FROST & SULLIVAN

50 Years of Growth, Innovation and Leadership

The Importance Of Ethical Hacking

Emerging Threats Emphasise The Need For Holistic Assessments

A Frost & Sullivan
White Paper

Chris Rodriguez
Industry Analyst

www.frost.com

"...the elevated threat landscape urgently dictates the need for a comprehensive, real-world assessment of an organisation's security posture."

1. EXECUTIVE SUMMARY

Businesses of all sizes are increasingly challenged to adopt new technologies such as cloud computing and virtualisation and business practices such as bring-your-own-device and IT outsourcing. To complicate this challenge, companies face increasingly targeted and sophisticated attacks. Attackers now range from organised crime rings to advanced nation-states and are highly organised, skilled, and motivated. Despite the prevalence of firewalls, IPS, anti-virus and other security technologies, many businesses continue to fall victim to these attacks due to unintentional configuration errors. As a result, companies are beginning to recognise the importance of human experience and analysis in a best-of-breed security architecture.

Ethical hacking companies offer tremendous value in their ability to share their advanced security knowledge and expertise with customers. This service enables businesses to adjust their security technologies, train their staff, and enact security practices that better protect critical systems and sensitive data. Ethical hacking services provide customers with objective and real-world assessments of security weaknesses, vulnerability, risk, and remediation options. As a result, ethical hacking is rapidly gaining attention as an essential security practice that should be performed on a regular basis.

However, businesses must be careful to select a reputable and experienced ethical hacker to ensure an efficient and productive assessment. Customers can better plan and implement a successful ethical hacking consultation by first understanding the challenges and best practices in this market. To better support both technical and business decision makers considering ethical hacking services, Frost & Sullivan has conducted interviews with key industry participants and customers to identify leading challenges and best practices as well as extensive secondary research. This paper presents these findings to provide customers with the knowledge necessary to justify and implement leading ethical hacking services into their security architecture.

2. THE COMPLEX THREAT LANDSCAPE

Major companies such as Google, RSA, and Sony have recently made headlines as victims of highly sophisticated cyber attacks that resulted in major security breaches and data loss. Data security breaches can involve massive amounts of sensitive customer data such as credit card numbers, social security numbers, passwords, and PINs. 77 million customer records were leaked in the 2011 Sony Networks data breach. In other cases, security breaches can involve the loss of valuable intellectual property or classified state secrets. In 2011, network security and encryption company RSA reported a serious vulnerability that affected millions of its SecureID tokens. Hackers were then able to penetrate the network of United States government contractor Lockheed Martin by exploiting this vulnerability[1].

1. Schwartz, Nelson. "RSA Faces Angry Users After Breach." *Business Day*. The New York Times, 7 June 2011. <http://www.nytimes.com/2011/06/08/business/08security.html>

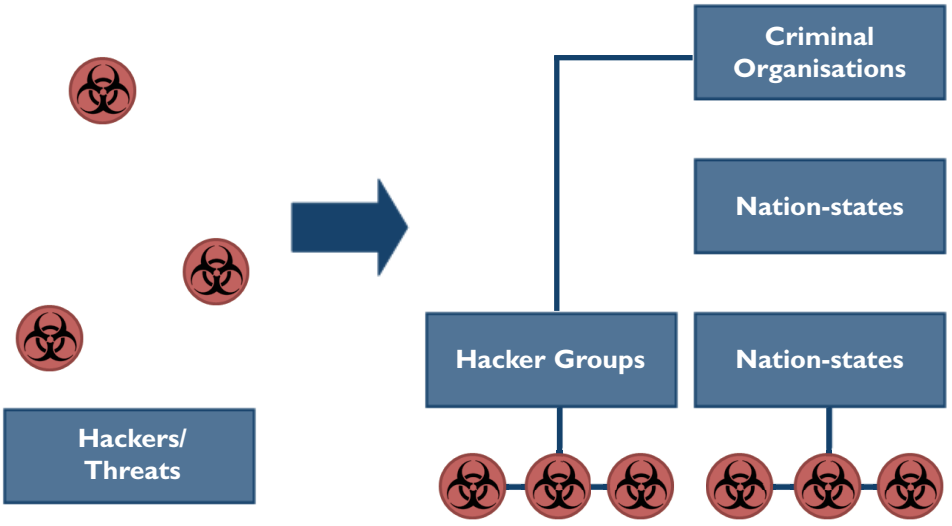
These attacks have been successful due to more sophisticated hacking techniques. In 2010 a complex cyber attack, named Operation Aurora, targeted Google's valuable intellectual property as well as sensitive data from 33 additional technology companies. Operation Aurora utilised sophisticated techniques such as encryption, a zero-day vulnerability, and remote backdoors to penetrate critical systems and evade detection[2].

Similarly, the Conficker worm spread rapidly in 2008 and included abilities to block malware and other remediation efforts. One of the most sophisticated worms was Stuxnet in 2010, which targeted Iranian nuclear production capabilities. Stuxnet utilised advanced malware techniques to obfuscate its activities and was highly targeted to subtly sabotage only a specific set of SCADA systems used in the facilities.

The increased sophistication and success rate for recent cyber attacks is directly related to the shift in attacker profile. Criminal organisations have long understood the value of sensitive business and customer data but have lacked expertise. Now, advanced cyber attacks such as Stuxnet and Operation Aurora are developed by experienced teams of programmers. As a result, these advanced threats indicate that nation-states and large criminal organisations are funding well organised, highly motivated, and expertly trained teams of programmers[3]. Chart 1 illustrates this shift in attacker profile.

