IIMC Library Clipping Service Source: News: Online: Forbes India Dated: 19-09-2021

It's time for cyber-insurance to become personal in the WFH age.

According to a recent report by Hewlett Packard, there has been a stupendous 238 percent increase in global cyberattack volume during the pandemic.

BY IIM CALCUTTA

According to a recent report by Hewlett Packard, there has been a stupendous 238 percent increase in global cyberattack volume during the pandemic.

As economic activities around the globe become pervasively digital, the ever-increasing cyber threat is outpacing most companies' ability to manage it effectively. Sensitive business information, such as employee personal information, client and corporate data, and intellectual property all are at an increasing risk of getting hacked. Along with them, other key elements of corporate infrastructure are also under growing threat from ransomware risks.

Commercial cyber-risk management activities such as ID theft resolution and credit monitoring have become ubiquitous all over the globe thanks to countless data breaches since the mid-2000s, and are exploding in the era of smartphone communication. Fast forward to the post 2020 era, phishing scams are running rampant amid Covid-19 which has blurred the distinction between workplace and home.

_RSS_According to a recent report by Hewlett Packard, there has been a stupendous 238 percent increase in global cyberattack volume during the pandemic. As a result, individuals are waking up to annoying (e.g., loss of private data and digital mementos from the phone) and often serious (e.g., loss of workplace data from the cloud) cyber-risks, and preparing to take control.

Many believe they are more productive when working from home compared to a traditional office setting thanks to flexible time-management and time saving benefits. However, quite a few of them—approximately 25 percent believe they are less productive while working from home, according to KuppingerCole. This is because in many parts of the world, even in developed countries, high-spec hardware like laptop and tablets, and software like video-conferencing tools and Database Management Systems require highly reliable and secure internet connection and a secure access to the corporate network via VPN, all of which are not guaranteed if one is working from home. While the governments in collaboration with network providers have been handling the issue of expanding fibre capacity given the critical importance of cyber-security in this new WFH setting, employers are steadily putting in place a whole range of efficient cyber-security measures for this 'new' work environment.

Ensuring efficiency is, however, just one factor involved in IT security measures applied to staff working from home. Another salient factor is the need to prevent cyberattacks, and step number one en route that goal is to know how WFH employees perceive their corporate cybersecurity posture. According to a survey, approximately 14 percent of WFH non-security experts are concerned about cyber-security when working from home. Furthermore, 25 percent of the non-security experts report an increase in fraudulent emails, phishing attempts and spam to their corporate email since the start of the COVID-19 crisis—this excludes cyber-attacks that have gone unrecognised.

Hence, the underlying message here is that there is anecdotal evidence from businesses that the Covid-19 pandemic has triggered a change of tactics used by cyber criminals who are now attempting to exploit weaknesses of remote IT security. So the major question here then becomes: What are these WFH-specific cyber-security weaknesses that have cyber-criminals drooling to compromise corporates?

MAJOR CYBER-THREAT FACTORS IN THE AGE OF WFH

Most employees in the WFH mode agree that they access more company data, and at a higher frequency, than they did pre-pandemic. The most common types of data accessed, according to KuppingerCole, is customer and operational data—43% each—and financial and HR records—23% each.

A significantly important new dimension specific to WFH is that office workers are increasingly using their work devices for personal tasks today. Based on surveys by leading IT and cyber-consulting firms including HP and Deloitte, approximately 33 percent WFH employees download more from the internet, compared to the pre-pandemic phase, and this statistic rises to 60 percent for those aged 18-24. Around 27 percent WFH employees surveyed used their work device to play online games when compared to the times pre-pandemic—a statistic that sharply rises to 43 percent for parents of children aged 5-16, who were spending more time with their children.

Close to 36 percent surveyed WFH employees use their work device to watch online streaming services—a figure that steeply rises to 60 percent among those aged 18-24. Around four in ten office workers used their work device for homework and online learning purposes. This statistic rises to 57 percent for parents of children aged 5-16. In the age of WFH, cyber-hackers are taking advantage of these shifting patterns of device-task mapping to tailor their phishing campaigns.

Globally, there was approximately a 54 percent increase in malicious actors who exploited gaming platforms between January and June of 2020, and directed users to phishing pages. In strong correlation to this statistic, during this same period, (i) there was an increase in gaming-themed malware such as Ryuk ransomware and samples of stealthy JavaScript downloader malware, Gootloader, masquerading as Fortnite hacks, and (ii) at least 700 fraudulent websites were found to be impersonating popular streaming services in just one seven-day period in April 2020.

In addition to the overlapping of work and personal activities on business devices, WFH office workers are also using potentially insecure personal devices (not protected anymore by corporate firewalls) to connect to their corporate environment. 88 percent divisional managers of IT departments are worried cyber-breach risk has risen only because employees are using personal devices for work. In addition, approximately half of these managers have enough evidence that compromised personal devices (about 1.5 attacks per minute) are being used to access business data during the ongoing pandemic.

