SEC
SECURITY EXECUTIVE COUNCIL
A research and advisory firm

COVID Work from Home Guidance

Considerations for Security Leaders

Contents

Introduction

The COVID 19 pandemic caused many companies around the world to shift from conducting work on company premises to almost entirely a work-from-home (WFH) environment in a matter of weeks. While some companies allowed small numbers of employees to WFH periodically or permanently prior to the pandemic, the notion of full-time teleworkers across all industries and the globe was a first in human history.

Because of this, the term “workplace” has taken on a whole new meaning. For today’s teleworkers, a “place of work” can be wherever they are at the moment, whether at home, in a vacation home, at a café, in an RV, or wherever they ideally have secure VPN internet access to their work files, colleagues or clients.

The expansion of the WFH dynamic introduces new and increased risk to the organization. It requires modification of behavior and demands flexibility from all concerned. Understanding what has changed, adopting new processes, observing new policies and meeting new requirements—all while meeting business objectives—is a challenging adaptation that many organizations and individuals will be called upon to execute.

In this paper, we will outline how the WFH environment may be impacting organizations in a variety of risk categories.

Communications and Training

By Jim Hutton

Arguably, the most important aspect of addressing the risk management elements of a work-from-home scenario is communications. Messaging and electronic exchange between and among employer and employees, vendors and suppliers, customers and prospects, and family and friends take on more importance in the absence of face-to-face engagement.

Employers and employees need to redouble their efforts at creating or modifying clear channels of communication to identify and manage exposures and risks in this new employment scenario. Particularly important will be those processes related to alerting, coordinating, and responding to threats and incidents.

To help ensure full communications support for teleworking employees, organizations will be well-served to validate processes and tools such as

- Alert lines
- Ethics and compliance hotlines
- 7x24 communications
- Dispatch functions
- Alarm and broadcast capabilities
- Monitoring technologies

All these should be reviewed to ensure interoperability and efficacy within the work-from-home environment.

GSOCs will play a critical role in communicating with teleworking employees by continuing to provide travel advisories, weather monitoring, alarm response, access control and executive protection support activities.

The velocity of changes in policy, process and workflow in the new environment can be daunting. Organizations must leverage technology in new and creative ways to ensure that appropriate notification, training, and compliance requirements are addressed, presented and understood by a dispersed audience. Paramount among these messages are instructions and guidance on both emergency and routine processes. Organizations can leverage virtual platforms to communicate with employees regarding training, certification and assurance programs, and life safety programs.

Physical Security

By Jim Hutton

While the organization's workplace-centric demands such as food service, parking and HVAC may diminish in a dispersed worker scenario, certain core physical security activities remain vital to reducing risks to the organization. Life safety systems, alarms and surveillance technologies and personnel and property protection systems remain pillars of enterprise risk reduction.

Appropriate staffing levels should be maintained to operate and maximize the risk management infrastructure. Regular preventive maintenance should be continued, or perhaps accelerated – especially those potentially disruptive projects that always seem to be deferred. Maintain a robust and agile liaison with property management teams as well as public safety officials.

Many of the considerations listed above may need to be extended to alternate work locations and homes as well. Responsible staff should ensure that employees working from home are able to access company tools, technologies, and counsel appropriate to emerging exposures presented by their new work setting. Education campaigns or refresher opportunities should be made available to extend a level of protection consistent with the organization's risk appetite.

Pay particular attention to the nature of activities teleworkers will be conducting off-site.

- Does the work require ergonomic support?
- What first aid and medical resources are available?
- Are additional physical protective devices required to minimize the exposure to workplace violence scenarios?
- Will business appointments or small groups require health and hygiene protocols?
- What are the requirements for secure storage of documents, samples, prototypes, etc.?
- Are home-based network requirements adequately protected? (More on this in **Information Protection and Recovery**.)

In sum, responsible organizations will need to re-think the physical security boundaries of risk mitigation that have traditionally been defined in duty of care and safe and healthy workplace requirements. Enlisting the employees in an awareness campaign to jointly identify and manage these areas will maximize available resources and demonstrate commitment to a safe and healthy organization.

Investigations

By Jim Hutton

Fact-finding, assurance, due diligence, employee relations and compliance investigations must now be conducted in a new paradigm.

In a dispersed work environment, investigations may be hindered by intermittent availability of information, evidence, exemplars, witnesses, and technologies.

This new investigative landscape demands renewed and perhaps modified policy and procedures. The organization must examine and restate its expectations and requirements for investigations. Legal and Human Resources must be enlisted to calibrate and approve proposed approaches and the organization must anticipate and adapt to new legislative requirements and adjustments to best practices.