"...assessment is the vital first step to enact effective security policies, procedures, and infrastructure that will prevent or mitigate the effects of a data breach."

Chart 1 – Shift in Modern Information Security Threat Landscape



2. Zetter, Kim. "*Google Hack Attack Was Ultra Sophisticated, New Details Show.*" *Threat Level.* Wired, 9 April 2012. <http://www.wired.com/threatlevel/2010/01/operation-aurora>

3. Markoff, John. "A Silent Attack, but Not a Subtle One." *Business Day* Technology. The New York Times, 26 September 2010. <http://www.nytimes.com/2010/09/27/technology/27virus.html>

"The objectiveness of a security assessment has a direct impact on the value of the assessment. An organisation cannot conduct a fair assessment of its security posture due to its preexisting knowledge of security weaknesses, security infrastructure, and the value of target systems."

These attackers represent an advanced persistent threat. They are capable of utilising advanced tools and techniques to target specific systems. They also have adequate resources to continue to attack their target until they gain access and can then remain undetected for periods of time after gaining entry. Unfortunately, in many cases hackers do not require the most advanced attack techniques and are able to penetrate network defences due to simple misconfigurations and other human errors.

Most businesses have essential network security technologies such as firewalls, intrusion prevention systems (IPS), and anti-malware software in place. These tools provide tremendous value by blocking the many common threats that businesses still face today but lack the requisite human analysis and logic to be 100 percent effective against targeted threats. Often, these tools simply need to be tested and adjusted. Now, the elevated threat landscape urgently dictates the need for a comprehensive, real-world assessment of an organisation's security posture. This assessment is the vital first step to enact effective security policies, procedures, and infrastructure that will prevent or mitigate the effects of a data breach.

3. BENEFITS FROM INDEPENDENT ETHICAL HACKING ASSESSMENTS

Unfortunately, many businesses may assume that they will not be targeted due to a lack of valuable data or may operate under outdated security practices. This strategy fails to acknowledge the dynamic nature of hacker groups' strategies and goals. Businesses now face an imminent threat and must adjust their security processes, policies, and architectures accordingly.

Complex Enterprise Networks Require Security Expertise

A major challenge for businesses is the complexity of security requirements due to changing hacking tactics, myriad security vulnerabilities, evolving business practices, new business technologies, and emerging security technologies. This can lead to large, complex networks that can be difficult to inventory and map. As a result, IT staff can simply overlook or forget about obsolete systems leading to high-risk network entry points. A third-party assessment will be necessary to find these overlooked vulnerabilities.

This complexity also creates numerous organisation-specific security challenges that are best solved by professionals with extensive expertise. This expertise is expensive to cultivate, and ethical hacking companies must invest heavily to develop the skills of their auditors. This enables auditors to maintain an up-to-date repertoire of hacking techniques which ensures accurate assessments and useful recommendations. Businesses can then leverage these expert recommendations to fix security vulnerabilities and implement security tools more effectively.

Unfortunately, many businesses cannot afford this level of security expertise. In addition to salary, there are numerous costs associated with ongoing training and skills development. Security professionals must regularly attend classes, seminars, conferences, and workshops to develop and maintain their skills. This prevents most businesses from developing the internal expertise necessary to simulate a real-world attack scenario. Businesses that do have internal security experts should also consider the insight provided by ethical hacking consultations as a supplement to their existing security expertise.

"...emerging technologies provide businesses with operational advantages such as virtualisation, cloud computing, and mobile devices. These technologies enable business agility and efficiency but also introduce new security concerns."

Ethical Hacking Services Provide Objective Analysis and Validation

Ethical hacking offers an objective analysis of an organisation's information security posture for organisations of any level of security expertise. The objectiveness of a security assessment has a direct impact on the value of the assessment. An organisation cannot conduct a fair assessment of its security posture due to its preexisting knowledge of security weaknesses, security infrastructure, and the value of target systems. This preexisting knowledge influences testing methodology or scope and provides inaccurate assessment results.

By comparison, hackers have no knowledge of these systems other than what they can gather. Hackers must scan for weaknesses, test entry points, prioritise targets, and develop a strategy that best leverages their resources. An ethical hacking company is best positioned to recreate this objective and honest evaluation and also offers a fresh perspective to find problems that the customer may be overlooking or forgetting.

Ethical hacking companies provide a valuable third-party validation of customers' security practices. This is necessary to demonstrate compliance with industry regulations. For example, the Payment Card Industry Data Security Standard (PCI DSS) Requirement 11.3 specifies the need for penetration testing once per year[4].

Security as a Business Enabler

Security breaches can be very costly yet are difficult to quantify or to predict. As a result, security is less of a focus for many businesses that would rather invest in revenue-generating technologies. This challenge is further compounded by the pressure for IT organisations to deliver valuable solutions while managing shrinking budgets.

4. "Payment Card Industry (PCI) Data Security Standard: Requirements and Security Assessment Procedures Version 2.0." PCI Security Standards Council. October 2010.

There are many emerging technologies that can provide businesses with operational advantages such as virtualisation, cloud computing, and mobile devices. These technologies enable business agility and efficiency but also introduce new security concerns. Due to these new security concerns, businesses should invest in ethical hacking assessments when investing in updated infrastructure or new technologies. These assessments are a necessary process to prevent expensive data breaches that can cost companies in the millions of dollars due to lost business, fines, or lawsuits. Proactive ethical hacking can prevent these losses and is much more affordable by comparison.

