Remote Working Cybersecurity Checklist

Best Practices for Working Remotely

Ecuron Inc. • 2929 Allen Parkway, Suite 200 • Houston, TX 77019 • 832.871.5970 • www.ecuron.com

032420 Remote Working Cybersecurity Checklist

With the coronavirus being a global concern and having a severe impact on life as we knew it, business operations and organizations worldwide can minimize the impact on businesses significantly by allowing employees to work remotely. While many businesses are struggling to implement remote working as quickly as possible it is more important than ever to follow some security guidelines – or it might come back to haunt them. While coronavirus is an unfortunate trigger that is causing the world to implement remote work in record time, remote work is here to stay and proper implementation from the start is essential.
To that end, we provide a remote working cybersecurity checklist that organizations can use as guidance when implementing remote working. While a complete checklist will look different for each organization, we want to provide you with a structured starting point for questions you need to ask yourself and with aspects you need to consider.

General Cybersecurity for Working Remotely

- ○ Ensure laptops and other devices have hardware encryption.
- ○ Where possible, ask that screen filters are used to make shoulder-surfing harder.
- ○ Make 2 factor authentication (2FA) mandatory for all remote workers - including email and when accessing any critical systems or applications.
- ○ Encourage staff to use password managers.
- ○ Remind staff NOT to open links or documents with Coronavirus information. Ask them to report these.
- ○ Remind staff about the need to protect confidentiality.
- ○ Ask staff NOT to defer critical updates to software.
- ○ Remind staff that surfing porn, amongst other things, is not allowed on company devices. It increases the risk of malware being downloaded.

- ○ Staff must not visit sites like illegal movie websites as they pose a risk of ransomware and malware infection.
- ○ Remind staff NOT to lend their machines to their children or other members of the family.
- ○ Stress the IMPORTANCE of NOT sharing passwords (remote working can lead to more password sharing).
- ○ Remind staff not to use unprotected networks for confidential information without a VPN
- ○ Disable Apple's Airdrop and Windows File Sharing features
- ○ Ask staff to disable Bluetooth functionality on workstations if they are not using it
- ○ Remind staff not to let other people plug devices into their workstation such as USB sticks or phones

Privileged Users

- ○ 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.

Phishing Emails

- ○ 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.

Online Meetings & Calls

- ○ Remind staff to MUTE the microphone when they are not speaking in a conference call.
- ○ Educate all staff to ensure webcams are blocked by default.
- ○ Remind staff NOT to leave their machines UNLOCKED, especially during a call or when visiting the loo.
- ○ 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.

Privacy

- ○ 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.
- ○ 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.

Exceptions

(Get ready to grant exceptions left, right and center)

- ○ If you don't have one yet, create an exceptions register.

- ○ Create a review of granted exceptions 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.

Check Cyber-Attack & Incident Response

- ○ Constantly remind staff to be alert for phishing emails and other attempts to compromise/steal account details.
- ○ Staff must report these emails and malicious activity.
- ○ Encourage them to call certain stakeholders (i.e. shareholders or C-level executives) if necessary.
- ○ Security staff must be extra vigilant and actively seek out suspicious activity (given the remote working habits of users this may be operationally expensive).
- ○ Ask IT and security staff (including outsourcers) to pick up the phone and call if it's important rather than solely to rely on email. Use a separate out-of-band app or something as simple as WhatsApp* groups for urgent communications.

  *WhatsApp should not be used for secure communications. If you are sending sensitive or confidential information you should use a more secure messaging app
- ○ Keep a printed copy of your procedures and checklists at home AND since these are typically confidential, make sure they are stored securely.
- ○ Remind all staff that it's ok to make mistakes (like 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.

Backup Backup Backup

- ○ Provide staff with software to ensure their critical documents are backed up.
- ○ Ask staff to back up their data on an approved external hard disk that is NOT permanently connected to the device.
- ○ Ask staff NOT to use external cloud storage services approved at the workplace when connecting remotely (safety controls in place at the workplace might not be effective when connecting remotely).
- ○ Ask employees to reach out to discuss any cloud storage or cloud service solution that they want to use.

APPENDIX

Current Cost of a Data Breach (Data as of July 2019)

Average cost of a breach worldwide:	$3.92 million
Average cost in the United States:	$8.19 million
Most expensive sector:	Healthcare with $6.45 million
Average size of data breach:	25,575 records
Average cost per record:	$150

PCI Fines (companies dealing with credit card data):

- $5,000 - $100,000 per month, depending on size of business

HIPAA Fines (companies dealing with healthcare and medical records):

- $100-$50,000 per violation with a max penalty of $1.5 million per year for violations that are identical.

Graham Leach Bailey Act (GLBA) (applies to financial institutions, not just banks):

- Up to $100,000 per violation for the company
- Officers and directors can be fined up to $10,000 per violation
- Also includes criminal penalties of up to 5 years in prison and the possibility of revocation of licenses

Sources:

- https://www.ibm.com/security/data-breach
- https://www.lbmc.com/blog/pci-compliance-fees-fines-penalties/
- https://compliancy-group.com/hipaa-fines-directory-year/
- https://www.shredit.com/en-us/blog/compliance/the-gramm-leach-bliley-act
- https://digitalguardian.com/blog/what-glba-compliance-understanding-data-protection-requirements-gramm-leach-bliley-act

About Ecuron

Ecuron is a boutique cybersecurity consulting company that specializes in preparing companies to face cyber threats. Our mission is to create a partnership with you, securing your data and protecting your organization every step of the way. For help developing and implementing an information- and cybersecurity strategy for your organization and for more information visit https://www.ecuron.com .