Changes and modifications to traditional processes should be highlighted and communicated to the workforce. Follow this up with training and validation, as necessary. A particular area of emphasis could be the restatement or inauguration of a “duty to cooperate” with an inquiry as part of the organization’s renewed mission and values.

Organizations that are subject to inspection, audit, or validation by third parties need to consider how best to facilitate the ongoing investigative interface with these key partners. Understanding the updated protocols used by government authorities such as tax and inspection functions, law enforcement and regulatory agencies, and processes for external certification or operating licenses will facilitate timely, effective, and efficient outcomes.

Investigations may be challenged significantly by the work-from-home model; understanding the changes to traditional processes will limit exposure to litigation, fines, and disruption. This “new normal” may also provide an opportunity to examine the efficacy of historic practices, to evaluate new technologies, to audition new partners or operating models, and to restate what investigative outcomes remain critical to a healthy operating environment.

Business Resiliency and Continuity

By Dan Sauvageau

Let’s explore some of the considerations and challenges that teleworking poses from a business resiliency and supply chain perspective.

For decades companies spent enormous sums of money to ensure their buildings were safe and secure and that business operations could run smoothly, efficiently, and uninterrupted when faced with crisis events. Investments were made to harden building infrastructure such as power, telecommunications, HVAC and computers systems to ensure backup systems were in place so that employees had access to the tools and equipment needed to run the company and service clients. In recent decades a new profession emerged where Business Continuity and Disaster Recovery professionals were hired, or dual-hatted individuals engaged, to conduct Business Impact Analyses (BIAs), drills and exercises to identify and mitigate threats to business continuity and build resiliency and recovery strategies into enterprise business operations and supply chains.

Since the COVID pandemic, the more immediate threats to business resilience come from the fact that much of the work across companies is being done at home without benefit of the robust, hardened, and time-tested infrastructure to support operations. Teleworkers share limited internet and Wi-Fi bandwidth with family members or roommates. Most don’t have backup power generators and are solely reliant on Wi-Fi and/or cell towers for their communications. Moreover, teleworkers are often ill-prepared with basic food and supplies to manage through a natural disaster such as a hurricane, earthquake, wildfire, or flood. In past crisis events, many companies would proactively or reactively house critical staff in hotels close to the office. Due to COVID challenges, that may not be a viable or health conscious strategy.

Other traditional crisis and business resilience tools companies rely upon include critical incident tracking systems that geo-fenced their buildings, weather alerts, and employee mass notification systems. All of these are largely rooted on company premises as the primary workplace. Companies may want to consider helping teleworkers better understand and be prepared for crisis events that may impact their home office. A more prepared, resilient teleworker is more likely to return to a business-as-usual state than an unprepared person when confronted with a crisis. Ensuring one has essential living supplies, backup batteries to charge computers or phones to use as a hot spot when power or Wi-Fi are down will make them more able to address their personal and company needs during and following a crisis impacting their home and community.

This work-from-home (WFH) landscape also demands a renewed and modified look at how dependent companies are on critical suppliers and supply chains. Even the best prepared and resourced multi-national corporations have faced some challenges adjusting to the WFH paradigm. Some companies reacted and responded well while others still struggle to find their way or survive.

Think about your small but critical supplier. How prepared are they to deliver products, services, or support to your company in the face of a natural or manmade disaster with their employees teleworking?

- How financially solvent are your critical suppliers given the economic hardships posed by COVID?
- If their business is struggling to survive financially, how likely are they to cut corners to save costs? Would you even know before it's too late?
- Will their quality control suffer under austerity measures?
- If they anticipate a problem with their service delivery to your company or experience a breach of your company or customer information that jeopardizes their contract, will you be alerted in a timely manner, or at all?
- How would any of these potential scenarios impact your business operations, customers, share price, or brand?

Vendors and suppliers that are subject to inspection, audit or validation by your company's risk, audit, or Q/A teams should consider how best to facilitate their work in the WFH environment and with the limitations and economic challenges brought about by COVID. Refreshing BIAs of your operations and those of critical suppliers, and perhaps including non-traditional partner stakeholders as part of the BIA process, may be worth considering.

The challenges every company is forced to address in this new operating environment, whether it's their own internal operational readiness and resiliency or the limitations of their suppliers, partners or other stakeholders, is cause to evaluate old and new business practices, BIAs, SOWs and contracts. Not doing so could have a significant impact on your company's bottom line, brand, reputation, or even survival.

