Pentest with Purpose Kit

F&C CPAs

Pentest with Purpose: Your Essential Resource Kit

Welcome to the "Pentest with Purpose" Resource Kit!

Thank you for attending our session on maximizing the security impact of penetration testing through focused, strategic efforts. In this resource kit, you will find valuable tools and materials designed to reinforce the key concepts we covered in class. From understanding the risks of unfocused pentesting to developing purpose-driven methodologies that align with your organization's risk profile, these resources will help you transform penetration testing into a powerful, targeted tool in your cybersecurity arsenal.

We hope these materials empower you to apply what you've learned and continue your journey toward more effective and impactful pentesting.

Committed to Your Success

At **F&C**, we leverage our deep expertise in cybersecurity, risk management, and enterprise technology to provide comprehensive solutions tailored to our clients' unique needs. Our commitment to purposeful penetration testing aligns with our broader approach to cybersecurity—focused, strategic, and industry-specific.

Drawing on years of experience, we've developed custom cybersecurity solutions, including a proprietary technology system for secure remote access to casino gaming machines. Our range of services also includes business data metrics, real-time reporting, and Microsoft-based software solutions designed to meet the specific compliance and operational requirements of industries we serve.

Our team of cybersecurity experts and technology innovators work together to identify, analyze, and implement solutions that go beyond generic fixes, ensuring that our clients not only meet but exceed their security and business objectives. By continuously staying at the forefront of technological advancements, **F&C** is able to offer dynamic, scalable, and effective cybersecurity strategies that protect what matters most.

Tax Solutions

Compliance

Business Services

Advisory & Strategy

Training

Enterprise Technology

Not a Silver Bullet: The Limits of Penetration Testing

By Bobby Simpson, CIO F&C CPAs

Penetration testing, or "pen testing," is a method used by businesses to find cybersecurity weaknesses in their computer systems by simulating a hacker's attack. Many organizations feel better about their security after running their annual pen test. But are their systems really more secure? In folklore, the magical silver bullet was used as protection against all sorts of monsters.

However effective they may be, silver bullets, even in the movies, don't always work. In real life, pen testing has the same problem. Not only does it not always uncover the real problems, but security improvements only happen when you fix the issues found during the test. This article explains why penetration testing should not be seen as a one-step solution, a silver bullet, if you will, and why a plan for fixing problems after the test is critical.

Pen Testing Isn't the Solution – Fixing Problems Is

One common misconception is that simply getting a penetration test will make an organization's systems secure. While it's true that pen tests can show where there are risks, that doesn't mean the system is safer just because the test happened. The test is like a medical check-up—it identifies problems, but it doesn't fix them.

Without a plan to address the problems that are discovered, a penetration test might give a false sense of security. You may feel that the test itself is enough to improve security, but nothing changes until the issues found are fixed. In some cases, staff might already know about some of the problems uncovered by the test, but they haven't been addressed due to limited time or resources. If these known problems aren't dealt with, the test doesn't add much value.

Start with a Basic Security Check

Before spending money on a penetration test, it's wise to perform a basic security review. This involves looking at your current systems to identify easy-to-fix problems, like weak passwords, unpatched software, or outdated firewall settings. Many times, pen tests reveal simple issues that could have easily been caught and fixed beforehand.

By taking care of the low-hanging fruit first, you can make better use of the pen test by focusing on more complex problems. You'll also save time and money by not paying a third party to uncover things your team could have identified on their own. This also allows your organization to enter the test with a better overall security setup, which helps get more meaningful results from the test.

Scoping the Penetration Test: Let Risk be Your Guide

If you choose to have a penetration test performed, scoping it correctly can make a huge difference in the outcome. The "scope", or focus and limits, of a test will determine what elements of your system are subjected to scrutiny. For example, some tests focus heavily on uncovering personal information, while others may focus on taking control of your website. Which is more important?

