MAY 2025

CURATED

SO WHAT?

THE FIVE CORE CONTROLS THAT PROTECT YOUR BUSINESS

READ ON

WWW.INCOMMSEC.COM

CYBERSECURITY CHALLENGES FOR UK SMES
MAY 2025
00101
0101
RANSOMWARE
AI-POWERED PHISHING ATTACKS
RANSOMWARE-AS-A-SERVICE
SUPPLY CHAIN VULNERABILITIIES
HYBRID WORK ENVIRONMENTS

Introduction

In May 2025, UK small and medium enterprises face an unprecedented cybersecurity challenge. With 43% of UK businesses experiencing cyber breaches in the past year and average fraud losses reaching £4,000 per incident, the question isn't whether your business will be targeted—it's whether you'll be ready.

The landscape has evolved dramatically. AI-powered attacks now create convincing phishing emails that bypass traditional detection methods. Ransomware-as-a-Service operations have democratised sophisticated attacks, making enterprise-grade threats accessible to low-skilled criminals. Supply chain vulnerabilities expose businesses through their trusted vendors, while hybrid work environments create new attack surfaces that didn't exist just five years ago.

Yet amid this complexity, a fundamental truth remains: most successful cyberattacks exploit basic security gaps. The UK's National Cyber Security Centre has identified five core control areas that, when properly implemented, defend against the vast majority of threats facing SMEs today.

This newsletter provides a comprehensive guide to implementing these five essential controls, drawing from real-world incidents, current threat intelligence, and proven defensive strategies that work for businesses with as few as 10-50 employees.

THE FOUNDATION OF CYBER RESILIENCE:
IMPLEMENT THE FIVE CORE CONTROLS THAT STOP 95% OF ATTACKS BEFORE THEY START.

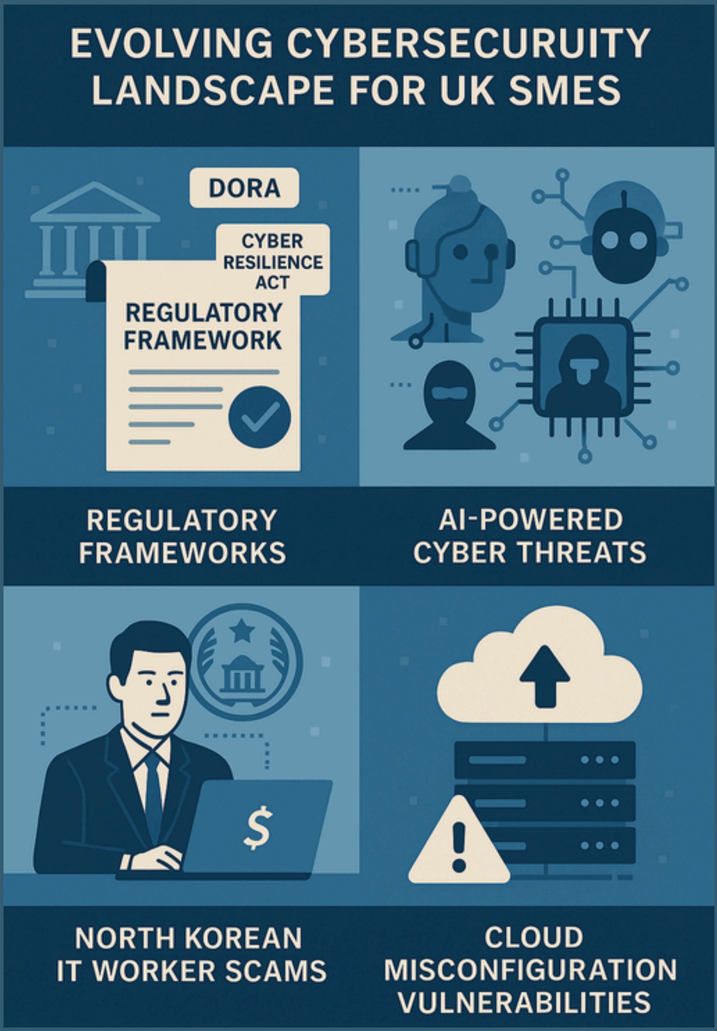
The Current Threat Reality: What's Changed in May 2025?

