CYBER MANAGEMENT ALLIANCE

Remote Working Cybersecurity Checklist

Version 1.1 1st April 2020

About Cyber Management Alliance

Established in 2015, Cyber Management Alliance is one of the world's leading cyber incident & crisis management service providers offering advisory, executive training and bespoke workshops in all aspects of cyber crisis management, incident planning, incident response testing and tabletop exercises.

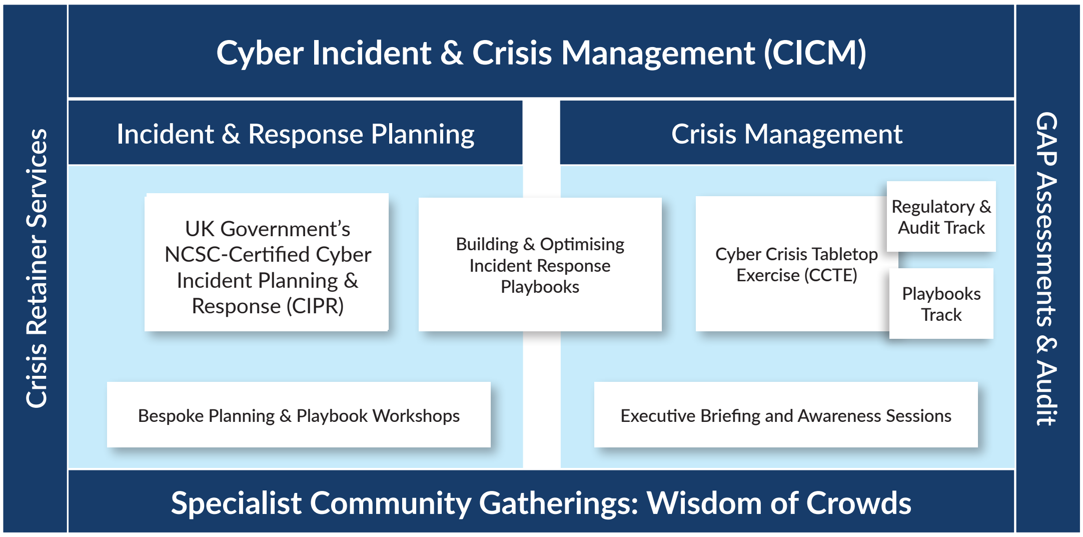
Cyber Management Alliance (CM-Alliance) is the creator of the internationally-acclaimed *NCSC-Certified, Cyber Incident Planning and Response* (CIPR) course. Previous attendees of the NCSC-Certified CIPR course and tabletop exercises include organisations including the United Nations, UK Ministry of Defence, several UK Police Forces, NHS Trusts, European Central Bank, Swiss National Bank, Microsoft, Ernst and Young, BNP Paribas and many others.

Services & Training Summary

At CM-Alliance, we believe that practice makes perfect when it comes to cyber crisis management. As part of our Cyber Incident & Crisis Management training and workshops we offer:

- **Incident Planning & Response:** This training is certified by the UK Government's NCSC and is titled Cyber Incident Planning & Response. This certified course is highly interactive and covers the various tactical and strategic elements of planning for a cyber-attack. The 'Building & Optimising Incident Response Playbooks' workshop focusses on creating and optimising incident response playbooks.
- **Crisis Management Tabletop exercises:** Our Cyber Crisis Tabletop Exercises (CCTE) are verbally-simulated, business-impacting, cyber-crisis scenario sessions where attendees discuss and review their actions and decisions.
- **Trusted Advisory:** Also referred to as vCISO (Virtual Chief Information Security Officer) our service is cost-effective and commercially viable to organisations of all sizes and covers cybersecurity, privacy, audits and assessments.