However, businesses should also consider a strong information security programme to be an investment in its name brand. This is particularly true for businesses that rely extensively on information technologies since a security breach can deter future business. For example, Epsilon Data Management lost customer data for 50 major international businesses in 2011[5]. Information security programmes and a strong security track record will soon be critical competitive factors for businesses in the technology and information security industry.

4. ETHICAL HACKING'S ROLE IN AN ENTERPRISE SECURITY ARCHITECTURE

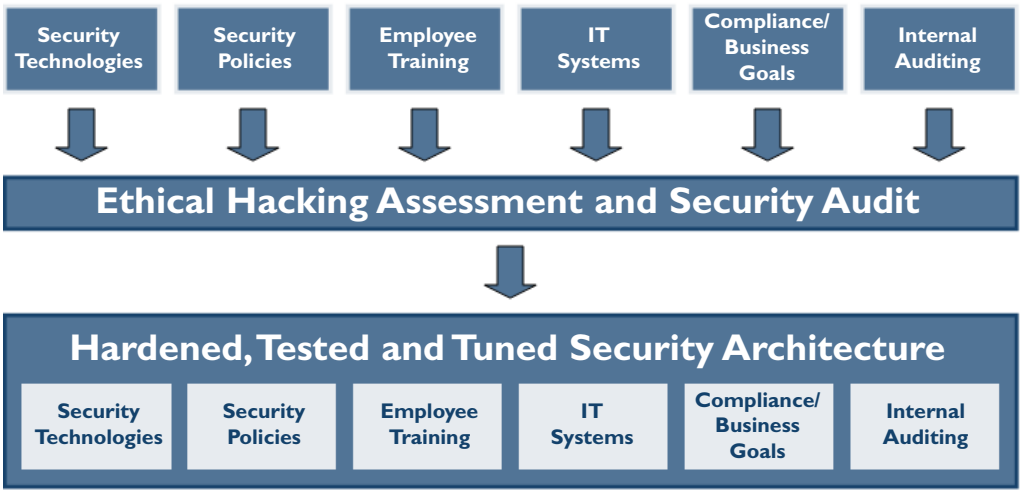
Since 2010, organisations of all sizes and across every industry have shown increased interest in ethical hacking. Businesses that recognise the value of these services must also understand how ethical hacking fits within a best practice IT security architecture.

The Missing Piece in the Security Puzzle

Ethical hacking services provide customers with objective, real-world assessments of their security architectures. This is a holistic analysis of an organisation's security posture including policies, network protection infrastructure, and end-user practices. The result of these assessments is actionable reports with valuable remediation advice tailored to the customer's unique IT environment, capabilities, and security objectives. This helps businesses to prioritise their security efforts, fine-tune security tools such as firewalls and IPS devices, adjust policies, and identify any necessary training. Chart 2 illustrates ethical hacking's unifying role in a best practice IT security architecture.

5. Lennon, Mike. "Massive Breach at Epsilon Compromises Customer Lists of Major Brands." *Security Week*. Wired Business Media, 2 April 2011. <http://www.securityweek.com/massive-breach-epsilon-compromises-customer-lists-major-brands>

Chart 2 – Ethical Hacking's Role in an Enterprise Security Architecture



Many organisations currently use automated testing tools and internal resources to assess their security posture. Tools such as penetration testing frameworks do provide valuable insights about the customer's security architecture. However, these tools lack the analytic capabilities offered by experienced ethical hackers.

As a result, automated tools can complicate the assessment process by reporting a high number of false-positive results or by simply listing countless vulnerabilities rather than identifying high-risk security vulnerabilities. This causes either less effective findings or increased time and labour costs necessary to identify useful assessment data. Additionally, IT organisations can simply forget to scan certain systems or enable the full suite of testing modules or the scanning tool may not discover more complex vulnerabilities. These missteps can lead to false-negatives and incomplete assessments.

Conversely, ethical hackers are highly proficient with automated tools and manual testing. This experience and proficiency enables the essential service of identifying any missed false-negatives and eliminating false-positives. Therefore, the value of ethical hacking services is the ability to achieve truly comprehensive and actionable assessment data. In addition, ethical hacking companies can identify the customer's particular security, operational, and compliance objectives before the assessment. These companies can then tailor the assessment and the report to focus on these objectives. The ethical hacking company adds further value by interpreting the results of the assessment data and presenting a prioritised plan of remediation to the customer.

What Does Ethical Hacking Involve?

The services offered by ethical hacking companies can vary substantially but customers should seek ethical hacking companies with a broad range of testing capabilities. Ethical hackers should offer external tests such as penetration testing, Web application testing, DMZ testing, and physical security testing, as well as internal tests such as phishing, Trojan virus attacks, and social engineering attacks.

Some tests, such as wireless network attacks, can blur these definitions, but proficiency in both external and internal network testing is a fundamental requirement to ensure an accurate security assessment. An example of this is trusted network attack simulations in which a hacker first enters the system of the target's partner, then launches attacks against less secured "partner-only" systems.

Ethical hacking companies should also provide analysis of customers' IT architectures and policies. In addition to these tests, vendors should offer training services to improve their customers' end-user awareness and security staff expertise. This will ensure security improvements and better results in subsequent assessments. These fundamental services are considered proactive assessments due to their ability to prevent security breaches.

Companies that have already been breached may require a security consultant that also offers reactive services such as malware analysis, reverse engineering digital forensics, and legal assistance. These capabilities do not prevent security breaches but can provide valuable security insight for a breached company.

