HOW TO PERFORM
A Cybersecurity Risk Assessment

Cybercrime cost Americans **$6.9 billion** in 2021, according to an FBI estimate, while the worldwide damage is projected to be more than **$10.5 trillion by 2025**, according to Cybercrime Magazine. With the increase in remote work and virtual meetings in the wake of the COVID-19 pandemic, businesses are more vulnerable to attack than ever.

Every organization—large and small—should have a strategy for protecting its digital assets. But before you can develop an effective cybersecurity plan, you need to perform a thorough, company-wide risk assessment.

ASIS

ABOUT ASIS INTERNATIONAL

ASIS is a global community of security professionals who collaborate and share learnings to advance security worldwide. Our 34,000 members range from entry-level managers to CSOs and CEOs, spanning all industries, including healthcare, banking, cybersecurity and more. ASIS brings together practitioners entrusted with protecting assets of every kind to connect across sectors and discover powerful partnerships. Begin building your network when you join the ASIS community.

STEP 1: DETERMINE INFORMATION VALUE

Audit your organization's data and see how valuable it is to competitors, criminals, and the organization itself. Calculate both short- and long-term impacts of data loss or leaks, including legal penalties, loss of productivity, and reputational costs.

STEP 2: IDENTIFY AND PRIORITIZE ASSETS

Work with management to determine the value of each asset and classify them based on their importance—mission critical, major, or minor.

STEP 3: RECOGNIZE THREATS, AND VULNERABILITIES

Criminals aren't the only threats to data security. Consider the likelihood of events like natural disasters, hardware failure, and user error, in addition to attacks like malware and phishing.

STEP 4: MINIMIZE THREATS AND VULNERABILITIES

Examine the controls that are in place and implement new ones as necessary. Evaluate both technical controls like encryption and authentication methods, as well as nontechnical controls like security policies.

STEP 5: ASSESS PROBABILITY OF RISK AND POTENTIAL IMPACT

How susceptible is your organization to an attack? Is your organization in an area prone to natural disasters? Think about how likely or often a scenario might take place, and the impact if or when it happens.

STEP 6: EVALUATE RISKS AND RECOMMEND CONTROLS

Resources are limited, so it is important to weigh the cost of prevention against the value of the asset involved. Categorize risks from high to low, with the most urgent ones requiring immediate action.

STEP 7: DEVELOP RISK ASSESSMENT REPORT

Create a report that details the value, risks, and vulnerabilities of each threat, and share it with management. Stakeholders will be more likely to follow through on your recommendations if they understand the likelihood of the threats and their potential cost.

LEARN MORE TODAY AT ASISONLINE.ORG