How to create a bespoke risk-based testing strategy

Shaun Weber – Penetration Testing Team Leader

Jed Kafetz – Cyber Security Practice Lead

claranet cyber security®

This eBook demonstrates how you can easily build a programme of offensive security testing that is bespoke to your organisation's IT estate, the data you want to protect and the risks you are likely to face.

The aim of this is to show you exactly where the organisation is vulnerable (and why) and what actions are needed to remediate those risks.

claranet cyber security®

Chapters:

claranet cyber security®

1. Smart questions **get smart answers**

The question is not "why conduct offensive security testing?" The question is "why make a concerted effort to test multiple IT assets, with different kinds of security testing, over a definite period, and then evaluate the results?"

Without a testing strategy, you might go about hardening your defences and improving your security posture with a piecemeal and random approach. Penetration test this application or that website, because it's the first thing on your agenda. Improve your cloud security settings or Active Directory controls because it's "free".

A security testing strategy enables you to take a methodical and thorough approach to testing assets across your IT estate, thus giving you a more complete picture of where your gaps and weaknesses lie and where you should focus your efforts.

2. Ten-dollar words

You may have noticed some hifalutin adjectives in our title. They're not just for show and we'd like to explain why.

"Bespoke" means a programme of offensive security testing that is tailored to your business and its data. All offensive security testing should begin with a scoping exercise that takes into account your goals, your IT estate and how it is used, as well as the threats you are likely to face. Just as one single penetration test should be scoped according to your particular needs, a programme of offensive security testing should also be scoped to the needs of your business.

"Risk-based" further defines what you should test and why. A risk-based testing strategy would take into consideration questions such as:

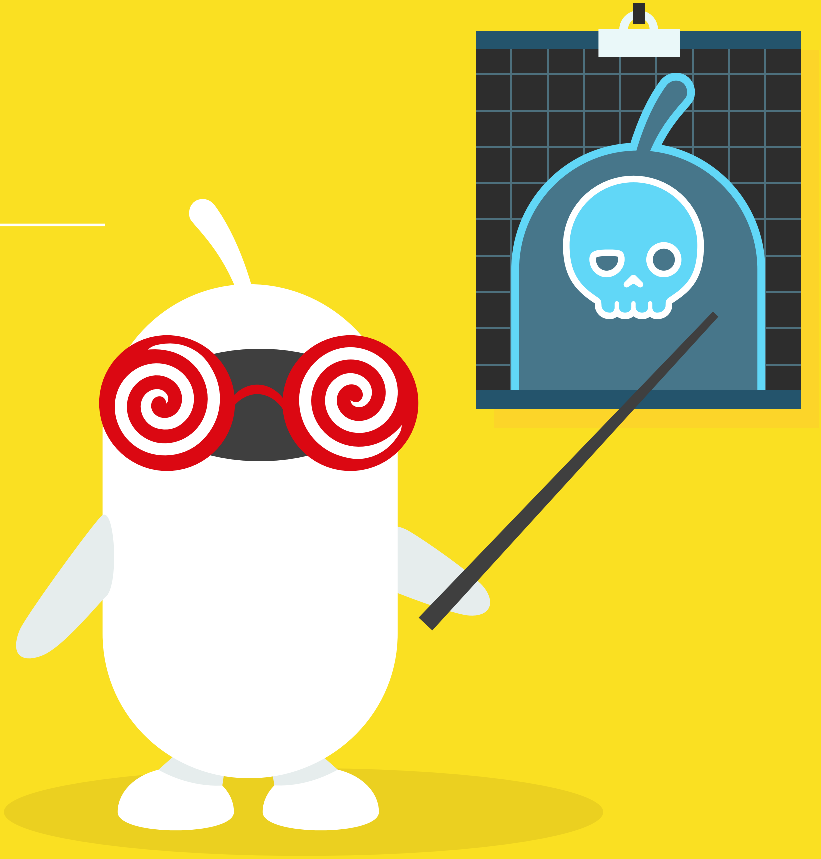
- **What are the greatest cyber risks that your industry and organisation face?**
- **What are the highest-priority and highest-risk assets in your IT estate?**
- **What is a cyber attacker likely to target and why?**

claranet cyber security®

1.
2.
3.
4.
5.
6.
7.
8.
9.
10.
11.
12.
13.