According to a YouGov survey, for the year 2020, approximately 69 percent of office employees have used personal laptops, printers, and so on, to execute corporate tasks more often since the pandemic began. This statistic is further distributed among activities such as using personal PC/laptop for office work (approximately 37 percent), using personal

PC/laptop to access organisational network and servers (about 32 percent), using personal scanner and printers to share work-related documents with other colleagues (about 34 percent), and using home printers to save files, through VPN, on the office network (about 20 percent).

Such activities amplify the already existing cyber-risk posture for firms with respect to client/business data privacy, repetitional damage, non-compliance, and loss of customer trust. Hence, in the WFH age, having strong endpoint security has become equally important to corporate businesses as having strong network security.

Even on a psychological level, behavioral research has found that approximately 10 percent WFH employees reported feeling tired or having little energy or motivation (e.g., missing social interactions with colleagues, distraction by family at home) while working from home, according to Society of Human Resource Management. This is a significant worry factor for corporations simply because tired or unmotivated employees are prone to making careless errors, and such errors could easily trickle into the organisation security space, jeopardising the latter with an increased risk of sensitive information or network compromise.

As an example, while working on a sensitive business file (or while configuring DBMS settings) you suddenly realise that you have laundry to pick up and, in a hurry, misplace the confidential document (or misconfigure the DBMS) in the wrong place. To put the importance of human behavior into perspective, a HP Wolf Security report states that in the year 2020, around 82 percent of office employees did WFH and 39 percent of them wish to WFH post the pandemic. Hence, it is not difficult to infer that cyber-risk in the age of WFH is going to significantly increase, than it was in the pre-pandemic era.

company data, and at a higher frequency, than they did pre-pandemic. The most common types of data accessed, according to KuppingerCole, is customer and operational data—43% each—and financial and HR records—23% each.

A significantly important new dimension specific to WFH is that office workers are increasingly using their work devices for personal tasks today. Based on surveys by leading IT and cyber-consulting firms including HP and Deloitte, approximately 33 percent WFH employees download more from the internet, compared to the pre-pandemic phase, and this statistic rises to 60 percent for those aged 18-24. Around 27 percent WFH employees surveyed used their work device to play online games when compared to the times pre-pandemic—a statistic that sharply rises to 43 percent for parents of children aged 5-16, who were spending more time with their children.

Close to 36 percent surveyed WFH employees use their work device to watch online streaming services—a figure that steeply rises to 60 percent among those aged 18-24. Around four in ten office workers used their work device for homework and online learning purposes. This statistic rises to 57 percent for parents of children aged 5-16. In the age of WFH, cyber-hackers are taking advantage of these shifting patterns of device-task mapping to tailor their phishing campaigns.

Globally, there was approximately a 54 percent increase in malicious actors who exploited gaming platforms between January and June of 2020, and directed users to phishing pages. In strong correlation to this statistic, during this same period, (i) there was an increase in gaming-themed malware such as Ryuk ransomware and samples of stealthy JavaScript downloader malware, Gootloader, masquerading as Fortnite hacks, and (ii) at least 700 fraudulent websites were found to be impersonating popular streaming services in just one seven-day period in April 2020.

In addition to the overlapping of work and personal activities on business devices, WFH office workers are also using potentially insecure personal devices (not protected anymore by corporate firewalls) to connect to their corporate environment. 88 percent divisional managers of IT departments are worried cyber-breach risk has risen only because employees are using personal devices for work. In addition, approximately half of these managers have enough evidence that compromised personal devices (about 1.5 attacks per minute) are being used to access business data during the ongoing pandemic.

According to a YouGov survey, for the year 2020, approximately 69 percent of office employees have used personal laptops, printers, and so on, to execute corporate tasks more often since the pandemic began. This statistic is further distributed among activities such as using personal PC/laptop for office work (approximately 37 percent), using personal PC/laptop to access organisational network and servers (about 32 percent), using personal scanner and printers to share work-related documents with other colleagues (about 34 percent), and using home printers to save files, through VPN, on the office network (about 20 percent).

Such activities amplify the already existing cyber-risk posture for firms with respect to client/business data privacy, repetitional damage, non-compliance, and loss of customer trust. Hence, in the WFH age, having strong endpoint security

has become equally important to corporate businesses as having strong network security.

Even on a psychological level, behavioral research has found that approximately 10 percent WFH employees reported feeling tired or having little energy or motivation (e.g., missing social interactions with colleagues, distraction by family at home) while working from home, according to Society of Human Resource Management. This is a significant worry factor for corporations simply because tired or unmotivated employees are prone to making careless errors, and such errors could easily trickle into the organisation security space, jeopardising the latter with an increased risk of sensitive information or network compromise.

As an example, while working on a sensitive business file (or while configuring DBMS settings) you suddenly realise that you have laundry to pick up and, in a hurry, misplace the confidential document (or misconfigure the DBMS) in the wrong place. To put the importance of human behavior into perspective, a HP Wolf Security report states that in the year 2020, around 82 percent of office employees did WFH and 39 percent of them wish to WFH post the pandemic. Hence, it is not difficult to infer that cyber-risk in the age of WFH is going to significantly increase, than it was in the pre-pandemic era.

