EasyChair Preprint

№ 9805

Learnings and Best Practices for Information Security Management Due to Covid-19 Induced Workplace Transitions (nWFH)

Guruprasad B Jayarao

September 4, 2023

Learnings and Best Practices for Information Security Management Due to Covid-19 Induced Workplace transitions (nWFH)

Guruprasad B Jayarao (EFPM-2018)

Department of Information Systems, Indian Institute of Management Indore

Abstract:

The global COVID-19 epidemic in 2020 has impacted all aspects of life and business, necessitating the adoption of new organisational working models, which was enforced on employees. As a result, the majority of the employees has been mandated to adopt new-work-from-home nWFH (PatriciaAkello, 2021),as soon as possible and where nWFH was feasible. The nWFH differs in various dimensions as compared to earlier WFH which was based on need basis and prior application by employees and approval by their managers and was controlled.Threats to information systems (IS Threats) have also risen in locksteps with this trend (Carlsten, 2021),Organizations were not ready to deal with dangers as a result of this unexpected and sudden transition from office to work from home. While investigating on the readiness of organizations, information security (infosec) managers voiced their concerns and indicated that best practices are their saviours. This study captures the VOISM (voice of infosec managers) on the best practices they have identified and improved upon during the pandemic situation.

Working from home is not a novel concept, it existed before the Covid-19 pandemic as well (Furnell, 2020) , (Grimm, 2021), (Baruch, 2000),WFH dates back to pre-industrial times. Earlier Only a few employees used the WFH before the Covid-19 outbreak (Milasi, 2021). In the current situation "nWFH is defined as the new normal and is here to continue,".

Keywords: nWFH, security best practices, Flexible work arrangements, FWA, pandemic & Information security threats, organizational readiness remote work, risk management, Qualitative research, Exploratory method

Introduction

As a cascaded effect of the improvements in digital technology which has enabled employees to connect from anywhere to perform tasks, has also brought in both advantages and challenges to businesses in the security context. According to the practitioners, the main difference between earlier WFH and now, is not more WFH workers, but "more access to critical applications and data", which all employees need to use from home. In comparison to prior WFH where, the vulnerabilities were minimised in terms of both employee numbers and attack surface (IT infrastructure like lap tops, desktops, home Wi-Fi, routers etc). Due to incremental attack surfaces and millions of devices connected via their own wifi/home network during the pandemic, has further caused some of the existing threats to increase by leaps like ransomware, DDOS, insider threats, BYOD related threats, home wifi issues, phishing etc. We provide the VOISM on the best practices which they believe in, if adopted, can lead to "security by habit" and not a "burdened practice".

Identified threat types and vulnerable attack surfaces:

The first step was to identify the threat types and the attack surfaces. The following table summarizes the threats types and attack surfaces which were showing increasing trends during the pandemic scenario when people worked from home. Sources of this data are from the discussions with security practitioners.

Threat Types	Vulnerable Attack Surfaces	How hackers use vulnerabilities
Ransomware	Unmanaged Endpoints – laptops, desktops, mobile devices, USB ports, USB devices	Ransomware is a kind of software that encrypts data on a computer. Through the use of encryption, cybercriminals force enterprises to pay a ransom to recover access to their information. Some variations include extra features like data theft to entice ransomware impacted organizations to pay
DDOS	Networks, wifi, Home networks	A distributed denial of service (DDoS) assault floods a targeted server or network with traffic in an effort to interrupt and overload a service, leaving it unworkable.
Insider Threats	Organization's database	An insider threat is a firm security risk. Unauthorized access to sensitive data or privileged

		accounts on an organization's network.
BYOD	Any personal devices, mobiles, laptops, external hard disks, unprotected devices, public wifi routers 4G,5G cellular devices, VPN, privately purchased hardwares	Attackers may hack a device held by an employee through phishing or malware. At this time, attackers have three options: Take data from the device's memory. Access the corporate network using the device's credentials.
Threat Types	Vulnerable Attack Surfaces	How hackers use vulnerabilities
Phishing	Emails, text messages, impersonating with Covid 19 related topics to lure the users, Social engineering attack vectors	Phishing is a cybercrime method where targets are approached by email, phone, or text message by a criminal acting as a genuine entity. It's still one of the critical social engineering assault vectors. Some phishing attempts are so complex that they seem totally benign. Can bypass the traditional security - email gateways etc