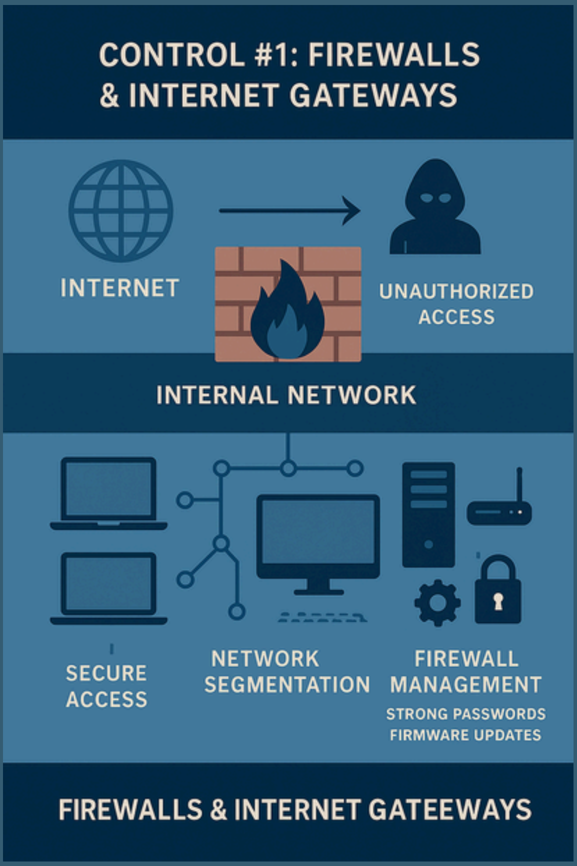
The cybersecurity landscape continues its rapid evolution, with several key developments reshaping the threat environment for UK SMEs. New regulatory frameworks are taking effect, including the EU's Digital Operational Resilience Act (DORA) and the phased implementation of the Cyber Resilience Act, creating compliance obligations that extend beyond traditional IT security.

Meanwhile, threat actors are leveraging artificial intelligence to accelerate attack development and deployment. North Korean IT worker scams have expanded into Europe, with operatives posing as remote developers across Germany, Portugal, and the UK, even targeting defence and government sectors. These sophisticated social engineering campaigns demonstrate how traditional hiring processes can become attack vectors.

The ransomware threat has intensified, with a 70% surge in attacks compared to the previous year. Modern ransomware groups employ "double extortion" tactics, stealing data before encryption and threatening publication unless paid. For SMEs, this evolution means that even comprehensive backups may not fully protect against reputational and regulatory consequences.

Cloud misconfigurations remain a leading cause of data breaches, with 76% of organisations having at least one over-permissive identity and access management policy. As SMEs accelerate cloud adoption, these vulnerabilities create significant exposure that attackers actively exploit.


EVOLVING CYBERSECURUITY LANDSCAPE FOR UK SMES
DORA
CYBER RESILIENCE ACT
REGULATORY FRAMEWORK
REGULATORY FRAMEWORKS
AI-POWERED CYBER THREATS
$
NORTH KOREAN IT WORKER SCAMS
CLOUD MISCONFIGURATION VULNERABILITIES



Control #1: Firewalls & Internet Gateways - Your Digital Perimeter

The Control:
Firewalls serve as the critical barrier between your internal network and the hostile internet environment. Every device—laptops, desktops, servers, and IoT equipment—must be protected by properly configured firewall technology that blocks unauthorised access while enabling legitimate business communications.

Implementation Essentials:
Modern firewall deployment requires blocking all unauthenticated inbound connections by default, creating a "deny-all" posture that only permits explicitly authorised traffic. Default administrative passwords on all network equipment must be replaced with strong, unique credentials that follow your organisation's password policy.

