QUALIZEAL

Cybersecurity Assessment and Testing - Identifying the Hidden Vulnerabilities in Your System

Preface

"As the world emerges out of the pandemic pause, the needs and expectations of businesses change, too. There will be new business objectives across the enterprise after the crisis that will require IT to adapt to new technology roles and develop new skills."

- Gartner

Post the advent of the global COVID-19 pandemic, digitization has metamorphosed the way we view and experience the world. Several enterprises, irrespective of their size, are rooting to turn themselves into a digital-first organization to not just stay one step ahead in the competitive landscape, but also deliver immense value to their customers.

In fact, according to the PwC 2022 AI Business Survey, 52% of enterprises have accelerated their AI adoption plans because of the global pandemic, and a survey by The AI Journal entitled "AI in a Post-COVID-19 World" revealed that almost close to three-quarters of business leaders (72%) feel positive about the role that AI will play in the future.

While digital expansion has been phenomenal over the years, the measures for security have also hit a vulnerable spot. Furthermore, the pandemic has also paved the way for cybercriminals, hackers and spammers to penetrate into the IT infrastructures as enterprises pit against each other in automating and digitizing their processes.

There have been ground-breaking advances in terms of rapid adoption of emerging technologies such as Artificial Intelligence, Machine Learning, IoT, and automated botnets. However, with several intrusions and penetrations of new technologies, it is only adding more to the dynamic cybersecurity challenges.

In case you're wondering how to identify and mitigate the hidden vulnerabilities in your system, cybersecurity assessment and testing is your go-to process that will make your IT infrastructure truly impermeable.

Here, we will explore in detail about:

- What is Cybersecurity Assessment and Why Should It Be on Top of Every Organization's IT Strategy?
- The Different Types of Cybersecurity Testing
- The Importance of Cybersecurity Testing in Preventing Cyber Attacks
- How to build an Actionable and Sustainable Cybersecurity Strategy?
- How Can QualiZeal Help in Making Your IT Infrastructure More Robust?

What is Cybersecurity Assessment and Why Should It Be on Top of Your Organization's IT Strategy?

Cybersecurity Assessment deals with the process of evaluating security measures of an organization to scrutinize the enterprise's overall security infrastructure. This process entails validating the organization's preparedness in terms of known and unknown vulnerabilities, attack vectors in the digital spectrum, and business processes.

Before getting down to the nitty-gritty details of why having a cybersecurity assessment on top of your priority list, let us take a look at some alarming facts.

- According to the 2019 Global Risk Data Report by Varonis, only 5% of company's folders are properly protected.
- As per the data by Emisoft Malware Lab, Ransomware cost US Local Governments more than a whopping $623 million in 2021.
- According to Coveware's Q3 2021 Ransomware Marketplace Report, the average downtime due to a ransomware attack was 22 days, in comparison with 19 days in Q3 2020.

It is imperative that cybersecurity testing falls on the top of an enterprise's priority list in order to lower the risk on the attack surface, and also help track the systems, applications, and network flaws. Furthermore, it also aids in devising appropriate defensive controls and helps keep all the policies and security guidelines in check.

That being said, cybersecurity assessment is not a one-size-fits-all. The scope of cybersecurity assessment varies from business to business based on various factors. For instance, the nature of business, its objective, the organization size, and the compliance that the business adheres to can be some of the many factors. With a customized assessment strategy, an organization will be able to not just spot its cyber strengths and weaknesses, but also help you devise a strategy to prioritize and solve them.

It is important for organizations to foster their business with proper security measures and get a holistic understanding of risks and threats by evaluating a few crucial components:

- Current assets
- Business compliance
- Vulnerabilities in the assets
- The Attack Surface
- Potential threats and risks on the assets.
- The Assets' cyber resiliency

Cybersecurity testing can either be done internally by hiring a specialized cybersecurity team or by hiring a third-party team of experts. We, at QualiZeal understand that every organization's cybersecurity strategy is unique and we utilize our expertise to assist businesses securing their environment according to their niche, requirements and demands, and we follow a thorough, systematic, and customized approach.