Research Methodology:

This study constitutes a subset of the main intended study on “exploring Organisational readiness to assess the risks of information security threats in nWFH scenario”. Recker (Recker, 2012) proposes a qualitative research strategy and methodologies to aid researchers in comprehending phenomena in context. We have used the Qualitative research method for this study to explore the readiness of organizations and during this study, we heard the voice of information security managers on the “best practices” as a path towards the overall readiness,” Silverman (Silverman, 2020) asserts that the intention of qualitative research is to know by experience of people”, hence we adopted the qualitative method by interviewing the managers in security to gain direct knowledge. With the limited literature on ORE in the present context of work from home and security threats, we intend to explore the context based on the semi-structured interviews of Infosec managers, chief information security officers -CISOs. The study is done in India and the participants are from small and medium organizations to understand their experiences. In this article, we are presenting the interim knowledge gained on the best practices from practitioners.

Participants Selection:

We used purposive method (Recker, 2012) of sampling based on industry knowledge of the author and network of security experts were identified for responding to our interviews. Accordingly, the author interviewed the security managers,practioners with overall experience ranging from 5 years to 25 years for a better coverage and gain rich knowledge.

Participants Table:

Participants	Type of Organization	Role	Overall Security Experience
P1	Reputed security products company & a subject matter expert	Engineering manager Engineering and SME on security	25+ years
P2	Security applications development organization	Sr Development manager	20+ years
P3	Solutions in video and security provider and video technologies	Head IT consultant - Security	5+ years
P4	Security Products development company	Product Manager	20+ years
P5	Mobile apps Development Organization	Vice president of Engineering	23+ years
P6	Start-up organization with 9 years presence	VP of Engineering	20+ years
P7	Software vendors in software as a service and web tech	IT Security Manager and auditor	18+ years

Interviews Summary:

Based on the threat types identified, we discussed with the participants on their best practices to minimize the vulnerabilities and threats. While the open ended questions to practioners were developed and discussed in the interviews, two main themes emerged – Technical practices and Managerial/ organizational practices, hence we are considering these two to classify the practices. To start with we asked the participants to order **Technology, Environment and Organization** in the order of priority. Majority of the participants opted to put Organization/managerial practices on top priority as compared to Technical practices and Environment, as per one of the participants P6

"So, so probably the organization comes first, org is the key enabler to decide what is information security how do they want to follow it, what are the practices they have in place so that definitions and all have to be driven from organization".

Hence we continued to prioritise Organization to understand the practices.

One of the participants P1 says as follows, which reflects on organization's policy

"Some companies, I mean it, but I think some companies have gone to the extent of even ensuring that they give a box to the employee with a good connection, and then they've configured it for them in a way when at home".

"So I'm actually saying, there are some companies, are, really following a method where they kind of give a secure wifi connection, and configured it in a way where they can monitor".

This can be affordable by bigger organizations but for smaller ones it's still a struggle, but as compared to a compromised device ,it's better to have such best practices.

Organization's Monitoring policy

Participant P1's response:

"*All your monitoring thing has been reduced. Now you cannot really monitor everything. What happens on my laptop when I'm working from home, these are the problems"*
"Monitoring is really important. Training all employees is very important and monitoring provides information on an insider to do something malicious is really important. If there's a chance of an insider causing a problem, it is most of the attacks happening from an insider, finding that bad element by monitoring is important and is a CISO's nightmare."

"In the office it was a controlled environment but now at home it's tougher"

Monitoring over a VPN and beyond enterprise firewalls is a challenge to this policy but as a best practice organizations should take a tough stand to add this monitoring policy and use relevant technologies for preventing any security incidents.

Training and security awareness policy

Organizational policies should include training and awareness as a continual process and monitor its employees for completion of mandatory trainings and compliance and it's a kind of enforcement there is no other way to bring secure work culture!

As per participant P6 :

"Yeah. so the only thing that this situation has brought in, is some of the training and awareness nuances has to be formalized into work culture, because going forward you will face your challenges, similar challenges and the model of work is going to turn into hybrid model so this is not like task phase that you have just crossed it and everything will be back to old status , no this is the new normal now."

