COVID-19 working from home increases cyber risk

Tips for mitigation

By Mercer's Karen Shellenback

Corporate response to the pandemic was swift in the last four weeks. Work from home (WFH) for large swaths of the knowledge worker population has been implemented on a scale not seen in the post-industrial age. Mercer research suggests that 67% of companies have already decreed mandatory WFH policies either company-wide or in locations or departments most affected by COVID-19 infections. (Mercer COVID–19 survey live results)

However, there is danger, every home device or wireless connection is a potential cyber risk entry point for malicious actors. Unsecured networked systems and devices open the opportunity for cyber criminals to access a distributed network of confidential internal and client information. Over 8.5 billion records were compromised in 2019 — that is a 200 percent increase from the number of records lost in 2018 and inadvertent insiders are largely responsible for this significant rise. (Source: IBM X-Force Incident Response and Intelligence Services (IRIS) 2020).

A Carnegie Mellon study found that many companies report that incidents caused by insider attacks were more costly or damaging than outsider attacks.

Fundamentally, cyber security is a people issue and there are strong correlations that cyber breach incidence is dependent on internal employee awareness, corporate preparedness, and worker sentiment. Sometimes, it is the people you trust the most — your insiders — that can inflict the most damage. The rapid response required of businesses to distribute their all workers in less than a week has opened potential holes in the firewall for many organizations. Research shows that remote access is often used to carry out the attacks. Are you prepared for increased insider threats? There are three types of critical insiders that may put your organization at risk: accidental, renegade, and malicious.

1

Accidental insiders can be hapless, negligent, overworked or unaware of how they risking the security of the organization. These individuals often do not know or do not regularly follow established security protocols, which often lead to misplaced or improper handling of personally identifiable information (PII) or other sensitive data.

Malicious actors target this group using phishing, spoofing, and other scams to manipulate individuals to do something that the employee thinks is legitimate but in reality is a pernicious threat. Such insiders often have no idea that what they are doing is detrimental to the organization, are not paying close attention, and inadvertently cause damage. The most common vectors malicious actors exploit in general, and especially during the pandemic, include:

- Tech-based culture of open sharing — uploading sensitive information to social media, email, storage or development sites
- Phishing and spoofing
- Access codes/passwords stored on devices on unsecured Wi-Fi or home networks
- PII stored on employee devices, sent to personal devices
- Employees merging personal and business on one system

Over 8.5 billion records were compromised in 2019, a number that's more than 200 percent greater than the number of records lost in 2018. The inadvertent insider can largely be held responsible for this significant rise.

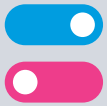
Source: IBM X-Force Incident Response and Intelligence Services (IRIS) 2020

How to fry a PHISH. Look for these clues ....

Generic greeting. Internet criminals use generic names like "First Bank Customer" or "Dear (Microsoft, Apple, Amazon, etc.) Customer" because it is just not profitable to type all the recipients' names out and send emails individually. If employees do not see their own name, they should be suspicious.

Generic subject line. Internet criminals also use generic subject lines such as "COVID-19: Critical message from the Governor's office" or "Coronavirus Map". Be suspicious of urgent coronavirus news or emergency notifications through email.

Hey friend. Emails that appear to be from a known colleague or friend may be "spoofed". While their name and even the email address may look legitimate, the message often says something such as "I though you would like this site" with a link. Never open these messages.



Forged link. Even if a link has a name in it that the user recognizes, it does not mean it actually links to the real organization. Users should hover over the link with their cursor to see if it matches what appears in the email. The address should be a standard corporate address. Do not click links that show a discrepancy, like extra random letters and numbers in the email address or what looks to be an offshoot address. You can check by going to the real company website via a new search in your browser.

The missing 's' for secure. Website addresses that do not display the 's' in the expression "https" are not secure and it is unsafe to enter personal information. Unfortunately, the presence of the 's' or the lock-box icon does not guarantee security, as scammers are able to replicate these safety indicators.

Requests for personal information. The point of sending phishing email is to trick users into providing personal information, and an email that requests is probably a phishing attempt.

Sense of urgency. Cyber criminals want users to provide personal information immediately, and to achieve that result, they make users think something has happened that requires fast action. The faster criminals obtain the information, the faster they can move on to another victim.

Nonstandard English. Sentence format that is other than formal standard written English. Misspellings, bizarre capitalization, usage or punctuations are giveaways of a fraudulent message.

Source: phishtank

2

Accidental insiders prone to phishing campaigns are not the only worry — renegade employees working from home during the pandemic are a substantial threat vector.