Analysis of a successful security breach provides businesses with the necessary knowledge to prevent or mitigate the effects of future attacks including awareness of existing vulnerabilities and insider threats. These services can also help the breached company to investigate the extent of the security breach including determining which data was lost and any responsible parties.

Prior to an ethical hacking consultation, the customer should determine their security objectives, asset priority, and scope of the test. An important consideration is the type of test that will be performed. Black box testing provides the ethical hacker with a minimal amount of data, while white box testing provides full system access and information.

Each testing methodology has its advantages. Black box testing allows the auditor to best emulate a real-world external attack scenario in which the attacker has limited knowledge to base decisions on. White box testing provides the most comprehensive assessment but is much more time consuming and costly. There are varying testing levels between these two extremes that offer balanced value and efficiency called grey box testing. Grey box testing may be necessary to test certain systems such as trusted network systems[6]. Table 1 below compares advantages and disadvantages for various testing methods.

Table 1 – Comparison of Advantages for Various Testing Methods

	ADVANTAGES	DISADVANTAGES
Black Box Testing	➢ Real-world results ➢ Less project risk/cost	➢ Less holistic ➢ More effort required
White Box Testing	➢ More holistic analysis ➢ More efficient audits	➢ Larger projects and more cost ➢ Less real-world data
Grey Box Testing	➢ Balance of cost/time and assessment scope ➢ Provides analysis not possible with pure black or white box tests	➢ Need for more careful project planning such as scope and expectations

Because black box testing is fast and less costly, businesses should begin with these tests. They should then move onto more comprehensive white box testing if possible or with some level of grey box testing to ensure deeper system testing.

5. BUSINESS CHALLENGES AND RISK MITIGATION

Although there is increased interest in ethical hacking, customers remain hesitant due to concerns about the business aspects of these services. Customers must fully understand these challenges and develop strategies to mitigate the risk that they present. This is an essential practice to better determine the appropriate project scope, methodology, and consulting company necessary to ensure a successful penetration test.

6. Scarfone, Karen, et al. "Technical Guide to Information Security Testing and Assessment: Recommendations of the National Institute of Standards and Technology." NIST Special Publication 800-115. US Department of Commerce. September 2008.

"...an external penetration test is a valuable starting point for the majority of businesses. This provides a real-world assessment of the many threats that an organisation faces in its daily operations."

Relatively High Business Costs and Project Size

The primary challenge for businesses that are interested in ethical hacking services is the perception that these services are very expensive. The specialised expertise necessary to conduct ethical hacking assessments is rare and valuable and therefore, can be relatively expensive compared to other professional services. Additionally, these consultations require extensive testing of customer systems and can be very time consuming depending on the complexity and size of the organisation and its IT architecture.

However, ethical hacking services are necessary to ensure that critical information security systems are deployed correctly and are functioning properly. Therefore, this cost should be planned in advance and included in an annual IT security budget.

To reduce these costs, customers should determine a more limited assessment scope to focus on. A smaller consulting engagement will also reduce the project risk, especially when interacting with an ethical hacking company for the first time. Businesses should determine what penetration tests are most applicable to their organisation. Each organisation faces unique security challenges depending on the nature of their business and their network environment. Therefore, each business must first evaluate its security challenges and any available historical threat data. This will enable the company to identify which tests are most appropriate and to prioritise their efforts accordingly.

For example, an external penetration test is a valuable starting point for the majority of businesses. This provides a real-world assessment of the many threats that an organisation faces in its daily operations. However, organisations such as manufacturing or utilities companies have minimal Internet-facing communications and would derive more value from internal penetration tests. If possible, businesses should begin with smaller, external penetration testing projects when first contracting an ethical hacker. This pilot project will reduce cost and risk while providing valuable insight into the ethical hacker's skills and professionalism. Customers should then expand the scope of their penetration tests as they become more familiar with ethical hacking services. This process is illustrated in Chart 3 below.

Chart 3 – Recommended Progression for New Ethical Hacking Customers

Impact on Operations

Ethical hacking consultations can be a very time consuming investment and will require some level of interaction with the customers' end-users, management, IT staff, and security staff. Businesses fear that this can be distracting to the daily operations of the IT staff and end-users which would result in lost productivity. However, the customer should determine the level of interaction that the ethical hackers will initiate with personnel during the planning stage.

This interaction is an important variable that customers can throttle to keep costs and distractions to a minimum during a penetration test. Unfortunately, hackers use social engineering methods to trick end-users into divulging information or credentials and thereby allow a security breach. As a result, the ethical hacker may also require a high level of interaction with IT staff and select end-users to determine potential social vulnerabilities. Businesses have the option to limit the ethical hacker's interaction with staff, but should increase this scope in future assessments if the budget permits.

"In many cases, even the knowledge that a business contracted an ethical hacking company can alarm investors and customers, or can make the company a target for hackers."

Fear of Consequences from a Negative Assessment

Despite the value that ethical hacking services provide, many organisations lack the mature attitude necessary to move forward with a consultation. The common misconception is that identification of vulnerable systems is an assessment of the IT staff's effort or an appraisal of the security team's expertise. As a result, fear of a negative assessment prevents businesses from identifying key areas for improvement.

Organisations of all sizes and sophistication levels can benefit from objective, expert, third-party analysis. This value requires a mature attitude towards security assessments and recognition of security objectives as a company-wide effort. The goal of an ethical hacking assessment should be to identify and secure vulnerable systems and practices in order to achieve a best-of-breed security practice. Businesses should not base any personal or group appraisals on the results of a security assessment. Awareness classes, reminders, and reward programmes can all help to improve an organisation's security maturity across all levels of management and staff.

