FourNet®

FourNet's Cyber Essentials Guide 2024

Contents

Introduction	03
The Current Threat Landscape	05
The Impact of a Security Breach	12
Crucial Elements of a Cyber Defence Program	14
How Can FourNet Help	16
Choosing the Right Framework	20

Introduction

Introduction

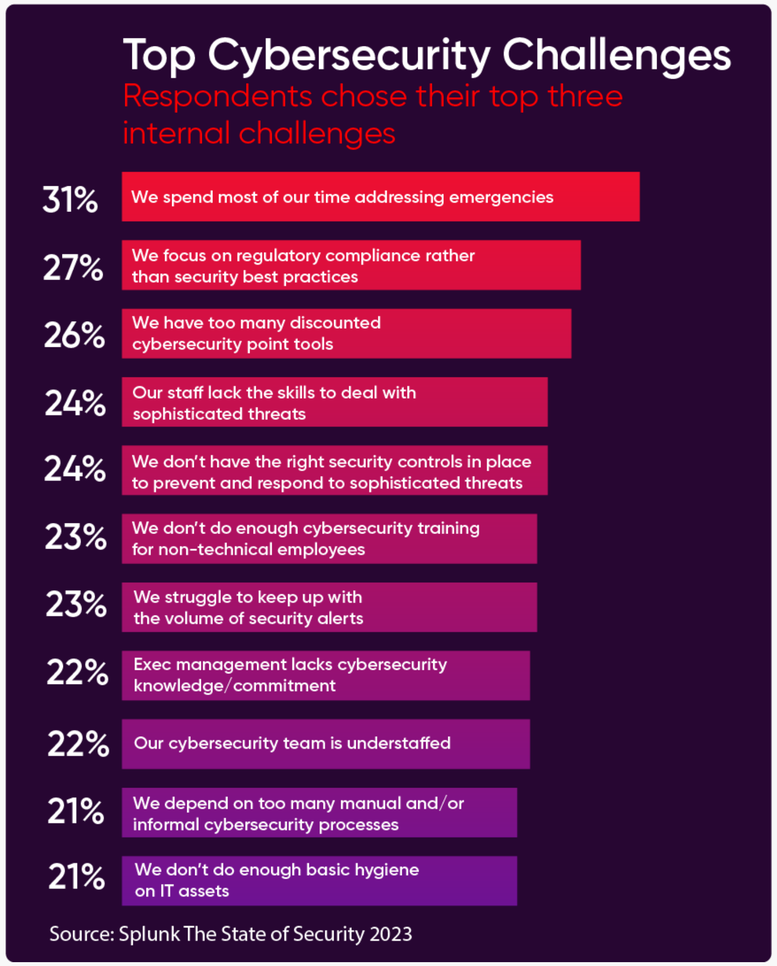
Cyberattacks and cybercrime are becoming more prevalent with each passing day. The UK government Cyber Security Breaches Survey for 2023 identified that 32% of businesses and 24% of charities suffered a breach or cyberattack in the last 12 months. However, it is larger organisations that are very much the target of cyber criminals: 59% of medium businesses, 69% of large businesses and 56% of high-income charities (with £500,000 or more in annual income) were targets of an attack.

2.39 million instances of cybercrime in the UK in the last 12 months

Of these attacks nearly one in three were successful for the criminals.

Cybercrime is a significant threat to businesses. It can lead to disruption of operations, breach of business and customer data, unauthorised access to networks, and more.

The Government Cyber Security Breaches Survey estimates that, across all UK businesses, there were approximately 2.39 million instances of cybercrime and approximately 49,000 instances of fraud as a result of cyber crime in the last 12 months.

