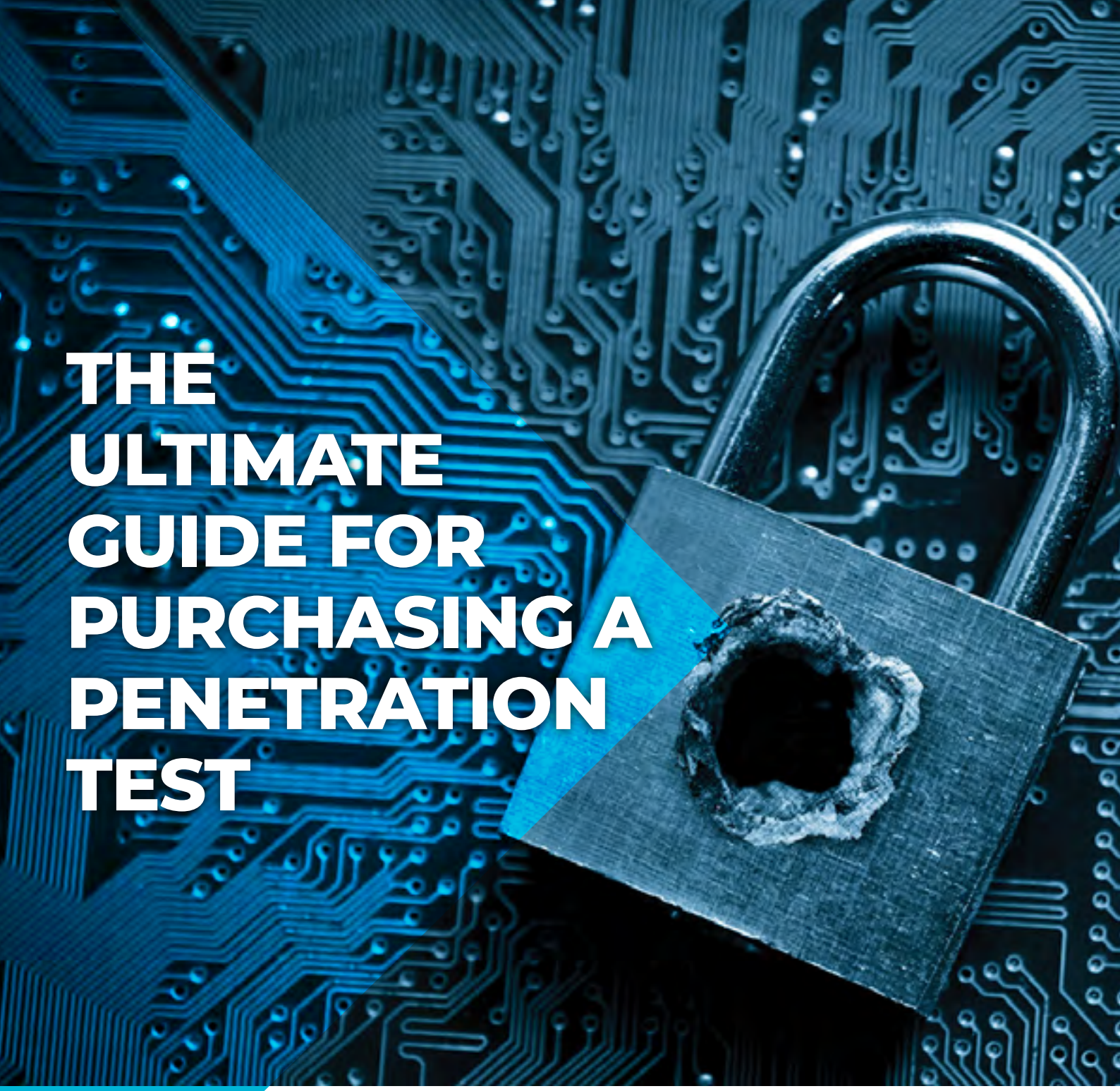
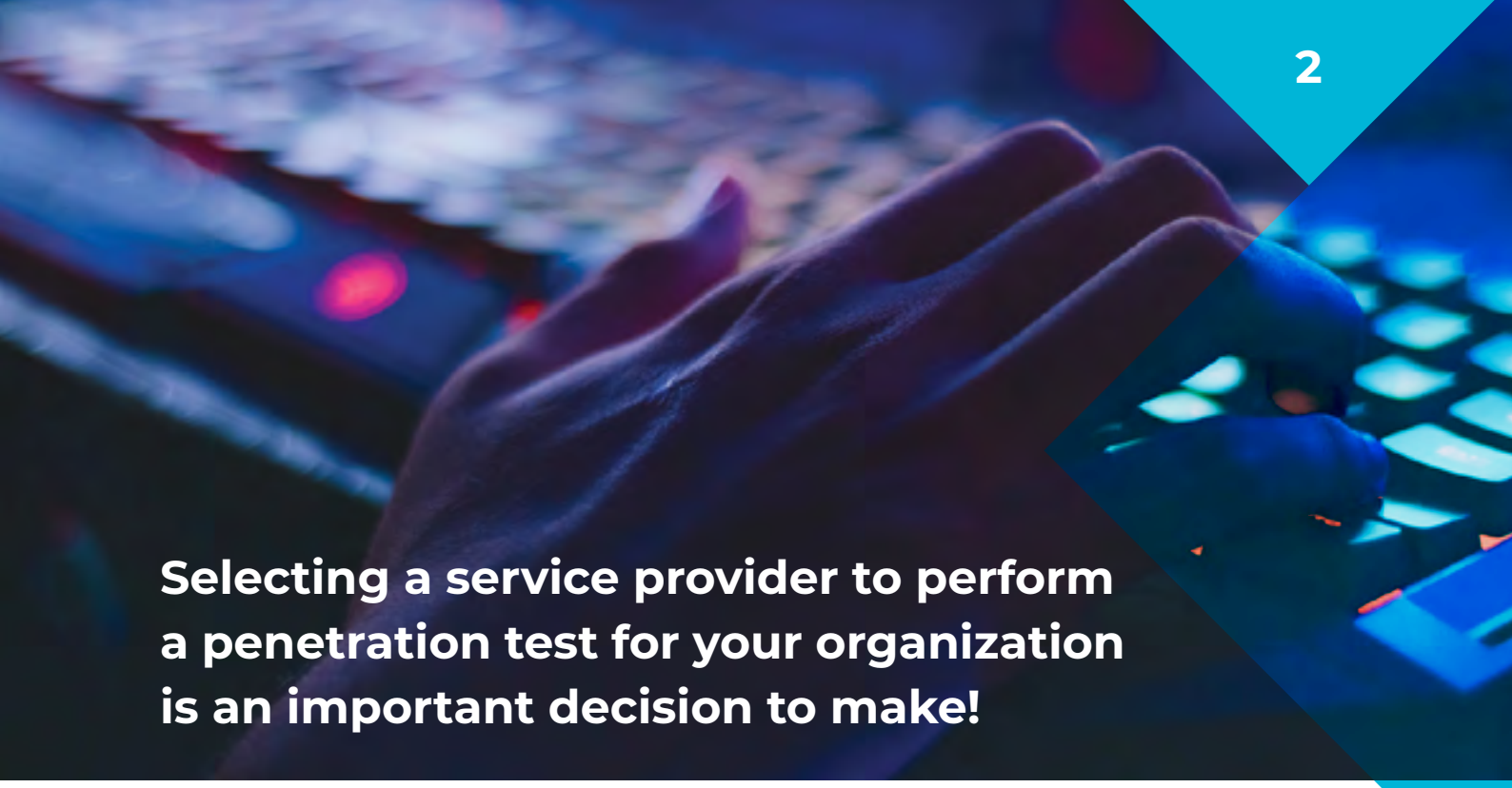