3. Expertise costs money, **but so does everything else**

There is an old saying: consultants borrow your watch to tell you what time it is. Ask a consultant and they'll tell you that it's only half true.



One piece of advice recurs multiple times in this eBook and we want to announce it upfront, loud and proud: the best way to devise a bespoke programme of offensive security testing is to **combine your knowledge of your business and its data with the expertise of a security consultant who can think like an attacker.**

They understand how an attacker would target your organisation, know how different types of testing will uncover the weaknesses and gaps in your security posture, and provide practical recommendations for how you can harden your defences. A security consultant can also advise you on how your budget will be best placed – so long as you are honest with them about your security budget and your organisational goals.

There. Now we've said it, we can move on to the interesting stuff – the real reason you're reading this. Buckle up. Let's get started...

4. Where to begin: IT asset mapping

Do you know what your attack surface is? Before deciding what you should test, you should understand what attackers can target. To understand your attack surface, you should **create an asset inventory which contains every asset in your IT estate and maps out how it is structured.** At the most basic level, this can be split into two categories:

1. External and web-facing assets

Alongside phishing campaigns targeting your users, any assets which are connected to the internet are the first portal of call for cyber attackers trying to gain a foothold on your network. This is because they can be easily discovered by attackers when researching your organisation.

Some of your external attack surface may be unknown to you. An attacker will likely conduct OSINT (open-source intelligence gathering) to find overlooked web-facing assets which they will attempt to compromise. Obsolete or unused assets are often targeted because organisations neglect to update and maintain the security controls for these assets.

To discover this hidden attack surface, conduct an OSINT exercise with the help of an offensive security consultant.

2. Internal infrastructure

Once an attacker has gained a foothold on your network, their next objective is internal reconnaissance, to gather knowledge of your internal infrastructure, as well as how it is configured and used. This will enable the attacker to make their next moves – lateral movement and privilege escalation – undetected. Because any attacker able to cause significant damage will gather this knowledge, you should too.

One way to better understand the internal infrastructure of your IT estate is to use a configuration management database (CMDB). IT asset management (ITAM) and configuration management are two distinct practices. While ITAM involves creating an inventory of IT assets, such as software, hardware, networks, and data, and managing their lifecycle, configuration management focuses on tracking the interdependencies between these assets in a configuration management database (CMDB). Doing so will give you a better idea of how an attacker will pivot around your network.

Other methods of mapping out and understanding your internal infrastructure include:

- **Active Directory enumeration**
- **Port scanning and service identification**
- **Host discovery**
- **DNS enumeration**

Hardening your defences in your internal infrastructure is one of the most effective ways to prevent your attacker escalating their privileges so that their attack does not go on to cause even greater damage.

5. What are you trying to protect and why?

Once you have a clear understanding of what attackers can target, you should aim to understand what they are likely to target. The outcome of this exercise is to **build a risk register which will eventually give you a clear overview of every vulnerability you are exposed to across your entire IT estate,** and allow you to plan your response based on your organisation's risk appetite. Your risk register is a living document which should be updated after each round of security testing.

First, ask yourself: **what are you trying to protect and why?** This will help you understand:

1. Which IT assets are highest value to you

2. Which assets present the greatest risk to your organisation

Remember that your highest priority assets and your highest risk assets are not always the same. When you create a risk register you must consider the context of how these assets are used and why they are required for the successful running of your organisation.