NEED OF PERSONAL INSURANCE TO IMPROVE CYBER SECURITY IN THE WFH AGE

It is quite obvious from the arguments made above that in the WFH age, the cyber-risk to corporations is only going to increase, primarily due to an increase in the cyber-vulnerability terrain contributed by WFH humans. Given the nature of the cyber-risks involved, it is safe to say that state-of-the-art security technology (e.g., anti-virus, firewalls, software security patches) will not result in the removal of this 'additional' cyber-risk. Though this point has repeatedly been made and rationalised in the last two decades by cyber-security experts, its relevance till today is mostly concentrated on mitigating residual cyber-risk in industrial and organisational settings.

However, with the advent of the WFH age, residual cyber-risk elimination/mitigation via third-party commercial products such as cyber-insurance need to penetrate and populate the 'personal user' space, instead of solely focusing on the corporate space, as is in current practice (a multi-billion dollar yearly business). This need is more felt in nations which have seen a big surge in cyber-attacks in the last five years, such as India (seen approximately a 457 percent increase in cyber breaches, according to VeriRisk).

To further drive home our point, according to ICICI Lombard General Insurance, Chinese hackers attempted approximately 40,000 cyber attacks (e.g., DoS, phishing) on WFH users in India in only the third week of June of 2020.

However, as per T.A. Ramalingam, CTO, Bajaj Allianz General Insurance, the individual cyber-insurance policy market is still at a much nascent stage in India, when compared to the corporate cyber-insurance policy market. As a result, the former market needs to grow rapidly fast in the WFH age, and work hand in hand with the corporate cyber insurance market, if India needs to effectively manage organisational (and personal) cyber risk going forward.

The working principle of cyber insurance solutions and impact on security

A victim (be it personal or an organisation) of a cyberattack can file a claim with their insurance policy provider to help pay for expenses (e.g., legal fees or document recovery), first-party costs (e.g., cyber extortion, cyber forensics, credit monitoring, civil fines and penalties, and privacy notification), as well as third party liability (e.g., electronic media liability, network security and privacy liability). The policy will have a coverage limit and a deductible, and could be sold as an add-on to homeowner's insurance.

The for-business cyber (re-)insurance solutions today diversify their clients into cyber risk categories (e.g., high, medium, low), and subsequently decide on the appropriate coverage, premium pricing, and deductible amounts. The same working principle carries over to personal cyber-insurance solutions also, except that such solutions will hold the WFH user directly liable for cyber-breaches on personal devices (used for work purposes), or work devices (used for family/leisure activities), without the business insurance firm of the organisation being held liable.

Apart from providing loss coverage as its salient functionality, cyber-insurance carries with it the promise of improving cybersecurity, known through principle, as well as mathematically verified through multiple research efforts by the information technology community (Pal et.al in IEEE INFOCOM 2014, Lelarge et.al., in IEEE INFOCOM 2008, and Shetty et.al., in WEIS 2010) since the early 2000s. This argument holds and is quite relevant in the personal insurance solutions

space simply because the premiums to be paid by the user is a function of his/her cyber risk posture, and hence cyber-insurance solutions align the incentives of the buyer with taking extra cyber-care of itself.

The range of insurables and personal insurance services in the WFH age

The personal cyber-insurance business could cover the following (but not limited to) cyber-crimes very relevant to the WFH age: (1) insuring against virus/malware compromised PCs, laptops, tablets, smartphones, IoT home devices, WiFi access points, and routers; (2) insurance against ransomware attacks that block an employee from accessing office data on his/her devices (however, one must be careful of paying back the ransomware launcher and should only do it with the consent of his/her personal insurance provider as it does not guarantee release of a decryption key or an additional ransom not being asked for after the first payment); (3) insurance against online harassment that blackmails an office employee with the fear of wrongful job termination; (4) insurance against data breaches; and (5) insurance against identity theft that may influence financial losses through unauthorised credit card transactions.

Apart from providing insurance to its customers, a personal cyber-insurance can also provide the following services: (1) providing WFH employees access to cyber-fraud specialists to assist in a fraud recovery and resolution process; (2) providing (consented) real-time cyber-monitoring of specific networks or devices in the WFH environment; (3) providing lawsuit filing recommendations for online libel or privacy breaches; and (4) replacing/retrieving/re-creating damaged/lost personal and financial data records.

To summarise, personal cyber-insurance is much needed in the WFH age, more so in nations with high cyber-vulnerability, or with growing economies increasingly under the radar of cyber-criminals (e.g., India). Personal cyber has grown very fast in certain western economies in the last 18 months, and one expects that by 2022, much of the cyber-insurance market around the globe may be engaging in selling personal cyber policies for WFH employees.

Source: https://www.forbesindia.com/article/iim-calcutta/its-time-for-cyberinsurance-to-become-personal-in-the-wfh-age/70679/1