Colleagues,

I am proud to present to you the revised Conference of State Bank Supervisors (CSBS) Executive Leadership of Cybersecurity (ELOC) Resource Guide, or “Cybersecurity 101.”

The number of cyber-attacks directed at financial institutions of all sizes continues to grow. Addressing new threats requires a concerted effort by Chief Executive Officers (CEOs), Presidents, and Board Members. Several years ago CSBS, on behalf of state regulators, launched the ELOC Initiative to engage bank executives and provide them with the tools to address cybersecurity threats.

Since its initial publication, “Cybersecurity 101” has served as a valuable resource for countless bank executives. In this update, however, you will notice several changes. Most notably, we removed previously included technical information, such as detailed instructions for activities performed by your IT and information security personnel. They will be incorporated into appendices and made available separately. The guide has also been updated to address both bank and nonbank institutions. We intend this document as a reference for both the banks that have formed the cornerstone of our economy for
hundreds of years, as well as the emerging technologies shifting our industry in exciting and challenging ways.

This guide is tailored to furnish Executives with the necessary tools to better understand and prepare for the threats faced by their institutions.

Thank you for taking the initiative to make your institutions, your customers, and your communities safer while online. Your leadership, determination, and willingness to adapt are instrumental to maintaining a robust, secure financial system.

John W. Ryan

President & CEO, Conference of State Bank Supervisors

Introduction

Financial institutions collect and protect highly sensitive information every day. The financial services industry is a vital component of the nation’s critical infrastructure—banks and nonbank financial institutions are the cornerstones of local communities, intrastate commerce, and the U.S. economy. As CEOs, Executives, and/or Board Members, you have the responsibility to adequately protect the money and information entrusted to you by your consumers; losing the trust of your employees and customers puts your institution on the path to disaster.

Cyber risks, like reputational and financial risks, threaten an institution’s bottom line. Attacks can be costly and compromising to customer confidence, and the institution may even be held legally responsible. Beyond the impact to an individual organization, though, cyber-attacks also have far-reaching economic consequences. Due to the inherent interconnectedness of the internet, a security breach at one financial institution can pose a significant threat to market confidence and the nation’s financial stability, as well as to other financial institutions. But in this time of technological advancement and
interconnectedness, it can be challenging to know how to best defend your institutions. With limited resources, how can risks be prioritized?

This guide addresses challenges faced by both bank and nonbank (also referred to as “non-depository”) institutions. It is intended as an easily digestible, non-technical reference guide to help executives develop a comprehensive, responsive cybersecurity program in line with best practices. As each institution is different, the advice in this guide can be easily customized to meet your organization’s unique threats, priorities, and challenges. While this resource guide does not guarantee prevention, it attempts to identify various resources—people, processes, and tools and technologies—that, when properly leveraged, work to reduce your cybersecurity risk.

It is our hope that this guide serves as a starting point to sustained collaboration between financial institutions and regulators. Together we can safeguard against new, persistent cybersecurity threats and contribute to a stable, prosperous economy.