Best Practice Security

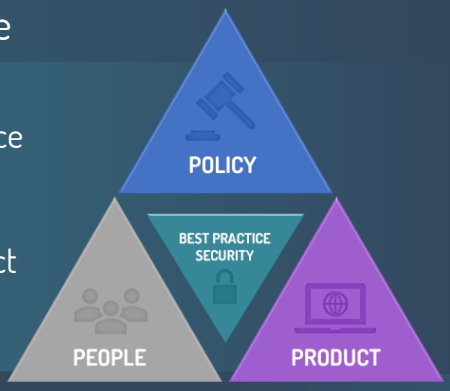
SAEPIO
INFORMATION SECURITY

BEST PRACTICE GUIDE

Securing your Remote Workforce

Saepio is an Information Security advisor that helps organisations reduce their cyber risk and improve security posture.

Security is more than technology. Best practice policy and process direct a successful security strategy. Products and people help enforce it.



As part of the Government's strategy for managing the Covid-19 outbreak, everyone is required to work from home where possible. This presents a number of unique information security challenges for most organisations; whether remote working is completely new to you or whether you've had to suddenly upscale your provision. This guidance is intended to help you manage your cyber risk effectively while your employees adjust to working from home.

Policy and Process

Policy

Best Practice Security

Policy & Process Review

Consider a review your corporate policies and procedures in relation to cyber management, update them where relevant and re-issue them to staff. If you have a way of getting staff to digitally sign their acceptance of them, then even better. You will need to decide on the policy and procedure checklists you want to circulate, but we would advise inclusion of at least the following:

Acceptable Use Policy
Employees and third-parties who use company equipment or information systems should be made aware of acceptable use, to ensure the company's information and information systems are being used responsibly.

Mobile Device Policy
This policy should specify the security requirements necessary to mitigate the associated risks of using mobile devices, tablets and laptops. If you are allowing staff to use their own devices please also consider a BYOD policy.

Password Policy
Weak passwords can be easily compromised using off-the-shelf software or public data breaches. The same credentials used across multiple sites or systems are especially vulnerable, so this policy should ensure the confidentiality and use of strong and unique passwords.

Incident Management Policy
This policy should define your approach to incident management and include how you prepare for an incident, detect one, respond to and contain one, how you will recover from one, and post-incident activities that need to occur.

Incident Reporting Procedure
The incident reporting process should clearly state the lines of communication and escalation to be followed in the event of an information security breach, and should also clearly define what constitutes a breach.

*policy and procedure templates can be provided upon request

Product

Best Practice Security

SAEPIO
INFORMATION SECURITY

TECHNOLOGY CONTROLS

Key Considerations

Endpoint Detection and Response
A remote workforce means there are now many more employee workstations sitting outside the corporate network. There are many people now connecting to the enterprise via home networks with no firewall protecting them, so having a robust endpoint protection tool in place is really important. Modern endpoint detection and response (EDR) solutions are designed to operate outside the corporate network. These solutions prevent malware and enable threat hunting. They also give you the ability to initiate immediate response actions, such as preventing new malware from running or removing malware from systems remotely.

Vulnerability Management
It's never been more important to keep your patching up-to-date. Use a vulnerability management tool to get a clear view of all the assets on your network, which ones can be exploited, and what you need to do in what order to effectively reduce your risk

Virtual Private Networks (VPNs)
Many corporate departments like Finance and Human Resources may be handling sensitive data outside the physical office for the first time, so require them to use a VPN to ensure a secure connection to your sensitive data. Do your research on your VPN provider, as many VPN tools (particularly freeware ones) are flawed.

Data Protection & Availability
Your staff need uninterrupted access to your corporate data to maintain productivity when working from home, but protecting that data and ensuring you remain compliant with data protection regulations can be a challenge, particularly where you have been heavily reliant on on-premise back-up and data discovery solutions. Consider a cloud-native SaaS platform for data protection and management across edge, on-premise and cloud workloads.