Security and Privacy Concerns

Ethical hacking has matured and become a more mainstream service in the past decade. However, businesses remain skeptical about the risk inherent with inviting a third-party to attempt to access sensitive systems and resources. Customers fear that ethical hacking companies may leak sensitive data. In many cases, even the knowledge that a business contracted an ethical hacking company can alarm investors and customers, or can make the company a target for hackers.

To reduce this risk, businesses should hire only ethical hacking companies that implement practices to ensure privacy and confidentiality. For example, ethical hacking companies should not keep any data or credentials after the consulting engagement. The ethical hacker should turn over this data to the customer along with the final report and then delete the data. Customers should then ensure that all Non-Disclosure Agreements (NDA) are signed prior to the assessment.

Project and Business Risk

Most importantly, customers should be careful to hire proven and professional companies. Ethical hacking companies should accredited by international trade organisations such as EC-Council and International Information Systems Security Certification Consortium (ISC)[2]. Ethical hacking companies must have board members with industry recognition, trustworthy reputations, and reputable experience. Their auditors should hold industry certifications as these indicate technical skill and often require background checks[7]. Ethical hacking companies should also perform background checks on their auditors and ethical hackers.

Customers must also be careful to select an ethical hacking company that is financially stable and implements mature business practices. The company should have strong share capital to reimburse customers in case it goes bankrupt or has other legal issues. This way, the customer can avoid wasting valuable resources on an incomplete penetration test. The company should regularly perform independent financial audits to ensure legal financial and accounting practices. These companies should also have reputable legal advisors due to the importance of NDAs, contracts, and legal compliance for ethical hacking services. An independent advisory board also indicates mature and reputable business practices.

Additionally, international and government trade organisations require that ethical hacking companies invest in insurance. Therefore, the ethical hacker should be insured and should provide civil assurance that it will reimburse the customer for any damages that penetration tests may cause.

Ethical hacking companies also demonstrate stability in a number of other ways. For example, financially stable companies perform extensive research and development activities and participate in the security community. These activities serve to improve the company's reputation, demonstrate its skills, and benefit the industry.

6. TOP TECHNICAL CONCERNS AND SOLUTIONS

In addition to these business concerns, many organisations have specific concerns about technical challenges that may arise during an ethical hacking consultation. By understanding these technical challenges, businesses can enact guidelines to mitigate any project delays or complications.

Stability and Reliability of Critical IT Systems

To infiltrate a network, hackers will use various tactics to force an IT system to allow access to restricted data or other off-limit resources. This can cause errors in the system resulting in corrupted data, unavailable resources, or other undesired behaviour.

7. "LPT – What is Penetration Testing?" EC-Council. <https://cert.eccouncil.org/certification/certificate-categories/licensed-penetration-tester-lpt>

As a result, many businesses fear that their critical IT systems may be disrupted during the course of an ethical hacking assessment. However, despite the effort to emulate a real-world attack scenario, experienced ethical hackers understand what tactics can damage systems and can then avoid these problems. Ideally, a quality ethical hacking service should provide a real-world security assessment with minimal risk to the stability or availability of customers' critical IT systems.

"If possible, ethical hacking companies should perform their tests in the customers' staging environments."

If possible, ethical hacking companies should perform their tests in the customers' staging environments. Staging environments should emulate the production environment as closely as possible to ensure accurate assessments. This will prevent any negative effects of the testing process from affecting critical systems on the production network.

However, a staging environment or a virtualised environment may not be available for testing in many cases. In the event that customers choose to conduct penetration testing in their production environment, they should first determine the value of their systems, determine risk, and decide what systems not to test. This will enable the customer to clearly define the scope of the tests prior to the assessment and avoid testing and breaking sensitive systems.

Quality Assessment Tools

There are many tools available for use by ethical hacking companies ranging from free open source software such as Nmap and THC-Hydra to enterprise-grade solutions such as CORE IMPACT Pro and Acunetix WVS. Free and open source software offers compelling functionality that is regularly updated by a community of users and developers. Commercial testing solutions offer cutting-edge functionality, proven reliability, and dedicated research and development. Table 2 lists popular tools that leading ethical hacking vendors offer.

Table 2 – List of Popular Commercial and Free Open Source Software Tools

COMMERCIAL TOOLS	FREE AND OPEN SOURCE SOFTWARE
➢ CORE IMPACT Pro ➢ Acunetix WVS ➢ Metasploit Pro ➢ Nessus ➢ eEye Retina ➢ Rapid7 Nexpose ➢ CST OnLine Digital Forensic Suite (DFS)	➢ Nmap ➢ THC-HYDRA ➢ Nikto Web Scanner ➢ Microsoft Baseline Security Analyser (MBSA) ➢ Secunia Personal Software Inspector (PSI) ➢ Open VAS ➢ Titania Nipper

By utilising a balance of open source tools and commercial solutions, ethical hacking companies can provide a breadth of assessment capabilities. Enterprise solutions can be very costly, and leading ethical hacking companies leverage open source solutions to reduce these costs. Conversely, ethical hacking companies should not rely solely on free open source tools as this may indicate a company that does not care or cannot afford to improve its portfolio with commercial tools.

Ultimately, an ethical hacking company should use the automated tools that they are most proficient with. Experienced ethical hackers will understand which tools to use for specific assessments. Ethical hacking companies should be transparent about the tools that they use and should be familiar with a breadth of testing tools in order to adapt to specific customer requests.