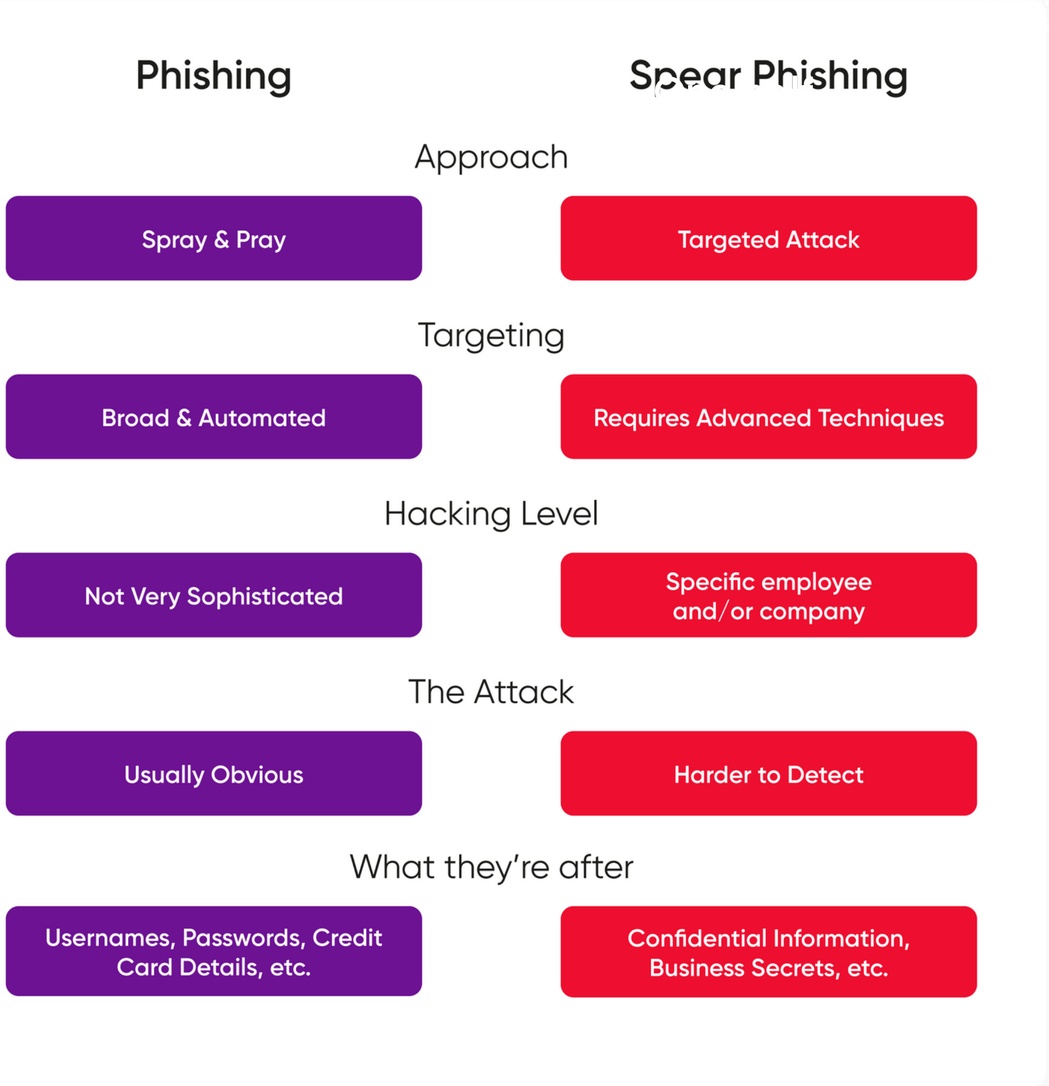


The Current Threat Landscape

Threats

Phishing & Spear Phishing

Distributed Denial-of-service (DDoS) is an attack which targets the resources of a server, network, website, or computer to take it down or disrupt services. DDoS attacks generally have a host system that infects other computers or servers connected to the network. DDoS attacks overload a system with constant flooding of connection requests, notifications and traffic. As a result, the system denies service requests by legitimate users. DDoS attacks don't benefit the attacker directly as they don't steal any information, it just compromises the systems so they can't function properly. Nonetheless, DDoS attacks can be damaging for businesses as it can halt operations and result in damages often as high as 100's of thousands of dollars via things like lost revenue, lost productivity and reputational damage.