THE ULTIMATE GUIDE FOR PURCHASING A PENETRATION TEST

Selecting a service provider to perform a penetration test is an important decision. Read this guide and you will discover:

- ✓ Why you should be cautious of "Automated" Penetration Testing.
- ✓ 10 revealing questions that will help you make the best purchasing decision.
- ✓ Big misconceptions that most people have about penetration testing.
- ✓ Common mistakes and pitfalls you can avoid when buying a penetration test.

PARTNERS
IN REGULATORY COMPLIANCE



Selecting a service provider to perform a penetration test for your organization is an important decision to make!

Hiring the wrong firm or person to do your penetration test means that the outcome of the exercise will be disappointing at best. Selecting the wrong penetration testing provider could result in:

Gaining a false sense of security

Penetration tests that are performed incorrectly will not properly identify the REAL concerns and exposures that exist within your technology environment. This can promote a false sense of security and lead you to believe that your network was not as secure as you may have thought.

Becoming confused and unclear what to do next

A penetration test should produce a clear understanding of the improvements that can be made to better secure and protect the organization from bad actors. Reports and deliverables that contain too much technical jargon tend to be ignored by executives who can allocate resources for cyber security improvements.

How can you select the right penetration test provider and avoid these outcomes?

Familiarize yourself with the 10 revealing questions contained in the remainder of this guide. Use them to assess various service providers and you will increase your chances of making the right purchasing decision.

