1. The Cyber Attack Simulation and Modeling

WOULD YOUR CLIENT AFFORD NOT TO?

2. Is your client`s confidential data secured?

3. COULD THE PUBLICLY-ACCESSSED INTERNET RAISE ANY SECURITY ISSUES FOR YOUR CLIENT?
As a unique Information Security provider, Cipher Security is committed to provide outstanding results regardless of the challenge complexity that an organization may face. Our fast, flexible and light footprints services may become one of the successful keys for your future market growth.

ARE YOU READY TO BOOST YOUR BUSINESS SUBSTANTIALLY BY OFFERING AN EXCEPTIONAL SERVICE TO YOUR CLIENTS?

The paper is focusing on the necessity to perform such an assessment in today’s global communication network reality and is helping the IT integrators, IT suppliers and Professional Services providers to better understand the compulsion of performing this process in all business areas.

The overall aim of this paper is to provide a comprehensive overview of a promising business growth channel – The Cyber Attack Simulation and Modeling service.
What is a Cyber Attack Simulation and Modeling service?

The Cyber Attack Simulation and Modeling service is an information security-related assessment demonstrating the cyber threats an organization is facing by an external offensive factor, as a part of the organizational risk management process.

During this test, an information security expert will try to infiltrate in the internal organization infrastructure from the publicly-accessed internet while being remote, unauthenticated, unauthorized (IT-wise) and undetected. The security expert has no prior knowledge or setup related to the target organization, acting from what is known as Black Box approach. The test is performed from “outside” the organization; in a similar manner an actual attacker would exercise the attack. Having limited information regarding the network infrastructure, the security expert will gather information from accessible resources, as attempting to safely gain access to the IT infrastructure.

This test offers precise insights about the external exposure of the organization confidential information and internal data via IT infrastructure, exposed systems and data files while demonstrating which security breach could eventually be used by a malicious source to gain competitive advantage.

Now you can help your clients to outplay their competition or other malicious factors attempts. By offering this service to your current and future prospects, you step on the secure path of becoming a trustable professional services provider. Leveraging the Cyber Attack Simulation and Modeling promotes and boosts your co-operation with your clients one step ahead your competitors. This unique service offers the most cost-effective win-win situation and it constitutes a decisive channel for growing your business.

DID YOU KNOW?
The first widely spread Internet worm, the Morris Worm, was written and set loose in 1988. It may have infected about 10 percent of all computers on the Internet. Although the Morris Worm was highly disruptive to the usability of the Internet, it didn’t disrupt business overall, because few businesses used the Internet for business transactions.

(Stopping Zero-Day Exploits For Dummies, 2014)

Victorious warriors win first and then go to war, while defeated warriors go to war first and seek to win
- Sun Tzu

The essence of Strategy is choosing what not to do
- Michael E Porter

However beautiful the strategy, you should occasionally look at the results
- Winston Churchill
First, the security expert discovers the target by gathering information from the publicly-facing organization interfaces. This stage consists mainly in the setting the goals, the reconnaissance and the discovery steps. After setting the objectives of the assessment, the security expert starts the search in the attempt of finding out as much as possible about the company and the System Under Test, in the quest of potential weaknesses.

Cipher Security is liable for the client data integrity as it uses US GOV best-practices for data protection. Although we have performed thousands of tests in all business areas, we have a perfect track-record of providing safe, secure and successful test. We consider our client’s service availability and data integrity as our most important objectives.

In the second phase, the security expert gains access to the system, with the aim to precisely determine which data could eventually be exposed if a real attack would occur. Using proprietary tools and work methods, the Cyber Security expert will gather evidences of the exposed data, while actively removing any potential risk might associate to such an act. As Cipher Security use the industry-top and US GOV best-practices all along the assessment, our Code of Standards guarantee exhaustive data integrity.
The third phase of the test is the reporting phase, in which the conclusions of the Cyber Attack Simulation and Modeling test constitute the basis of a written report. The successful and unsuccessful penetration vectors and the security failures that allowed to the external factor to intrude in the internal infrastructure are accurately described. The report contains detailed references concerning the level of associated risk of the discovered security failures. This report will also include some actionable elements, whose immediate application will help the organization to improve its security robustness. The findings are presented in explicit and coherent way, allowing the clients’ team to effortlessly and clearly understand the identified issues and the remediation suggestions. However, if a direct communication situation would eventually be demanded, Cipher Security will happily assist your company in the discussion with your client.

The most important aspect of the Cyber Attack Simulation and Modeling assessment is that at all phases and in any given stage there is absolutely zero data exposure risk for the tested organization. As the clients’ data integrity is Cipher Security highest priority, all the steps are performed under supreme cautionary actions, excluding even the slightest potential risk for the client. All the Cipher Security internal procedures are designed and created in respect of the governmental agencies best practices. For the evidence gathering phase Cipher Security is using secure and encrypted channels of communication, using DLP best-practices and perimeter security best-practices.

