PRUDENTIAL
Associates

A subsidiary of Stern Strategies International, LLC (SSI)
9900 Belward Campus Drive, Suite 225 • Rockville, MD 20850
Tel: 301-279-6700 • Fax: 301-251-0670

prudentialassociates.com

FREE Law Firm Network Security Assessment *

Bar Association of Montgomery County, MD Members Only

Your firm's network is at RISK and is VULNERABLE, despite what your "IT guy" tells you.

Don't spend tons of money on the assessment telling you that you are vulnerable, spend money on implementing security controls to secure your network and actually protect your critical data. In 2011, the FBI met with representatives from 200 of the largest U.S. law firms to warn them that law firms represent a major target of hackers. Why? Law firms hold vast collection of sensitive client documents containing personally identifiable information – data of significant value to hackers.

Have a security and technology services firm with specific and substantial knowledge of the legal services industry and the vulnerabilities that you actually suffer protect your network and client data. Over 50 years of serving the Maryland legal community you have likely trusted us before and thus you know that you can now.

Your network and your client data IS at risk. We are not selling fear but reality. Let us perform a comprehensive IT Security and Risk assessment, identify the specific risks and solutions, then we can address them and protect you going forward. The first step is the FREE of Cost basic security assessment, contact us to discuss and schedule.

Our Assessment Process

Prudential Associates is offering a free preliminary cyber security assessment of your firm to assess current posture of security controls implemented at your firm to protect the confidentiality, integrity and availability of sensitive data. Our free preliminary cyber security assessment is based on guidance provided by National Institute of Standards and Technology (NIST). Our firm will assess your firm's security by utilizing NIST's cybersecurity framework categories:
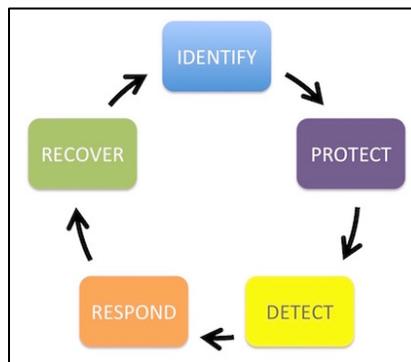
Cybersecurity Framework Functions

ONLY THE SERVICE ITEMS IN GREEN BELOW ARE INCLUDED IN THE FREE BASIC ASSESSMENT

1. **Identify**

The identify function helps increase an organization's understanding of their resources and risk. We will:

- identify user access level to your business information,
- assess administrative privileges, passwords complexity requirements
- ensure that unauthorized persons do not have access to sensitive data
- Identify that account reuse is not happening.

2. **Protect**

The protect function supports the ability to limit or contain the impact of potential information of cybersecurity event. We will:

- assess and identify current security patch levels on installed operating systems and software
- review security patch update policies and settings
- review network firewall policies for ingress and egress traffic and review security of wireless access points.

3. **Detect**

Our security assessment activities under the detect function will assess how your firm's detection security controls timely discover information security or cybersecurity events. We will:

- review installed malware detection and antivirus software
- review log collection and monitoring activities as logs are critical to identify suspicious activities and for incident response
- deploy our EDR solution for 14 days and report back on any anomalies detected

4. **Respond**

The respond function supports the ability to contain or reduce the impact of an event. We will:

- take action on any anomalies detected by our EDR solution **billable rate applies.

5. **Recover**

The recover function help an organization resume normal operation after and event. Under this function, we will:

- assess your backup strategy of your critical data
- review in disaster recovery plan the roles and responsibilities actions that your firm will take in case of an incident
- review and assess your firm's respond function by reviewing disaster recovery plan (if available)

6. **Reporting**

At the end of assessment, we will furnish a basic security assessment report (6-8 pages) reflecting your firm's cybersecurity posture. This report provides a risk analysis of potential issues we will uncover during assessment. Our cybersecurity experts with review report with your firm, discuss the findings in detail and answer any questions you may have.