Grant Thornton

An instinct for growth™

Penetration testing

How robust is your cyber security framework?

Testing your network security

Sophisticated cyber attacks pose a serious threat for organisations today. Many businesses, including those in the FTSE 100, have had their data compromised due to insecure systems and a lack of safeguards. Data breaches can have serious financial and legal implications, as well as lasting reputational damage.

Most modern business models are built around online processes and electronic communications. While this streamlines operations and improves business agility, it also creates a series of cyber vulnerabilities. If exploited, these vulnerabilities can lead to data breaches and significant business disruption.

What are the implications?

Data breaches can leak commercially sensitive information and staff or customer details. This can lead to customer distress, loss of assets, long term reputational damage, and regulatory fines or censure. Business disruption can grind your business to a halt leading to reputational damage and lost opportunities.

What are the key considerations?

Cyber threats refer to a potential malicious attempt to damage or disrupt a business computer network or system. They evolve on a daily basis and organisations need to continually re-assess the risks and associated controls. Businesses should continuously assess their exposure to both internal and external attacks, weighing them up against client information, networks and current systems.

An effective cyber security framework should incorporate preventative, detective and corrective solutions. To test the robustness of the cyber security defences, organisations should undertake regular vulnerability assessments and penetration tests:

- Vulnerability assessments explore and identify weaknesses in cyber security controls. Identification is the first step in mitigating risk and creating a secure network. They can also help to validate the design of cyber security controls.
- Penetration tests form the next step in reviewing the robustness of cyber security defences. These tests exploit the identified vulnerabilities, with the aim of breaching an organisation's security perimeter – thus testing how effectively security controls are operating.

What is a penetration test?

A penetration test essentially aims to gain unauthorised access to a network. It mimics what a person with a malicious motive would attempt to achieve. It applies a range of techniques, including social engineering, to breach an organisation's security perimeter.

'A 2017 survey found that 46% of UK businesses experienced a cyber security breach or attack in the last 12 months[1]. Penetration testing can help identify vulnerabilities which can be exploited by an attacker.'

1 'Cyber security breaches survey 2017', by Ispo Mori Social Research Institute, commissioned by the Department for Culture, Media & Sport

Approaches to penetration testing

Technology is not infallible and nor are people. An effective penetration test should assess network vulnerabilities from both the cyber standpoint and the human element. It should mirror different types of attack, based on the amount of information an attacker might have or their preferred technology.

Black box

Black box testing simulates an external attacker who does not know anything about the system. All the information the tester has is an IP address or website. This mimics an attack from a group like Anonymous.

Types of review

Typical areas assessed for both black box and grey box testing include:

Content filters screen inappropriate or malicious content. By limiting the type of content that can be accessed, organisations reduce the risk of phishing scams or downloading malware or ransomware. A penetration test can assess the effectiveness of a content filter.

Infrastructure reviews assess the system and network infrastructure for vulnerabilities. The review checks network devices to test for vulnerabilities in key components, such as the authentication and authorisation models. Infrastructure reviews can either simulate an external or internal threat to a network.

Vulnerability assessments test the operating effectiveness of IT and cyber security controls across the network. They check a specified IP address to identify exposure to both internal and external attacks.

Website screening uses specialist automated tools to assess for vulnerabilities. This is supported by manual testing to check how the server is configured to protect against malicious attacks.

Wireless assessments test the security of a wireless network. It uses passive detection software to identify any access points on the wireless network or associated connected devices, which could provide unauthorised access or allow Over the Air (OTA) data to be intercepted.

Grey box

Grey box testing simulates an attack from someone with partial knowledge of a system, such as an employee. The client will give the tester limited information about the target system.

Types of review

Typical areas assessed for both black box and grey box testing include:

Content filters screen inappropriate or malicious content. By limiting the type of content that can be accessed, organisations reduce the risk of phishing scams or downloading malware or ransomware. A penetration test can assess the effectiveness of a content filter.

Infrastructure reviews assess the system and network infrastructure for vulnerabilities. The review checks network devices to test for vulnerabilities in key components, such as the authentication and authorisation models. Infrastructure reviews can either simulate an external or internal threat to a network.

Vulnerability assessments test the operating effectiveness of IT and cyber security controls across the network. They check a specified IP address to identify exposure to both internal and external attacks.

Website screening uses specialist automated tools to assess for vulnerabilities. This is supported by manual testing to check how the server is configured to protect against malicious attacks.

Wireless assessments test the security of a wireless network. It uses passive detection software to identify any access points on the wireless network or associated connected devices, which could provide unauthorised access or allow Over the Air (OTA) data to be intercepted.

Social engineering

This is where the tester attempts to gain information from company insiders through psychological manipulation. It plays on human responses to trick people into giving network access, information or passwords.

Types of review

Employee awareness assessments for email fraud (phishing, smishing and vishing). These are common social engineering techniques and when well crafted, may be indistinguishable from genuine communications.

To assess employee awareness, a penetration tester may apply any of the methods below. These identify vulnerabilities and highlight the potential impact of a similar attack:

- Phishing uses email and tricks recipients into sharing data, following a harmful link or downloading malicious content.
- Smishing is essentially SMS phishing and uses text messages to trick recipients.
- Vishing is a variant of phishing and aims to get sensitive information over the phone.

Physical security tests assess how unauthorised access to a building can affect network and data security. A tester uses psychological manipulation to enter the premises and review how the network can be targeted, or what data can be retrieved.

How we can help

Our penetration tests assess how robust a cyber security system is in practice. They simulate common methods used by attackers, taking into account both the technical and human elements which make up the full security perimeter. We help organisations understand the full range of vulnerabilities and implement improved controls to mitigate those risks.

At Grant Thornton, our cyber security experts can develop a bespoke penetration testing plan to meet your business needs and unique IT environment. We can undertake the full suite of testing or conduct individual assessments, as required. Our experts can test for vulnerabilities around particular areas of concern, or help identify unforeseen issues across the network.

Our subject matter experts have significant experience in IT and cyber security, working with clients across all industries. The team can assist in the following areas:

- Cyber security governance and strategy
- Cyber security architecture
- Firewall configuration and management reviews
- Firewall rule-set reviews
- Audits of security controls
- Information security management reviews
- Physical security reviews (including FCA)
- PCI-DSS reviews and audits
- Training and awareness sessions for staff and senior management

Sandy Kumar
Chair of Financial Services Group
Head of Business Risk Services UK
T +44 (0)20 7865 2193
E sandy.kumar@uk.gt.com

Manu Sharma
Head of Cyber Security
Business Risk Services
T +44 (0)20 7865 2406
E manu.sharma@uk.gt.com

Nicholas Smith
Lead Penetration Tester
Business Risk Services
T +44 (0)20 7865 2407
E nicholas.r.smith@uk.gt.com

Grant Thornton
An instinct for growth™