Custom Tool Requirements

Off-the-shelf tools may not work with certain applications or configurations during the course of a penetration test. In this case, the ethical hacking company should have the skills to code an automated testing tool. This technical capability is increasingly important due to the emerging attacker profile of well trained and highly skilled attackers. These attackers will automate the process of testing network entry points as much as possible but can also develop targeted testing programmes when necessary.

Customers should seek ethical hacking companies with the expertise to create testing programmes that are tailored to the customer's specific environment. This provides more comprehensive penetration testing assessments. However, the process of creating custom tools will also increase the project time and costs.

Therefore, the ethical hacking company should offer a portfolio of professional-quality, custom-developed tools available for customers. The company should support and update these tools to prevent any delays during an ethical hacking assessment to maintain lower project costs. Custom tools will demonstrate technical skill and offer unique functionality not offered by publicly-available tools.

Assessment Accuracy

Many businesses consider ethical hacking services to be an unnecessary luxury and will rely solely on automated scanners. However, automated tools lack the logic and analytical capabilities to determine which vulnerabilities are already configured correctly, already fixed, or are erroneous results. Instead, automated tools report long lists of vulnerabilities to the user who is then responsible for further investigation. The ethical hacker must then verify all vulnerabilities before reporting them to the customer. This prevents the customer from wasting valuable time or resources to investigate any false-positives.

Additionally, automated tools may be susceptible to false-negatives, which are less visible but far more dangerous. Automated tools that miss vulnerabilities and report false-negatives provide the customer with a false sense of security. Consequently, ethical hackers that rely solely on an automated tool cannot identify all of the security weaknesses within an organisation. Hackers may still be able to penetrate the businesses' security by using a different automated tool, a custom tool, or manual testing.

Leading ethical hacking companies will utilise a variety of tools, expert analysis, and manual testing to ensure accurate assessments that eliminate false-positives or false-negatives.

Report Technicality

Ethical hacking companies provide value in their ability to apply expert security analysis to the findings of their automated tools and manual tests. This allows the ethical hacker to provide useful risk assessments and security recommendations. Unfortunately, there is a wide range of expectations from both the ethical hackers and their customers regarding the amount and type of data that should be delivered. Ethical hacking assessments must result in useful and actionable remediation advice that communicates relevant assessment results to the appropriate reader.

To do this, reports must be tailored to both technical readers and to management as this broad audience will have very different goals and requirements. Management will expect risk assessments, project summaries, business consideration, and action plans. Conversely, more technical readers will require a comprehensive list of vulnerabilities including proof of concept verification, impact, severity, and affected systems. Most importantly, a leading ethical hacking company will provide detailed remediation recommendations.

7. VENDOR SPOTLIGHT: HIGH-TECH BRIDGE

In its independent analysis of the ethical hacking market, Frost & Sullivan has identified a leading European provider of expert ethical hacking services with compelling value named High-Tech Bridge (https://www.htbridge.com/). High-Tech Bridge specialises in ethical hacking, security auditing, and computer forensics, but does not integrate or resell any third-party products. This allows the company to perform more objective and thorough assessments compared to large product vendors, value-added resellers, and system integrators. Despite High-Tech Bridge's success in Europe, the company is available to serve customers globally.

Expert Ethical Hacking

High-Tech Bridge is proficient with a range of proactive external and internal penetration tests to enable security assessments ranging from targeted to holistic. High-Tech Bridge offers fundamental external penetration tests including DMZ testing and Web application testing. For customers that require internal testing, High-Tech Bridge can simulate insider attacks, as well as social engineering, phishing, and Trojan attacks. High-Tech Bridge also offers hybrid attacks such as wireless network and trusted network attacks.

High-Tech Bridge utilises a combination of commercial and free open source software but also offers a strong portfolio of custom-developed testing applications when necessary for unique customer environments. Therefore, High-Tech Bridge ensures expert analysis and assessments but also utilises free or open source software when possible to keep costs low for customers. Most importantly, High-Tech Bridge offers insurance and civil assurance for any damages that the penetration tests my cause. However, the company prevents the need for these assurances as much as possible by avoiding disruptive or damaging tests.

"Proactive services are typically more affordable and customers should invest in those services to prevent a costly security breach from ever occurring."

Breadth of Security Consulting Services

High-Tech Bridge goes beyond penetration testing with additional proactive services such as security consulting, auditing, and training services. These services enable customers to leverage High-Tech Bridge's security expertise to improve their security architectures and knowledge. As a result, High-Tech Bridge proactive services can greatly help a business to prevent a security breach and are very valuable.

Proactive services are typically more affordable and customers should invest in those services to prevent a costly security breach from ever occurring. However, companies that have already been breached will require specialised security services. For these businesses, High-Tech Bridge offers reactive services such as malware analysis, digital forensics, legal assistance and reverse engineering. Businesses that have been breached should perform these services in order to understand what enabled the attack and how to fix it. This understanding of security flaws is necessary to prevent future breaches. For example, computer forensics can help to find the source of a data leak and the extent of the data loss while also providing the necessary information to prevent future data security breaches. Table 3 lists High-Tech Bridge's portfolio of proactive and reactive services.

Table 3 – List of Proactive and Reactive Services

PROACTIVE SERVICES	REACTIVE SERVICES
➢ Internal Penetration Testing ➢ External Penetration Testing ➢ Training ➢ Security Audits/Consulting	➢ Digital Forensics ➢ Legal Guidance ➢ Malware Analysis

In-depth, Actionable Reporting

High-Tech Bridge works extensively with customers to identify and understand their goals and expectations. This allows High-Tech Bridge to tailor the assessment and report to provide more valuable data for the client's business needs. All findings are verified prior to being reported to the customer to prevent any false positives.