This thought emphasizes the need for training & awareness policy to be of high importance.

We can have organizational policies to include such important policies but in practice we see employees tend to deviate the policies and it's a very difficult question to answer, as participant P6 says so : "***So the reason is that from a pure employee perspective most of them do or do not***

realize the repercussions of loss of data and loss of reputation. They are not too aware of the impacts of what happens , they feel that doing these things is burdening. In addition, when they are actually on official work that they are assigned to do , they are bound to cut corners."

Also same thoughts are from participant P5

"Extra burden on them. They think it infringes on their freedom."

So what practices can help here? As participant P5 reinforces the use a visible tool, can help here

"We have an internal wiki detailing Security Best Practices across different niches and domains (mobility, web application development). We keep this wiki updated. We also mandate employee training through LinkedIn learning courses".

While wiki come from old school, but still its use as a mandatory practice of having wiki documented in organizational policy seems to be relevant in this situation too.

Other practices at organizational level can include as participant P5 asserts in strong voice

"Policies , procedures , manuals , therapeutics like security titbits popping up on people's lap top , reminding them always helps in reinforcing .. security tips delivered through the screen savers etc matters a lot in as organizational practice and form security circles to implement at ground level in the organizations and a highly placed peer reporting to avoid insider threats should get us better in readying the organization and adoption as a best practice ….."

These statements and novel thoughts of moving towards building security culture in organization from ground up, can help in employees owing the security and develops "security by habit".

Zero trust management as organization's policy:

Trust no one or no device policy at organizational level seems to be the echo and voice of most of the participants.

As participant P5 puts with clear voice

"Laptop, VPN most important no BYOD , adopt zero trust …"

As per participant P6
Zero trust ?that makes sense, from a long run perspective it's a good answer but however to get it in practicality for every organization is next to impossible depends on how big an organization or what is the kind of work they do I guess when its UI kind of work etc ,so is it worthwhile? what is the ROI to do all of these?.."

Though the participants believed zero trust management as a policy can help, it brings out a very important point on "budget constraints" and return on investments(ROI).

Adequate security budget as organizational policy:

The security budget should be adequate enough to accommodate the costs of technology products which are of utmost relevance, not all technologies need to be procured!

P5 puts it like this
"Employee Training, Building internal security tool sets (if budget permits) - which our organization does."
While allocating adequate budget is important as a policy, but as P5 puts it, its equally important to building internal tool sets ,building them inhouse can be an organizational best practice call to employees, which can spring up innovation from employees to build their own tools instead of buying costly tools. Also this is a very important managerial aspect of digging into their teams to unearth the hidden technical talent, which can help in developing inhouse tools for security.

Onboarding third party contractors: Security binding organizational policy

On this question what's the best practice which can help prevent third party contractors or suppliers from breaching security?

P6 says

"Now the line is getting blurred ,because a contractor or internal employee is legally bound by the contract, but he is no, it's no different from an internal employee or contractor ."

P1 says

"A lot of companies, what the clients(contractors), they do work for , We have some things in place. Best practice in place, the thing is, you have a good organizational environment that people are like outsourcing companies like, xxxx, and yyyyy. They create a separate office for a particular client. People come to office work and then go. Some of them even have a requirement that they leave mobile phones outside ,it's possible in big companies and not for small companies."
To conclude on the third party contractors to be bound by the organizational policy which lays down the steps the contractors to strictly adhere to and monitored by competent authority pays back to the organization, if not for creating separate offices for contractors for working or remote working.

At this point we reached a saturation on the responses for managerial/organizational practices hence we concluded.

Technical Best Practices:
The responses to technical best practices were very encouraging and all the participants were eager to answer.

Password rotation as a best practice:

Participant P6 asserts..
"Forced password rotation , sometimes whatever that minimal password length all those kinds of password rotation , password strength you will have to enforce, there are things certainly it is not possible but to that extent possible, we should try to see what is the login logout time and what are being accessed, which will hold good even when you are at office but more so when its home , in office at least you had option of doing some firewalls via proxies for access we could prevent from certain sites to be accessed, but protect the systems within your organization because it can contain malware, phishing all of those, when people working from home all these firewall kind of endpoint security is left up to them which is difficult to enforce with this being the criterion its lot more challenging and lot more.. more potential of having security issues .."
"Yeah.it can be as simple as changing your password every month , nothing has happened in the last three years why should I change?"

