Cybersection

Cybersecurity Task Force Announced

The department has announced the formation of a Cybersecurity Task Force designed to educate and inform companies and individuals under its regulatory supervision about information security, with a focus on cybersecurity issues and challenges. The task force is comprised of regulatory, legal, and information technology staff, whose goal is to help businesses reduce vulnerability; prevent and defend against cyberattacks; and minimize damage to consumers and investors after a cyberattack.

The task force launched a **website** in September aimed at offering a variety of resources that may be useful in adopting a more vigilant attitude toward cybersecurity. Two examples of resources available on the website:

- The Federal Financial Institutions Examination Council (FFIEC) **self-assessment tool** to guide financial institutions in evaluating their cybersecurity risks; and
- A **guidance** [PDF] released by the Securities and Exchange Commission's Division of Investment Management emphasizing best practices and warning compliance officers of the potential securities law violations that could occur due to failure to address deficiencies in cybersecurity programs.

The department's task force efforts are an extension of the Commonwealth of Pennsylvania's **approach** to protecting the security of its digital resources.

"As cybersecurity threats to businesses and institutions continue and increase, the need for the financial services industry to implement effective cybersecurity measures is more pressing than ever," stated Secretary of Banking and Securities Robin L. Wiessmann.

The department strongly encourages all of its regulated entities to develop cybersecurity attack prevention and mitigation plans, including:

- Identifying and assessing their own cybersecurity risks, and evaluating means and methods for protecting their networks and data;
- Regularly running vulnerability assessments and penetration tests of their networks;
- Using encryption for customer and investor data;
- Keeping their operating systems up-to-date; and
- Employing and frequently updating anti-virus and anti-malware software.

In addition to implementing technical measures, businesses should recognize that the weakest links in a secure system may be an employee, a third-party vendor, or even a customer. Businesses should train and evaluate their staff and vendors, and educate their customers, to ensure that they understand the risks presented by cybersecurity threats. All parties should be vigilant in protecting their data, and the networks and data of their counterparties.

For more information, visit the department's cybersecurity website at
www.dobs.pa.gov/businesses/cybersecurity