10 Questions

You Should Ask a Cybersecurity Firm Before Hiring Them To Do A Penetration Test

Q1: *Is an actual human completing the penetration test?*

Why ask? Buyer beware - many low cost penetration tests are ”automated” and involve little to no human effort. This is a BIG problem because real cyber attacks launched by actual computer hackers are not automated. Attackers use critical thinking, logic and reason to carry out sophisticated and organized cyber attacks. A good penetration test should simulate their approach instead of being limited by the capabilities of tools designed to “automate” the penetration test. Automated penetration tests are naturally silly because they assume that the same steps should be taken to compromise every organization. Organizations are inherently unique with unique security controls and work processes. This requires a human to strategize and develop equally unique attack strategies during a penetration test.

OUR ANSWER:

All penetration tests purchased from us are assigned to one or more qualified Cybersecurity Analysts who make use of tools, critical thinking, logic and reason to simulate an actual cyber security attack. We are not restricted to the rigid confines of a tool that automates the process. Every penetration test presents an opportunity to launch attacks that are tailored to the specific vulnerabilities and predisposing conditions of the organization.

piregcompliance.com
info@piregcompliance.com
(646) 863-9050

Q2: *Is the person conducting the penetration test qualified and experienced?*

Why ask? If you decide to remodel your kitchen, do you hire a professional contractor who specializes in remodeling kitchens and has decades of experience - or - do you give a teenager a hammer and hope for the best? There are many IT professionals and generalists who claim to be proficient in the art of penetration testing, but have every intention of learning on your dime. Hiring someone who does not have experience and is not certified is a risky move. Look for someone who has conducted at least 75+ penetration tests and holds one or more of these industry certifications (and do not be afraid to ask for proof!):

- **Certified Ethical Hacker (CEH)**
- **Offensive Security Certified Professional (OSCP)**
- **GIAC Penetration Tester - (GPEN)**

OUR ANSWER:

All of our Penetration Testers hold professional-level industry certifications and boast years of actual field experience. Furthermore, penetration testing is one of the core services offered by us. On average, a Penetration Tester working at Partners in Regulatory Compliance will complete 3-4 penetration tests a month. They are masters of their trade - true experts that will do the job right!

piregcompliance.com
info@piregcompliance.com
(646) 863-9050

Q3: *Can they explain the difference between a penetration test and a vulnerability scan?*

(Bonus Question): Will they perform a vulnerability scan while doing the penetration test at no extra cost?

Why ask? One of the biggest misconceptions is that a vulnerability scan and penetration test are the same exercise. This means that many cybersecurity firms will sell you a penetration test but will only perform a vulnerability scan (sounds like a rip off!). Vulnerability scans will identify Common Vulnerabilities and Exposures (CVE) such as open ports, mis-configured devices and systems that are not patched. Penetration testing attempts to exploit those vulnerabilities in an effort to compromise systems and controls. It is common for hackers to scan your network and find vulnerabilities, but they don't stop there. Based on their findings, they proceed to launch specific attacks designed to exploit the discovered vulnerabilities. **Be sure you are getting what you pay for. Don't purchase a penetration test only to have a vulnerability scan completed.**

OUR ANSWER:

We recognize the difference between vulnerability scanning and penetration testing. In fact, we consider them two separate and unique services. We do however conduct a vulnerability scan as part of our reconnaissance work for each and every penetration test. We use the results of the scan to formulate our attack strategy. The good news is that we also provide the results of the vulnerability assessment to you, the customer, in addition to our penetration test findings - consider it a two for one deal!