While strict policy of password rotation should be enforced, the above statements brings out employee attitude towards the adherence to technical practices which has to be dealt with some form of deterrence policy, hence here we see a mix of both organizational, technical practices converge here and should be built into the work culture.

Technology driving the environments at home as a best practice:

"The Technical environment I am assuming is more on software aspects some of the things holds good when you are in office or home depends on environment you are , while on one side of the it's more like a work life balance people at least tend to have a differentiation between office and home , now that has got blurred in the big picture , what you say office environment or home environment that has got blurred or merged now so that has also happened somewhere like a mixed bag some of it were not expected some were good and some were not.."

Technology in this context means the softwares to be used when people work from home.The restrictions administered through endpoint management - to use only approved softwares on the laptops is one of major voices we heard. Even if you allow personal devices, provide the OS and image, which can be downloaded through your own private cloud. This can be the take away for small and medium organizations.

IP address, authentication ,Identity and Access management(IAM) as best practice:

"No not more access privileges you just.. your authentication has to be more expanded and more robust like if you are working from office you can say access to AWS server can be only from this IP ,now we have to give individual access to all the people who need access to servers , one might be their wifi if it's not a static IP it keeps changing , you might have to keep changing IPs for giving access so that has brought in little more effort on the management side because at the end of the day people still need access."

We have added the IP address management to the whitelisting best practice. 2 FA two factor authentication and multi factor authentication are preferred. While weighing the cost factor 2FA

is not costly whereas MFA can be costly , hence weighing based on the ROI is important small and medium organizations. usage of IAM – identity and access management can be inhouse of through AWS amazon web services or GCP – Google cloud platform.

Individual device management as a best practice:

Lock your systems if you are not working on them.

"No be it laptop or mobile phones all the same , that means more or less the similar, whether they work from office or not , and from software aspect is, everybody is a professional whose working for the company so ideally they say or it is said that if you not are in front of the system you lock it and go about doing your other work, in home you tend to be in a different kind of environment, so you may or may not lock your computer which will also mean that its a potential hazard and there will be others at home going and coming who are ideally not bound by the NDA or the confidential contracts of the organization.."

Managed Endpoints & Encryption as a best practice:

"For example, we made sure that people take the laptop outside and all that, and if the laptop gets stolen. We did the endpoint security encryption, endpoint was encrypted, the laptop was encrypted."
"You use more stronger encryption method at home and that can be done is what we are following."

Endpoint encryption is a best practice, some organizations follow this but for small and medium organizations need to balance the costs.

Managed endpoints and usage of endpoint management software

Oh managed endpoint? Yes that helps to the limitation of what it used to be in office, the same thing it does here in the new condition. It does help to some extent, Iam sure there are challenges and then just managing it over a VPN connection for everybody, products like ePO e-policy orchestrator will help for sure , but using this kind of products over VPN has to be explore or might have been solved by now."
"Now there are EDR(endpoint detection and response) solutions right? Others are there, but I think for those, people have to install EDR solutions ,which is an integrated solution that has both data collection in real time and continuous monitoring." "Might be costlier for small organizations."

Participant P7 also talks on the same practice

"Being a product manager I follow and promote best practices like ,VPN,2FA,encryption and EDR solutions from Technology standpoint"

There are a number of tools which can help, but as said earlier the best practice is to develop internal tool sets which can overcome any budget constraints.

Software OS updates, security patches updates as best practice:

What bubbles up as a common security issue?

Participant P2 had responded as

"Not having good antivirus installed on business endpoints, not updating authorized OS patches, antivirus updates regularly, absence of multi-factor authentication, improper authorization implementation, not being aware of the usage context - personal/business."

Strong enforcement through the endpoint management softwares to do routine health check if the OS patches ,security patches ,antivirus updates are done and force the updates is a deemed technical best practice.

Routine Security Audits as a best practice:
Participant P2 :

"Continuous security audits, compliance audits(implementation, training), Proper security process, implementation of standard security tools, strict compliance enforcement, continuous security patch updates, employee training, constant awareness of new breach vectors."
"Today, compliance is a standard procedure and can be outsourced. However if costs are a factor then one has to trust employee actions and remind regularly."