The Importance of Cybersecurity Testing to Shield Your Organization from Cyber Threats

When you look back at history, right from when Robert Morris launched his infamous worm to cause a complete shutdown of the network at the Massachusetts Institute of Technology (MIT), there have been a whopping 5.4 billion ransomware attacks, and this number is just in 2021 (Source: Statista).

Before we get down to the nitty-gritty details discussing the significance of security testing, let us first comprehend and understand the most common cyber-attacks that are executed and how it will affect your organization's reputation.

Phishing

This is one of the most basic kinds of cyberattacks that is prevalent to this date. A malicious attacker will send an authentic-looking email which could include a link, if opened will guide to a different website where the hacker can steal your organization's sensitive data and information.

SQL Injection

In this case, more often than not, the attacker has identified an organization's SQL vulnerabilities and will try to exploit them, thereby making the SQL server run a questionable query to get access to user information.

Malware

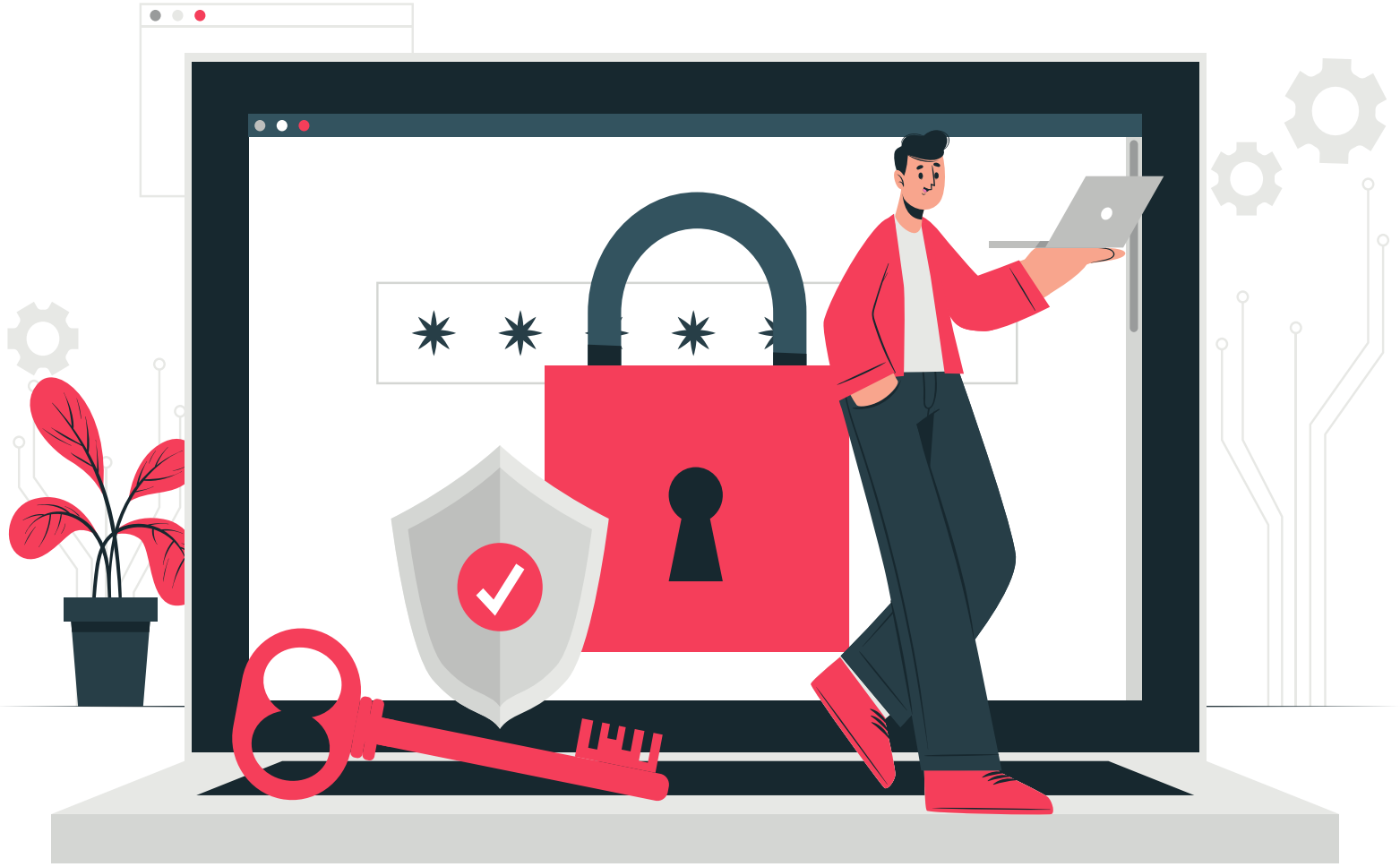
A malware involves a cluster of cyber threats, and this list includes (but not limited to) trojans, viruses, and worms, and your system can be easily susceptible to these attacks by introducing them through software downloads, exploiting operational vulnerabilities or even email attachments.

