Cybersecurity in 2021: Test Your System to Protect Vital Data

Cybersecurity is a significant global threat, particularly for the financial sector where essential data must be protected at all costs. A major cyberattack on the U.S. government in late 2020 potentially exposed the sensitive data of dozens of agencies. This was a stark reminder that no business or government entity is immune to highly consequential cybersecurity breaches that have increased in sophistication and frequency for years.

BasisCode welcomes having our clients do their own security penetration tests on our systems, so they can be assured that we're the best possible partner committed to the highest level of data security. While we're obtaining our own security testing, we also recommend that our clients regularly conduct their own penetration testing on their environments.

What is Penetration Testing?

Penetration testing involves systematically attempting to break down a firm's security barriers in their network and data storage systems to expose potential vulnerabilities. These vulnerabilities can ultimately be addressed and remedied before real criminal hackers have the chance to uncover and exploit them.

As Benjamin Franklin once keenly noted, "an ounce of prevention is worth a pound of cure." Penetration testing is a transparent, proactive approach that BasisCode urges its clients to deploy with our software, with their other critical IT and security vendors, as well as with their own systems.

Top Tips for Penetration Testing

1. **Hire a professional:** Hackers aren't just criminals; there's a wide trove of IT professionals who make it their mission to expose potential IT frailties in order to guard against malicious cyber behavior. Hire one as a partner to examine all of your security measures.
2. **Change the company:** Conduct security penetration testing regularly, such as once a year. Instead of hiring the same IT expert to carry it out, work with a different professional every year to ensure well-rounded expertise and different approach.
3. **Share the results with the vendor:** BasisCode recommends clients undertake security penetration testing on their vendor's systems and provide them the results. In our case, discovered risks that are deemed a medium or high risk will be immediately addressed.
4. **Take ownership:** Participating in penetration testing increases stakeholders' knowledge of security risks while more authority over their cyber security. This knowledge will be useful and can be easily applied to other systems, internal and third party. While vendors may hold the IT expertise, clients should play a role in protecting their data, and this strategy is one way to do that.
5. **Collaborate:** If the cost of security penetration testing is prohibitive, connect with other clients of the specific vendor to share the cost and the information.
6. **Practice other security measures:** Security penetration testing is an important way for users to ensure they're putting up the best defense

against cyber intrusion, but it’s not the only one. Employ a comprehensive cybersecurity strategy that includes tactics like employee training, vulnerability scanning, single sign-on or multi-factor authentication, which are additional precautions that can enhance security.

Working with sensitive financial data involves a significant amount of trust between service providers and clients. Penetration testing is just one way to establish trust and feel confident that the systems you rely on every day are strong. But this is only true if you share the results! Let BasisCode and other vendors you work with know about any security risks that come up in the penetration testing and get their assurance that they will address any critical issues.

Ultimately, it is imperative that your systems, and those of your vendors, have a proven security foundation to start with. Regular testing should be an add-on that reaffirms the security of the user authentication and data transfer/storage protection that is already in place.

Ready to take your compliance management to the next level? Reach out to our team to get started.