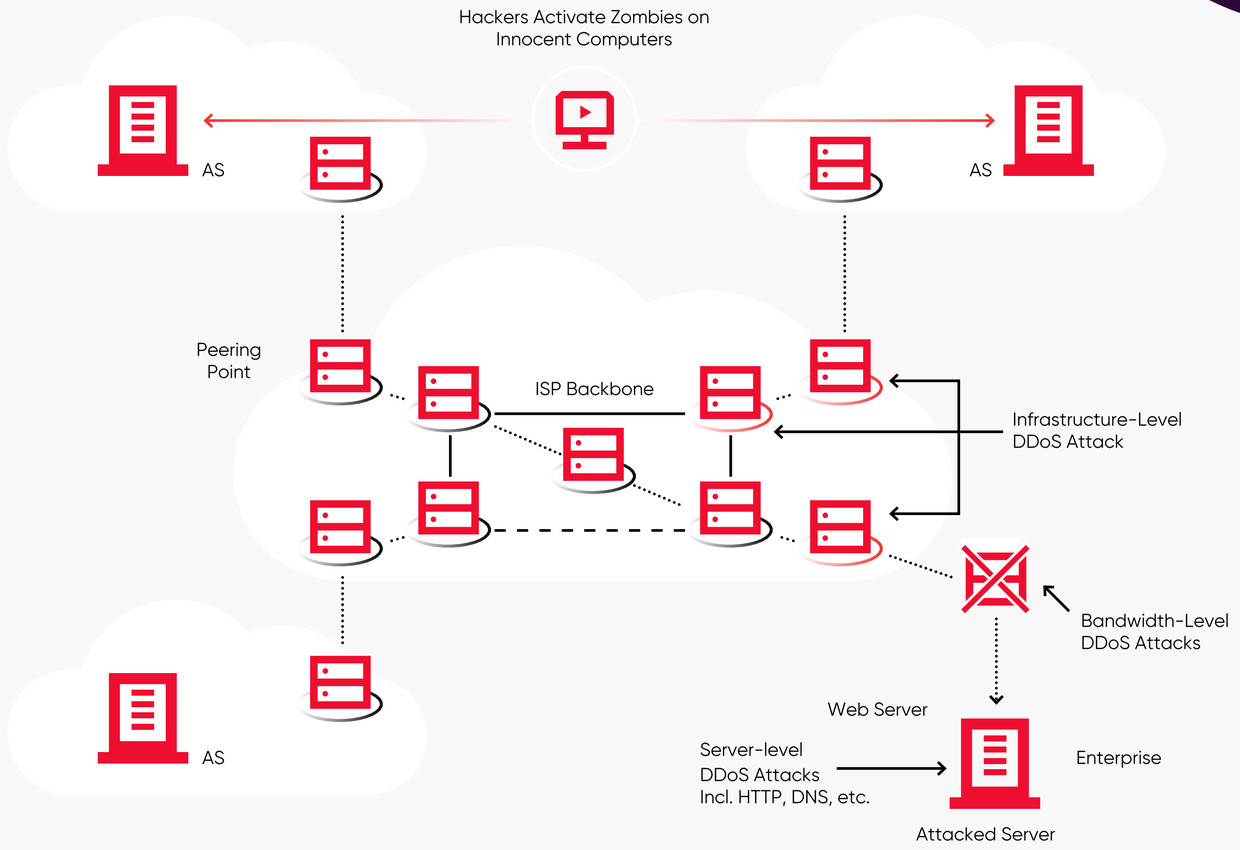


Threats

Distributed Denial-of-Sercice (DDOS)

In the first half of 2023 cybercriminals launched roughly 7.9m DDoS attacks – a 31% year on year increase.

Distributed Denial-of-service (DDoS) is an attack which targets the resources of a server, network, website, or computer to take it down or disrupt services. DDoS attacks generally have a host system that infects other computers or servers connected to the network. DDoS attacks overload a system with constant flooding of connection requests, notifications and traffic. As a result, the system denies service requests by legitimate users. DDoS attacks don't benefit the attacker directly as they don't steal any information, it just compromises the systems so they can't function properly. Nonetheless, DDoS attacks can be damaging for businesses as it can halt operations and result in damages often as high as 100's of thousands of dollars via things like lost revenue, lost productivity and reputational damage.