You never want weaknesses, of course, but some are certainly more important than others, because of the potential for financial impact, or damage to your organizational reputation or mission. Having a test performed before you determine your risk is like having a checkup with the doctor without telling them about your symptoms. They may find the biggest problems, but they may not. So, defining risk in various aspects of your organization is the first step to defining a good scope for a pen test. Once that is complete, find a security provider that has experience with your industry, or at least with the elements of your system that constitute your greatest risk. Choosing a provider who understands you is a great way to get the most out of the money you spend on testing.

Fixing Problems is the Hard Part

Once the penetration test is done, the real work begins: fixing the issues that were found. This process, called remediation, is often overlooked or underfunded. Many organizations focus on paying for the test but don't allocate enough resources to pay someone to actually fix the problems it uncovers.

In reality, the improvements in security don't come from the test itself, but from the work done afterward to address the vulnerabilities the test reveals. This can require more effort and money than the test itself, especially if the issues are complex. Fixing problems might mean updating software, investing in new technology, or retraining staff on security practices.

This is why it's important to budget for remediation, and choose a separate provider for this work, when planning a penetration test. At a minimum, you should budget at least as much on fixing the problems as you did on identifying them. Otherwise, the test might end up being a wasted expense, with the same security risks still present after the test.

Ongoing Effort: Security is Never "Done"

It's also important to remember that a pen test only shows vulnerabilities at a specific point in time. Security is a constantly changing field, with new threats and vulnerabilities emerging all the time. The results of a pen test are just a snapshot, and even if you fix all the issues found, new risks will develop as your systems and the technology landscape evolve.

To stay secure, organizations should think of security as an ongoing process, not a one-time task. Regular security reviews, training, and updates to policies should be part of your long-term strategy. Pen tests can be a useful tool, but they work best as part of a broader security program that includes continuous monitoring and improvement.

By integrating security into daily operations and budgeting for periodic tests and fixes, organizations can better protect their sensitive data and systems from evolving threats.

Conclusion

Penetration tests are a valuable tool in identifying security weaknesses, but they are not a complete solution on their own. The real value of a pen test comes from addressing the vulnerabilities it reveals. Without a commitment to fixing those problems, the test may only provide a false sense of security.

By starting with a basic security review, planning for comprehensive remediation, and treating security as an ongoing responsibility, organizations can significantly improve their overall security posture. Only then will penetration testing truly help make your systems safer.

Scan to add
Bobby to
your contacts

Bobby Simpson
CHIEF INFORMATION OFFICER (CIO)

☎ 405-395-5191
405-471-9619
✉ bsimpson@finley-cook.com
601 N. Broadway Avenue
Shawnee, OK 74801

F&C CPAs
FINLEY-COOK.COM

10 Critical Steps to Prepare for a Penetration Test

Why Preparation is Critical for Effective Penetration Testing

Penetration testing is a powerful tool in identifying vulnerabilities within your organization’s security infrastructure. However, jumping into a test without proper preparation can lead to incomplete or misleading results. The checklist provided highlights the foundational steps that must be taken to ensure the test is both effective and accurate. These steps aren’t just recommendations; they’re essential for safeguarding your systems, ensuring the test's validity, and maximizing the value of your cybersecurity efforts.

The Risks of Skipping Preparation

Skipping any of these steps could lead to serious consequences. For instance, running a test on outdated systems or software might identify vulnerabilities that have already been addressed with patches, rendering the test less useful. On the other hand, neglecting to back up data or test recovery processes could lead to significant data loss if a test inadvertently disrupts your environment. By fully preparing, you ensure that your penetration test will focus on finding and addressing the real, current risks that your organization faces, rather than wasting time on issues that could have been avoided through basic hygiene.

Ten Things To Do Before Performing A Penetration Test

1 **BACK UP YOUR DATA:**

Data is one of your most critical assets. A thorough backup routine ensures that, in the event of a mishap during a penetration test, your data remains secure and retrievable. This is crucial because a penetration test simulates real-world attacks, and disruptions—although unlikely—are always a possibility. A tested backup and restore process can prevent any potential losses from escalating into bigger problems.