The renegade insider can be summed up with the mantra: **"established security rules and protocols do not apply to me."** This group of insiders are aware of enterprise-wide cyber security policies and procedures, but they understand how to manipulate vulnerabilities, such as loosely enforced policies and procedures, or how to exploit technical runarounds in networks or systems. The renegade is a tech-savvy individual who bends the rules for his/her own purposes, uploading information to the cloud or downloading unapproved applications onto their system — not with malicious intent, but for personal, productivity or convenience reasons.

In an age where the constancy of attacks can lead to apathy and desensitization — this group may not "see the harm, in fudging the rules a bit", especially if it seems no one is really watching. In the new somewhat "wild west" of WFH where everyone is just trying to get work done, organizations must understand that accidental insiders prone to phishing campaigns are not the only worry. In an attempt to work around slow or ineffective processes and technology, the WFH renegade can be a significant risk to your organization.

3

Malicious insiders are the third group. If organizations are not be able to stay in business and terminate staff, or require employees to go on furlough or take reduced pay or hours, a more sinister security threat can emerge — malicious insiders. These individuals make a conscious decision to deliberately cause harm and usually revel in the damage they create. While revenge or sabotage is the primary motivator especially during corporate downturns, the main motivations of malicious insiders include:

- Revenge or sabotage
- Monetary gain
- Notoriety or power
- Espionage
- Coerced, exploited or extorted

A US Secret Service/CERT® report revealed factors related to the profile, psychology, and motivations of malicious insiders. This seminal study found that negative work-related events were the impetus for most malicious actions. The research reveals that at the time of the reported attack, approximately **six out of ten perpetrators** (59 percent) **were former employees or contractors** of the victim organization. Approximately half (48 percent) of the 59 percent had been dismissed, another third (38 percent) had resigned and a much smaller percentage (7 percent) had been laid off. The remaining **four out of ten perpetrators** (41 percent) **were current employees or contractors**.

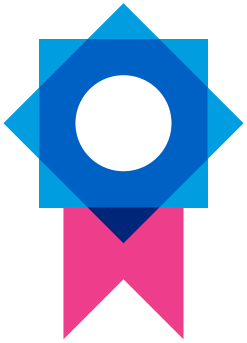
Malicious insiders can also be recruited malcontents, cyber terrorists, system administrators or executives with extensive access privileges, "greater good" or "social justice" activists, proprietary spies or nation-state actors , and even those who are coerced or extorted by outside forces. These unexpected vectors can cause extreme financial or reputational damage.

Recommended actions for executives

Understanding employee and former employee sentiment is important to assessing the motivation for an attack and in assessing the sophistication of your company's defenses. Especially when more and more employees are now working from home, creating an environment where employees play an active and pivotal role in safeguarding sensitive information is a fundamental requirement. What can corporate leaders do?

- **Leverage comprehensive, multidimensional approaches to cyber governance —** requiring the engagement of the board and the executive leadership team. Formulating a specific cyber risk leadership team during the pandemic will help identify new threats and required mitigation efforts. Maintain clear lines of communication/partnership among human resources, legal, and cybersecurity teams.
- **Assess specific threats emanating from a large-scale WFH endeavor —** what vectors are now open or more vulnerable than before the WHF policy was implemented? Update business continuity plans, incident plans, playbooks, and scenario testing. "These efforts should include, but not be limited to, preparing for the temporary or permanent loss of key staff and leadership, the evacuation of a Security Operations Center, or a serious attack where only a portion of staff are able to work". (Cyber Risk Grows as COVID-19 Spreads, 2020 MMC.)
- **Establish updated data loss mitigation procedures and recovery plans —** develop contingency plans for addressing a breach of employee data (risk mitigation). Create a corporate risk tolerance strategy.
- **Dedicate specific budgets and resources for insider-threat countermeasures**
- **Review and update the current cyber insurance policy**
- **Understand third party vendor security measures —** require comprehensive contracts or service-level agreements (SLAs) that clearly define cyber risk policies, procedures, who has access, controls, responsibilities, and liabilities. Make sure the team knows the data protection policies of your solution providers in terms of data center management, security options enforced in the software, data encryption in transit, encryption of data at rest, cloud storage and policies for asset management and data destruction. Understand their systems as well as their data breech action and recovery plans.
- **Implement tight access control and restrict privileged users —** ensure that employees and contractors only have access to equipment, sites, and data that they need to do their jobs. According to the 2019 Varonis Data Lab Report:
  - 17 percent of all sensitive files were accessible to every employee.
  - 58 percent of companies found over 1,000 stale user accounts.
  - 27 percent of a company's users had removal recommendations, and were likely to have more access to data than they require.
  - 15 percent of folders were uniquely permissioned and only 5 percent of folders were protected.
- **Build an enterprise culture of awareness, trust, and cyber hygiene —** start at onboarding and build through the employee lifecycle.