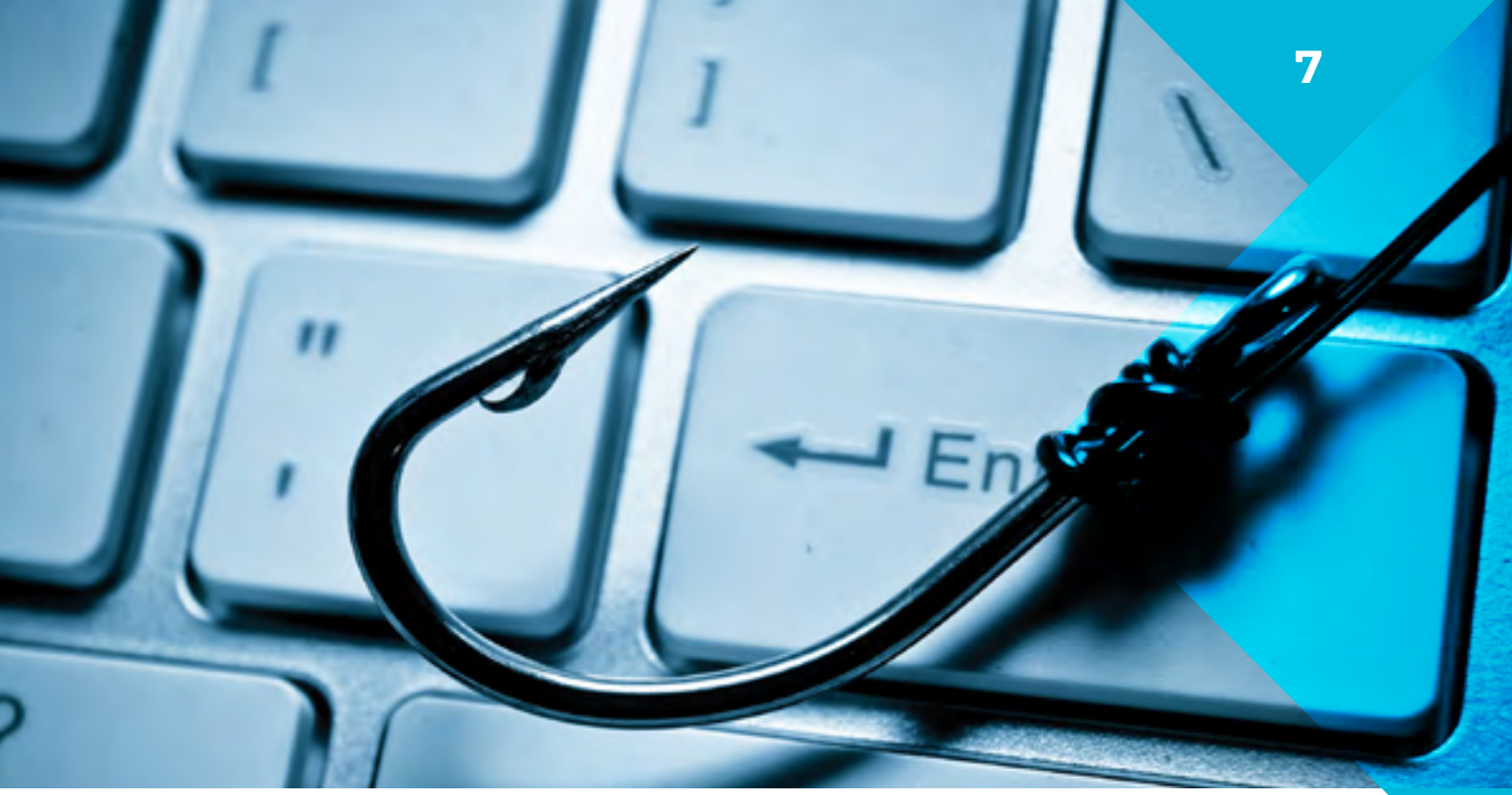
piregcompliance.com
info@piregcompliance.com
(646) 863-9050

Q4: *Do they insist on having a discussion about Rules Of Engagement prior to doing the penetration test?*

Why ask? It is important to discuss the inherent risks associated with penetration testing and it is also important to determine how intense the testing will be. For example, is the penetration tester allowed to transfer, delete or alter data once a system is compromised? Are they allowed to launch Denial of Service attacks that may cause service disruption? Can they test during normal business hours? These are just a few questions that need to be discussed and answered prior to executing a penetration test. Rules of Engagement allow for risk(s) to be mitigated and establish guidelines for testing.

OUR ANSWER:

Every penetration test performed by us begins with a mandatory Rules of Engagement discussion. The decisions made during the conversation are formally documented and signed off by both parties prior to starting any testing activities. Proper expectations are set, boundaries are established and risk is properly mitigated.



Q5: *Do they include social engineering attacks as part of their testing procedures?*

Why ask? Not all penetration tests include the same types of attack vectors which mean that many providers will not launch social engineering attacks such as **email phishing.** Social engineering is a wildly popular method for hackers to circumvent traditional security controls such as firewalls. The vast majority of all successful cyber attacks involve some element of social engineering. So this attack vector should absolutely be included in any penetration test performed.

OUR ANSWER:

Every penetration test performed by us will include social engineering attacks. Targeted phishing emails are sent to employees to try and establish false trust and influence them to take urgent action that results in negative consequences - just like the real hackers do.

piregcompliance.com
info@piregcompliance.com
(646) 863-9050

Q6: *Do they provide flexibility with logistics and scheduling or does the penetration have to be completed during their normal business hours?*

Why ask? Many cybersecurity firms will demand that the penetration test be completed during their normal business hours and if you request to have the work done at night or over the weekend (if you are worried about possible disruptions to business) then the provider will seek additional compensation or refuse. It is important that you have the ability to control when the penetration test will take place.

