3. Security Toolkit: Assessing Your Current Cyber Security Practices

Full Security Assessments

In addition to self-assessments to guide your cyber security decisions, your organization should also consider a more complete assessment, often conducted with the help of outside experts. Below is information on what a security assessment usually entails and what you can do after the assessment to apply what you learn.

What is a Security Assessment?

A security assessment is an opportunity for your firm to look at your approach to technology and evaluate how secure you really are. This includes looking at your current security software, services, and practice, as well as your security training for staff and your general readiness for cyber security incidents. But it also includes analyzing the equipment and software you use, your technology is configured, your IT practices, your technology policies, and data management practices. It is always better to know where your office is vulnerable to attack before an attack happens so that you can not only prepare for attacks, but also make informed decisions about which risks are acceptable and which are not.

These types of reviews and assessments are typically done periodically, not just one time. Some large law firm legal technology experts liken security assessments to annual physicals. Your organizations's technology environment and practices are always evolving, and we are always seeing new vulnerabilities and exploitation techniques emerge. An assessment should be done at least every 2 to 3 years, though some recommend doing assessments annually.

The process usually starts with selecting a vendor, then a rigorous discovery process, followed by reports from the vendor and planning how to move forward from those reports and recommendations. Vendors who perform assessments, called auditors or assessors, typically help firms address questions they have and come up with solutions that work or better fit budget constraints while keeping firms informed about the impact of new approaches and solutions on associated risks. The end result should be a comprehensive plan to improve security over time,

as well as a plan to assess those improvements as they are implemented.

The Nuts and Bolts of a Security Assessment

Selecting a Vendor

Before your assessment can begin, you need to find an auditor or assessor. Talk to the legal community about who is doing these assessments. Look at the specific areas in which assessors might work (e.g. if you have concerns about inventory management specifically, you should find an assessor who has worked on inventory management solutions before). You can also seek grant funding help for your assessment (including from LSC, as described below).

Discovery

Once you've selected your vendor, your assessor will start to collect information about your office to learn as much as they can about your organization's security vulnerability and practices. The size of this process can vary greatly, but around a month of discovery is not typical.

Your vendor will want a vast variety of information. Your assessor will review your organization's security policies (things like Window Server security, access and use policies, and your "bring your own device" policies). Your IT team and administrators will need to be involved in this process, and people from around the office might have to gather information for the vendor or participate in interviews. You will also likely have to give your assessors access to some of your technology and software with user accounts.

This phase of the assessment may also include internal and external "penetration testing," a type of testing where assessors try to break into a organization's systems to see how secure they are. This kind of testing may be done more regularly than the fuller assessments. Assessors may also attempt phishing and social engineering attacks to see if your organization's users are particularly vulnerable to these methods of attack.

Doing all follow-up work and providing all information your assessors request is critical. In order to provide useful advice, assessors need an understanding of your business and practice. This increases the likelihood that they will uncover lurking vulnerabilities, but also that they'll propose strategies that are cost-effective and match with your organization's actual work and processes. For instance, in an office where advocates collaborate very often with users in Google Docs, an assessor must know not to suggest a policy requiring advocates to work only in the firm's Office 365 environment. Assessors can only know these details if the organization works closely with them during the discovery process.

Outputs and Follow-Up with Assessors

When your assessor finishes gathering supporting information, they'll prepare reports for you, in which they'll identify and describe the vulnerabilities they've found and their relative risks.

Assessors will typically make recommendations on the specific technologies in use, new technologies that might be implemented in your organization, changes to business practices, changes to the insurance you carry, and user changes to practices around user management and support.

Assessors will typically prepare multiple reports. First, they'll create a business-level report, a summary for non-technical audiences, that the office can share with leaders and committees. They'll also create more detailed technical reports. These actionable reports should be directed at IT staff to explain what's wrong and how to fix it.

After Your Assessment

A security assessment is only a first step. Once the assessment is complete, you'll have a good idea of what to do next.

Start by reviewing the reports prepared by your assessor. Next, meet with the assessors to discuss their findings. This will also be a chance to ask any follow-up questions or get clarification on any of the findings.

Next, bring the findings to relevant members of your management team and to the right staff. Work with them to start developing a plan of action. It makes sense to start with low-cost items that you can implement quickly, but this is also the time to start planning for harder, more expensive, longer-term projects.

For long-term planning, you may have your local IT teamwork with the assessor to develop technical and operational solutions. As you take on more complex, long-term projects, track your progress and employ project-management strategies to make sure you are headed towards your goals and following the advice of your assessors. This may also include things like directed fundraising or changes to your planned budget.

Funding Through LSC

Overview

LSC offers Technology Improvement Project (TIP) Grants. These grants fund technology related assessments, including an IT security audit. The maximum amount for funding is $35,000 if the project includes an IT security audit. Funding generally covers 12 or 18- month projects. Some offices have worked with general TIG applications before; TIP applications are shorter and simpler than full TIG application. TIP applications do not include a pre-application or invitation requirement.

Eligibility

To be eligible for a TIP grant covering assessment, your office must be current LSC Basic Field-

General, Basic Field-Migrant, or Basic Field-Native American grant recipients. Your office also must be up to date according to milestone and payment schedules on any existing TIG projects before starting a TIP project.

To Apply

Applications are available in GrantEase, LSC's online grant management system.

- 2021 Application Guide
- Video Tutorial
