11 Benefits of a

RISK ASSESSMENT

INNOVEX

In simplest terms, a risk assessment helps an organization to strengthen its security. But this in-depth evaluation offers many more specific benefits that prove invaluable to any organization.

Here are 11 benefits of a risk assessment, for the company, for the IT group, and for everyone:

Identify security vulnerabilities — A risk assessment will evaluate an organization's system by considering external as well as internal threats. In doing so, a risk assessment will identify current security vulnerabilities, inefficiencies, and noncompliances with standards for security policies. This benefits an organization by clearly creating a list of specific security problems and stating which problems are of the highest risk.

Determine new security requirements — With an understanding of an organization's weaknesses, a risk assessment can next determine what steps must be taken to eradicate these identified weaknesses and strengthen the system's security.

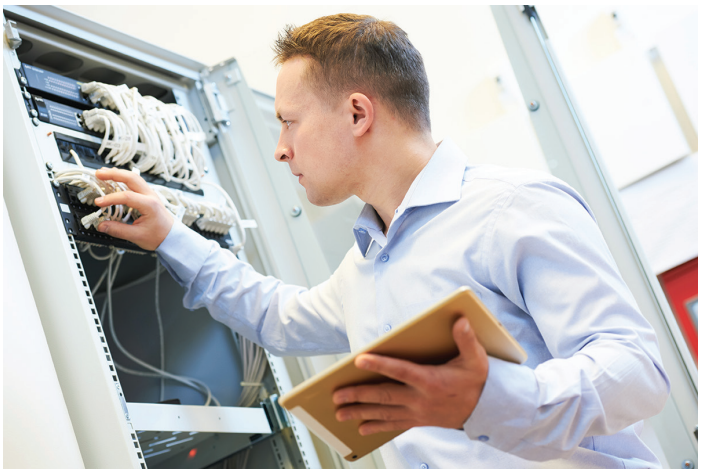
Justify spending — The details of a risk assessment can help an organization to understand the financial risks of potential security exploitations. Also, a risk assessment can help to calculate the costs of security improvements and express the long-term financial benefits of investing in security efforts before an attack.

Make smart purchases — The information a risk assessment provides can help an organization budget for security appropriately. Once aware of its current weaknesses, an organization can allocate resources for the solutions. For instance, the details of risk assessment can help prevent an organization from overspending on a problem that does not require an expensive solution.

Improve planning — An organization must understand its current security risks in order to plan the architecture of its network for the future. Thus, the strengths and weaknesses identified by a risk assessment provide valuable help to an organization's development of new security plans and policies.

Document due diligence — Finally, a risk assessment and resulting remediation can also validate an organization's efforts to enforce proper security measures. They may act as evidence to government regulators, insurance companies, business partners, and the like that you are employing the requisite security to protect your data and network.

Beyond the numerous benefits a risk assessment brings to an organization's security efforts, it also affords specific benefits to the IT group and to the company as a whole.



BENEFITS FOR THE COMPANY

Educated employees — Beyond its security benefits, a risk assessment has the added value of increasing employee awareness of security measures and risks. And this increased knowledge leads to increased efficiencies. For example, employees may be more

likely to use security best practices in daily operations (i.e. avoiding risky activities like disclosing passwords, or learning how to recognize suspicious events).

Increased motivation — The fact that a risk assessment is underway at an organization demonstrates to its employees that security is a significant concern; the company acts like it is and, so, employees must follow suit. Also, with a renewed understanding of the profound impacts of security risks, employees may feel an increased sense of motivation and productivity within their teams.

Improved communication and decision-making — As a risk assessment involves many people, it can help to start a conversation about security and its many risks. Moreover, the detailed information provided by a risk assessment can help to ease decision-making; people within an organization will be on the same page about what the major security threats are to and what needs to be done about them.

BENEFITS FOR THE IT GROUP

Boost productivity — The security assessment, the review of processes, and the plans for improvement, all help an IT group to gain a new knowledge and perspective of their system. By acting as something of a self-analysis, a risk assessment can also help an IT group to plan for future changes in its security efforts.

Help make budget choices — If provided by an outside service, the objectivity of a risk assessment can help an IT group demonstrate to management the importance of spending resources on security measures. Moreover, the information provided can help to estimate the budget required for these security improvements.

A risk assessment will help initiate improvements in an organization's security posture. But it can also bring efficiency to other areas, such as financial planning and company communication.

ABOUT INNOVEX

Technology is at the heart of every business organization. We are the single source developed to support your entire technology infrastructure, from your document systems to your servers — our focus is you.

Whether you use our Technology Products, Managed Services, or IT Professional Services, our integrated offerings simplify your business' operations, giving you the efficiencies you value. We stay current in technology that constantly changes, and are committed to providing you service excellence.

A 50-year-old independent, locally-owned company, we're also one of the fastest-growing companies.* We are here for you now and will be in the future.

*Providence Business News' Book of Lists, 2016

INNOVEX

Your Technology, Our Focus

innovex.tech | Rhode Island 401.232.7000 | Massachusetts 617.903.5300