- **Focus on low priority systems as much as high priority systems —** insiders most often rely on unsophisticated methods and systems. The majority of insiders compromise computer accounts, create unauthorized backdoor accounts, or use shared accounts in their attacks.
- **Proactively address negative or potentially negative work environment issues** such as furloughs, layoffs, restructuring, performance reviews, personal financial stress, and/or negative engagement scores through targeted change management and action planning techniques. Anticipate and plan for extra risk protection during this tense health and employment crisis period. Plan and execute WFH isolation abatement through positive, honest communication, and monitor those employees most likely to be impacted and or/disruptive.
- **Monitor and address suspicious behavior —** track and link employee and contractor sentiment/engagement to cybersecurity measures.
- **Conduct exit interviews with terminating employees** to build alumni relations and positively manage the separation process.
- **Deny access to corporate computer assets immediately on dismissal —** assume a future cyber incident as a potential response from the terminated employee or ex-contractor.
- **Offer all employees cyber risk hygiene education** or offer a cyber risk (with WFH focus) refresher course. Phishing emails are on the rise — especially targeting at-home workers with messages containing important COVID-19 information and alerts from seemingly reputable organizations. In an effort to stay safe, employees may forgot about discerning obvious red flags to access these urgent messages. Clicking on these notices can lead to the release of sensitive information, malware, and theft of remote access logins and user credentials. Deploy organization-wide training and testing on the importance of mitigating risky behaviors and overall cyber safety. Consider requiring compliance with testing/sign off for all employees. (see next section, WFH cyber hygiene refresher course for ideas)
    - **Provide regular updates or touchpoints — easy online access to information, resources, and support after the training.** Provide regular updates to employees on cybersecurity protocols (i.e., short fun videos, etc.)
- **Foster a culture and response team** in which it is "safe" to raise concerns, seek guidance, and report suspicious behavior.
- **Appoint a designated resource** whom employees can ask if an email is legitimate or report other security or cyber threat concerns (often the cyber risk or IT team).



WFH cyber hygiene refresher course should include:

- Keeping a clear and secure desk
- Process for accessing the VPN with MFA, complex password requirements
- Protecting data on the move — both devices and information
- Safekeeping of company devices or company information in public areas to avoid screen viewing and theft
- Data protection, secure storage, printing, and destruction of sensitive documents
- Secure email procedures, recognizing and avoiding phishing, spoofing, etc. Provide specific guidance pertaining to requests for personal (PII) or financial information, or requests to transfer money
- Secure personal Wi-Fi access — change default settings and create complex passwords or maintain a separate Wi-Fi for work. Do not use public Wi-Fi
- Appropriate social media practices
- Requirements for timely application of updates and patches sent from IT to laptops, desktops, mobile, and even potentially non-corporate devices
- Warnings to avoid using personal email to send and receive company files, emails or information
- Requirement to avoid storing data, files or company information on iCloud or cloud-based external accounts
- Use of unsecured personal connections, Wi-Fi, products, websites or video conference rooms
- Use of company approved software only. Avoid use of free and/or unsanctioned products. Inform employees of what software is approved — for example: Zoom, Slack, Google Drive, Google Hangouts, etc.
- Video conferencing do's and don'ts including turning off email and IM during client or external video conference calls to avoid inadvertently sharing company information
- Backup system requirements and best practices

Mitigating cyber risk is everyone's responsibility

In order to maintain business continuity, many organizations have sent their employees home to work during this global pandemic. This major disruption in normal business practices poses challenges to data security, intellectual property, and overall risk. Other safety and cost cutting options for many organizations are untenable — so finding ways to mitigate the WFH cyber risk challenge is imperative (and may become even more so if a sizeable percentage of your workforce never comes back into the office after the health risks subside).

Understanding the risks, especially among those who have unfettered internal access to proprietary and confidential knowledge, information, and systems is paramount in launching a strategic and protective force field. Building strong positive sentiment with current employees, independent contractors as well as former employees or "at risk employees" is crucial to cementing a protective barrier.

While organizations today are very worried about breaches caused by sophisticated outside hackers, HR professionals, and corporate cyber leaders are the first line of defense in mitigating risk from both negligent and malicious insiders. We suggest that organizations ascertain their own risk tolerance and plan a specific WFH cybersecurity strategy accordingly. Educating employees across the enterprise, hiring right, and supporting cyber staff in the existential work that they do are critical to offset the growing cybercrime challenge.