At the end of the assessment, High-Tech Bridge presents its full findings to the customer in multi-section reports. The first part is an executive summary that is less technical but outlines security findings, risk, business continuity, costs, and necessary steps. The second section is a technical report that lists all vulnerabilities found. This section provides analysis for each vulnerability issue including discovery, verification, proof-of-concept, and other relevant technical details.

The third section is a security improvement guide that lists the vulnerabilities and provides remediation solutions for them. This practice allows High-Tech Bridge to report the relevant, actionable data to the appropriate reader and assures an appropriate level of technicality for each audience.

High-Tech Bridge reports are comprehensive and identify areas for improvement. However, these reports also communicate any positive findings that High-Tech Bridge identifies. This approach provides a more comprehensive assessment of business risk and security weaknesses based on factors such as target value, exploit difficulty, and environmental factors. By addressing positive findings as well as negative findings customers can better understand what security practices work and why. Customers can then learn from these examples and replicate this success throughout its organisation. In addition, this approach facilitates greater teamwork, reduces fear of a negative assessment, and improves cooperation with IT staff that may otherwise be very wary of a third-party assessment.

"Sony would like to thank High-Tech Bridge SA Security Research Lab for professional and responsible disclosure of the vulnerability and work with Sony to help protect our customers."

Industry Participation, Research, and Development

High-Tech Bridge focuses heavily on research and development as evidenced by its dedication of half a million dollars to this activity in the first quarter 2012. This focus on research and development is a critical differentiator that enables High-Tech Bridge to deliver valuable security and auditing services. The High-Tech Bridge research lab contributes to the company's toolsets and knowledge base by researching new hacking and defense techniques while also publishing white papers and other materials freely to the security community.

High-Tech Bridge also devotes resources to find and responsibly disclose new vulnerabilities in prominent enterprise software. Through its research High-Tech Bridge has helped 150 technology vendors including major companies such as Sony and HP to fix 413 vulnerabilities in their products[8]. High-Tech Bridge advisories are publicly available on the corporate website, National Vulnerability Database and vendor websites such as the Secunia Vulnerability Database[9]. This industry involvement and ongoing research demonstrates the company's commitment to expert security knowledge and services.

High-Tech Bridge is an active member in many security organisations including Open Web Application Security Project (OWASP), Online Trust Alliance, PCI Security Standards Council and others. The company also participates in multiple conferences and industry events such as Swiss Cyber Storm and DEFCON Switzerland.

8. "Security Update Program for VAIO Computers." Sony eSupport. 5 January 2012. <http://esupport.sony.com/US/perl/support-info.pl?template_id=1&info_id=946>

9. "Secunia Advisory and Vulnerability Database." Secunia. <http://secunia.com/community/advisories/search/?search=high+tech+bridge>

"High-Tech Bridge is advised by Schmidt, Jaton & Associates, a premier law firm in Geneva. This provides High-Tech Bridge and customers with assurance of legal compliance and comprehensive legal protection for critical matters such as NDA and contractual agreements."

Company Maturity and Reliability

High-Tech Bridge is a proven and stable company with mature business practices. For 2012, High-Tech Bridge announced an increase in share capital up to 3.3 million USD[10]. This provides extensive assurance that the company will be able to reimburse customers in case of any reason that the company cannot complete a project. This share capital is much higher than the minimum share capital of 20,000 USD required and offered by smaller ethical hacking companies.

High-Tech Bridge is advised by Schmidt, Jaton & Associates, a premier law firm in Geneva. This provides High-Tech Bridge and customers with assurance of legal compliance and comprehensive legal protection for critical matters such as NDA and contractual agreements. The company also utilises independent financial audits to ensure legal accounting practices.

High-Tech Bridge has experienced and reputable board members and a separate advisory board. Furthermore, High-Tech Bridge employs experienced security professionals full-time. High-Tech Bridge pays for its auditors' training and testing for a range of certifications including Licensed Penetration Tester (LPT), Computer Hacking Forensic Investigator (CHFI), and Certified Ethical Hacker (CEH) from EC-Council, as well as eLearnSecurity Certified Professional Penetration Tester (eCPPT), Certified Information Systems Security Professional (CISSP), GIAC Reverse Engineering Malicious Code (GREM), and Check Point Certified Security Expert (CCSE). Chart 4 lists essential ethical hacker credentials and certifications.

Chart 4 – List of Essential Ethical Hacker Certifications

All staff must pass background checks and must sign corporate NDA and other legal protection contracts. As the company is based in Geneva, High-Tech Bridge can provide customers with the privacy and confidentiality afforded under Swiss law. High-Tech Bridge is one of few ethical hacking companies to hold the ISO 27001 certification that ensures confidential and secure storage and transfer of customer data. This helps to reassure customers and alleviates worries of security and privacy concerns.

10. "High-Tech Bridge announces capital increase and adapted expansion strategy for 2012." Yahoo Finance. Yahoo, 7 February 2012. < http://finance.yahoo.com/news/high-tech-bridge-announces-capital-130000913.html>

8. CUSTOMER CASE STUDY AND KEY LESSONS

Frost & Sullivan interviewed Mr. Viktor Polic CISSP CRISC CISA, an information security industry expert, about his experience with ethical hacking services at a large multi-national organisation. This organisation has a large and complex network (offices in 55 countries globally) with a mature security programme. However, the organisation recognised ethical hacking services as the inevitable next phase in its information security programme.

