THE SOUTH EAST CYBER RESILIENCE CENTRE

INFORMATION PACK

CONTENTS >

WELCOME TO **THE SOUTH EAST CYBER RESILIENCE CENTRE**

Thank you for joining our community of businesses in the South East who are taking action to improve their cyber security. You are now part of an exclusive network of businesses from across the region, from sole traders to SMEs through to national and international organisations.

Being a part of our community is **free of charge** and we are delighted that you have decided to join us.

This information pack will provide you with access to national guidance on cyber security, free online resources and toolkits and a tabletop exercise to really assess your business resilience plans against a cyber-attack. You will also receive regular updates from the SECRC team including the latest information about emerging threats.

Cyber security is a fast-moving threat and can be a minefield to navigate. Once you have read your information pack and utilised the guidance and tools available, you may identify gaps where you feel you need more support from the SECRC.

If you are unsure what additional support might be right for your business our SECRC team can help guide you. We are here to help you to protect your business, as well as support you with your risk management and business resilience.

Being a part of The South East Cyber Resilience Centre will enable us to help you to:

- ✓ Learn more about Cyber Resilience.
- ✓ Easily access Government recommended free tools from the National Cyber Security Centre.
- ✓ Find local certifying bodies should you want to achieve Cyber Essentials or Cyber Essentials 'Plus' accreditation.
- ✓ Identify and secure relevant and affordable cyber security services.

WHO MAKES UP **THE SOUTH EAST CYBER RESILIENCE CENTRE?**

MEET THE TEAM

Our Centre is led by two police officers, they fulfil the roles of the Centre Director and Head of Cyber and Innovation.

Meet the full team on our website www.secrc.co.uk/meettheteam

OUR NON-EXECUTIVE DIRECTORS

We have established a Board of Non-Executive Directors who are responsible for setting the strategic direction of the centre, making sure that we serve the needs of the local business community. Our Non-Executive Directors are all from organisations with premises in and around the South East and therefore have a passion to protect businesses in the region and support the region's economy.

Meet our Non-Executive Directors at www.secrc.police.uk/our-board

OUR ADVISORY GROUP

Our Advisory Group are professionals who come from a diverse range of industries and play a key role in providing guidance, advice and support around the initiatives and work the SECRC undertakes.

Meet our Advisory Group at www.secrc.police.uk/advisorygroup

OUR CYBER ESSENTIALS PARTNERS

Our Cyber Essentials Partners are official providers of Cyber Essentials Plus Certification and have been accredited by the Information Assurance for Small and Medium Enterprises Consortium (IASME).

Once on board our Cyber Essentials Partners can help your organisation achieve Cyber Essentials and Cyber Essentials Plus Certification.

Meet our Cyber Essentials Partners at www.secrc.police.uk/cyberessentialspartners

> “The SECRC is an exciting and forward-facing initiative which establishes a strong partnership between Policing, Academia, and the Private sector in educating and fighting the continual threat posed by cyber criminals, and the danger they pose to UK companies.”

IDENTIFYING YOUR **CYBER RISKS**

Cyber security is what a business needs to have in place to minimise the risks of being hit by a successful cyber-attack.

A successful attack can cause significant harm to a businesses finances and reputation. It can stop a business being able to operate by preventing access to critical infrastructure, systems, and data. It can also result in the loss of personal data impacting on customer confidence and the bottom line of your business.

However, a lot of these attempted attacks can be prevented by understanding the individual risks and vulnerabilities of your business. By putting the right mitigations in place, you can ensure you are as protected as you can be.

To identify your businesses' cyber security risks, you need to look at three key areas: Technology, Processes and People. These will give you a good indication of where risk mitigations need to be implemented to increase protection.

TECHNOLOGY

Using outdated software and applications, having no anti-virus software are just some of the technology related risks that could impact the security of the devices you use.

PROCESSES

Cyber security policies and procedures set standards of behaviour for employees of all levels. These policies are designed to mitigate against cyber-attacks and to help businesses manage the impact of any successful attacks.

PEOPLE

People are your strongest asset and often your weakest links. Empower your employees with the knowledge and confidence to identify and flag their cyber security concerns.

As with any risk to your business you cannot 100% guarantee it will not happen, but you can reduce the risks significantly by implementing basic cyber security practices.

As a member of The South East Cyber Resilience Centre we can help your organisation avoid common cyber-attacks, and help you demonstrate that your company takes cyber security seriously, protecting the data it holds.

RESOURCES, TOOLS, AND SUPPORT FOR BUSINESSES

The National Cyber Security Centre (NCSC) is the UKs independent authority on Cyber Security. The centre has vast technical capabilities and expertise which they utilise to produce practical guidance for businesses and the public. They are a fantastic resource for the very latest Cyber Security advice.