Denial of Service (DoS)

In the case of DoS attacks, the attacker would try to completely disrupt the entire network of your organization by sending humungous volumes of traffic that would eventually get overloaded, resulting in a total collapse.

The four kinds of cyberattacks mentioned above are just a scratch on the surface, and we have to acknowledge that considering the alarming number of cyberattacks that happen every year, it is crucial to take the necessary steps to ensure that these attacks don't happen to your organization. This is exactly where the significance of cybersecurity testing lies.

In order to make sure that you build an impenetrable digital fortress to protect your IT infrastructure, security testing must be a mandate, irrespective of the organization's size. When your infrastructure is put under a microscope, you don't just identify the weakness and technical flaws, but you can also identify the vulnerabilities and subsequently repair them.



The Different Types of Cybersecurity Testing and How to Zero Down on The One for Your Organization

There are several types of assessments in the cybersecurity domain. Each type has its own uses and scope that would aid in reduction of cost breaches and help fine-tune your IT infrastructure's defense capabilities. It is an undeniable fact that we live in an era of highly sophisticated and pointed cyber-attacks that irrespective of the organization's size, it is one of the most important steps to invest in cybersecurity to mitigate risks and enhance overall resistance.

Here are some of the most common types of cybersecurity assessments, each type with varied approaches that serve a plethora of objectives, with the one common goal being: prevention of cyber-attacks. Following is the list of some of the distinctive scope-driven cybersecurity testing types.

Vulnerability Assessment:

One of the most oft-beat cybersecurity assessments conducted in the industry, Vulnerability Assessment is an automated method of testing with a restricted scope, specifically to identify security bugs or flaws present within the assets. Assets, in this context, can be applications, networks, infrastructure, codes, or anything that is a crucial aspect of your product depending on the assessment's objective. After running the test, the flaws are categorized based on the impact that they could have on a business's bottom-line.

Penetration Testing:

Penetration testing entails the further scrutinization of the categorized flaws found in the vulnerability assessment. It is a deeper testing methodology to exploit the vulnerabilities to test the security posture of an organization through the eyes of an attacker. The categorized bugs are further pitted together or used as a standalone flaw to analyze how the organization can be hacked if an attacker spots the open vulnerabilities.

More often than not, this test is used as a proactive identify and measure the security gaps and stay in-line with the already established compliances and regulations.

Compromise Assessment:

This kind of testing is often conducted by reviewing the infrastructure, the connected end-point logs, the traffic, and the activities to discover Indicators of Compromise (IoCs). This is a more sophisticated and high-level security testing that is done to track down the attacker who has either been active in the recent past or even someone who is currently accessing the environment.

Furthermore, a compromise assessment may also be conducted in the case of mergers and acquisitions to ensure that all the industry-specific compliances and regulations are met.

How to Build an Actionable and Sustainable Cybersecurity Strategy?

> It takes 20 years to build a reputation, and a few minutes of cyber-incident to ruin it.
>
> — **Stéphane Nappo**, VP – Global Chief Information Security Officer, Groupe SEB

With the overwhelming rate of cyberattacks happening day in and day out, strategizing and implementing a robust cybersecurity plan is no longer an option, but a necessity. Having a cybersecurity strategy in place will help extend protection against any attack in the organization. Furthermore, a well-thought out, actionable and measurable plan will enable timely detection of risks and breaches that would allow the organization to react and tackle effectively.