Threats

Man-in-the-middle (MITM) attack

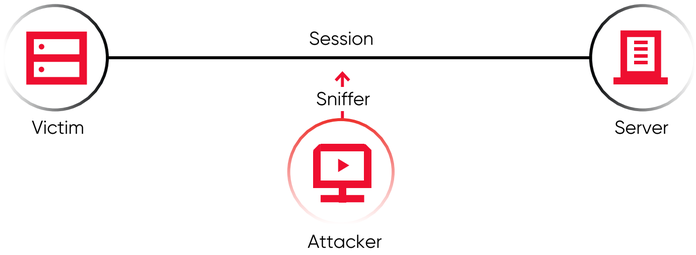
25% of UK businesses say their security teams do not have a formal resilience strategy

A MitM attack occurs when a hacker inserts themselves between the communications of a client and a server. Here are some common types of man-in-the-middle attacks:

Session Hijacking

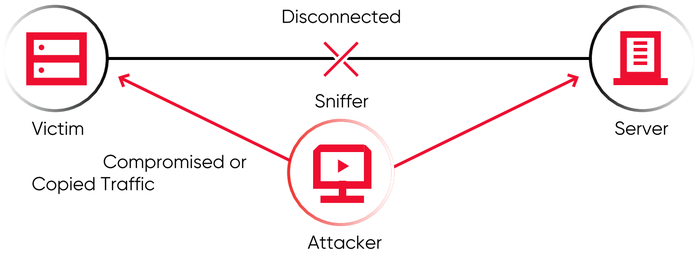
Cybercriminals use session hijacking to gain control of the victim's sessions and get access to resources or data. The most common method is IP spoofing, where the hijacker uses the IP of the trusted client to avail unauthorized services from a server or application.

Step 1: Hijacking the Session



95% of HTTP servers are vulunerable to MitM attacks

Step 2: Assuming the Victim's IP Address



Threats

Malware Attack

Malware or malicious software is designed for compromising a system for a purpose. A user can unknowingly download malware that infects a system and replicates itself. Malware can be designed to act in many ways, just like software. Some popular types of malware include:

1. Macro viruses
2. Trojans
3. System or boot-record infectors
4. Polymorphic viruses
5. Stealth viruses
6. File infectors
7. Logic bombs
8. Worms
9. Droppers
10. Ransomware

66 Days

The number of days to discover a Cyber-Attack

600%

Increase in Cyber Crime Due To COVID-19 Pandemic

Macro viruses

Macro viruses target the initialization sequence of an application to compromise programs such as Microsoft Excel or Word.

System or boot-record infectors

These infectors attach to executable codes residing in parts of a disc. Boot-record infectors can connect to a hard disk's Master Boot Records and even boot sectors of USB flash drives. The infectors are initialised when someone boots using the compromised disk or drive.

Logic bombs

Logic bombs are pieces of malicious codes that get initialised when predefined conditions are met. Attackers can program logic bombs to serve a range of purposes.

Droppers

Droppers help viruses find their way into your networks and systems. Most often, your antivirus will not detect droppers as they don't contain the malicious code- they just lead to it!

File infectors

File infectors find their way in your system through executable codes like .exe extensions. The infector becomes active when you access the .exe file or the executable code.

Worms

Worms don't need a host file to propagate themselves on a network or system. They are self-contained forms of viruses.

Ransomware

Ransomware can take the form of any virus that holds a victim's data hostage for ransom. Ransomware attacks often encrypt data or files and demand money in exchange for decryption keys.

Stealth viruses

Stealth viruses hide under the guise of system functions. They also infect your computer's defenses to stay undetected.

Trojans

Trojans are non-replicating viruses that gain unauthorized access to a system. Trojans often camouflage themselves in the form of legitimate software.

Polymorphic viruses

Polymorphic viruses replicate endlessly to sabotage systems. They use dynamic encryption keys every time to avoid detection.

Threats

Drive-by-Attack

Drive-by attacks use various online resources to compromise a user's system. The malicious code can be inserted in internet ads, HTTP or PHP codes on websites, or even applications. Contrary to other forms of Cyber-Attacks, a user doesn't have to do anything to initialise the malicious software or virus. A single click on a pop-up window or website link can do the job! Drive-by attacks are increasingly used to spread viruses and malware. The attacks take advantage of security vulnerabilities in apps or websites to exploit victim systems. These include not updating the app, flaws in security patches, bugs, and more.