2 **INVENTORY YOUR DEVICES AND SOFTWARE:**

Knowing what you’re working with is the first step in protecting it. Without an accurate inventory of all devices, software, and connected systems, you could miss securing key components during your penetration test. This comprehensive view allows for a more focused and efficient test by identifying all potential entry points.

3 **UPDATE AND PATCH EVERYTHING:**

Running a penetration test on unpatched or outdated systems gives you a false sense of vulnerability. Many common security flaws are addressed in regular patches, so ensuring all updates are applied before the test helps focus the effort on real, undetected issues, not those that have already been resolved by vendors.

4 IMPLEMENT MULTI-FACTOR AUTHENTICATION (MFA):

MFA adds a critical extra layer of protection by ensuring that even if a password is compromised, unauthorized access is still blocked. By enabling MFA across systems, you not only strengthen security but also reduce the attack surface, which allows the penetration test to focus on more complex vulnerabilities rather than the low-hanging fruit of password breaches.

5 USE AN UP-TO-DATE FIREWALL:

Firewalls are a critical defense against unauthorized access. They filter and block suspicious activity before it can infiltrate your network. Testing without verifying that your firewall is up-to-date risks skewing the results of the penetration test. Ensure that your firewall is configured properly and running the latest version to give a clearer picture of your network's security.

6 USE ANTIVIRUS AND ANTI-MALWARE SOFTWARE:

Antivirus and anti-malware software are essential tools in the constant fight against malware. Running these tools during a penetration test helps identify any malicious programs that might already exist and protects your system from new malware during the testing process.

7 TRAIN YOUR STAFF:

Even with the best security technology, human error remains one of the biggest risks to any organization. Well-informed employees can act as a first line of defense, recognizing phishing attempts and other social engineering attacks. Properly training your staff ensures that your penetration test will reveal technological vulnerabilities, not merely human errors that could easily have been avoided.

8 CREATE AND TEST AN INCIDENT RESPONSE PLAN:

When a security incident occurs, a well-prepared and regularly tested incident response plan can mean the difference between a contained threat and a widespread breach. Testing this plan before a penetration test ensures that if any real-world issues arise during testing, your team will know exactly how to handle them. Additionally, the test itself can serve as a way to further refine and evaluate the plan's effectiveness.

9 REVIEW AND LIMIT USER ACCESS:

Controlling access to sensitive information is a critical security measure. Before conducting a penetration test, ensure that only the necessary individuals have access to specific systems. This limits the risk of insider threats and minimizes the number of potential entry points that need to be tested.

10 GET INSURANCE AND DO YOUR PART:

Cybersecurity insurance helps mitigate the financial impact of a breach, but it's important to ensure that your policies are up to date and that you've met all necessary requirements before the penetration test. Failure to do so could leave you unprotected in case of a security incident, whether real or simulated during the test.

According to IBM's Cost of a Data Breach Report, organizations that implement a well-tested incident response plan and extensive security measures **save** an average of **$2.66 million in** breach costs.

"Being prepared for a penetration test is like locking all your doors before you leave the house—it's the first step in making sure your security stands up to the challenge." – Bobby Simpson

F&C specializes in providing tailored enterprise technology and cybersecurity solutions designed to help Tribes and enterprises strengthen their security strategies. With years of experience working alongside clients in diverse industries, we offer comprehensive services—from assessing risk profiles to implementing advanced technological protections. Our team blends deep expertise in accounting and cybersecurity to help analyze needs, prepare for threats, and build resilient defenses. Whether you're focused on post-pentest remediation or need ongoing support to maintain a strong security posture, we're here to ensure your organization is protected and future-ready.