There are a number of ways to determine this:

- **Consider where your sensitive personal data and/or financial data is stored. How do users and user groups access this?**
- **Consider which assets will cause the greatest disruption to business continuity if they are compromised e.g., key services and systems that employees require to complete their daily work.**
- **Consider which assets will cause the greatest financial risk and cost to your organisation if they are compromised e.g., key services and products that customers use.**
- **Consider any compliance obligations, such GDPR, or industry-specific regulations such as HIPAA or PCI DSS. The consequences of a data breach will also impact how your assets are categorised on your risk register.**
- **Consider which assets attackers will use to gain a foothold on your network or escalate their access privileges.**

One way to get a better understanding of which assets present the highest risk is to work with an offensive security consultant. Though may understand what you are trying to protect, being able to think like an attacker enables security consultants to provide guidance on the exact techniques they would use.

claranet cyber security®

6. Consider how your **environment is used**

Change introduces risk via security vulnerabilities that go unmonitored. Consider website updates and new code releases for web-facing applications as changes that are likely to introduce new vulnerabilities. Which assets change most frequently and why?

Which user groups handle the most sensitive data? How do users access your highest priority or highest risk assets? Because attackers will find ways to target these, such questions should be in the forefront of your mind as you move on to the next stage of devising your risk-based testing strategy.

claranet cyber security®

7. **Scenario planning:** what are your principal security concerns?

The next step to devising your security testing strategy is to establish what risks you want to protect your organisation from. An effective way to achieve this is scenario planning.

This involves **creating hypothetical scenarios to establish your principal security concerns.** Here are some example scenarios with principle security concerns which you can use:

- **An attacker gains access to an official social media account and posts disinformation which affects the share price of the company**
- **An attacker gains access to a database containing confidential information about your employees**
- **An attacker gains access to a database containing customers' payment card information, then exfiltrates this data**
- **An attacker gains access to a web application or software in a production environment, and disrupts or publicly defaces it**
- **An attacker gains access to a cloud storage environment, then uses this to pivot to an on-premise environment**

Brainstorming your principal security concerns can be guided using the CIA triad. Any scenario which negatively impacts the Confidentiality, Integrity or Availability of your highest-priority assets should be tested.

This will enable you to take a risk-based approach to building your strategy for offensive security testing.

claranet cyber security®

8. Need help finding out? **Get a Security Risk Assessment**

If you are unable to complete this stage yourself, or require validation that your principal security concerns are correct, get a security risk assessment. This is a consultancy exercise designed to gather information on your organisation's current and future security risks which you can then monitor and update over time. A security risk assessment will help you evaluate the risks to your organisation, forecast your cyber security budget and maintain compliance with regulatory requirements.

Security Risk Assessment Methodology

This six-stage process is designed to help organisations identify, manage, and mitigate the cyber security risks they face

STAGE 1: SCOPING	STAGE 2: THREAT MODELLING	STAGE 3: RISK ASSESSMENT	STAGE 4: RISK EVALUATION	STAGE 15 INHERENT RISK	STAGE 6: REPORTING
During the scoping stage, we will look at your objectives to understand your current security strategy, challenges and business objectives	We will define scenarios matching your principal security concerns, likely threat actors, and the tactics, techniques and procedures they will use.	We gather information using interviews and analysis of documentation to better understand vulnerabilities, and the likelihood and overall impact of threat events occurring.	We map out and evaluate the existing security controls, including policies, processes and their supporting documentation.	We collate and analyse all gathered information to understand how the existing risks can be mitigated by implementing new security controls. Then we prioritise the greatest risks.	Finally, we compile a report detailing all vulnerabilities identified and the risks impacting the organisation, including security recommendations for mitigating those risks.

Afterwards, a security consultant can help you devise a plan of offensive security testing which treats your principal security concerns as hypotheses to be confirmed or denied. They will look at your principal security concerns within the context of your IT estate, then devise a number of security tests which realistically replicate how an attacker would target your organisation.

1.
2.
3.
4.
5.
6.
7.
8.
9.
10.
11.
12.
13.

9. Choose your weapon: **what types of offensive security testing** should you use?

The next step is to decide which assets need to be tested more (or less) frequently and how you will test them. First, let's look at an overview of what kinds of offensive security testing are best for different assets across your IT estate why.