During the assessment time, that generally takes about one week, our security experts will keep an open communication channel with client point of contact and will keep him update on a constant basis.

WHAT A CYBER ATTACK SIMULATION AND MODELING IS NOT:

The Cyber Attack Simulation and Modeling is not once in a lifetime test. It provides a snapshot about external exposure at one precise moment. Depending on the organization security requirements, it should be performed on a regular basis.

The Cyber Attack Simulation and Modeling does not guarantee the complete information security. This test should be combined with internal penetration tests and other information security services in order to increase the level of protection.
Why do we consider the Cyber Attack Simulation and Modeling service “a must” service?

We live in the information Era. Unfortunately, it is also the competition Era. It is almost impossible for an organization today to function properly without the absolute privacy of its internal information, therefore it is critical to identify and control any possible threats that might come from external factors, such as business competitors or malicious factors.

Today, millions of organizations and billions of people solve their issues, regardless of the issues nature, using the internet. Unfortunately, malicious factors are also using this global network in order to satisfy their own motivations. The studies show that cybercrime is increasing year after year in intensity and in advanced used technology.

In 2014, the cybercrime was up 10.4% if compared with the cybercrime in 2013.

A data breach report for 2014 illustrates how the breaches, especially the hacking activity, increase in the last 10 years.

![Number of breaches per threat action category over time](chart.png)
No matter if the malicious factors are interested in financial gain, industrial, military or political espionage or different types of hacktivism, the threats are menacing every single internet user, individual or powerful multinational organization. The cybercrime evolved as fast as the internet did and looks like the battle became a never ending competition about who is a better computer user.

***

To name two recent resounding data breaches that demonstrate the power of the malicious factors, we cite the cyber attacks over two of the largest players in the US health industry, namely Premera Blue Cross and Anthem Inc. Frustrations and high concerns landed in an instant above each of the companies customers when they found out that their personal, financial and medical data have been exposed. In the attempt of reducing those concerns, one of the major healthcare providers and health insur er, Premera Blue Cross, made available two years of free credit monitoring and identity protection services to anyone affected by the 2015 data breach incident. Can you imagine the costs of 2 years of identity protection and credit monitoring for 11 million customers?

---

**SO ASK YOUR CLIENT**

What would it cost your organization if you face a data breach?

Can you anticipate how could be affected the image of a bank being cyber-attacked?

---

**IF YOUR CLIENT ASKS**

Would we lose customers if there was a security breach in our organization?

*the answer is surely* YES.
Bridge the gap of a strategic business growth by offering your clients the Cyber Attack Simulation and Modeling Service.

The statistics are even more concerning. Two studies, presented below, illustrate how the motivation of the cyber attacks changed in the last decade. It might look like a good sign the fact that the trend line of financial breaches is obviously decreasing, but actually it is the other way around if we look at the figures; the number of espionage breaches significantly increase, while the number of financial incidents is still on the top.

---

**FEBRUARY 2015**

The second largest US health insurer Anthem Inc. stated at the beginning of February 2015 that it was hit by a massive cyber security attack and the records of 78.8 million customers were exposed during the “very sophisticated attack”. The information included names, birthdays, social security numbers, addresses, email addresses, employment information, including income data (Reuters).
Premera Blue Cross, one of the major health care providers and insurer in US, disclosed on March 15, 2015 that an intrusion into its networks may have exposed the personal, financial and medical records of 11 million customers. Although the initial attack occurred in May 2014, the attack was discovered only at the end of January 2015.

(www.premeraupdate.com)

Our daily experience is proven by statistics. If couple of years before, mainly the financial organizations were forced to give a top priority to secure their data, now just isn’t so any more. As the espionage incidents are undoubtedly increasing, today any organization has to become proactive in its attempt to keep all the data secured.

The reason why the Cyber Attack Simulation and Modeling service is becoming more and more an absolute necessity today is again validated by the statistical analysis of the confirmed breaches in the last 10 years.

The graphic illustrate how the external threats increased significantly mainly in the last 5 years, while the internal breaches kept a constant, low level.
For the last 5 years, we can see that the external breaches still represent the majority, with more than 80% from the total number of breaches.

The threats are obviously expanding. We, at Cipher Security, believe prevention is better than cure. This is why we have decided to proactively come in our partners’ assistance, by offering a white-label service, absolutely secured and safe.

The Cyber Attack Simulation and Modeling test gives a unique opportunity to all those acting in the field of security to access an innovative business growth channel.
A breaches report from 2014 shows us how do breaches occur.