Modern Information Security Challenges

More specifically, the organisation was interested in ethical hacking as a response to shifting organisational network boundaries. This shift is the result of adoption of new technologies such as cloud computing and practices such as outsourcing. These technologies provide more robust information flow but also necessitate the ability to go beyond traditional technical controls.

Furthermore, the increasing availability of tools and pervasiveness of threats highlighted the organisation's need to more accurately understand its actual security posture. As a result, the organisation sought to identify how likely they were to be exploited, if it was possible, who could do it, and to quantify the risk compared to the perception of risk.

High-Tech Bridge Value

Mr. Polic prefers to contract with multiple auditors to benefit from an array of different skill sets and tools. Initially, High-Tech Bridge passed preliminary requirements such as international standards, staff certifications, code of ethics, portfolio, legal protection, and experience, but the organisation still had to verify the company's expertise. To do so, the organisation contracted High-Tech Bridge for a smaller assessment project to evaluate the company's technical knowledge and skills. After successfully passing this test, the organisation will consider High-Tech Bridge for more comprehensive assessments in the future.

High-Tech Bridge worked closely with the customer throughout the assessment with lots of data sharing by both parties. High-Tech Bridge offered good interaction with the customer's team, provided a draft of the report to the customer, and included the organisation's comments throughout the report. The final report was very detailed and showed evidence of expert analysis rather than reliance on automated tools. In addition, High-Tech Bridge also highlighted positive findings to encourage successful security practices.

High-Tech Bridge displayed a high level of technical proficiency and the essential ability to effectively communicate its findings and recommendations to the customer. Overall, the customer considered the consultation to be a success. This organisation now considers High-Tech Bridge's services to be a valuable complementary step to its security programme.

"High-Tech Bridge displayed a high level of technical proficiency and the essential ability to effectively communicate its findings and recommendations. Overall, I considered the consultation to be a success."

Viktor Polic, CISSP, CRISC, CISA

Lessons Learnt

Based on the organisation's experience with High-Tech Bridge and other ethical hacking companies over the years, Mr. Polic outlined some key lessons to ensure a successful penetration test. First, trade shows and industry events are great opportunities to gauge an ethical hacking company's abilities through live demonstrations. Ethical hackers should have extensive experience, certifications, insurance, and a published code of ethics. Customers should perform small consultations to verify the consultant's technical skill, communication skills, and professionalism. This also reduces investment risk when consulting new auditors.

Customers should test all systems if possible. If this is too costly, then the customer should prioritise testing efforts to harden the most critical systems with sensitive data. The customer should also consider factors such as availability, risk of downtime, and security goals to determine the project scope prior to the project implementation.

If possible, businesses should develop relationships with a few reliable and skilled ethical hacking companies with diverse skills and tool sets. This ensures that the organisation will achieve maximum security coverage and find vulnerabilities that a lone consultant could miss. Ethical hackers should provide actionable reports based on in-depth analysis rather than long lists of results from automated testing tools.

"Frost & Sullivan recommends that customers invest in annual ethical hacking assessments by leading companies such as High-Tech Bridge."

9. FROST & SULLIVAN FINAL WORD

Given the rapidly advancing sophistication level of cyber threats, businesses cannot afford to rely on untested and unproven security architectures. Businesses in every industry and of any size are now targets for attacks ranging from commodity threats by amateurs to highly-targeted, complex attacks enacted by organised and highly motivated professionals.

This represents a monumental challenge for even the most sophisticated organisations due to complex IT environments including security solutions, end-users, policies, and new technologies. In reality, no organisation can achieve 100 percent impenetrable security due to the highly dynamic and complex nature of networks and information security systems. However, businesses must increase the effectiveness of their security architectures to the point that they will not be targeted for hackers. The goal should be to achieve a security architecture that would require enough of the attacker's resources to penetrate that would cost the hacker more than the data is worth.

Businesses can accomplish this goal by assessing asset value, quantifying risk, prioritising security efforts, and then finding and correcting security weaknesses. Ethical hacking services are the best way to attain the valuable assessments and recommendations necessary to properly implement these complex security architectures.

Ideally, Frost & Sullivan recommends that customers invest in annual ethical hacking assessments by leading companies such as High-Tech Bridge. Otherwise, customers should engage ethical hacking companies that provide expert, objective analysis, in-depth reports that exclude false-positives, identify security strengths, and provide actionable recommendations. Organisations should contract with ethical hacking companies for smaller consulting engagements until they find an ethical hacker that provides best-of-breed services.

London
4, Grosvenor Gardens,
London SWIW ODH,UK
Tel 44(0)20 7730 3438
Fax 44(0)20 7730 3343

Oxford
4100 Chancellor Court
Oxford Business Park
Oxford, OX4 2GX, UK
Tel: +44 (0) 1865 398600
Fax: +44 (0) 1865 398601

Silicon Valley
331 E. Evelyn Ave. Suite 100
Mountain View, CA 94041
Tel 650.475.4500
Fax 650.475.1570

+44 (0)20 7730 3438 • enquiries@frost.com
http://www.frost.com

ABOUT FROST & SULLIVAN

Frost & Sullivan, the Growth Partnership Company, partners with clients to accelerate their growth. The company's TEAM Research, Growth Consulting, and Growth Team Membership™ empower clients to create a growth-focused culture that generates, evaluates, and implements effective growth strategies. Frost & Sullivan employs over 50 years of experience in partnering with Global 1000 companies, emerging businesses, and the investment community from more than 40 offices on six continents. For more information about Frost & Sullivan's Growth Partnership Services, visit http://www.frost.com.