Maximizing Your Pentest Results: What Comes Next

Now that you've completed the penetration test and identified vulnerabilities within your system, it’s time to shift focus to post-pentest actions. The real value of a penetration test isn’t just in discovering weaknesses but in how you respond to them. By addressing the vulnerabilities uncovered during the test, you can prevent future security breaches and build a more resilient infrastructure. This process involves more than just patching issues—it requires developing a strategy to continuously monitor, adapt, and evolve your security posture. In the following section, we’ll guide you through the critical steps to take after your pentest to ensure that your organization strengthens its defenses and maximizes the long-term impact of the testing efforts.

Post-Test Checklist

1

BACK UP YOUR DATA:

Data is one of your most critical assets. A thorough backup routine ensures that, in the event of a mishap during a penetration test, your data remains secure and retrievable. This is crucial because a penetration test simulates real-world attacks, and disruptions—although unlikely—are always a possibility. A tested backup and restore process can prevent any potential losses from escalating into bigger problems.

2

INVENTORY YOUR DEVICES AND SOFTWARE:

Knowing what you’re working with is the first step in protecting it. Without an accurate inventory of all devices, software, and connected systems, you could miss securing key components during your penetration test. This comprehensive view allows for a more focused and efficient test by identifying all potential entry points.

3

UPDATE AND PATCH EVERYTHING:

Running a penetration test on unpatched or outdated systems gives you a false sense of vulnerability. Many common security flaws are addressed in regular patches, so ensuring all updates are applied before the test helps focus the effort on real, undetected issues, not those that have already been resolved by vendors.

According to Gartner, organizations that effectively act on penetration test results can reduce their risk of a major security incident by up to 40%.

Cybersecurity for Tribes and Tribal Gaming: Navigating Unique Challenges

Cybersecurity is a critical concern for all organizations, but for Tribes and their enterprises, the stakes are even higher. The combination of Tribal sovereignty, diverse program services, and revenue-generating gaming operations presents distinct cybersecurity challenges. Tribes must approach security with strategies tailored to these unique factors, focusing on protecting sensitive data, preserving sovereignty, and maintaining the integrity of gaming infrastructures.

Why Cybersecurity is Different for Tribes:

- Sovereignty and Limited Backstops: Unlike non-Tribal entities, Tribes may not have state or federal laws to fall back on when dealing with cyber threats. Sovereign regulations place the responsibility squarely on Tribes to establish and enforce their own cybersecurity policies.

- Diverse Program Services: With services ranging from healthcare to financial distributions, Tribes manage a wide array of sensitive data. This data requires robust protection from increasingly sophisticated cybercriminals who target healthcare records, financial data, and more.

- The Gaming Target: Tribal gaming, a critical source of revenue, attracts cybercriminals aiming to exploit financial transactions or gain access to personal information. The remote locations of some gaming establishments also add complexity to recruiting skilled cybersecurity personnel, making effective protections even more vital.

Avoiding the Panic: Strategic Cybersecurity Measures

While cybersecurity is undeniably important, it’s equally important not to fall into the trap of panic-driven spending on “silver-bullet” solutions that promise to fix everything. True security begins with understanding your actual risks and addressing them methodically. For Tribes, this means identifying key vulnerabilities in critical areas and applying targeted solutions.

For example, penetration testing is often misunderstood. A proper pentest will always find a way in—what matters most is the potential business impact of the identified vulnerabilities. The real question is whether the test revealed a risk that could critically harm your Tribe’s operations, or simply found minor weaknesses that, while important, are less of a threat than issues like ransomware.

> **"Effective cybersecurity isn't just about finding vulnerabilities; it's about identifying which ones really matter to your business and addressing them with focused, strategic actions."**
>
> – Bobby Simpson, CIO

Transition to Post-Pentest Action: Moving from Testing to Protection

Once you've completed a penetration test, the journey to stronger cybersecurity doesn't end—it's just beginning. Understanding the results and developing a concrete plan of action are critical to ensuring the test leads to meaningful improvements in your security posture. Here's what to focus on after your pentest:

1. Understand and Share the Results:

After reviewing the report, make sure everyone in your organization—from leadership to IT—understands the weaknesses uncovered during the test. Ensuring transparency across departments helps align resources for effective remediation.

