Primerus™ takes the initiative on the cybersecurity front

"I think computer viruses should count as life. I think it says something about human nature that the only form of life we have created so far is purely destructive."
— Stephen Hawking

As Chair of the Quality Assurance Board (QAB) for Primerus™, I recently wrote a letter to all of our member firms outlining the steps that our international alliance of law firms is taking to prevent cyber-attacks and to ensure that sensitive data is properly safeguarded.

The April 14 letter addressed what we believe will become an existential threat to law firms around the world which do not remain focused on the increasing sophistication of cybercriminals and cyberhackers as they continue to become more brazen and determined in illegally obtaining financial information from businesses and individuals around the world, including the information of our Primerus™ law firms and our clients.

In short, Primerus™ law firms have mounted a counterattack against computer hackers and others, marshalling our forces and legal expertise to recommend a series of practices that our member law firms will adopt to better secure their systems, fortify their networks, and strengthen their data security measures. That counterattack is intended to be focused and strategic. There is an apt quote by Ma Huateng, founder and CEO of Tencent Holdings, that is directly applicable to the intentions and processes for our new cybersecurity initiative: "*There should be order if the development of the cyber world is to be sustainable*."

The Cybersecurity Initiative that the QAB recommended was recently approved unanimously by the Primerus™ Board of Directors. The initiative was the result of a collaborative effort among members from the QAB's Cybersecurity Subcommittee, the QAB, and the Primerus™ Board.

Significant analysis was undertaken by the Subcommittee, which assessed both client needs and expectations as well as how Primerus™ firms can differentiate themselves from competing non-Primerus™ law firms. Many thanks are due to those Subcommittee members for their selfless efforts. They include: Iker Dieguez, *Cacheaux, Cavazos & Newton*, Mexico City, Mexico; Kengo Nishigaki, *GI&T Law Office, LC*, Tokyo, Japan; Dr. Johannes Struck, *Brödermann Jahn*, Hamburg, Germany; Dale O. Thornsjo, *O'Meara Leer Wagner & Kohl, P.A.*, Minneapolis, Minnesota; and Chair, Ken Rashbaum, *Barton LLP*, New York, New York. As is apparent, the Subcommittee was both international and inter-Institute in composition.

As noted in the letter, input for the initiative was provided by Primerus™ members from around the world and underscored the importance of letting clients – and potential clients – know that Primerus™ member firms are able to represent them with a level of cybersecurity not matched by most other law firms in the world. As Ken Rashbaum stated to the QAB: "The Primerus™ Cybersecurity Standards will serve as an announcement to Primerus™ clients and to potential Primerus™ clients that member law firms meet legal, ethical, and client business requirements for secure controls over their client information and in their law firm advice to clients. Going forward, these standards will differentiate Primerus™ firms from those which do not have these controls over client and firm electronic information and will establish a baseline for clients to know that Primerus™ firms will take good care of their critical information."

Additionally, the standards permit Primerus™ firms to have confidence in recommending our fellow Primerus™ firms to our own clients who demand such cybersecurity and data protection standards in order to do their work. The standards offer a clear roadmap for our member firms in how to attain that cybersecurity level both strategically and economically.

Of added importance, it permits Primerus™ to have the ability to confidently market its Primerus™ firms as "The World's Finest Law Firms," a trademarked phrase that now reaches a global audience.

For accountability purposes, the Cybersecurity Initiative will require all Primerus™ firms to report on their compliance or non-compliance with the six minimum cybersecurity standards

established in the new program. The report must be filed on or before September 15, 2023, and will address the following standards:

1. Multi-Factor Authentication for law firm network login (code sent upon login attempt to a different device that must be entered for access to network), for remote access or any access to cloud systems.
2. Privileged Access Management and Identification Policy (establishment and termination of law firm network access), with Access Logs and Processes for Audits of Access Logs.
3. Data Security Policy with Security Patch Management.
4. Security Incident Plan and Breach Notification Policy and Processes.
5. Internal Risk Assessment and Security Monitoring Policy.
6. Disaster Recovery and Business Continuity Plan.

Many of you will find that your law firm has already implemented most, if not all, of the initial cyber controls. If not, the audit will ask you to discuss what measures have not been undertaken and to provide an estimated date by which they can be implemented. Member firms that are not in compliance with the six minimum standards as of September 15 must implement those that are lacking and certify their full compliance no later than January 31, 2024. A second phase – featuring five additional cybersecurity controls – will follow after the completion and implementation of the minimum standards. Additional information on these more advanced controls will be provided to you in the weeks to come.

Rest assured that Primerus™ stands ready to assist member firms in meeting these compliance goals, offering educational Coffee and Conversation sessions with cybersecurity experts; instructional videos; detailed written materials providing step-by-step help; and lists of third-party vendors and others with cybersecurity expertise, including fellow Primerus™ firms, to assist in accomplishing the standards.

As technology advances, our cybersecurity protections policies will need to keep pace, equipping law firms of any size with the tools to protect their and their clients' data from illegal cyber activity. Beginning with this base, Primerus™ firms will be able to build upon our capabilities far easier than would have been the case without this new foundation. In other words, our Primerus™ firms will be able to become increasingly differentiating in the future from other law firms.

With your help in the implementation of these cybersecurity controls, we will make our collective efforts as Primerus™ members stronger and better for ourselves and our clients.

Best regards,
Marc Dedman
Chair, Quality Assurance Board