Client Alert: Cybersecurity – No More Excuses

Related Services

Data Strategy, Privacy and Security

Related Industries

Financial Institutions

CLIENT ALERT | 7.1.2015

Unless you've been under a rock for the past year, you're aware that perhaps top on the list of "risk management" items is the need to ascertain the viability and efficacy of your data security programs. Banking industry and agency literature has been replete with warnings and highlights. On June 30, 2015 the federal agencies, through the FFIEC, published their promised Cybersecurity Assessment Tool (CAT) to help institutions, including those too small to have specific cybersecurity assessment resources, evaluate cybersecurity risks and preparedness.

Management and boards have been aware of the importance of understanding and assessing the risks in their institutions for cybersecurity issues and the associated liability for quite some time. Institutions that fail to undertake a comprehensive review and determination of that risk and implement appropriate safeguards do so at significant peril. No system is perfect, but failure to assess the situation and take appropriate remedial measures is a recipe for liability issues.

Use of the CAT

The CAT (and likely other tools) will be used by examiners to review and understand the level of risk present in an organization. It will also be used to assess actions taken by institutions in light of that threat. Institutions (and their boards) would be well-served to use the same process provided by the CAT to review and assess cybersecurity risk in their organization, and to implement appropriate measures to counter that risk.

The CAT provides that every banker and board be on notice of the threat, and provides a tool that sets a common "best practice." The tool takes away the ability of the institution to plead ignorance with regard to identifying and mitigating cybersecurity risks.

No system is perfect or impenetrable. The daily news is replete with cybersecurity and data breach issues involving large sophisticated organizations and even the federal government.

However, those instances of breach do not provide cover for institutions and their boards when it comes to their individual responsibilities to assess organizational risk and implement appropriate safeguards. And, importantly, to document their efforts in that regard in not only board minutes but in the underlying files relating to the CAT analysis and follow-up.

The level of risk varies among institutions, and there is no "one size fits all" when it comes to this area of risk and risk mitigation. The CAT however provides a uniform source for understanding what is likely to be the regulators' primary perspective on addressing the matter.

Additional Resources

The CAT provides institutions and their boards with additional tools and resources to assess cybersecurity risk in the form of a user guide as well as an online presentation. It also provides direction to other materials available to institutions to identify and to address this potentially significant risk.

Risk Constituencies

Financial institutions also have additional constituencies to consider in the process. There are privacy considerations for customers and liability issues for shareholders of stock organizations. Actual financial losses for the institution are very possible, and of course "reputation risk" issues abound with data breach problems once they become public.

Management and boards should review indemnification provisions in governance documents as well as generalized and special insurance coverage opportunities. And the time to do that isn't when the breach has already occurred.

Conclusions

There is far too much "notice" now in the industry to enable institutions to claim surprise with regard to the risk and exposure related to cybersecurity. Now with the CAT there is no excuse for not using the tool, at a minimum, to inquire and take appropriate protective measures.

Regulators and plaintiff's lawyers will be looking at how institutions respond to this enhanced risk and what steps they take to identify the nature and level of the risk and mitigate the likelihood of a cybersecurity event.

For more information about the CAT, please contact your Vorys lawyer or Jeff Smith at jesmith@vorys.com or 614.464.5436.