Port and service management demands careful attention—only necessary network services should remain active, with all others disabled or blocked. Regular firmware updates within 14 days of vendor release ensure protection against newly discovered vulnerabilities. Administrative interfaces must never be accessible from public networks, requiring secure internal access or VPN connections for management tasks.

Real-World Impact:
A UK manufacturing SME discovered attackers had compromised their network through an unpatched firewall vulnerability that had been publicly disclosed three weeks earlier. The breach remained undetected for six weeks, during which attackers accessed customer databases and financial systems. The incident resulted in £180,000 in direct costs, regulatory fines, and customer contract cancellations that impacted revenue for eight months.

Advanced Considerations:
Next-generation firewalls offer application-layer inspection, intrusion prevention, and threat intelligence integration that significantly enhance protection beyond traditional port-based filtering. For SMEs, managed firewall services can provide enterprise-grade capabilities without requiring specialised in-house expertise.

Network segmentation using firewall rules isolates critical systems from general business networks, containing potential breaches and limiting attacker movement. This approach proved crucial for a professional services firm that contained a ransomware attack to their guest network, preventing spread to core business systems.

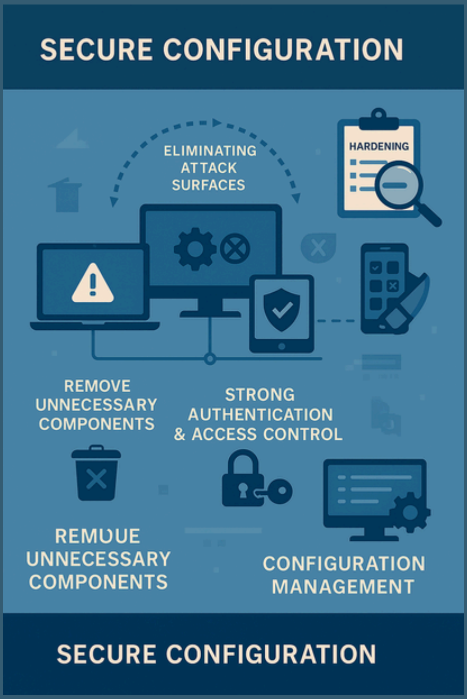
Control #2: Secure Configuration - Eliminating Attack Surfaces

The Control:
Secure configuration involves systematically hardening all devices and applications by removing unnecessary components, implementing strong authentication, and maintaining proper access controls. This control area addresses the reality that most systems ship with convenience-focused defaults that prioritise ease of use over security.

Implementation Essentials:
Comprehensive asset inventory forms the foundation of secure configuration, requiring detailed documentation of all devices, applications, and services within your environment. This inventory must include ownership, purpose, configuration details, and update status for each component.

Default credentials represent a critical vulnerability that attackers routinely exploit. Every system component—from network equipment to applications—must have default passwords replaced with strong, unique credentials. Administrative privileges require careful management, with separation between standard user accounts and elevated administrative access.

Regular configuration reviews ensure that security settings remain appropriate as business needs evolve. Automated configuration management tools can help maintain consistent security postures across multiple devices and detect unauthorised changes.


SECURE CONFIGURATION
ELIMINATING ATTACK SURFACES
HARDENING
REMOVE UNNECESSARY COMPONENTS
STRONG AUTHENTICATION & ACCESS CONTROL
REMOUE UNNECESSARY COMPONENTS
CONFIGURATION MANAGEMENT
SECURE CONFIGURATION

Real-World Impact:
A retail SME suffered a data breach when attackers discovered a development server that retained default administrative credentials. The server, originally deployed for testing, had been forgotten during a rapid expansion period. Attackers used this access to pivot into production systems, ultimately compromising customer payment information and triggering regulatory investigation.

Advanced Considerations:
Configuration management frameworks like the Center for Internet Security (CIS) Controls provide detailed guidance for hardening common operating systems and applications. These frameworks offer specific recommendations that SMEs can implement without extensive security expertise.