TRUSTED ADVISORY & RETAINER SERVICES


Crisis Retainer Services
Cyber Incident & Crisis Management (CICM)
Incident & Response Planning
Crisis Management
UK Government's NCSC-Certified Cyber Incident Planning & Response (CIPR)
Building & Optimising Incident Response Playbooks
Cyber Crisis Tabletop Exercise (CCTE)
Regulatory & Audit Track
Playbooks Track
Bespoke Planning & Playbook Workshops
Executive Briefing and Awareness Sessions
Specialist Community Gatherings: Wisdom of Crowds
GAP Assessments & Audit

Remote Working Checklist

Thank you for downloading the Remote Working Cybersecurity Checklist. This is by no means a comprehensive list but we hope you find it useful and it helps you be more prepared for cybersecurity attacks. Remember you can always get in touch with us if you need specific advice. We are contactable on info@cm-alliance.com.

Cybersecurity	**Check**
■ Remind staff about the need to protect confidentiality	□
■ Remind staff **NOT to lend** their machines to their children or other members of the family	□
■ Remind staff that you are **MONITORING** their activity as per your policies and terms and conditions of employment	□
■ **Update of software and OS**: Ask staff to keep all their devices (corporate and personal) fully updated	□
■ **Provide a VPN** and or remote working solution for your staff (ensure you validate the VPN solution)	□
■ Send out regular reminders about **critical software and mobile updates** (ex: Abobe, Apple, Android, Chrome, Firefox) and ask staff to update (show them how to using recorded screencasts if necessary)	□
■ **Disable email forwarding** for all accounts OR set up an alert if email forwarding is switched on	□
Passwords	
■ Staff **MUST not share** passwords via emails or SMS messages (where really necessary, phone the other party)	□
■ Ask staff to use password managers (a very strong password for the password vault, written down & stored safely)	□
■ Remind staff that you will NOT call them about password resets (to help avoid being scammed)	□
■ Make 2 factor authentication (2FA) mandatory for all remote workers	□
■ Including email and when accessing any critical systems or applications	□
■ Ensure you have BACKUP CODES in case 2FA does not work	□
■ Use an APP for 2FA rather than SMS (free apps include Google's authenticator)	□
■ Store these backup codes safely, preferably in a locked safe	□
■ Ensure you know how to backup and restore the 2FA tokens you are using (ex: Google Authenticator etc)	□
Mobile Equipment *(Remember these are now critical devices and must be treated as such)*	
■ Ensure all your mobile equirpment has **hardware encryption** (where not possible, software encryption is ok)	□
■ All mobile devices must have FULL disk **encryption**	□
■ If you are renting laptops/desktops please ensure that you **WIPE the hard disks** to ensure no residual data is left behind. This MUST be on top of your to-do-list when things go back to "normal" OR when you have to return the machines	□
■ Where staff are using personal devices, remind them **not to download Apps** from non-trusted sources. They are HIGHLY likely to contain malware	□
■ Mobile devices are now **business critical** machines and must be subject to the same stringent policies like software-updating, backup, protective-controls	□
■ Keep extra stock of mobiles,laptops,microphones and other peripherals	□
■ If possible use Googe's DNS servers or CISCO's umbrella DNS and force all laptops & mobile devices to use these. Advice staff to do the same on their personal devices (if unsure, ask for external help)	□

Continued...

Remote Working Checklist (cont)

Privileged Users *(Hold the keys to the kingdom)*	**Check**
Find out more about our e-learning training for privileged users email us on info@cm-alliance.com or call us on +44 (0) 203 189 1422	
■ Ensure you inform all IT and business privileged users and:	□
■ Remind them of their responsibilities	□
■ Insist that they DO NOT login for DAILY tasks with high privileges	□
■ Demand that they REPORT all errors/confess to mistakes immediately	□
■ Ensure they use 2-factor-authentication at all times.No exceptions	□
■ Ensure that NO procedures are bypassed (no emergency change without approval etc)	□