Web & Email Security
Ensure web and email protection by implementing web filtering technologies to prevent employees from visiting malicious websites, and implement email filtering rules to block spam and phishing emails. Review your outbound filtering, encryption and data loss prevention policies to ensure staff don't accidentally send sensitive information to the wrong people.

Multi-Factor Authentication and Single Sign On
Wherever possible, implement an MFA solution for staff to access critical applications. This will help secure your logins against attackers exploiting weak or stolen credentials. Single Sign On improves user experience and reduces forgotten password helpdesk calls.

Some useful help from our technology partners!

- **Okta:** 6 months free-of-charge, no obligation, single sign on (SSO) and MFA to secure remote access
- **Druva:** 6 months free-of-charge, no obligation, data protection and back-up for O365 and Endpoints, up to 300 users
- **Mimecast:** 3 months free-of-charge, no obligation, Web security / DNS protection
- **Rapid7:** 60 days free-of-charge, no obligation, Security Monitoring / SIEM
- **Varonis:** 60 day, free-of-charge, no obligation, VPN, DNS, and web proxy monitoring
- **KnowBe4:** Free-of-charge security awareness training materials for your employees

Partners: We're proud of the strong relationships we've formed with others in the security indistry. The wealth of information security knowledge in Saepio's network enables us to deliver the risk reduction outcomes desired by our clients

Red Sift | Druva | Malwarebytes | DUO | Rapid7 | Varonis | Okta | KnowBe4 | Pentest People | Mimecast

*please get in touch if you'd like to understand more about these and other vendor offers available to you during lockdown

People

Best Practice Security

SAEPIO
INFORMATION SECURITY

THE HUMAN ELEMENT

Keep your staff safe and secure

Many of your staff may already be used to home-working and the cyber risks associated with it, but for some this transition may be completely new. You may have employees feeling quite out of their depth, or those that are struggling to balance work-life with home-schooling their children, so regular helpful communication is key.

How To Guides

Staff may well now be using technologies they are unfamiliar with. Consider writing them some 'how to guides'. Use your LMS if you have one to upload training content that they can access from home, otherwise send them details of how to access training content stored elsewhere. Make sure they also know how to contact you for support and to report any issues.

Cloud Services and Applications

Encourage staff to contact you if they want to use any new cloud services or applications, so that you can sanction their use. Remind staff to only download applications from trusted sources, and to carefully read and review the privacy notice and settings for any apps that they install.

Video Conferencing

Ask staff to only use sanctioned video-conferencing applications, and remind them to set a password and review their privacy settings. We recommend having video off as default. Also, remind staff not to have confidential conferences or telephone calls next to smart home listening devices, such as Alexa.

Software Updates

Remind staff to check for software and application updates daily for all their devices, and not to put off installing them.

Securing Home Internet Access

Ask staff to check their router is not still set to the default password, and that they have enabled strong encryption for the WiFi network (WPA2). Advise them to contact their internet service provider if they are unsure how to check/change settings.

Scam Alerts

Cybercriminals have wasted no time in exploiting peoples' fears around Coronavirus (Covid-19). Make sure you are sending them regular updates on what to watch out for: phishing emails, fake charity websites, CEO Fraud, fake IT/HR emails etc. If you don't already have a formal security awareness training program in place, then consider implementing one as soon as possible.

SAEPIO SECURITY AWARENESS TRAINING SERVICE

Saepio deliver a fully managed security awareness training service using the KnowBe4 platform, for in excess of 20,000 end users, so we are well-versed in methods to help keep your staff cyber-safe. If you would like any advice on ways to manage your 'human firewall' during this time then please do get in touch. We have a range of free, no obligation, resources that we'll happily share with you.

1. Baseline Testing
establish the level of your organisational risk

2. Train Your Users
foundational and ongoing regular training events

3. Phish Your Users
regular testing to change security behaviour

4. Analyse Results
define risk areas, target training and phishing

5. Repeat & Mature
increase difficulty, target departments, vary training