Automated compliance scanning tools can continuously monitor configuration drift and alert administrators to potential security gaps. For resource-constrained SMEs, cloud-based configuration management services offer enterprise capabilities without significant infrastructure investment.

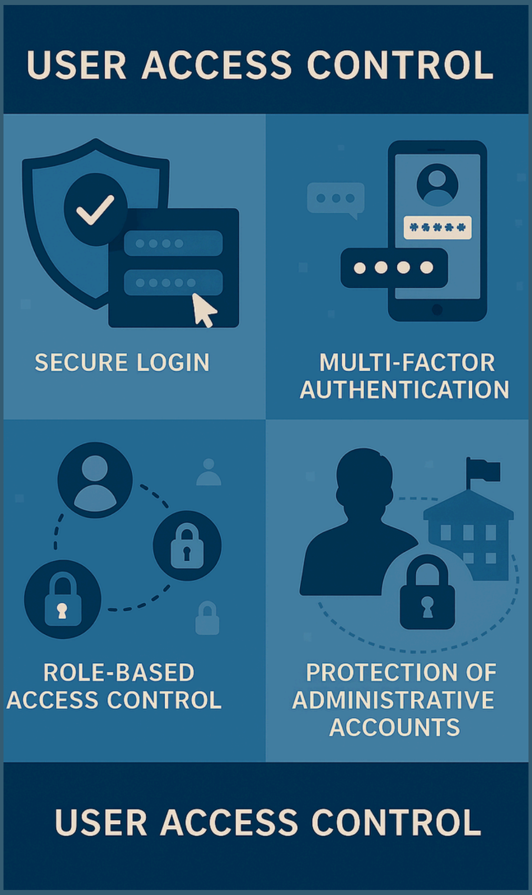
Control #3: User Access Control - Managing the Human Element

The Control:
User access control encompasses the policies, procedures, and technologies that govern how individuals access systems and data within your organisation. This control area addresses the reality that 74% of breaches involve the human element, whether through compromised credentials, social engineering, or insider threats.

Implementation Essentials:
Unique user credentials eliminate the risks associated with shared accounts, ensuring accountability and enabling proper access tracking. Multi-factor authentication (MFA) provides essential protection against credential theft, particularly for cloud services and remote access systems where traditional network controls may not apply.

Role-based access control limits data and system access based on job requirements, implementing the principle of least privilege throughout your organisation. Formal user lifecycle management ensures that new employees receive appropriate access promptly while departing employees lose access immediately.

Administrative account protection requires additional security measures, including separate credentials for administrative tasks, enhanced monitoring, and restrictions on administrative account usage for routine activities.


USER ACCESS CONTROL
SECURE LOGIN
MULTI-FACTOR AUTHENTICATION
ROLE-BASED ACCESS CONTROL
PROTECTION OF ADMINISTRATIVE ACCOUNTS
USER ACCESS CONTROL

Real-World Impact:
A professional services firm discovered that a former employee had retained access to client files for three months after termination due to informal access management processes. The ex-employee had downloaded confidential strategic plans and pricing information, which later appeared in a competitor's proposals. The incident resulted in client contract losses and legal action that cost the firm over £250,000.

Advanced Considerations:
Privileged access management (PAM) solutions provide sophisticated controls for administrative accounts, including session recording, approval workflows, and automatic credential rotation. These tools significantly reduce the risk of administrative credential compromise.

Identity governance platforms can automate user lifecycle management, ensuring consistent application of access policies and reducing the manual effort required for user administration. For SMEs with complex application environments, these solutions can dramatically improve security while reducing administrative overhead.

Control #4: Malware Protection - Defending Against Evolving Threats

The Control:
Malware protection encompasses the technologies and processes that detect, prevent, and respond to malicious software threats. Modern malware includes traditional viruses, sophisticated ransomware, fileless attacks that operate entirely in memory, and AI-enhanced threats that adapt to defensive measures.