Phishing Emails & Scams	**Check**
■ Remind staff **NOT** to open links or documents with Coronavirus information. Ask them to report these	□
■ Remind staff that it's **ok to make a mistake** and that they should own up if they have:	□
■ Accidentally clicked on a suspicious file and or link	□
■ Opened a suspicious PDF or Word, excel file with a macro	□
■ Staff **MUST** report malware/ransomware infections immediately	□
■ Caution staff about **remote helpdesk calls** purporting to be from Microsoft or other computer vendors	□
■ Remind staff to be cautious about pop-ups about VIRUS warnings when surfing the web	□
■ **Important Communications:** If relevant, remind staff that critical emails only come from a specific email like hr@someone.com OR that the CEO never sends email from his email account	□

Policy & Illegal Activity	**Check**
■ Take this opportunity to remind users about your AUP or Acceptable Usage Policy (and other policies)	□
■ Remind staff that surfing porn sites on corporate machines, amongst other things, is illegal	□
■ Remind staff that using corporate devices to entice hatred, research terrorist related activities is illegal:	□
■ IT staff must be reminded	
■ NOT to use corporate machines to run hacking tools	□
■ NOT to attempt illegal activities (like attempting malicious hacking, scanning etc) on office time OR using any other corporate resources	□
■ Staff MUST report malware/ransomware infections immediately	□
■ Staff must be conscious of the **employer's reputation** when tweeting social messages on Twitter, Linkedin etc	□
■ Remind staff they **MUST not use** unapproved USB flash drives and unapproved cloud services	□
■ Remind staff **it's ok to make mistakes** (ex: sending emails to wrong recipients, clicking on a malicious link, causing an outage etc) and that they MUST own up immediately. Stress that in most cases there will be NO repercussions	□

Continued...

Remote Working Checklist (cont)

Working Remotely, Online Meetings & Calls	Check
Remind staff **NOT** to have confidential calls and business discussions near SMART SPEAKERS like Amazon's Alexa, Apple's Homepod and Google's Home	□
Remind staff to **MUTE** their microphone when they are not speaking in a conference call	□
Educate all staff to ensure webcams are **blocked** by default (physically and by the conference app you use)	□
Remind staff **NOT** to leave their machines UNLOCKED, especially during a call or when visiting the loo, especially in a public place	□
Ask staff **NOT** to work from coffee shops or public places (if possible) – especially if they are on confidential calls or working on confidential documents	□
Request staff NOT to use '**Print to email**' feature offered by printers	□
"**Buddy up**" with a colleague & swap mobile numbers and check-in each morning	□
Remind staff to be cautious about pop-ups about VIRUS warnings when surfing the web	□
Ask staff **NOT to defer** critical updates to software	□
If possible, ask that screen filters are used to make shoulder-surfing harder	□
Ask staff **NOT to use just any VPN** solution to access corporate resources. This is quite important as VPNs are recommended as a way to stop snooping and interception. However, **several VPN softwares are malicious**	□
Staff **MUST not** switch on forwarding of corporate emails to their personal emails AND OR must not use alternative email clients to access corporate email	□

Exceptions & Change *(Get ready to grant exceptions left, right & centre)*	Check
If you don't have one yet, create an 'exceptions' register	□
Create a review-by-date and put multiple calendar reminders for you/your team to review them	□
Where possible, have a 'No way this is an exception' list	□
Pay special attention to change management and carry out a weekly or monthly review	□

Privacy	Check
GDPR and PECR (privacy and electronic communications regulations) still apply. Please remind staff of their obligations	
Remind all staff of their responsibility to **respect** the privacy of your clients and your staff	□
Remind IT and cybersecurity folks to be extra vigilant for possible malicious activity on user accounts	□
Ask staff **NOT to PRINT** personal information	□
Staff must be reminded **NOT** to email personal information via email OR store personal information in non-approved locations	□
Staff members may be exchanging personal phone numbers and or emails. If possible avoid this OR ask staff to prepend **'delete-later'** to the name of staff if they save these details	□

Continued...

