Information Security Risk Assessment

INDUSTRY BEST PRACTICES TO KEEP YOUR DATA SECURE

Today organizations are shifting from a pure compliance approach to a broader risk-mitigation and data-protection strategy. Prioritizing your organization's most critical assets, their vulnerability and your organization's risk tolerance are essential elements of designing the most effective security risk management program. The Trustwave Information Security Risk Assessment is designed to help you take a holistic approach to your security and compliance process so that you can make the best decisions about capital, resource and regulatory costs, while continuously protecting your organization.

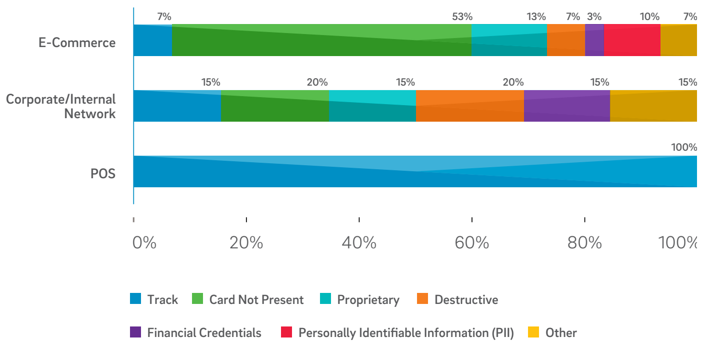
Information At Risk

Information security risk refers to the possibility of business damage due to a loss in confidentiality, integrity or availability of information. As technology advances, information, information storage and delivery mechanisms are more distributed, accessible and complex. High profile data compromises, data loss or misuse, or the inability to access critical information could all lead to unfavorable press and reputation damage. A thoughtfully created and executed cyber security framework, that reflects appropriate risk tolerance, is a fundamental part of an organization's governance structure. This holistic approach to the controls used to protect your organization's information and system assets is the first step in protecting your brand image.

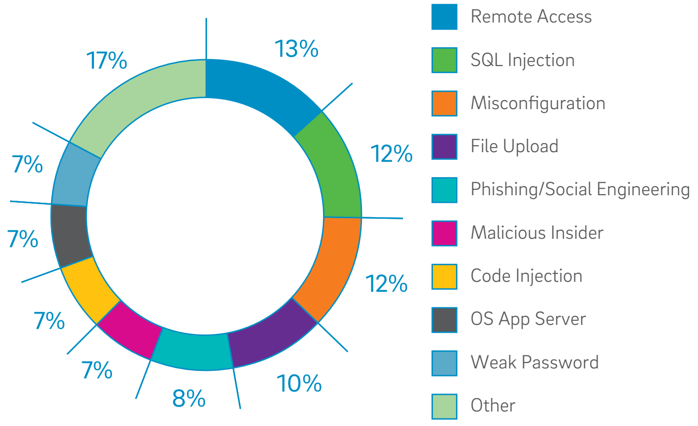
Why Do I Need A Risk Assessment?

Put simply, a risk assessment is the examination of a business's assets, the threats to those assets and the adequacy of the controls in place to protect them from misuse, or compromise. Risk assessments are the foundation of every security best practice and are the first step in the formulation of an effective risk management program. For example, your organization may need to comply with a variety of compliance regimes—such Health Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley, Federal Financial Institutions Examination Council (FFIEC) and Payment Card Industry Data Security Standard. A risk assessment is the foundation for the business actions you will take to achieve compliance with these mandates.

Types of Data Targeted



Method of Entry



Source: 2016 Trustwave Global Security Report

A Strategic Opportunity

For an enterprise faced with multiple compliance requirements as well as the changing security needs of the business, risk is both a four-letter word and an opportunity. Risk assessments serve as the foundation for a strategic approach to marrying business goals with security and compliance requirements while helping to create an effective long-term risk management program.

The Trustwave Information Security Risk Assessment is right for any organization looking to assess their security risk posture and develop a risk management framework for tailored objectives.

With our experience and expertise in completing risk assessments, tailored for businesses of all sizes, Trustwave is the right partner to help you assess — and address — your vulnerability to existing and evolving threats.

How Do We Get Started?

The biggest challenge for organizations is figuring out where to begin. Trustwave's Information Security Risk Assessment simplifies this effort with our expert consultants who help take an organization of any size through each phase of the process with the proven Trustwave methodology. The resulting assessment findings provide the basis to build or refine the most appropriate information security program for your organization. Trustwave consultants will determine the best methodology assessment framework for your business, customized to your specific business goals.

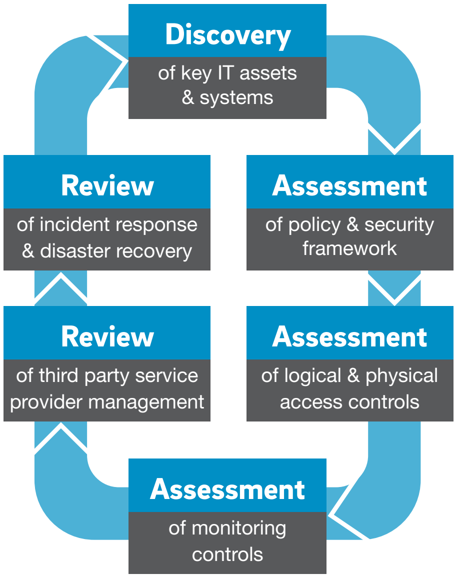
Trustwave's Approach

The goal of the assessment is to identify key IT security deficiencies that put your business at risk and translate your assessed IT risks into business saving decisions. Trustwave consultants have unparalleled experience assessing organizations' security controls. The assessment takes your organization through three steps:

Discovery A risk assessment begins with a clear understanding of the business goals, potential threats, likelihood of compromise and the impact of the loss. This is achieved with a comprehensive interview process involving all aspects of the organization; such as senior management, IT administrators and key stakeholders.

Assessment Once the threat landscape and business risk appetite is clearly defined, the current security posture must be determined and the security gaps exposed and documented.

Remediation Armed with the assessment information in-hand, our experts can provide proactive guidance on the best security controls to mitigate your business risk. These can include a combination of technology, policy, process and procedure.



Discovery of key IT assets & systems

Assessment of policy & security framework

Assessment of logical & physical access controls

Assessment of monitoring controls

Review of third party service provider management

Review of incident response & disaster recovery

Business Saving Decisions

Trustwave's risk assessment approach examines both the maturity and ongoing effectiveness of your information security program and security infrastructure through an iterative process of information gathering and vulnerability identification. We will identify the threats and associated vulnerabilities for each of your identified critical assets and determine the severity and impact upon the asset's confidentiality, integrity and availability. With this information in hand, we can determine your current level of risk and recommend the appropriate and necessary safeguards. Your risk assessment can become a strategic turning point for your organization's approach to data security and risk mitigation to protect your business daily.

For more information: www.trustwave.com