	THREAT MODELLING	PHISHING/SOCIAL ENGINEERING SIMULATION	PENETRATION TESTING	CONTINUOUS SECURITY TESTING	RED TEAMING	PURPLE TEAM
objective	We will define scenarios matching your principal security concerns, likely threat actors, and the tactics, techniques and procedures they will use.	To identify and measure how resilient your employees are against social engineering attacks, identify which user groups are most susceptible and where additional training is needed.	Identify all possible vulnerabilities that exist in a specific application, system, or scope; understand these in an organisational context; report on the risk they introduce; define suitable remediations at a single point in time.	Identify all possible vulnerabilities that exist in a specific application, system, or scope; understand these in an organisational context; report on the risk they introduce; define suitable remediations on a continual basis.	Identify weaknesses and strengths in an organisation's security controls; report on the organisation's ability to withstand a targeted real-world attack.	Evaluate and report on the effectiveness of your detection and response controls; improve your team's capability to identify and defend against real-world attacks.
outcomes	Adopt secure application development and DevSecOps practices. Build more targeted security controls in response to high-impact, high-likelihood threats.	Build the first line of defence, sometimes known as "the human firewall". Targeted training for the most vulnerable user groups.	Remediate critical vulnerabilities to lower the risk of harm caused by a cyber attack. Validate security posture. Adhere to regulatory and compliance demands.	Remediate critical vulnerabilities to lower the risk of harm caused by a cyber attack. Validate security posture.	Improve security controls at critical choke points to minimise the impact of cyber attacks. Target investment where security controls are not performing. Reassess and/or remove ineffective controls.	Improve the performance of existing detection and response controls. Invest in controls where there are gaps. Develop suitable training to continuously improve your team's performance.
format	Collaborative consultant-led analysis.	Simulated phishing campaign and employee awareness training.	Consultant-led analysis of security weaknesses in a target asset.	Automated scanning tools combined with consultant-led analysis of weaknesses in target assets.	Offensive team-led attack simulation.	Attack simulation with offensive/ defensive team-led collaborative exercise.

Fig. 4: Table showing the objectives, potential outcomes and format for each security testing type

claranet cyber security®

1.
2.
3.
4.
5.
6.
7.
8.
9.
10.
11.
12.
13.

So you can choose the right tool for the job, it’s worth understanding the pros and cons of each type of security testing,so you know what (and who) they are designed for.

