

# Cybersecurity Risk Assessment

## CDW-G's Five Steps to Cybersecurity Risk Assessment

Organizations face a constant barrage of cybersecurity threats. Botnets, malware, worms and hacking are just a few things that keep IT managers awake at night, wondering if their network is safe and strong enough to deflect the next attack. Rather than reaching for a sleep aid to get through the night, organizations need a coherent methodology for prioritizing and addressing cybersecurity risks.

Here's one for the taking.

Too many organizations either suffer from a "security paralysis," in which it is impossible to prioritize areas for remediation with their limited resources, or attempt to apply a few "best practices" in the hope that what worked for another organization will work for them. Neither of these approaches is a rational strategy for protecting information assets or maximizing the value returned from investments in security.

While some organizations have the ability or the obligation to engage in a formal risk assessment process, sometimes organizations may want to pursue an assessment internally. CDW-G, a provider of information technology (IT) solutions to governments and education, advises organizations to consider five steps to develop a solid foundation for the organization's security strategy. These steps are ideal for organizations requiring simple guidance on getting started. Organizations are also encouraged to invest the time and effort into developing meaningful results, as well as understanding any existing risk assessment requirements.

CDW-G's team of technology specialists and systems engineers provided these general steps, based on their experience and expertise in evaluating and designing technology solutions for government agencies, educational institutions and healthcare facilities.

To get started, organizations need to bring together decision makers from across the organization. A group of five to seven people works best, but the goal is to have all departments represented (e.g. IT department, finance department, program offices):

- ✓ **Identify information assets** – Consider the primary types of information that the organization handles (e.g., social security numbers, payment card numbers, patient records, designs, human resources data), and make a priority list of what needs to be protected. As a guide, plan to spend no more than one to two hours on this step
- ✓ **Locate information assets** – Identify and list where each item on the information asset list resides within the organization (e.g., file servers, workstations, laptops, removable media, PDAs and phones, databases)
- ✓ **Clarify information assets** – Assign a rating to your information asset list. Consider a 1-5 scale, with the following categories:
  - 1 – Public information (e.g., marketing campaigns, contact information, finalized financial reports)
  - 2 – Internal, but not secret, information (e.g., phone lists, organizational charts, office policies)
  - 3 – Sensitive internal information (e.g., business plans, items subject to non-disclosure agreements)
  - 4 – Compartmentalized internal information (e.g., compensation information, layoff plans)
  - 5 – Regulated information (e.g., patient data, classified information)

This classification scheme enables the organization to rank information assets based on the amount of harm that would be caused if the information was disclosed or altered. The team should strive to be realistic here, and aim for consensus.

- ✓ **Conduct a threat modeling exercise** – Rate the threats that top-rated information assets face. One option is to use Microsoft's STRIDE method, which is simple, clear and covers most of the top threats. It is also worth considering using an outside consultant with experience in this area to facilitate conversation. Develop a spreadsheet for each asset, listing the STRIDE categories on the X axis:

**STRIDE:**

Spoofing of Identity

Tampering with Data

Repudiation of Transactions

Information Disclosure

Denial of Service

Elevation of Privilege

On the Y axis, list the data locations identified in Step 2. For each cell, make estimates of the following:

1. The probability of this threat actually being carried out against this asset at the location in question

2. The impact that a successful exploitation of a weakness would have on the organization

Use a 1-10 scale for each of the above (e.g., 1 is "not very likely" or "this would not have a large impact," 10 is "quite probable" or "catastrophic"). Then multiply those two numbers together and fill them into the cells. The spreadsheet should be populated with numbers from 1 to 100. This activity will likely take a full day for smaller organizations and several days for larger ones.

- ✓ **Finalize data and start planning** – Multiply all the cells in each of the worksheets by the classification rating assigned to the asset in Step 3. The result is a rational and comprehensive ranking of threats to the organization. It includes both the importance of the assets at stake and a broad spectrum of possible contingencies. A reasonable security plan will start tackling the risks identified with the highest numbers.

Many organizations set thresholds as follows:

1-250: Will not focus on threats at this level

250-350: Will focus on these threats as time and budget allow

350-450: Will address these threats by the end of the next budget year

450-500: Will focus immediate attention on these threats

These thresholds are just examples, and in practice, the results will likely be skewed either towards the top or bottom of the scale, so organizations should adjust responses accordingly.

The goal of the risk assessment exercise is to lay a foundation for sensible security planning. Going through a risk assessment exercise alone will not actually fix security problems; the real work – building protective, risk-reducing solutions – still lies ahead.

CDW-G recommends that organizations align security spending with specific threats and to focus on cost-effective measures. Having a prioritized list of threats enables organizations to focus their efforts on the areas that matter most and avoid spending on security technologies or activities that are less essential or irrelevant to fixing identified problems.

Source: *CDW Government*

