DigitalXRAID
CYBER SECURITY EXPERTS

RETAIL INDUSTRY

How retailers can stay secure against increasing cyberattacks

The retail industry has suffered an increasing frequency of cyberattacks in recent years

In recent years, cyberattacks have become a common occurrence for businesses across various industries. The retail industry has not been spared, with several high-profile cyberattacks occurring over the last year.

One such attack happened to WH Smith, the second successful cyberattack on the company, following one which also targeted the company's online bookshop in October 2021.

This ebook will delve into the recent WH Smith cyberattack, as well as the proliferation of other attacks on retail organisations such as The Works, KP Snacks, SPAR, Funky Pigeon, and JD Sports.

It will also share tips on what retailers can do to protect themselves from the increasing threat of ransomware and cyberattacks.

The WH Smith cyberattacks

On October 15th, 2021, WH Smith, a well-known British retailer, announced that it had suffered a cyberattack on its online bookshop.

The attack resulted in the theft of customer data, including names, addresses, email addresses, and payment card details.

WH Smith stated that it had immediately taken steps to mitigate the impact of the attack and had launched an investigation.

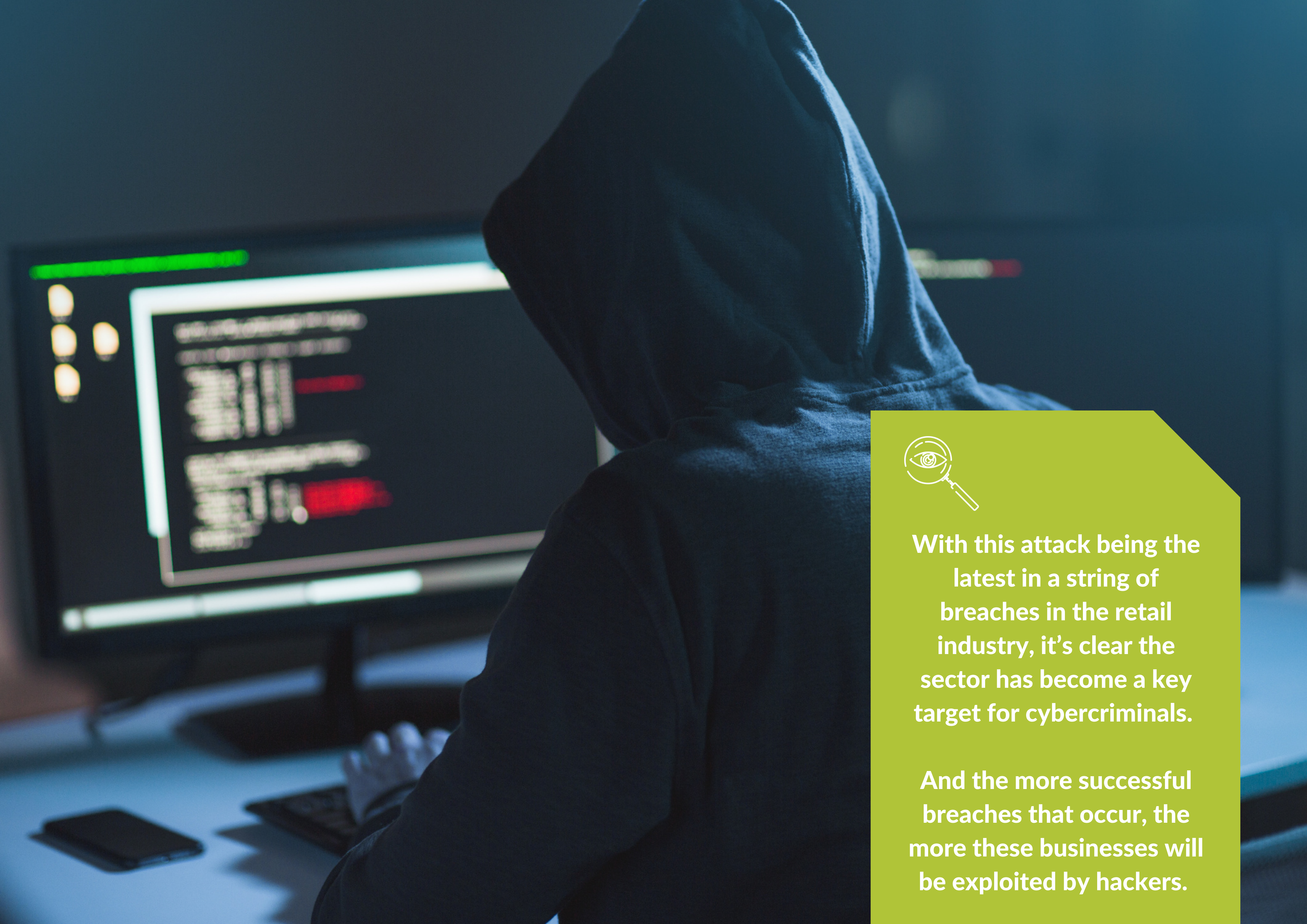
The attack was carried out using ransomware, a type of malware that encrypts the victim's files and demands payment in exchange for the decryption key.