Implementation Essentials:
Comprehensive endpoint protection requires antivirus and anti-malware software on every device, with automatic updates ensuring protection against the latest threats. Regular scanning schedules detect dormant malware that may have evaded real-time protection.

Application control prevents users from installing unauthorised software, reducing the risk of malware introduction through legitimate-appearing applications. Trusted source policies ensure that software installations come only from verified vendors and official distribution channels.

Email and web filtering provide critical protection against malware delivery mechanisms, blocking suspicious attachments and preventing access to known malicious websites. These controls intercept threats before they reach end-user devices.

Real-World Impact:
A logistics SME fell victim to a sophisticated fileless malware attack that bypassed their traditional antivirus solution. The malware, delivered through a convincing phishing email, operated entirely in system memory and established persistent access through legitimate administrative tools. The attack remained undetected for four months, during which attackers accessed customer shipping data and financial records.

MALWARE PROTECTION FOR SMEs
VIRUSES
RANSOMWARE
FILELESS ATTACKS
AI-ENHANCE THREATS
EMAIL & WEB FILTERING
SANDBOXING
ENDPOINT DETECTION AND RESPONSE
MALWARE PROTECTION FOR SMEs

Advanced Considerations:
Endpoint detection and response (EDR) solutions provide advanced threat hunting capabilities that can identify sophisticated attacks that bypass traditional antivirus protection. These tools analyse behavioural patterns and can detect previously unknown threats.

Sandboxing technology isolates suspicious files and applications in controlled environments, allowing safe analysis of potential threats. Cloud-based sandboxing services make this enterprise-grade capability accessible to SMEs without significant infrastructure investment.

Control #5: Patch & Security Update Management - Closing Vulnerability Windows

The Control:
Patch management involves the systematic process of identifying, testing, and deploying security updates across all systems and applications. This control area addresses the reality that unpatched vulnerabilities represent one of the most common attack vectors, with automated scanning tools making vulnerability discovery increasingly rapid.

PATCH & SECURITY UPDATE MANAGEMENT
14
AUTOMATED PATCHING
VULNERABILITY SCANNING
TESTING ENVIRONMENTS
PATCH & SECURITY UPDATE MANAGEMENT

Implementation Essentials:
Comprehensive patch management requires maintaining current inventories of all software and systems, including version information and support status. Critical security patches must be applied within 14 days of release, balancing security needs with operational stability requirements.

Automated update mechanisms reduce the manual effort required for patch deployment while ensuring consistent application across all systems. However, critical business systems may require testing procedures to validate that updates don't disrupt essential operations.

Legacy system management presents particular challenges, as unsupported software cannot receive security updates. These systems require either replacement with supported alternatives or additional compensating controls to mitigate increased risk.

Real-World Impact:
A healthcare SME experienced a ransomware attack that exploited a vulnerability in their practice management software. The vulnerability had been patched by the vendor six weeks earlier, but the practice's informal update process had delayed installation. The attack encrypted patient records and disrupted operations for two weeks, resulting in regulatory fines and significant recovery costs.

Advanced Considerations:
Vulnerability management platforms provide automated scanning and prioritisation capabilities that help SMEs focus on the most critical security gaps. These tools can integrate with patch management systems to streamline the entire vulnerability remediation process.

Patch testing environments allow SMEs to validate updates before production deployment, reducing the risk of business disruption while maintaining security. Cloud-based testing services make this capability accessible without significant infrastructure investment.

Building a Comprehensive Defence Strategy

Integration and Coordination:
The five core controls work most effectively when implemented as an integrated defence strategy rather than isolated security measures. Firewall logs can inform malware protection systems about suspicious network activity. User access controls can trigger additional authentication requirements when patch management systems identify high-risk vulnerabilities.

Regular security assessments validate that all five controls remain effective as business needs and threat landscapes evolve. These assessments should include both technical testing and process reviews to identify gaps in implementation or maintenance.