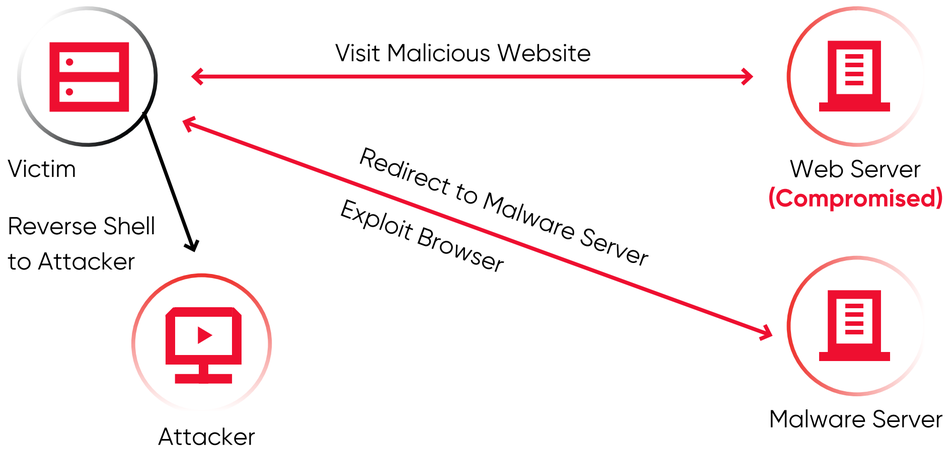
The attacks also run in the background and are not visible to the user. As a result, you can't take any concrete steps to identify incorrect codes. Only being proactive can help businesses protect themselves from drive-by attacks.

92%

of Malware is Delivered by Email

One half

of all Cyber-Attacks Specifically Target Small Businesses.



Threats

Password Attack

Password attacks enable cybercriminals to gain unauthorized access to user accounts and networks. Someone in your office can just guess or look around your desk to steal your password. That's why it's always recommended not to write down your passwords. Attackers may also spy on your network, use decryption tools, and use brute force to break your passwords.

A range of precautions can help save you from password attacks. You can program your system to lock accounts after a few wrong passwords. Using two-step authentication is also an excellent way to keep your accounts safe from prying eyes.

The total cost of cybercrime to the UK economy is estimated to be

£27 billion

per year

98%

of Cyber-Attacks rely on Social Engineering.

73%

of Passwords are Duplicates.

The Impact of a Security Breach

The impact of a security breach

In addition to the time and resources required to clean up the mess, cyber breaches can damage your organisations reputation and competitive position, impact on valuation, cause public embarrassment and reduce trust. According to Splunk's annual State of Security report for 2023, only 4% of respondents say they had suffered incidents but experienced no significant consequences.

Whatever the avenue, once the bad guys get in, they've got time to get comfortable. On average, respondents tell us that it's 2.24 months, or about nine weeks, from the moment a bad actor penetrates their systems until appropriate parties are aware of it. That's a lot of time to steal or break things.

Splunk's State of Security 2023 UK assessment

The security picture in the UK is bleak. UK respondents report having suffered from a recent breach at twice the rate of their peers in Western Europe (68% versus 34%) and have run afoul of regulations more often (64% versus 24%). Moreover, UK respondents are more likely to say that these incidents have had real consequences, such as hurting their company's valuation (37% versus 25%).

Two key drivers: 26% of respondents say they are overwhelmed by false positives and alerts that lack context (versus 15% across the rest of Western Europe) and 30% say their cybersecurity posture is based on regulatory requirements rather than security best practices (versus 20% across the region).

Resilience also lags: 25% of UK respondents say their security teams have not yet developed a formal resilience strategy — five times the rate of organisations in the rest of the world. And just 16% have a formal approach to cyber resilience that has been instituted organisation-wide (versus 35% of organisations in the rest of the world)."

Source: Splunk The State of Security 2023

Incidents Experienced in the Past Two Years

52%	System compromise
52%	Data breach
51%	Business email compromise
49%	Ransomware attack
46%	Impersonating your org's website
46%	DDoS
41%	Software supply chain attack
40%	Insider attack
40%	Account takeover/stolen credentials

Effects of Incidents Over the Past Two Years

57%	Significant IT time/personnel needed for remediation
48%	Breach of confidential data
41%	Lost productivity
40%	Public disclosure of a data breach
39%	Competitive position of the organisation was hurt
31%	Shareholder value/company valuation was diminished
30%	Termination/prosecution of employees/executives
4%	We suffered incidents, but the impact was not major

Crucial Elements of a Cyber Defence Program

5 Crucial Elements of an Effective Cybersecurity Program:

Defence, Defences and Defence

Learning and acquiring knowledge from actual attacks that compromised your system can lead to effective and practical defenses. Your defense should be built only on controls that have proven successful in preventing real-world attacks for the best results.

