Trustwave®

# Making the Business Case for Penetration Testing

**Chief information security officers (CISOs) know that a consistent penetration testing program is a crucial element in any cyber security program, helping them uncover both known and previously unknown vulnerabilities. But amid numerous other budget demands, persuading their fellow leaders and board members that pen testing is a worthwhile investment can be a challenge.**

CISOs understand that cyberattacks are a bigger organizational threat than ever, and that in-house security teams are already understaffed and overworked. Security teams also generally lack the specialized expertise to identify vulnerabilities and develop a roadmap for remediation or patching. It's up to CISOs to explain these realties to their non-technical counterparts, helping them grasp the magnitude of the risk, as well as the value and trustworthiness of a reputable testing partner.

## The risk is difficult to overstate

It's common for C-suite and other executives to assume that an automated vulnerability assessment is sufficient to protect digital assets. Few members of the C-suite are equipped to understand that while vulnerability testing is a vital cog, pen testing goes far deeper and offers specific solutions rather than mere automated alerts.

But while non-technical executives may know little about technology, there's one thing they understand well: risk. When a CISO is asked how the company can afford penetration testing on top of other digital security measures, an effective response is to flip the question around: "Can we afford not to protect our customer data, intellectual property, and reputation from today's relentless attacks?"

Any CEO, CFO, or CRO who keeps up with the business press will see the validity of this argument. Almost daily, another prominent business admits it has suffered a breach. Perhaps it's a healthcare organization brought to its knees by ransomware. Or a retailer that sees customers' personal information released to the Dark Web. Or even a defense contractor whose stolen data could compromise national security.

Such breaches cost victim organizations in revenue, reputation, downtime, and market value. It's no wonder that according to IBM's annual data breach report, the cost of a breach rises every year—most recently to an average of $4.35 million.

Top executives and board members will readily see that the cost of **industry-leading penetration testing** pales by comparison to the potential consequences of a breach.

## "Will testers steal our data?"

Some executives hesitate to engage third-party testing partners, fearing the very firm they're hiring will steal their IP or use vulnerabilities to launch an attack. "After all," this line of thinking goes, "whether they're wearing a white hat or a black hat, they're all hackers at heart."

This objection isn't entirely unreasonable, which is why the reputation and professionalism of the testing partner is so important. At Trustwave, our best-in-class pen testers are full-time, vetted company employees. Unlike some firms, we don't use external contractors who take important knowledge about your systems with them when they move on to the next job.

With more than 150 certified researchers, Trustwave SpiderLabs can point to over 25 years of industry leadership in vulnerability research and findings. We've discovered more than 30,000 vulnerabilities (including 9,000 with ratings of high or critical) and perform over 100,000 hours of tests globally each year.

Moreover, SpiderLabs is **certified with five accreditations** by the international security standards body **CREST**, including Vulnerability Assessment (VA), Intelligence-Led Penetration Testing (STAR), Penetration Testing (PEN TEST), STAR-FS Intelligence-Led Penetration Testing, and the new **OWASP Verification Standard (OVS)**.

## “Can’t we do it in-house?”

Another common sticking point for executive teams is the need for third-party penetration testing. They look at the IT org chart and ask whether a few staffers might be tasked with probing for bugs.

There are two answers to this question. First, IT staffers are overworked and have been for some time. A long-term global labor shortage means corporate tech and data security groups will remain stressed for the foreseeable future. So, the idea of just grabbing a couple of idle IT folks and asking them to run pen tests is a non-starter.

Second, in-house tech workers, no matter how talented, are simply too close to the company’s assets and systems to dispassionately probe them for vulnerabilities. Rather than ask an IT employee to probe for weaknesses in an app they helped develop, it’s far better to bring a second, objective set of eyes to the issue.

And then there’s the question of expertise and experience. Penetration testing is both science and art. Trustwave’s SpiderLabs professionals take great satisfaction in finding flaws that could lead to catastrophe. In one recent pen test for a leading global bank, Trustwave tackled an app the bank had extensively tested in-house—and found a business-logic bug that could have allowed attackers to exfiltrate money. Think about how much value a finding like that delivers.

But such findings don’t just happen. They are the result of deep experience, expertise, and hard-earned intuition. That’s the kind of message CISOs need to get across to help their leadership team understand the true value of pen testing.

To learn more, visit the **penetration testing section** of our website or **contact us**.

Trustwave®

**www.trustwave.com**