The SECRC has put together some of the top resources the NCSC has produced to make it easy for your business to access them. Just click on the headings to get more information:

SMALL BUSINESS GUIDE

www.ncsc.gov.uk/collection/small-business-guide

An easy-to-understand guide with five key steps you can take to manage your cyber security risks.

SECURING YOUR SOCIAL MEDIA CHANNELS

www.ncsc.gov.uk/guidance/social-media-how-to-use-it-safely

Social media is a wonderful way to stay in touch with family, friends and keep up to date on the latest news. It is important to know how to manage the security and privacy settings on your accounts, so that your personal information remains inaccessible to anyone but you.

CYBER ACTION PLAN

www.ncsc.gov.uk/news/cyber-aware-action-plan

Answer a few questions and get a personalised list of actions to help you or your business improve your cyber security.

10 STEPS TO CYBER SECURITY

www.ncsc.gov.uk/collection/10-steps-to-cyber-security

Guidance is designed to help organisations protect themselves in cyberspace. It breaks down the task of defending your networks, systems, and information into its essential components, providing advice on how to achieve the best possible security in each of these areas.

EXERCISE IN A BOX

www.ncsc.gov.uk/information/exercise-in-a-box

An online tool which helps organisations test and practice their response to a cyber-attack. It is completely free, and you do not have to be an expert to use it. It includes two exercises, a technical simulation, and a tabletop exercise. You just need to register for an account.

NCSC BOARD TOOLKIT

www.ncsc.gov.uk/collection/board-toolkit

Boards are pivotal in improving the cyber security of their organisations. The Board Toolkit has been designed to help board members get to grips with cyber-security and know what questions they should be asking their technical experts.

Continued >>

RESOURCES, TOOLS, AND SUPPORT FOR BUSINESSES (CONTINUED)

CYBER SECURITY TRAINING FOR STAFF

www.ncsc.gov.uk/training/v4/Top+tips/Web+package/content/index.html#/

Your staff are your first line of defence against a cyber-attack. The NCSC has developed an e-learning training package 'Stay Safe Online: Top Tips for Staff' to help educate your staff on a range of key areas including phishing, using strong passwords, securing your devices, and reporting incidents.

EARLY WARNING SERVICE

www.ncsc.gov.uk/information/early-warning-service

Helps organisations investigate cyber-attacks on their network by notifying them of malicious activity that has been detected in information feeds.

ACTIVE CYBER DEFENCE (ACD)

www.ncsc.gov.uk/section/active-cyber-defence/introduction

This programme seeks to reduce the harm from commodity cyber-attacks by providing tools and services that protect against a range of cyber security threats.

CYBER INFORMATION SHARING PLATFORM (CISP)

www.ncsc.gov.uk/section/keep-up-to-date/cisp

This is a joint industry and government initiative run by the NCSC and a good place for network defenders to find help and speak with likeminded people.

OTHER RESOURCES

The SECRC has put together some top resources from other areas to make it easy for your business to access them:

CYBER INCIDENT RESPONSE PLAN TEMPLATE

www.secrc.police.uk/post/cyber-incident-response-plan

A cyber security incident response plan provides a process that will help your business, charity or third sector organisation to respond effectively in the event of a cyber-attack.

HAVE I BEEN PWNED

www.haveibeenpwned.com/DomainSearch

Have you setup your organisation for domain search protection with Have I been pwned? A free service that's worthwhile to keep you notified about any of your domain emails featuring in data breaches which would be a precursor for business email compromise (really important if 2fa is inactive) and phishing email campaigns.

INFORMATION SECURITY POLICIES

www.sans.org/information-security-policy

In collaboration with information security subject-matter experts and leaders who volunteered their security policy knowledge and time, SANS has developed and posted a set of security policy templates for your use.

Continued >>

RESOURCES, TOOLS, AND SUPPORT FOR BUSINESSES (CONTINUED)

GET READY FOR CYBER ESSENTIALS

www.getreadyforcyberessentials.iasme.co.uk

Cyber Essentials is an effective, Government backed baseline scheme that will help you to protect your organisation, whatever its size, against a whole range of the most common cyber-attacks.

Cyber-attacks come in many shapes and sizes, but the vast majority are very basic in nature, carried out by relatively unskilled individuals. They're the digital equivalent of a burglar trying your front door to see if it's unlocked. Our guidance is designed to prevent these attacks.

Sometimes, organisations are unsure about where to start to prepare for Cyber Essentials. This simple tool is a series of questions that have been developed to lead you through the main parts of the Cyber Essentials requirements. If there are areas where you need to put more controls in place, you will get a link to guidance about how to make those changes. At the end of this process, you will get a list of actions outlining what steps you need to take to prepare for Cyber Essentials and links to specific guidance on those actions.