In this case, the attackers demanded a ransom in bitcoin in exchange for the decryption key.

WH Smith did not disclose whether it paid the ransom. However, the company suffered a second attack, with hackers accessing staff data, in 2023.

Data that may have been breached includes names, addresses, National Insurance numbers and dates of birth of the firm's current and former UK staff.

Advice from the Police and the Government’s National Cyber Security Centre (NCSC) implores organisations not to pay any ransoms.



With this attack being the latest in a string of breaches in the retail industry, it’s clear the sector has become a key target for cybercriminals.

And the more successful breaches that occur, the more these businesses will be exploited by hackers.

Increase in cyberattacks on retail organisations

Over the last year, several retail organisations in the UK have been targeted by cybercriminals.

The Works, a discount retailer, and KP Snacks, a snack food company, also suffered data breaches that resulted in the theft of employee data.

Within the same month, Funky Pigeon, an online greeting card retailer, announced that it had suffered a cyberattack that resulted in the theft of customer data, including names, addresses, and payment card details.

More recently, JD Sports, a popular sports retailer, suffered a ransomware attack, just one month before the attack on WH Smith occurred.

The attack disrupted JD Sports' IT systems, forcing the company to shut down its online operations temporarily.

A news article following the WH Smith attack quoted a data privacy law expert warning that

> **Retailers are at a higher risk of cyberattack because of the large amount of data they hold on their customers and employees.**
>
> **There is also enhanced reputational risk and potential for disruption because retailers are so reliant on public trust and confidence, which cyber incidents threaten to undermine. This makes the retail sector an attractive target.**

Last year, more than 300 of the James Hall-supplied SPAR stores were hit by a cyberattack so severe that many also had to temporarily close their doors to customers.

These closures were a result of whole IT system failures, with some stores unable to process card payments.

Alongside the payment disruption, wholesale ordering functions and manufacturing operations at the James Hall depots were affected.

This attack on SPAR’s infrastructure also comes soon after the attempted hack on Tesco and the Fat Face data breach.

Like much of the cybercrime we have seen over the last 12 months, the attack on SPAR was confirmed as ransomware.

> **“The Government's Cyber Breaches Survey revealed that 39% of businesses in the UK had suffered a cyberattack during the previous 12 months.**

The increase in cyberattacks on retail organisations highlights the need for the sector to take steps to protect themselves

What retailers need to do to protect themselves

Cybercriminals will want to cause as much pain as quickly as possible to ensure they get the financial reward.

Shutting down Operational Technology (OT) until money is paid is a smart and sinister way to deploy ransomware. We're increasingly seeing instances of cyberattacks affecting the physical environment too.

There are some steps that retailers can take to protect themselves from the increasing threat of ransomware and cyberattacks.

Educate Employees

Employees are often the weakest link in an organisation's cybersecurity defenses but they can also be your first line of defence.

Retailers should educate their employees about the risks of cyberattacks and provide them with training on how to identify and respond to suspicious emails, links, and attachments.

One common tactic used by cybercriminals to steal sensitive information or gain unauthorised access to a network is phishing.

Phishing is the use of fraudulent emails, text messages, or other forms of communication that appear to be from a reputable source but are designed to trick the recipient into clicking on a malicious link or attachment, or disclosing sensitive information.

To prevent the company from falling victim to phishing attacks, retailers should conduct regular phishing simulations to test their employees' awareness and ability to identify suspicious emails and links.

These simulations can help employees recognise common tactics used by cybercriminals, such as using urgent language or creating a sense of fear or urgency to prompt a quick response.

Ongoing training and education on cybersecurity best practices are critical to ensuring that employees are equipped with the knowledge and skills necessary to protect the organisation's sensitive data and systems. By investing in employee education and awareness, retailers can strengthen their overall cybersecurity defenses and reduce the risk of falling victim to a phishing attack.

Implement Multi-Factor Authentication

Multi-factor authentication (MFA) is a security measure that requires users to provide two or more forms of identification before they can access an account or system.