Prioritisation

Businesses should only focus on controls that can reduce risk most effectively and protect the organisation from dangerous cyber threats. Also, the control should be feasible enough to be implemented in your computing environment.

You can identify Sub-Controls to implement by visiting the CIS Implementation Groups.

Measurements and Metrics

You should have standard metrics or KPIs in place so that all stakeholders like IT, executives, officers, and auditors can stay on the same page. Metrics are also necessary to monitor the effectiveness of your security measures and make improvements.

Continuous Diagnostics and Mitigation

You should always be proactive and monitor your security measures' effectiveness. Any issues should be resolved as soon as possible to ensure the integrity of the following actions.

Automation

Automation helps businesses ensure compliance with controls and gain a scalable and reliable way to fight off cyber threats. Automation also increases efficiencies and saves both time and labour.

How Can FourNet Help

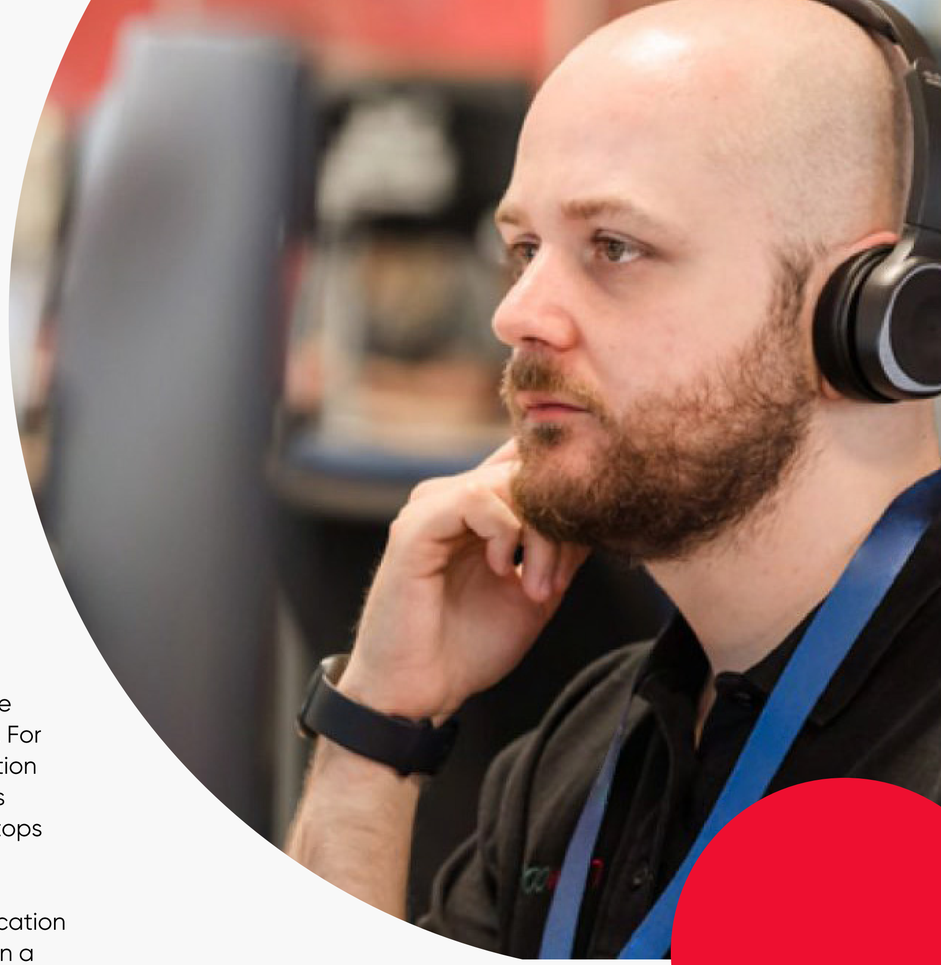
Our 7 Stage Approach to Cybersecurity

FourNet leverage cutting-edge technologies, intelligent automation, and advanced analytics, matched with our industry leading cybersecurity experts to help organisations protect themselves from the ever-evolving cybersecurity threat. We work collaboratively with customers to understand current capabilities, diagnose a plan of action to remediate any existing vulnerabilities and then provide managed security services to ensure you remain secure.