<table>
<thead>
<tr>
<th>Method</th>
<th>Percentage</th>
<th>Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>Utilized some form of hacking</td>
<td>81%</td>
<td>+31%</td>
</tr>
<tr>
<td>Incorporated malware</td>
<td>69%</td>
<td>+20%</td>
</tr>
<tr>
<td>Involved physical attacks</td>
<td>10%</td>
<td>-19%</td>
</tr>
<tr>
<td>Employed social tactics</td>
<td>7%</td>
<td>-4%</td>
</tr>
<tr>
<td>Resulting from privilege misuse</td>
<td>5%</td>
<td>-12%</td>
</tr>
</tbody>
</table>

As shown, malicious incident numbers are steadily increasing.

For the 2013 year, the statistics mention 1,367 confirmed data breaches and 63,437 security incidents while in 2014 there were 2,122 confirmed data breaches and 79,790 security incidents.

Knowing more about how breaches occur is a secure path in preventing them. This may enhance the overall information security level of your client’s organization and there is no better marketing strategy than having outstanding results that satisfy entirely your client needs. The Cyber Attack Simulation and Modeling test is one-of-a-kind business growth enabler.

You can help your clients to always be one step ahead of the competition and its malicious attempts. By offering this service to your current and future clients, you step on the secure path of becoming a trustable professional services provider, which will undoubtedly bring you also one step ahead your competitors. This unique service offers the most cost-effective win-win situation and it constitutes a decisive channel for growing your business.
BUSINESS BENEFITS FOR YOUR CLIENT

Avoiding a data exposure may save substantial amount of money (estimated 6-7 figures numbers) that otherwise should be used for remediation and notification costs.

Providing comprehensive and elaborated evidence of an organization ability to detect and mitigate risks will lower the security audits costs and may impress the organization clients/customers and contribute in consequence to business growth.

Audit teams may use the Cyber Attack Simulation and Modeling test data for internal regulatory compliance inspections.

The data offered in the Cyber Attack Simulation and Modeling test report increase the awareness of information security’s importance at the highest management level, providing a substantial basis for approval of larger security budgets.

Supports the evaluation of the effectiveness of other security products that the organization is using or is just thinking to implement.

The service may lay the foundations for greater co-operation with your client.
Supports the IT staff in their attempt to precisely identify the real and potential data exposures and allow them to adapt their security strategies to proactively eliminate identified security issues.

The Cyber Attack Simulation and Modeling test is the best prioritizing method for the IT team.

The benefits of performing a Cyber Attack Simulation and Modeling service for you

Being aware of Cyber Attack Simulation and Modeling service’s high economic potential, Cipher Security uses the opportunity offered by this information security necessity and is ready to offer to its business partners an amazing new business growth channel.

We are ready to provide under your umbrella an outstanding Cyber Attack Simulation and Modeling service, being fast, flexible, light footprint and with zero effort on your side.
BUSINESS BENEFITS FOR YOUR COMPANY

Cyber Attack Simulation and Modeling service may represent an amazing business growth channel in the near future.

Exercising the Cyber Attack Simulation and Modeling has proven to be an outstanding business enabler, with sequential projects as a common practice.

Cyber Attack Simulation and Modeling service may secure the business relationships with your actual clients and enables you to establish new business relationships.

Offering to the market an “out-of-the-box” service might just place you few steps ahead your competitors.
Is this service an external penetration test?

No. The Cyber Attack Simulation and Modeling is not an External Penetration Test.

While a penetration test will show the current cyber risks an organization is facing, the Cyber Attack Simulation and Modeling will demonstrate a safe and controlled cyber infiltration incident.

As the Penetration Tester will examine the logical aspect of current security status of an organization, the Cyber expert will use all available attack vectors to accomplish an infiltration. In addition to logical and technical attacks, the consultant will use Social Engineering, Spear Phishing and proprietary practices to attain successful demonstration.

The focus of the Cyber expert is to imitate real-world scenarios and attack flows, rather than using automated scanners and filling a pre-written report template.

Few words about us

Cipher Security is a unique Information Security provider that operates in respect with its main values - integrity, accountability, reliability, partnership.

As we are a trustworthy partner, always aiming excellency as a standard, we are ready to completely fulfill our partners requirements and to surpass theirs high-quality expectations, delivering outstanding value to any challenge. For this reasons, our palette of services includes World-class Distributed Denial of Service Tests (DDoS), Cyber Workshops, Infrastructure and SCADA Penetration Tests, Tailor Made “malicious” Development etc.

Israeli-based, we address our innovative services to a vast scope of industries; from Banking and Investments sector, through the Industrial domain and Critical Infrastructure, to vendors and service providers from around the world.
Did you know?

87%

of organization where a case of penetration has occurred have a database record of the incident and still this has gone unnoticed.
Did you know that a computer gets attacked every 39 seconds on average?

The attacks are happening just now.

There are clients searching for a solution just now. Don’t lose time, be the first to offer the Cyber Attack Simulation and Modeling service to your customer.

www.cipher-security.com