Published on *The National Law Review* https://natlawreview.com

Your “Top Ten” Cybersecurity Vulnerabilities

Article By:

Brian G. Cesaratto

Adam S. Forman

Cybersecurity has never been more important, or challenging, to address. For many employers, even figuring out where to start may seem like an overwhelming challenge. The first step—and one that should be done at least annually—is to focus on the adequacy of your organization’s cybersecurity planning processes, if any, in place. To jump-start your year-end cybersecurity planning, here are our “top ten” vulnerabilities to put on your list.

Vulnerability No. 1. **No, or inadequate, security program in place.** It is essential that your organization have a written, formalized cybersecurity program that assigns and enforces individual job responsibilities. The absence of a written plan documenting your cybersecurity program is a significant gap that leaves you more vulnerable to a cyberattack. If your organization already has adopted a written security plan, review and, if necessary, update it periodically (no less than annually) to determine how your organization will comply with the plan to protect your systems and staff. Cybersecurity is everyone’s responsibility.

Vulnerability No. 2. **No recently conducted vulnerability and risk assessments.** A comprehensive, well-documented vulnerability assessment will identify gaps in your workforce management and information technology security policies, procedures, and technical controls. A formalized risk assessment will address the risks of cyberthreats exploiting the gaps revealed by the vulnerability assessment. Vulnerability and risk assessments, which may be conducted with the assistance of cybersecurity counsel under the protection of the attorney-client privilege, are fundamental building blocks for reducing cybersecurity vulnerabilities.

Vulnerability No 3. **No evaluation of weaknesses or gaps in your controls in light of statutory requirements and potential common law claims.** This highlights your compliance gap and legal exposure arising from poor technical and administrative controls (e.g., inadequate or nonexistent policies), particularly in financial services, health care, or where your location and business lines subject you to requirements of state data privacy and breach laws. The absence of particular controls may constitute statutory violations or be cited in litigation as evidence of red flags.

Vulnerability No. 4. **No formalized patching process or inadequate enforcement of the current process to ensure its systematic implementation.** Failure to expeditiously address known

vulnerabilities carries potential liability. A formalized, well-documented and enforced patching process may avoid gaps in failing to timely patch a known vulnerability and help reduce exposure.

Vulnerability No. 5. **No insider threat program.** Most data breaches are caused by insiders—either employees or trusted third parties (or their employees). Not having in place an insider threat program (that includes an insider threat vulnerability assessment) increases your vulnerability to insider threats.

Vulnerability No. 6. **Lack of connection to the cybersecurity community.** Did you know that the leading wireless (WiFi) encryption protocol (WPA2) has recently been cracked by a new method called “KRACK” (short for Key Reinstallation AttaCK)? Did you know that the National Institute of Standards and Technology (known as “NIST”) has recently proposed significant new guidance in password administration? The new guidelines recommend, for example, increasing usability, including a blacklist of poor choice passwords and allowing passwords of at least 64 characters in length to support the use of pass phrases. These are just examples of the ever-changing cybersecurity landscape. Your organization should establish contact with the cybersecurity community, including cybersecurity counsel, to facilitate training and education within your organization and to maintain current on best practices and technologies.

Vulnerability No. 7. **Lack of stringent configuration management.** If your organization does not use a baseline of secure configurations for each of its information and communications systems and related hardware before each goes live or before any implemented changes, then you are vulnerable. The vulnerability from permitting the live implementation of default configurations (e.g., default passwords), for example, is an ever-present and frequently overlooked vulnerability that requires rigorous oversight.

Vulnerability No. 8. **Lack of stringent remote access management.** If your organization permits remote access by its personnel, your potential attack surface is expanded. Granting remote access requires a combination of stringent best practices, such as rigorous human resources and technical controls (including monitoring remote access usage).

Vulnerability No. 9. **Failing to consider available cybersecurity data.** If you are not looking at the available cybersecurity data for your particular industry, you are likely not making the most informed decisions. Don’t fly blind—there is data out there for all industries that you can use to inform your vulnerability analysis.

Vulnerability No. 10. **No incident response plan in place.** No matter the level of stringent controls you put in place, you have to be prepared for the eventuality of a data incident or breach. Being reactive because you do not have a plan in place tested through training, including table-top training exercises, leaves you vulnerable.

The foregoing list is non-exhaustive. Your list may be different. Hopefully, our recommendations get you thinking about your cyber protections for the coming year.

National Law Review, Volumess VII, Number 361