# THE IMPORTANCE OF PERIODIC SECURITY ASSESSMENT

Every company is a target today, no matter what kind of business it does. Hackers and cybercriminals are after data, which they can monetize in several ways. As usual, it pays to be proactive and have a preventive plan in place – periodically assessing IT security is a great recipe for avoiding data breaches and consequently business disasters.

Would you fly on a plane that hasn't had its regular safety inspection? Or take a long trip with a car that looks like it came from the junkyard? You wouldn't. But how does this relate to IT, you ask? Maintenance is important, and security plays a big role in maintaining your IT environment sharp. An IT assessment is much more than just a great mechanic – it takes on the role of the engineers who helped design your vehicle.

IT never stands still; it is constantly evolving, and becoming very complex, as a result. As an organization's IT infrastructure changes over time, it can develop a few cracks in its shell. Those are called vulnerabilities. More so, attackers are inventing new methods of attacks that target these vulnerabilities. Therefore, your IT environment might have been secure yesterday, but today and tomorrow are another story.

Having an independent expert occasionally check for possible "IT cracks" and blind spots can save you a lot of trouble down the road. Sure, you can have your own personnel perform a security check, but this has proven ineffective many times over. Security professionals think like hackers, have vast expertise and experience, and they look for cracks where internal staff wouldn't even imagine.

## The cost-effective journey to optimal security

A security assessment could be the first step on a cost-effective journey to optimal security. Let's be honest – there is no such thing as bulletproof security when it comes to IT. Security is always a compromise. And companies that only address it from the cost part of the equation usually skip the long-term implications of not taking care of data in the right way.

Security can be cost effective as well. You don't need to purchase new devices every few months – the goal is to correctly configure your existing security solutions so they can effectively protect your IT environment and data.

In order to do so, NIL's security experts will perform a security assessment and deliver a detailed evaluation of your IT environment so your team can take care of the holes that might lead to data leaks. As with chains – your IT security is only as strong as its weakest link.

## The right approach is crucial

When thinking about security, it is necessary to have a comprehensive approach. You need to take into account every aspect – from your security policies, web, application, SCADA/industrial systems, network design and firewalls, to your employees. And don't forget that you need to think about security at every stage of your IT lifecycle.

There are simply no shortcuts when dealing with IT security. Not just looking into all areas of potential risk, also performing the assessment in the right order, with the right methods and tools, is very important. Only a complete security assessment is a valuable one.

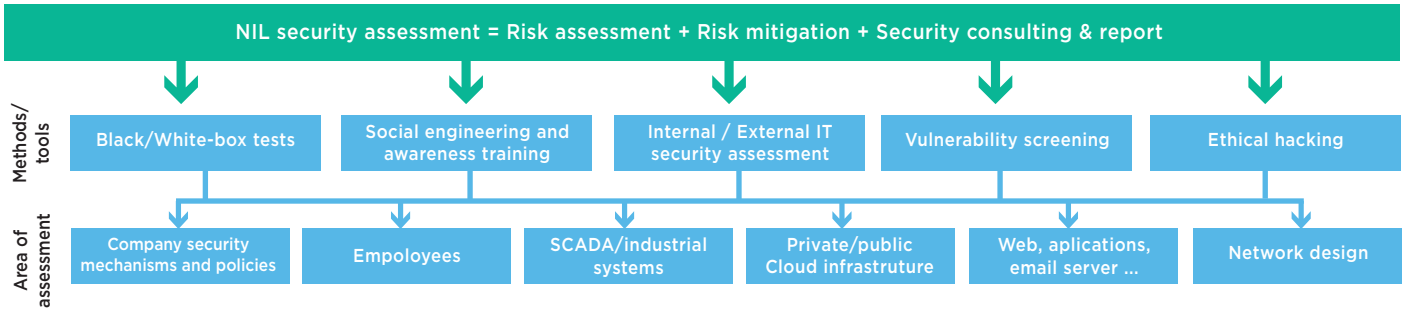
NIL

## GOALS AND STEPS OF THE ASSESSMENT

1. Pre-test phase of discovery and collecting the information about the target system and services.
2. Automated vulnerability scanning with the goal of narrowing the scope of subsequent manual tests.
3. Manual validation test executed and focused on vulnerable areas from step 2 – selective methods provide credible elimination of "false alarms", which are typical for the previous steps of detecting vulnerabilities.
4. Analyzing the risk information and mapping it with the business environment and processes – tracking where threats and vulnerabilities are occurring.
5. Assessment of security risks, consequences of abuse, and complexity of risk/vulnerability, and elimination of false risks.
6. Detailed report of tests, observations, and risks with recommendations on how to address them.
7. Presentation of the report.

**At NIL, we deliver.** After the conclusion of the assessment, you will be provided with an in-depth summary and a detailed technical report with identified security threats. Included in the report will be recommendations on how to cost-effectively protect your IT environment.

## Assessment methods, tools, and potential risk areas




## What should you know before choosing a security assessment expert?

Not every vulnerability poses a big security risk — they have different roles in business (processes). When choosing a security assessment expert, your key criterion should be professionalism. Keep in mind that great security assessments come from vast experience and knowledge, therefore the service provider needs to employ several security experts.

As with doctors, when dealing with security, you should go with experts. And, please, do not let the price play the major role when selecting the provider of the service – the best security assessment cannot be the cheapest.

## The questions you should answer before deciding on a security assessment expert

- Can the provider deliver proof of managing modern and complex IT infrastructures, preferably in your vertical (banking, e-commerce, government ...), and not just possess a specialized security assessment and audit certification?
- Who is part of the provider's assessment team? What security certifications/specializations do these people have?
- To what extent will the provider's assessment team collaborate with your own IT experts?
- What kind of reports and results can you expect from the provider?
- Will the report enable you repeat/resolve any issues on your own?