However, the billion-dollar question is, "how to effectively build and implement it?"

While the strategy in itself will vary from business to business, here are a few things that you need to know and will get you started.

Get A Holistic View of Your Current IT Infrastructure

You will have to get started at the bottom to thoroughly understand where you stand in terms of risk tolerance and other prevention capabilities. A good way to go about this could be to start with mapping the unique attributes of your organization onto a risk assessment framework. Doing this will help you identify and categorize your processes based on their level of vulnerability to cyber-attacks.

Create a Bi-Directional People Alignment Approach

A bi-directional people alignment approach will help you serve two purposes: 1) To involve the top management and stakeholders and make them understand the significance of investing in top-notch cybersecurity measures, and 2) To convince your other staff members to incorporate the best-in-class security practices to avoid any malicious attacks.

In simpler terms, it is absolutely essential that employees at every level of the organization are aware of cybersecurity policies. This is because most cyber-attacks spawn off because of careless workers, inside agents, disgruntled employees, and third-party users.

Set Your Metrics

Once you are done with your risk assessment, you will be able to identify the most valuable and critical business processes that are significant enough to cause an impact in the case of a breach. Furthermore, you will also be able to spot the areas that require specific focus in terms of security. This method will let you have a 360-degree, holistic view of your entire IT infrastructure, and will aid you in determining where you need to allocate your cybersecurity budget.

That being said, a strategy without any measurable outcomes is like walking blind in the middle of a dense forest. Establish the metrics that are critical, and for starters, you can conduct a comparative analysis between Key Risk Indicators (KRIs) and Key Performance Indicators (KPIs).

Doing this will help you in eliminating bottlenecks by removing ineffective processes, and will thereby improvise your strategy.

Lastly, Avoid, Accept, Mitigate, and Transfer

Avoid: As much as possible, most of the cyber-attacks can be avoided if the organization avoids doing certain activities that could compromise their cybersecurity framework.

Accept: For minor risks that have already been identified, it is a wise decision to deal with them then and there, rather than wasting valuable resources on something so insignificant

Mitigate: It is advisable that you reduce the impact caused by critical risks by mitigating the chance of their occurrence.

Transfer: It is always prudent to distribute ownership equally among employees so each of them knows their responsibilities in case of a security breach.

How Can QualiZeal Help in Creating a More Robust and Streamlined IT Infrastructure?

With the ever-changing technological landscape, cyber-risks are also evolving simultaneously. In case your organization is still using the outdated maturity-based model, it is a necessity that you shift to a risk-based approach.
Cybersecurity assessment and testing must be conducted rigorously and continuously with a pronounced emphasis on the high-risk areas.

A recent study by Deloitte states that the alarming increase in cyber threats is directly related to the rapid digital transformation wave that organizations are undergoing after the global pandemic. This, in turn, contributes to the readiness of several organizations to pay ransoms to keep their business running.

In fact, according to the Internet Crime Report 2021 by the Federal Bureau of Investigation, ransomware attacks will focus more on critical infrastructure, as governments steer their interests in the digital transformation of various divisions such as the public health sector, food and agriculture sector, commercial facilities, and even in the manufacturing sector.

Shockingly enough, there has also been a rapid increase in the penetration of Ransomware-as-a-Service (RaaS) over the past 18 months and is predicted to double its growth in the coming years. RaaS is operated as a business model by the cyber-attack groups wherein malicious solutions are made easily available to criminals.

These insights into cyber-attacks and how organized these units are performing these crimes are just a scratch on the surface. And while your organization is undergoing this rapid digital transformation phase, you leave your IT infrastructure more susceptible to such malicious attacks.

Our team at QualiZeal have decades of knowledge and expertise in the cybersecurity assessment and testing space and we serve varied business-specific niches. We are industry-agnostic, and our adept team has the experience and capability to serve across a spectrum of industries, verticals, and organization sizes.

Equipped with robust security testing methodologies, our process transcends beyond just uncovering the vulnerabilities in your applications, but also ensures that any potential risk is mitigated. Want to avail our services? Schedule a Meeting with us today!