	THREAT MODELLING	PHISHING/SOCIAL ENGINEERING SIMULATION	PENETRATION TESTING	CONTINUOUS SECURITY TESTING	RED TEAMING	PURPLE TEAM
What it’s good at	Identifying weaknesses in your application development model, capturing design requirements for better security at the start of the application design, and helping prioritise suitable security investment in the form of DevSecOps tools and processes.	Simulated phishing campaigns help train users not to fall prey to social engineering attacks which enable attackers to gain a foothold on your network.	Good at providing a broad and thorough overview vulnerabilities, but only within the scope of assets which are being targeted. For commercial reasons, scoping often makes penetration testing narrow but thorough.	Testing any web-facing assets that are part of a large application estate and/or are frequently updated.	Provides a more realistic simulation of how an attacker would behave. Red Team exercises are better at testing the existing defences which you have in place and therefore are best suited to organisations with an advanced security posture.	Helps your defenders improve their response in a realistic attack simulation. Purple Team exercises are best suited to organisations with an advanced security posture.
Which assets will gain the most benefit from it	Web-facing assets that are still in the early stages of design, such as: • Websites • Software • Applications	• Employees • Email systems	Pentesting is broadly applicable to most assets, including devices, buildings, applications, and networks (both internal and external).	External (web-facing) assets and the infrastructure they run on. Especially anything that is frequently updated, such as: • Websites • Software • Applications	Sometimes uses a phased approach covering multiple IT assets across the killchain. Best suited to any asset for which you have a principal security concern which you wish to confirm or deny.	Anything your defenders will need to protect in the midst of a cyber attack. Any assets that attackers will use to escalate their privilege.
Do we need it?	Control costs by identifying and remediating vulnerabilities early in their lifecycle and avoiding post-dev re-coding Address the increasing attack surface created by application development and release and the impact of this on your risk profile Identify risk and apply security controls tactically by understanding how data flows to and from the application and who can access this Ensure the organisation’s application development processes are compliant	All organisations should conduct some form of employee awareness training on phishing and social engineering.	Penetration testing is perhaps the most fundamental way to stay on top of your security health. Significant events often lead to needing a penetration test, such as a new system being introduced into the organisation, acquiring or merging with another organisation, or (most commonly) fulfilling compliance requirements Point-in-time penetration testing provides a snapshot of security at a specific juncture so you can focus resources on key applications and systems.	Continuous Security Testing goes one step further than penetration testing to identify assets and analyse vulnerabilities non-stop in a continuous loop. When used together with penetration testing, the two services provide a broad coverage across your changing attack surface.	To understand whether Red Team exercises are an appropriate, ask yourself: • Do I understand my risk profile in-depth and have a corresponding security strategy in place, or is this a goal we’re working towards? • Has my penetration testing programme been yielding the same results, or is it continually coming across new and unexpected findings? • Are we on top of our vulnerability patching and remediation demands, or are we still working towards best practice? • Does my team have the skills and confidence to benefit from a Red Team, or would they struggle to perform in this kind of exercise?	When the time is right, organisations may attempt to achieve some of the following outcomes with Purple Team exercises: • Create an incident-ready defensive team that knows what to do and how to collaborate in a real-world attack scenario • Prepare your team to develop detection and response playbooks • Bring your defensive team’s offensive knowledge up to date with the end goal of improving their detection capability • Assess the performance of detection and response investments (for example, that are part of a managed service) to measure return on investment, communicate these findings, and consider improvements
Typical cadence	Ad hoc	Initial training should be compulsory for employee onboarding. Subsequent simulated phishing campaigns can be staged and continual.	Can be carried out annually or on a regular basis, but typically only one asset at a time will be tested.	Scanners run 24/7. Reports are generated on a monthly basis, but users can generate custom reports at any time.	Can be repeated annually, or when there are significant changes to high priority assets, or in advance of a significant compliance audit.	Can be repeated annually, or when there are significant changes to high priority assets, or in advance of a significant compliance audit.

Fig. 5: Table comparing the various types of security testing and the assets they are most effective at testing

1.
2.
3.
4.
5.
6.
7.
8.
9.
10.
11.
12.
13.

10. Budget and cadence: **how much dictates how often**

Deciding what assets you should test with a limited budget can be tricky. Consider the overall goals of your security testing programme: **is it compliance? Is it hardening your perimeter? Do you want to improve security controls around your highest priority assets? Do you want to prepare for the worst or limit the blast radius of such an attack?** A risk-based approach will also consider the impact and likelihood of certain outcomes again your appetite for risk.

A security consultant can help devise the most cost-effective approach to choosing the right methods of testing for your business and its security posture.

claranet cyber security®

11. How are we going to **clean up this mess?**

Once you have conducted your testing, it's time to decide how you will approach remediating the security risks you have uncovered. There is no one-size-fits-all approach to deciding where you should focus your efforts. How you approach remediation will depend on a number of factors such as:

1. Your budget and the size and expertise of your team
2. Your risk profile: the threats your organisation is likely to face based on your industry and the kinds of data you store and process
3. Any industry regulations, as well auditing or compliance standards which you are obliged to adhere to

Offensive security consultants can bring their expertise to this exercise too. Based on the context of your IT estate, your budget, security posture, and the expertise of your team, they can advise you on the best approach remediating your security vulnerabilities. Below are some broad guidelines on how you might approach remediation, as suggested by our consultants:

1. **Update your risk register** whenever you receive reports at the end of any offensive security testing, to ensure that you have a clear picture of where your vulnerabilities lie. Then you can make an informed decision on what to do next based on the severity of the risk, the potential impact to your business and its likelihood of being exploited. Whether you will accept or mitigate that risk will also depend on your budget and the size of your team.

