment or mitigation; and escalating information to appropriate

stakeholders. Cyber resilience encompasses both planning and testing to maintain and recover ongoing operations during and following a cyber incident.

• Assessment factors: incident resilience planning and strategy; detection, response, and mitigation; escalation and reporting.

Institutions should analyze the results of the two portions and use them as a guide to determine whether the institution's inherent risk profile is aligned with its level of cybersecurity maturity across the various categories. (*See* Table 1.) In the event that the two are not aligned, the institution should adapt its practices so as to better inform its risk management strategy. Institutions should repeat the analysis over time to provide continuing guidance as to cybersecurity preparedness.

CONCLUSION

The FFIEC will periodically update the assessment tool as the cybersecurity landscape and threats evolve, particularly with respect to minimizing the burden for financial institutions with low cybersecurity risk profiles. Additionally, financial institutions are encouraged to comment on the assessment tool, pursuant to a forthcoming notice in the Federal Register. The FFIEC also provides various additional resources on the FFIEC Web site to assist institutions in improving their cybersecurity.[2]

While the assessment tool is currently voluntary, the Office of the Comptroller of the Currency and the Federal Reserve Board have announced plans to incorporate the tool into their examination process for evaluating the safety and soundness of financial institutions by late 2015 or early 2016.

Table 1
Cybersecurity Assessment Tool Summary[3]

Part I: Inherent Risk Profile	**Part II: Cybersecurity Maturity**
Least, Minimal, Moderate, Significant, Most	*Baseline, Evolving, Intermediate, Advanced, Innovative*
Technologies & Connection Types	Cyber Risk Management & Oversight
Delivery Channels	Threat Intelligence & Collaboration
Online/Mobile Products & Technology Services	Cybersecurity Controls
Organizational Characteristics	External Dependency Management
External Threats	Cyber Incident Management & Resilience

[2] The user guide is available at: https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_User_Guide_June_2015_PDF2_a.pdf. Additional resources are available at: http://www.ffiec.gov/cybersecurity.htm.

[3] Source: Federal Financial Institutions Examination Council.