OUR ANSWER:

Our clients have every right to request testing activities to take place after normal working hours, including nights and weekends. We never charge extra and are happy to perform the test in alignment with your desired schedule, not ours.

Q7: *Do they make their penetration testers readily available during the testing process?*

Why ask? Some abnormal activity may be detected by your security tools or employees during a penetration test and it is imperative that you have instant access to the penetration tester to verify that they are the responsible party vs a legit attack from a bad actor. Many service providers make it impossible to contact the penetration tester(s) directly.

OUR ANSWER:

Our penetration tester(s) share their contact information at the start of every engagement with the customer. We encourage our customers to freely contact them during a penetration test if they suspect suspicious activity. It is important to verify that the penetration tester is responsible for the suspicious activity and not an actual hacker!

Q8: *Does their report include information that matters and is actionable or is it a simple list of open ports and discovered vulnerabilites?*

Why ask? While it is good to know the results or basic discovery and reconnaissance efforts, a final report for a penetration test should include more than a list of open ports and vulnerabilities. The objective of a penetration test is for you to understand how an actual hacker would logically attempt to exploit your vulnerabilities and the sequencing of attacks they would deploy so that you can improve your security control framework. So your report should include meaningful and actionable information such as:

- ✓ **A comprehensive narrative of the testing event provided by the penetration tester**
- ✓ **A detailed evaluation of each attack vector, including visual diagrams, evidence of success, and specific remediation recommendations.**

OUR ANSWER:

Our reports are focused on providing detailed information about the logic and sequencing of attacks. They also contain valuable remediation recommendations. We are also happy to provide a sample report for you to review as part of your evaluation and purchasing process!

piregcompliance.com
info@piregcompliance.com
(646) 863-9050

Q9: *Do they hold a formal meeting to present their findings, or they simply forward your report and wish you the best?*

Why ask? The deliverable for a penetration test is typically a formal report that explains the outcome of the penetration test in the form of findings and recommendations. It is important for the penetration tester to take the time and review the contents of this deliverable with you and other interested stakeholders so that a crystal clear understanding can be achieved and you know exactly what to do next. Interpreting the report on your own can be difficult due to the technical information contained within.

OUR ANSWER:

Every penetration test is concluded with a formal "Presentation of Findings" meeting. Typically this meeting will last 1-2 hours and is an opportunity for the person who completed the penetration test to review the content of the final deliverable. They will explain how they were able to launch successful cyber attacks, discuss the systems they were able to compromise and most importantly - thoroughly explain the recommendations that can be made to improve your overall cybersecurity posture.

piregcompliance.com
info@piregcompliance.com
(646) 863-9050

Q10: *Do they offer customer loyalty discounts for repeat customers and allow monthly payments for penetration testing?*

Why ask? It is recommended that penetration testing become an operational component of an organization's cybersecurity program. The exercise should be conducted periodically according to organizational policy and regulatory requirements. If you are going to conduct an annual penetration test, wouldn't it be nice to receive a discount for being a loyal customer? And wouldn't it be nice to pay for annual penetration testing services as an operating expense instead of a capital expense?

OUR ANSWER:

We offer loyalty discounts to returning customers and allow clients to commit to 2 or more years of penetration testing services and pay for the expense monthly.

YOUR PURCHASING CHECKLIST!

10 Questions You Should Ask a Cybersecurity Firm Before Hiring Them To Do A Penetration Test	COMPANY A	COMPANY B	PARTNERS IN REGULATORY COMPLIANCE
Is an actual human completing the penetration test?			✓
Is the person conducting the penetration test qualified and experienced?			✓
Can they explain the difference between a penetration test and a vulnerability scan?			✓
(Bonus Question): Will they perform a vulnerability scan while doing the penetration test at no extra cost?			✓
Do they insist on having a discussion about Rules Of Engagement (ROE) prior to doing the penetration test?			✓
Do they include social engineering attacks as part of their testing procedures?			✓
Do they provide flexibility with logistics and scheduling or does the penetration have to be completed during their normal business hours?			✓
Do they make their penetration testers readily available during the testing process ?			✓
Does their report include information that matters and is actionable of is it a simple list of open ports and discovered vulnerabilites?			✓
Do they hold a formal meeting to present their findings or they simply forward your report and wish you the best?			✓
Do they offer customer loyalty discounts for repeat customers and allow monthly payments for penetration testing?			✓

piregcompliance.com
info@piregcompliance.com
(646) 863-9050