2. Develop a Remediation Plan:

Create a detailed, actionable plan to address the issues uncovered. Prioritize the most impactful vulnerabilities first, and ensure your team knows what steps to take and when to execute them.

3. Re-test and Confirm:

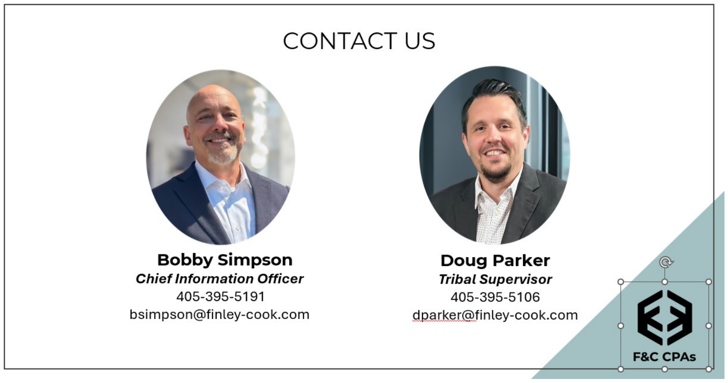
Once remediation is complete, conduct a follow-up test to ensure the fixes have worked and no new vulnerabilities have been introduced. This step ensures your efforts have made your organization stronger than before.

F&C's Expertise: Supporting Tribes in Every Phase of Cybersecurity

F&C has extensive experience helping Tribes and enterprises navigate their unique cybersecurity challenges. From assessing risks and performing thorough penetration tests to building post-test action plans, our team offers tailored solutions designed to protect your data, your sovereignty, and your operations.

"Cybersecurity for Tribes isn't just about defense—it's about building resilience. Our goal is to ensure that your systems not only survive threats but come out stronger."
– Bobby Simpson, CIO

Whether you need help identifying vulnerabilities, developing a strategy, or securing your gaming and enterprise operations, F&C can guide you through every step of the process.



CONTACT US

Bobby Simpson
Chief Information Officer
405-395-5191
bsimpson@finley-cook.com

Doug Parker
Tribal Supervisor
405-395-5106
dparker@finley-cook.com

Innovation & Expertise
Built Upon History &
Heritage

F&C CPAs

601 N. Broadway Avenue
Shawnee, Oklahoma 74801

Phone: 800-375-3286
Email: info@finley-cook.com

With headquarters in Shawnee, Oklahoma, and satellite offices stretching from Alaska to Wyoming, F&C CPAs is proud to offer tailored regional solutions while maintaining our strong local identity.

Our team of over 200 diverse professionals, including CPAs and specialists, is dedicated to providing comprehensive services across various sectors, from Accounting to Tax.

For over 35 years, we have partnered with Tribal enterprises and other organizations to deliver high-quality, innovative solutions. At F&C, we promise personalized attention, proactive communication, and transparency, ensuring we consistently exceed our clients' expectations.

We're Here to Help: Your Ongoing Resource

Cybersecurity is an ongoing journey, not a one-time event. The insights and tools shared in this resource kit are designed to give you a solid foundation, but as your organization’s needs evolve, so too do the challenges. Whether you need additional guidance, assistance with implementing security measures, or further penetration testing to assess new risks, our team is here to provide continuous support.

Our commitment extends beyond simply identifying vulnerabilities. We’re dedicated to helping you build stronger defenses, respond to emerging threats, and ensure that your organization stays secure. As your trusted partner, we’re ready to work with you every step of the way, making sure your cybersecurity strategy not only addresses today’s challenges but is prepared for the future. Reach out anytime for expert advice or customized solutions that fit your unique needs.