2. **Organisations with a less-developed security posture** should begin by building a patch management programme for their external, web-facing assets. Because this external infrastructure is the first thing attackers will target, preventing this initial compromise is low-hanging fruit and should be tackled first.
3. **Organisations with an advanced security posture** – such as those with an effective vulnerability management programme, or those who have already secured the vulnerabilities on their external infrastructure – should use their risk register to prioritise securing their most critical assets first and tackling the greatest risks to their organisation first.
4. **Build in time for remediations.** It is likely that your tests will not run simultaneously and you will receive reports on a staggered basis. Build in gaps between your various rounds of security testing to effect your remediations. Again, the amount of time that you should build in to deliver your remediations will also depend on the size of your team and the level of expertise you have in-house. Update your risk register once each remediation is complete.

12. Two large reports and some KPIs please – **evaluating your successes**

Improving your security posture is an incremental and iterative process. Penetration testers often point out that their favourite clients are the ones who make their jobs harder; after implementing the remediations from a pentest report and hardening their defences, organisations make it harder for pentesters to reach their goal, but in the process graduate to the higher climes of security maturity.

As mentioned earlier, the end goal of a perfect testing strategy would be a complete and up-to-date risk register, mapping out the vulnerabilities present across your entire IT estate. If a CISO, or anyone in the IT and security teams wanted to, they could consult a comprehensive document which shows exactly where the organisation is vulnerable (and why) and what actions are needed to remediate those risks.

Sadly, we do not live in a perfect world, and instead teams are often hampered by the realities of budget constraints and an IT skills shortage. This means that organisations are often on a journey towards improving their security posture by conducting as much security testing as they feasibly can, and aiming to include more testing (when the conditions are good.)

If you are on this journey, one way to evaluate your progress is to compare the reports from the successive rounds of security testing. If you have not successfully implemented the required remediations, then you will likely see the same vulnerabilities and the same recommendations come up over and over. If you do, you'll know you're not achieving your goals.

As a team, if you are trying to measure and report the success of your risk-based testing strategy, some useful KPIs include:

1. **Increased coverage of your network or IT estate within a specific timeframe**
2. **Reduced mean-time-to-remediation once vulnerabilities are discovered**
3. **Reduced time to patch when new zero-days or critical vulnerabilities become public**

Ultimately, measuring the success of your security testing programme should be considered a temporary stop on a never-ending journey. Your business will change,your IT estate will change, while cyber attackers will invent new and more effective ways of targeting the new defences that you have built. Like high-performing athletes at the top of their game, organisations with a strong security posture get there by not resting on their laurels. Your security testing programme will likely run through this current calendar or financial year, and once you're into the next, it's time to regroup, take a deep breath and start again.

13. Why choose us

Claranet Cyber Security is Claranet's dedicated security division committed to helping organisations develop their security posture and build resilience in the face of changing cyber risk. In the never-ending race to keep up with new threats and secure new technologies, we help you make modern happen.

We ask the right questions to uncover the rationale for change behind your security requirements, identifying your business drivers, people and process challenges, and critical threats. This leads us to the solution you really need – something flexible, scalable, and outcome-driven.

Our capabilities span continuous offensive security, SOC-enabled cyber defence, risk consultancy, and training, all of which are underpinned by a 25-year pedigree in penetration testing.

CREST

CYBER ESSENTIALS

C|CISO CERTIFIED CHIEF INFORMATION SECURITY OFFICER

CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL CISSP®

PCI Security Standards Council® QUALIFIED SECURITY ASSESSOR™

CRISC® Certified in Risk and Information Systems Control™ An ISACA® Certification

Assured Service Provider in association with National Cyber Security Centre CHECK Penetration Testing

CERTIFICATION BODY CYBER ESSENTIALS PLUS

C|EH™ Certified Ethical Hacker

claranet cyber security®

Contact us:

Tel: +44 1924 284 280

1.
2.
3.
4.
5.
6.
7.
8.
9.
10.
11.
12.
13.