Retailers should implement MFA for all their accounts and systems to reduce the risk of unauthorised access.

Regularly Backup Data

Regular data backups can help retailers recover quickly from a ransomware attack.

Retailers should back up their data regularly and ensure that the backups are stored securely offsite.

However, with the progression and proliferation of cybercrime – ransomware in particular – back-ups are less efficacious in the face of increasingly sophisticated cyberattacks so can't be taken as the only mitigation step.

Develop an Incident Response Plan

Retailers should develop a response plan for cyberattacks, including ransomware attacks.

The plan should include steps for identifying and containing the attack, restoring systems, and communicating with customers and employees.

Conducting Regular Penetration Testing

One critical step that retailers can take to protect themselves from cyberattacks is to conduct regular penetration testing.

Penetration testing is a simulated cyberattack that helps identify vulnerabilities in an organisation's systems, networks, and applications.

Penetration testing provides valuable insights into an organisation's security posture by simulating the actions of a real attacker.

This testing can help retailers identify weaknesses in their security controls, such as outdated software, weak passwords, or unsecured networks.

Once identified, these vulnerabilities can be addressed before they can be exploited by an attacker.

Penetration testing should be conducted regularly, ideally once every six months or after any significant changes to an organisation's IT infrastructure.

Penetration testing can also help organisations comply with regulatory requirements, such as the Payment Card Industry Data Security Standard (PCI DSS) or the General Data Protection Regulation (GDPR).

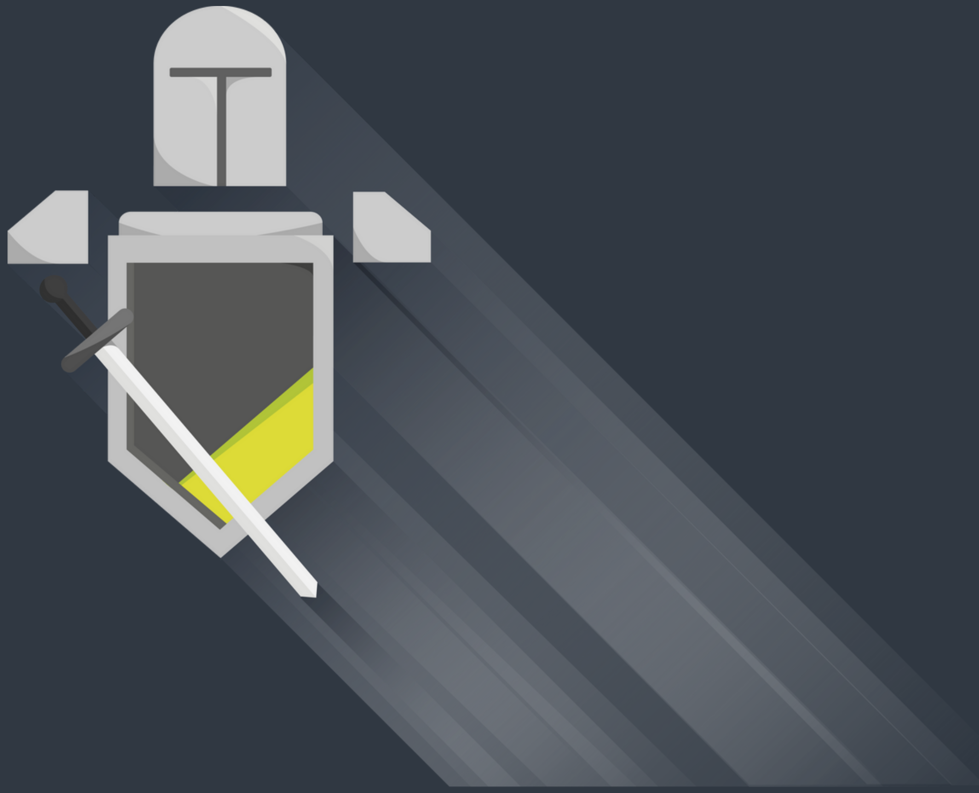
Proactive Monitoring

In addition to the above steps, retail organisations can proactively prevent ransomware attacks by implementing a Security Operations Centre (SOC) service.

A Security Operations Centre (SOC) is a centralised unit responsible for monitoring, detecting, and responding to security incidents within an organisation's IT infrastructure.

By outsourcing their security to a managed security services provider that offers SOC services, retailers can leverage advanced security technologies, specialised security expertise, and round-the-clock monitoring and response capabilities.