Powered by market-leading technology, our state-of-the-art SOC provides round-the-clock monitoring, incident response, and threat intelligence services. Our team of experienced cybersecurity professionals works in unison with your organisation, utilising advanced tools and methodologies to swiftly detect, analyse, and mitigate threats. We augment your existing capabilities, ensuring a seamless integration that optimises your cybersecurity posture.

247/365

Security expert support



It is essential that any organisation using technology today, understand their cyber risk and their ability handle a cyber-attack should the worst happen. FourNet Assess, enables organisations to get a total review of their Cybersecurity. At FourNet, we don't approach cyber security as just a technical issue, our methodology revolves around three key elements of information security:

People

Data security is everyone's responsibility within the organisation. Therefore, it is vital to ensure people are trained so they can identify known security threats and associated techniques. Further training to then understand the appropriate action when they detect or suspect a security issue should also be performed. With appropriate training, we can begin to change human behaviour so that everyone in the organisation becomes part of the first line in defence against cyber threats (for example identifying and avoiding clicking on a likely infected file).

Process

In addition to awareness training for the people in the organisation, it is key to review and develop our processes. IT business processes together with documentation and controls are key to maintaining a secure data environment. The goal of our assessment is to identify your security strengths and weaknesses, and to provide advice as to the improvements the organisation should be considering relative to your security posture.

Technology

Most organisations have multiple layers of security technologies in place to protect the organisation from the different types of attacks experienced "in the real world". For example, a data security firewall to protect the organisation from unauthorised access over the internet or an antivirus platform to protect the data servers and computer desktops from infection are typical examples. Unfortunately, this approach alone is no longer good enough to protect the organisation from the ever-growing number and sophistication of IT security threats and attacks. At FourNet we believe in a "defence in depth" approach, utilising multiple technologies, techniques and processes that interact with each other to help maintain an adaptive security defence posture for the organisation.

How we can help

FourNet Assess has been designed to address these elements, delivered in 3 key stages.

1

A Security risk assessment to baseline the organisation against best practice so you understand where you are.

2

A deep dive technical review of the security technologies currently in place, gathering observations, gaps, and recommendations for improvements.

3

A full assessment report detailing findings & recommendations.

Get Started

Choosing the Right Framework to Protect Your Organisation

Choosing the Right Framework

It is essential that any organisation using technology today, understand their cyber risk and their ability handle a cyber-attack should the worst happen. FourNet's cybersecurity assessments enables organisations to get a total review of their Cybersecurity. Approaching cybersecurity not just as technical issue, our methodology revolves around three key elements, people, process and technology.

Choosing the right cybersecurity framework depends on the regulatory requirements and strategic objectives of your organisation.

These are some of the main frameworks that FourNet are experienced in administering:

NIST

The National Institute of Standards and Technology (NIST)'s framework provides guidelines for U.S. organisations to identify, protect, detect, respond to, and recover from cyberattacks.

CIS Controls

The Center for Internet Security (CIS) Control Framework provides best practices for organisations seeking to protect their networks from cyber threats. The CIS Controls are divided into three categories: Basic, Foundational, and organisational.

PCI-DSS

Developed by a council of major payment processors, the Payment Card Industry Data Security Standard provides a comprehensive set of requirements for securing systems and preventing unauthorized access to customer information.

Cyber Essentials

.This is the primary framework for the UK, established by the NCSC (National Cyber Security Centre). The framework covers 5 main areas: firewalls and routers, secure configuration, access control, malware protection, and patch management.

Cyber Assessment Framework for Critical National Infrastructure

Critical National Infrastructure (CNI) are those facilities, systems, sites, information, people, networks and processes, necessary and essential for the country to function and upon which daily life depends.

FourNet®

Thank you

Learn More

Manchester Office (HQ)
3 Scholar Green Road,
Cobra Court,
Manchester. M32 0TR

Tel: 0845 055 6366

Derby Office
Wyvern Business Park, Stanier Way,
Derby. DE21 6BF

Tel: 0300 303 1200

fournet.co.uk

London Office
83 Victoria Street,
London. SW1H OHW

Tel: 0203 503 0003

FourNet PR & Media Office Tim Reid

e-mail:

treid@fournet.co.uk