Incident Response Preparation:
Even comprehensive preventive controls cannot guarantee complete protection against all threats. Incident response planning ensures that your organisation can quickly detect, contain, and recover from security incidents that bypass preventive measures.

Effective incident response requires predefined procedures, designated response team members, and regular testing through tabletop exercises. Communication plans should address both internal coordination and external notification requirements, including regulatory reporting obligations.

Continuous Improvement:
Cybersecurity effectiveness requires ongoing attention and refinement. Threat intelligence feeds help organisations understand emerging risks and adjust defensive measures accordingly. Security metrics and monitoring provide visibility into control effectiveness and highlight areas requiring additional attention.

Regular training ensures that all employees understand their role in maintaining organisational security. This training should address both technical procedures and general security awareness, helping staff recognise and respond appropriately to potential threats.

Regulatory Compliance and Business Benefits

Meeting Regulatory Requirements:
The five core controls align closely with emerging regulatory frameworks, including the UK's Cyber Security and Resilience Bill and EU regulations affecting UK businesses. Implementing these controls provides a strong foundation for compliance with current and anticipated requirements.

Documentation of control implementation and maintenance activities supports compliance reporting and demonstrates due diligence in the event of incidents or audits. Regular compliance assessments help organisations identify and address gaps before they become regulatory issues.

Business Value Creation:
Beyond regulatory compliance, strong cybersecurity controls create tangible business value. Customer confidence increases when organisations can demonstrate robust security practices. Competitive advantages emerge when security capabilities enable new business opportunities or partnerships.

Operational efficiency improves when security controls are properly integrated with business processes. Automated security measures reduce manual effort while providing more consistent protection than ad-hoc approaches.

REGULATORY COMPLIANCE & BUSINESS BENEFITS
LEGAL COMPLIANCE
BUSINESS GROWTH
CUSTOMER TRUST
AUTOMATED SECURITY
REGULATORY COMPLIANCE & BUSINESS BENEFITS

Conclusion: Building Resilient SME Cybersecurity

The five core cybersecurity controls—firewalls and internet gateways, secure configuration, user access control, malware protection, and patch management—provide a proven framework for protecting UK SMEs against the vast majority of cyber threats. While the threat landscape continues evolving with AI-powered attacks and sophisticated ransomware operations, these fundamental controls remain essential for organisational resilience.

Implementation success requires commitment from leadership, adequate resource allocation, and ongoing attention to maintenance and improvement. However, the investment in these controls pays dividends through reduced incident risk, regulatory compliance, and enhanced business capabilities.

Remember that cybersecurity is not a destination but a continuous journey of improvement and adaptation. The controls outlined in this newsletter provide a solid foundation, but they must evolve with your business needs and the changing threat environment.

Three Key Takeaways for SME Leaders:

1) Start with the fundamentals: The five core controls address the attack vectors used in the majority of successful breaches. Implementing these controls effectively provides significant protection against both opportunistic and targeted attacks.

2) Integrate security with business operations: Security controls work best when they support rather than hinder business objectives. Proper implementation enhances operational efficiency while providing protection.

3) Plan for continuous improvement: Cybersecurity effectiveness requires ongoing attention, regular assessment, and adaptation to changing circumstances. Build security management into your regular business processes.

The cyber threat landscape will continue evolving, but organisations that implement and maintain these five core controls will be well-positioned to defend against current and emerging threats while supporting business growth and success.

"The best time to plant a tree was 20 years ago. The second best time is now." - Chinese Proverb

This wisdom applies perfectly to cybersecurity—while you cannot change past security decisions, you can start building robust defences today that will protect your business tomorrow.

READY TO STRENGTHEN YOUR CYBER DEFENCES?

Contact our team to discuss how we can help you implement these five core controls and build a more resilient security posture for your business.
ENQUIRIES@INCOMMSEC.COM

MAY 2025

CURATED

WANT TO HAVE A SAY?

ASK A QUESTION OR GET IN TOUCH

ENQUIRIES@INCOMMSEC.COM

WWW.INCOMMSEC.COM