PANEL OF EXPERTS **Cybersecurity**

FROM OUR SPONSOR

The Secret to Good Cybersecurity

William M. Prohn
Managing Director,
Dopkins & Company, LLP

Dopkins & Company, LLP
CERTIFIED PUBLIC ACCOUNTANTS AND CONSULTANTS

Most, if not all, business leaders are now aware of the myriad cyber threats posed by their company's reliance on computer technology including Internet-based data storage and communications. However, many are still not establishing effective controls within their organizations to combat and respond to those threats, even when required to do so by legislation, regulation or contractual obligation. The reason for this may be the sheer size of the problem: there are so many threats, so much data, so many users, stake-holders and scenarios to address, that is just easier to hope it doesn't happen. But, as we all know, hope is not a strategy!

The reality that often gets lost in this overwhelming cloud of cyber threats is that they don't all pose a risk to everyone or, if they do, all those risks are not of equal concern. If one were to identify which specific problems are likely to manifest themselves in one's own environment, and how great an impact they would have IF they occurred, then a strategy could be crafted to defend against and recover from the biggest of these risks. We are all well aware of the tremendous destruction which can be wrought by hurricanes, tornadoes, wildfires or earthquakes. But, in Western New York we are also cognizant of the extreme unlikelihood of these disasters befalling us. Therefore, our defense strategies are focused on extreme cold, lake-effect snow and the like.

A Cyber Risk Assessment allows a business to narrow its focus to the (relatively) few cyber threats which are most likely to occur and how big an impact they would have IF they did occur. When you have a short list of worries, you can begin to focus on what steps (controls) could be implemented to reduce the likelihood of the threat, or reduce its impact, or create a way to recover more quickly if and when the threat might hit. A Risk Assessment need not be an expensive, complex or formal occasion. It should be as comprehensive as possible involving all critical functions within a business, with well-documented, consensus findings, and repeated frequently (at least once per year). Often, a half-day facilitated workshop can produce an effective Risk Assessment.

The result of a Risk Assessment is a Prioritized (most risk on top) List of Risks faced, with a list of the controls that are (or should be) in place to mitigate the risk. The purpose is to identify what an organization should be doing (spending) to reduce the risks. You don't need to spend money on tornado shelters, no matter how effective they are, if tornadoes are not a big risk for you. Simply put, a Risk Assessment identifies risks (a ransomware attack shuts down all operations for a month) and the controls that could help (a current backup, end-user training, cyber liability insurance, email filters, etc.). Now, you have a strategy for where to invest resources, and can establish tactics (timelines, training courses, relevant coverages and deductibles, etc.) to implement over the next budget year. Once these controls are in place, next year's Risk Assessment will likely yield a different risk list, since at least some of the current risks have been sufficiently mitigated by the new controls.

I once performed a detailed cyber controls assessment for a small not-for-profit, which resulted in a prioritized list of 27 key controls which needed to be implemented to address the risks identified by leadership. The compliance officer was nearly overwhelmed at the prospect of implementing so many new initiatives. The CEO stated that, "on the contrary, I'm relieved there are only 27, I used to think there were thousands!"

Four Things to Help Keep Your Business Safe

Establish these processes and controls to reduce the risk of human error.

This Cybersecurity Awareness Month, arm your employees with the tools they need to help protect your network throughout the entire year.

1 Enable Multi-Factor Authentication

2 Use Strong Passwords

3 Recognize & Report Phishing

4 Update Your Software

For a Strategy to get Started with a Cybersecurity program contact:
William M. Prohn
wprohn@dopkins.com

Dopkins & Company, LLP
CERTIFIED PUBLIC ACCOUNTANTS AND CONSULTANTS

200 International Drive | Buffalo, NY 14221 | 716.634.8800