There are some of the benefits of outsourcing to a managed security services provider with a SOC service.



Real-time Monitoring

SOC service providers monitor retailers' networks and systems in real-time to detect any suspicious activity that could lead to a cyberattack.

They use advanced technologies, such as machine learning and artificial intelligence, to analyse logs and alerts from various security devices to identify and respond to potential threats.

Rapid Response

SOC service providers have dedicated security teams that can respond quickly to security incidents.

They can investigate incidents, contain them, and mitigate the damage caused by the attack.

Expertise

SOC service providers have a team of security experts with specialised knowledge in various security domains, such as network security, cloud security, and endpoint security.

These experts can provide valuable insights and recommendations on how retailers can improve their security posture.

Scalability

SOC service providers can scale their services based on retailers' changing security needs.

As retailers grow and expand their IT infrastructure, SOC service providers can adapt their security services to accommodate the new environment.

Compliance

SOC services can help retailers comply with industry regulations, such as PCI DSS and GDPR, by implementing security controls and processes that meet the requirements of these regulations.

> **Retailers can protect themselves from ransomware attacks without straining existing resources, by outsourcing SOC services to a managed security services provider.**

Retailers should consider partnering with a reputable and experienced managed security services provider to keep their defenses strong, stay ahead of cyber threats and manage the cost and ROI of their cybersecurity.

Additional security measures

Supply chain security

Most organisations understand the importance of an overall security strategy. However, this also means hackers will start searching for new ways to breach. The SPAR attack particularly highlights how criminals are leveraging back-door entrances through the supply chain to gain access.

Rather than hit SPAR directly, it was James Hall as the third-party supplier that became the weak link. To mitigate these dangers, it is essential that retailers understand the risk of working with third parties and ensure that well-defined security policies and frameworks such as ISO 27001 are put in place.

Liability around breaches must also be contractually agreed, and businesses should look to implement regular penetration testing to protect their networks as well as demonstrate their due diligence.

Network Architecture

The attack on SPAR is particularly interesting given the franchise structure of the organisation.

While we don't know the full details, it is likely that the hackers targeted HQ servers and moved laterally across the IT systems – travelling from the corporate network through to the credit data environment to disrupt payment processes.

For a retail business to protect itself from this kind of movement, NetOps teams should always avoid developing a flat network architecture and instead implement well-defined separation policies. This can be the difference between a single compromised device and a breach that shuts down an entire organisation.

Cyberattacks on retail organisations are becoming increasingly common, and retailers need to take steps to protect themselves.

The recent WH Smith cyberattack is just one example of the damage that a cyberattack can cause. It's crucial for retailers to educate their employees and develop a proactive response plan for cyberattacks.

In addition to these steps, retailers need to stay up to date on the latest cybersecurity threats and vulnerabilities.

Retailers should be conducting regular vulnerability assessments and penetration testing to identify and address any weaknesses in their systems, by working with third-party cybersecurity experts to ensure that their systems and data are secure.

Ultimately, retailers cannot afford to take cybersecurity lightly.

Cyberattacks can result in significant financial losses, damage to reputation, and loss of customer trust.

By taking proactive steps to protect themselves, retailers can reduce their risk of falling victim to a cyberattack and minimize the impact if one does occur.

The solution is an ‘always on’ Security Operations Centre

Following a cyberattack, retailers such as WH Smith and SPAR have had to dust off their playbooks and look at their recovery techniques and backups strategies.

While it is essential to have those back-ups in place, the reality is that a Security Operations Centre (SOC) service, monitoring for attacks day and night, would have mitigated the risks of the breach.

The biggest lesson that retailers, grocers and all sectors can take from these attacks is that it’s not the case of ‘if’ a business will be attacked, but ‘when’.

With a SOC in place however, attacks can be detected and responded to before they become a critical event.

If you’re looking into how you can better protect your business, get in touch with us. We have some of the highest qualified security professionals in the country ready to help you take your first step to safeguard your organisation.

DigitalXRAID

CYBER SECURITY EXPERTS

Need the Best Defence Against Cyber Threats?

Call us now on 0800 090 3734

info@digitalxraid.com   digitalxraid.com

British Assessment Bureau UKAS MANAGEMENT SYSTEMS 8289 ISO 27001 INFORMATION SECURITY MANAGEMENT

British Assessment Bureau UKAS MANAGEMENT SYSTEMS 8289 ISO 9001 QUALITY MANAGEMENT

CYBER ESSENTIALS CERTIFIED PLUS

IASME CONSORTIUM

CREST

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