REASONS WHY YOU SHOULD HIRE A HACKER IN THIS

Cybercrime cost globally could hit a £4.9 trillion mark by 2021; Cybercrime events cause a certain degree of havoc to organizations, even after so much investment in security upgrades.

The question is how do businesses deal with such predisposition to these attacks? Well, the answer is just in the hands of a smart hacker who can discover a backdoor and get access to sensitive data. For example, the intelligent and smart young Hamza, a computer engineer from Algeria who was spending some time in his home smiling while he hangs up although the US said he did not hang. But because the bank was not careful enough, they do not close their windows and doors and do not know how to protect their money; if he got respected and hired the bank will save $4000. He was not a bad person after all.

Organizations' must recognize the weaknesses in their cyber security, before and not after they're subjugated by hackers. On the other hand, to win this battle, you'll need to think like a hacker.

Here Are The Reasons Why You Should Employ A Hacker In 2017.

The Risks are greater In 2016 Yahoo revealed that 1billion accounts were damaged in the largest data breach in history. And as cybercrime becomes more and more highly developed, the danger posed to businesses by hackers will only amplify. Leaving your organization prone to a data breach could cost a massive £4.25m (on average) without considering the pain caused and brand damaged.

There are no limitations to these attacks as big intercontinental companies are not left out, the latest Government Security Breaches Survey found that 74% of small organizations reported a security invasion in the previous year.

For any business, a security defect that goes undetected is an enormous risk, and when GDPR (General Data Protection Regulation) hits in 2018 the stakes will only increase. Operations will begin in 2018 as The EU General Data Protection Regulation will preside over how businesses handle customer data. Compliance won't be easy, and the risk of non-compliance is enormous, with a fine of £17million. Big organizations aren't out of harm's way; therefore a thorough upgrade would be needed to secure data and to guarantee compliance. Tesco was recently lucky to escape a £1.9bn fine for a recent data breach.

How Hackers Will Heighten Your Cyber Security

Not every hacker wants to attack your business, create a monetary loss, execute unauthorized code and leak your sensitive data. There are hackers out there who are paid to defend organizations and not make worse. 'White hat' or 'ethical hackers', are security professionals who organize actions from cyber criminals and attacks. They're not your usual dark web lurking creeps.

Ethical hackers are IT security experts -- trained in hacking techniques and tools -- recruited to recognize security susceptibility in computer systems and networks. According to ITJobsWatch, the average salary for an ethical hacker is £62,500. Considering the average cost of a data breach sits at £4.23m, that's a little price to pay. Businesses and government organizations stern about IT security hire ethical hackers to investigate and make safe their networks, applications, and computer systems.

Unlike malicious 'black hat' hackers, ethical hackers will pencil down your vulnerabilities and offer you solutions and knowledge needed to fix them. Ethical hackers are hired to also perform infiltration tests – Controlled attacks on your computer system designed to detect

Proneness. But instead of taking advantage of your business, ethical hackers will document security error and you'll get insight into solving the problem. It's your responsibility to act on the ethical hacker's guidance - this is where the hard work begins. Without these infiltration tests, an organization's security space is prone to attack by malicious hackers.

Finding Ethical Hackers

Thankfully, the days of hiring underground hackers and bargain with bitcoins are over. There's now a populated market of qualified security professionals to choose from, complete with official ethical hacking certifications. Ethical hackers, or penetration testers, can be hired just like any other professional, but be certain to get concrete evidence of your hacker's acquired skills. Candidates with the CEH (Certified Ethical Hacker), CHFI certifications, which I have both and more have shown mastery of a wide range of hacking techniques and tools. Additionally, CEH certified professionals must submit to a criminal background check. These experts are committed to their profession and do not use their hacking knowledge maliciously, there are bounties and rewards and Legal Hacker Employment

It's imperative to know what you require from your ethical hacker. Create a clear statement of expectations, provided by the organization or an external inspector. Ethical hackers shouldn't be hired to provide a broad overview of your policies, but to provide solutions to specific problems. So ask specific questions like "Do we need to review our web app security?" or "Do our systems require an external penetration test?"

Before hiring an ethical hacker to conduct a penetration test, businesses should make certain a catalogue of systems, people and information are readily available.

Abdulaziz AL-Humoud
Senior Security Engineer