Remote Working Checklist (cont)

Cyber-attack & Incident Response	Check
To find out more about our UK-Government NCSC certified course on incident planning and response, email us on info@cm-alliance.com or call us on +44 (0) 203 189 1422	
■ Constantly remind staff to be on alert for phishing emails and other attempts to compromise/steal account details	□
■ Staff must report all phishing emails and malicious activity	□
■ If staff suspect something malicious, encourage them to call certain stakeholders, especially if they do not receive any response via existing channels	□
■ Security staff must be **extra vigilant** and actively seek out suspicious activity (given remote working habits of users this may be operationally expensive)	□
■ Ask IT and security staff (including outsourcers/partners) to pick up the phone and call if it's important rather than rely on email. Use a **separate out-of-band app** or something as simple (not very secure) as WhatsApp groups for urgent communications	□
■ Keep a **printed** copy of your procedures and checklists at home AND make sure they are **not** easily accessible	□
■ **Monitor** endpoints (laptops etc) more closely and if possible use EDR type tools urgently	□
■ **Never too late**: Start working on your Cyber Incident Planning & Response strategy now	□

Backup Backup Backup	Check
■ Provide staff software to ensure their critical documents are backed up	□
■ Ask staff to back up data on an approved external hard disk that is **NOT** permanently connected to the device	□
■ Ask staff to use only approved cloud storage services (if permitted)	□
■ Encourage staff to reach out to discuss any cloud storage or cloud service solution that they want to use. Cloud services include but are not limited to: • File sharing services • File storage and synchronisation • Project management apps or services • Collaboration tools and services • Note taking and storage services • Photo storage and sharing services	□

HR & Mental Health & Occupational Health	Check
■ Check that HR have got in place policies to deal with occupational health in a remote working setting. Remote working may be the norm for a sustained period. Practices such as "working from the sofa" can produce other health issues i.e. back problems. Formal policy and risk assessments are strongly recommended	□
■ Remind staff that they should reach out to discuss any mental health issues	□
■ Set clear **work-time boundaries**. (Remote working can often lead to unrealistic expectations where the assumption is that staff will be available at all times)	□
■ **Enable staff to confidentially send** critical messages (health, safety, mental health, security, crisis) quickly and securely. Do this preferrably via a mobile app. DO NOT use email please	□

Continued...

Remote Working Checklist (cont)

Video & Audi Conferences	Check
Send out regular reminders to staff about using only officially approved conference apps	□
Remind staff to read about and be aware of basic security and privacy settings like:	□
Having a password for every meeting or conference call	□
Camera must be switched off OR blocked by default, for both the host and attendees	□
Microphone is on MUTE by default	□
Kicked out participants CANNOT rejoin	□
Ask staff to ensure their meetings are NOT being recorded	□
If you are recording please inform all participants	□
Remind staff to EXIT or close the app once the conference is complete	□

Helpdesk & Support	Check
Support staff MUST be on high alert and challenge password resets or ‘strange’ requests	□
Ensure you review/audit permissions and privileges of helpdesk staff	□
If possible, introduce extra user identity verification for all users	□

Useful Links

- Our UK NCSC-Certified Cyber Incident Planning & Response Course - **Click here**
- Our Building & Optimising Incident Response Playbooks Workshop - **Click here**
- Our Cyber Crisis Tabletop Exercise (CCTE) Download and Page - **Click here**
- Our Cybersecurity blogs - **Click here**
- Our Insights with Cyber Leaders -**Click here**
- Our Resources Page - **Click here**
- Our Webinar BrightTalk Webinar Channel - **Click here**

CYBER
MANAGEMENT
ALLIANCE

Author: Amar Singh.

Edits by Aditi Uberoi

Contributors: We wish to thank the following for contributing to this document: James Mckinlay, Stephen Massey, Mihir Joshi, David Cass and Tee Patel.

✉ info@cm-alliance.com http://cm-alliance.com ☎ +44 203 189 1422 @cm_alliance