The health check of all the endpoints are a must and this a healthy practice.

IP-whitelisting as a best practice :

Participant P6 says ***,"We can avoid security issues if the employees devices with proper authentication and authorizations policies are in place and there is proper white-listing mechanism for consulting organizations***."
While the best practice of IP white-listing for contractors is considered ,organizations also can review if it can be applied for their employees?

Providing Laptops with organization's configured image as a best practice:

As Participant P4 says – "***All the laptops are VPN configured and secured organizational image is on all the devices and the employee will have no freedom or options to invite a threat."***
This also applies to contractors as per participant P4
"all the contractor laptops and systems are secured as per the IS policies and standards with secured image and VPN configuration."

Monitor, Monitor , Monitor as a best practice
Participant P7 says

"I believe in monitor , monitor and monitor!"

P3 echos the same ***"Monitoring antivirus console on regular basis, Monitoring DLP breaches, is very critical apart from other monitoring for compliance".***

To conclude monitoring is very critical regardless of employees work location, more so when then work from remote. This needs support from top management on allocating budget required for such tools or for inhouse development is again reiterated here.

We reached a saturation on participant's responses at this point and hence we concluded.

Conclusion:

A number of best practices from two categories - Technical and Managerial/Organizational emerged from a rich and elaborate discourse during the semi structured interviews. We have covered small and medium organizations as the participants, as they may have resource constraints both on people and they operate on shoe string budgets and this has been proved from the discussions that small and medium organizations "of course are resource constrained". We also want to emphasize here that some of the practices may have been already been followed, but based on the rich insights gathered from this study, we hope this helps the other small and medium organizations to become cognizant of the best practices and they can choose from this study to become more secured organization and develop security culture in a long run.

Key References:

1. Baruch, Y. (2000). Teleworking: benefits and pitfalls as perceived by professionals and man- agers, New Technology, Work and Employment, vol. 15, no. 1, pp. 34-49 https://onlinelibrary.wiley.com/doi/epdf/10.1111/1468-005X.00063
2. Babbs, A. (2020). How to leverage data security in a post-Covid world, Computer Fraud & Security,vol.2020,no.10,pp.811,https://www.sciencedirect.com/science/article/pii/S136137232030107X
3. Borkovich, D.J., & Skovira, R.J. (2020). Working from Home: Cybersecurity in the age of COVID-19, Issues in Information Systems, vol. 21, no. 4, pp. 234-246, Available online: https://iacis.org/iis/2020/4_iis_2020_234-246.pdf
4. Carlsten, F., Hultman, E. and Nilsson, D. E, Work from Home – Information Security Threats and Best Practices, A qualitative study in the era of COVID-19 ,Master Thesis
5. Clarke, N.L., Furnell, S.M., & Talib, S. (2010). An Analysis of Information Security Aware- ness within Home and Work Environments, 2010 International Conference on Avail- ability, Reliability and Security, Paper 26, https://ieeex- plore.ieee.org/document/5438096
6. Furnell, S., & Shah, N.S. (2020). Home working and cyber security – an outbreak of unpre- paredness?, Computer Fraud & Security, vol. 2020, no. 8, pp. 6-12, http://www.sciencedirect.com/science/article/pii/S1361372320300841
7. Grimm, J. (2021). Securing the remote workforce in the new normal, Computer Fraud & Security, vol. 2021, no. 2, pp. 8-11,
8. Milasi, S., González-Vázquez, I. & Fernández-Macías, E. (2021). Telework before the COVID-19 pandemic: Trends and drivers of differences across the EU, https://www.oecd-ilibrary.org/economics/telework-before-the-covid-19-pan- demic_d5e42dd1-en
9. Patricia Akello , Kim-Kwang Raymond Choo (2021), Nicole Lang Beebe. Volitional Non-Malicious Insider Threats : At the Intersection of COVID-19,WFH, and Cloud -Facilitated Shadow-Apps AISeL 2021 Proceedings
10. Recker, J. (2012). Scientific research in information systems: a beginner's guide, Heidelberg, New York, Dordrecht, London: Springer Science & Business Media
11. Silverman, D. (2020). Qualitative research, 5th edn, Los Angeles: Sage Publications