TEST FILTERING CHECK

www.swgfl.org.uk/services/test-filtering

Check Your Internet Connection Blocks Child Abuse & Terrorist Content.

CONFIGURE O365'S PHISHING REPORT ADD-IN

www.ncsc.gov.uk/guidance/configuring-o365-outlook-report-phishing-for-sers

Setup O365 to enable users to have access to a report phishing button on the toolbar. It will send a phishing report to your Security Operations Centre (SOC) and the NCSC.

POLICE CYBERALARM

www.cyberalarm.police.uk

Police CyberAlarm is a free tool backed by policing and funded by the Home Office to help your business understand and monitor malicious cyber activity. Police CyberAlarm monitors the traffic seen by a member's connection to the internet. It will detect and provide regular reports of suspected malicious activity, enabling organisations to minimise their vulnerabilities.

> “Membership at The South East Cyber Resilience Centre is a fantastic way to receive up-to-date news on local cyber threats, and tips and guidance on how I can increase my business's cyber resilience.”

Website Designer and Social Media Freelancer

CYBER SECURITY SERVICES

REQUEST A QUOTE VIA OUR WEBSITE
www.secrc.police.uk/services

The resources, tools and guidance that have been provided within this welcome pack are designed to allow you to take basic steps towards increasing your businesses resilience to cyber-attacks.

Once you are ready to take the next step, we offer a range of relevant and affordable cyber security services designed to help businesses identify their vulnerabilities, asses current plans and policies and work with their teams to build their cyber awareness.

We deliver our services using an innovative talent pipeline programme, where the region's leading universities in cyber skills partner with local policing and the private sector to provide commercial training and oversight for students to deliver this work. Our students are all from universities within the South East and work under the guidance of acknowledged and experienced national cyber specialists, delivering each service using industry standard tools and techniques.

REMOTE VULNERABILITY ASSESSMENT

We can scan your network remotely, like an attacker might, and see if there are obvious weaknesses present which they might choose to exploit.

INTERNAL VULNERABILITY ASSESSMENT

Find out how much damage an attacker could do if they did manage to breach your network or launch an attack from the inside.

FIRST STEP WEB ASSESSMENT

The 'First Step Web Assessment' has been designed by our private-sector experienced security team to not only provide you with an initial assessment of your website. This is a service to assess your website.

WEB APPLICATION VULNERABILITY ASSESSMENT

How secure is your website? Does it contain vulnerabilities just waiting to be exploited? Our assessments can help identify these weaknesses so you can fix them.

SECURITY AWARENESS TRAINING

Ensure your staff are aware of the risks associated with cyber and how to protect themselves and your business.

Continued >>

CYBER SECURITY SERVICES (CONTINUED)

CORPORATE INTERNET DISCOVERY

Find out what information an attacker can gather about your business and how it can be used in a cyber-attack

INDIVIDUAL INTERNET DISCOVERY

Harvesting online information about senior team members in your business can help an attacker craft a convincing phishing email. Find out what exists online about you and your team, and how it could be used in an attack.

CYBER BUSINESS CONTINUITY EXERCISE

Practical scenario-based exercises tailored for your organisation to test your business continuity plan and your recovery plan in the event of an attack.

SECURITY POLICY REVIEW

Find out how robust your current cyber security policies are and what can do to improve them.

> "Just a short note to say a massive thank you to the SECRC, who delivered a great Security Awareness Training session to our staff. I have to say, mostly they find IT deadly boring and probably groaned when they saw my email to book into the training session! However, we got some really positive feedback and they all stayed engaged right to the end."

A representative from the Thames Valley Partnership

REQUEST A QUOTE
VIA OUR WEBSITE
www.secrc.police.uk/services

STAYING CONNECTED

Our team at the SECRC are friendly, knowledgeable and on hand for you to contact for support and guidance should you need us.

To stay up to date with the latest news from us and the wider security industry, please follow us on our social media channels.

In the coming weeks, we will be in touch to see how you are making use of the information and resources that we have provided to see if you need any additional support from us.

The South East Cyber Resilience Centre is looking forward to working in partnership with you and your organisation to make the South East region a more cyber resilient place to live, work and do business.

FOLLOW US ON LINKEDIN

linkedin.com/company/crc-south-east

FOLLOW US ON FACEBOOK

facebook.com/CRCSouthEast

FOLLOW US ON TWITTER

twitter.com/CRCSouthEast

FOLLOW US ON INSTAGRAM

instagram.com/CRCSouthEast