Information Protection and Recovery

By Dan Sauvageau

Safeguarding a company's sensitive or proprietary information while teleworking requires more care and attention from employees than safeguarding data in a company office. While security controls, culture and risk tolerance clearly differ across companies, traditional safeguards and measures are within reach of most companies, regardless of their size and resources. Such measures include:

- Physical ones such as access controlled perimeters/doors/rooms, CCTV, video analytics, visitor controls, shredders or secure bins, locking files and guard posts.
- Robust IT systems with controls to thwart intrusions, breaches, data loss and insider risk attempts to cause harm.
- Less visible controls such as background checks, clean desk policies, formal management and informal peer oversight of employee activities.

Apart from IT VPN and PC controls, virtually none of the measures listed above are applicable in a typical WFH environment. While some fastidious or seasoned teleworkers no doubt go to great lengths to protect information they work on at home, they are the minority. Think for a moment of likely WFH settings: active children afoot, students remote learning, family members, roommates and friends coming and going, and all the other distractions within a home compared to a calm, controlled, relatively secure office environment. The chances of information unintentionally being lost, shared, improperly disposed of, or unprotected are great. So are the opportunities for intentional misdeeds, such as theft by external parties or rogue employees looking for personal gains. How can employees and organizations protect information in such environments?

The topics and suggestions below can help protect information that a company's risk management team deems appropriate to send off-site with teleworkers. These suggestions are not intended for extremely sensitive or classified information that does not belong anywhere outside a company's secure offices, labs or classified working areas. If teleworkers feel the information they are taking home is too sensitive to protect, encourage them to consult with their manager, risk or security.

Education and Awareness. Companies use many different methods to differentiate between internal, sensitive, proprietary, trademarked, confidential and proprietary information. It's the responsibility of company management to ensure employees understand what information is sensitive and how to safeguard it when in use, at rest, in storage and in transmission. A company may remind teleworkers of their obligations to safeguard company information through a variety of methods including:

- E-mail reminders
- Screen pop-ups
- Awareness campaigns (October is National Cyber Security Month!)
- Messaged coffee mugs, mouse pads, post-it notes

- Periodic team/management meetings

Policy. It may also be prudent for a company to create a telework policy that clearly spells out the special circumstances and risks of working from home and an employee's unique responsibilities. (This policy would complement existing codes of conduct and ethics documents.) A telework policy would aim to ensure sensitive information has distinct methods of data and information protection in hardcopy or electronic form while considering a less controlled WFH environment.

Telework policies would also need to address any unique governmental laws, regulatory guidelines or mandates pertaining to information or data privacy, such as HIPPA, GDPR and other information protection acts that govern their company locations. Security leaders may want to remain current with changes, updates and court rulings on as the world navigates through this pandemic and its far-reaching implications.

Dedicated workspace. To the extent possible, encourage teleworkers to dedicate workspaces that are private and separate from highly active or travelled parts of the home to safeguard company information even more so in an environment of reduced controls.

Clean desk policy. Encourage teleworkers to clear desks and work surfaces. This will keep company information out of sight of casual home visitors, domestic help, and service and repair persons. This is especially important for employees who live with roommates.

Visual security. Keep PC screens and sensitive information out of the view of other occupants and ensure PC cameras used for video conferences don't have a field of view of sensitive information.

Lockable files. Keep work material in a lockable file or drawer separate from personal information or files.

Manage and appropriately dispose of sensitive documents. Encourage employees to eliminate or reduce the need for printed materials. If this isn't practical, require the use of a company-approved cross-cut shredder. If a printer is required for work at home, consider supplying employees with company printers to allow for greater control. This way if the printer requires servicing or reaches end of life, it can be effectively managed as a corporate asset rather than discarded and potentially retrieved by someone looking for sensitive information from its internal storage.

Computer security and controls. According to published reports by U.S. intelligence and law enforcement agencies, cyber actors are watching for opportunities to exploit the weaknesses created by the new COVID teleworkers. Simply put, it's much easier for cyber thieves to hack into hundreds of millions of less secure home computing environments than fewer, often better defended company systems.

Computer security controls for teleworkers will vary depending on many factors, including the size and resources of the IT department, whether teleworkers use personal or company equipment, hosted virtual desktops (HVD) or VPNs. Some of the more basic and fundamental considerations that are not beyond the reach of companies with limited IT security capabilities may include:

- **Phishing scam awareness**: Educate or re-educate teleworkers on the risks posed by phishing scams as well as how to recognize and avoid them. Remind teleworkers to promptly notify their IT department of phishing scams and other anomalies.
- **Safeguard passwords:** Just because teleworkers are in familiar settings at home doesn't mean they can become lax with passwords, leaving them exposed or systems logged on unattended, especially if the home has other tenants and visitors.
- **Avoid Public Wi-Fi**: Remind teleworkers of the risks posed by open, unsecured public Wi-Fi, especially as they tire of being confined at home and look to get out and change their scenery.
- **Avoid or protect local storage back-ups:** If teleworkers locally back up computer files in addition to or aside from the cloud, they must remember to properly safeguard those files.
- **Secure home Wi-Fi routers:** This will reduce the risk of unauthorized access to home networks. Also remind them to take care when joining or signing on to known Wi-Fi networks, as scammers can create similarly named systems to trick them into entering their password for capture.
- **Use only company VPNs to conduct company business:** Company VPNs will hide IP addresses, properly encrypt data, mask locations, and provide other essential controls.
- **Update anti-virus software**.
- **Avoid USBs:** Unless they are from a trusted source or company provided with password protection, USBs can be altered to upload malicious code or steal information. Companies may consider disabling USB ports on company-provided computers altogether to eliminate risk of introducing malicious code through them and to control data loss through their use.

Layer security for executives and key personnel. Due to their positions and access to sensitive company information, these individuals may require additional, heightened levels of controls in to their WFH environment. For decades, security executives spent considerable time identifying and assessing the risks to these groups of employees and designing and installing myriad visible and stealth security controls and devices around C-suites, private offices, and secure labs. Now and for the foreseeable future, many of these people will spend more time in home offices.

Most will not have anything close to the safety and security features they have in place while on company premises, not to mention a quick-response security staff. These individuals are the face of your company. They possess knowledge and access to valuable company secrets, client assets or sensitive strategic plans. They remain potential targets of disgruntled employees, customers, violent activists, criminals, and competitive intelligence interests. The WFH environment with its fewer security safeguards requires security professionals to reassess the threats and risks posed to these individuals. Updating home risk assessments to take a fresh look at physical, operational, and technological risks and threats may be prudent, especially with the ever evolving and rapid adoption of technical and home automation tools.

Workplace Violence Mitigation and Executive Protection

By Dan Sauvageau

What implications does the new workplace have when it comes to managing and mitigating violence to employees or protecting executives?

For countless years, the strategies that companies employed to safeguard employees included measures such as gates, access-controlled doors, CCTV, staffed lobbies, mass notification systems, guards, and education. Executives were often surrounded with an enhanced level of physical and technical security features within the C-suite. Furthermore, companies relied on an educated and trained workforce to recognize and report early warning signs for potentially violent acts. Many companies tested their workplace violence plans and security systems with drills, exercises, internal partners and law enforcement agencies.

What is a company security team to do now that the employees they are supposed to protect are scattered across hundreds or thousands of homes that serve as their workplace? To what lengths does a company go to protect employees working away from traditional offices? What is the scope of their responsibilities and duty of care? At some point these questions will likely be answered through legislation or tested in court cases. Should a company wait for either of these occurrences or be proactive in considering how their workplace violence (WPV) policies, practices and approach may be altered to address a geographically dispersed workforce?

Internal threat assessors and WPV management teams, along with employees, will need to create or modify clear channels of communication to identify and report potential and actual incidents of threats and violence. Without traditional building controls and notification systems, new processes related to alerting, coordinating and responding to threats and incidents will need to be developed. Organizations may be well served to create partnerships with law enforcement agencies across communities where employees reside, rather than just with the few that have jurisdiction over a company building or campus. Education and training efforts will need to be reviewed and modified. Companies may need to reassess the responsibilities and expectations they place on employees when it comes to their safety in a WFH environment.

In addition to a broad programmatic review of their approach to WPV, companies will have to decide what to do when faced with known, imminent, or foreseeable threats to employees and executives. In the past, on company premises they may have increased security vigilance, guard patrols, or hire off-duty police to patrol a building or campus. Should those same measures be redirected to a teleworker's home or other remote work location? Does extending security protection to WFH locations increase or decrease a company's liabilities should something go wrong? Would it be preferable for a company to equip the targeted employee with safety tips and information or leave it to them to contact law enforcement?

Should security provide executives with some measure of security at their homes now, whether or not they did prior to the COVID pandemic? Given the amount of time executives are now working from home and the increase in civil unrest and violence occurring across some cities, is it worth re-examining their existing home risk assessments, alarm systems and emergency procedures to see if they remain appropriate in light of the potential changes in the threat landscape and police response?

These are all risks that must be re-imagined and assessed along with questions that should be discussed among stakeholders such as Legal, HR, and Security. Ready or not, organizations will be called upon to understand what has changed, adopt new processes, modify policies, re-double and re-work education and awareness campaigns.

Visit the Security Executive Council web site to view more resources addressing COVID-19.

Contact us if you need assistance in COVID-19 strategic planning, response or recovery at contact@secleader.com

Visit the Security Executive Council website: https://www.securityexecutivecouncil.com

Watch our 3-minute video to learn about how the SEC works with security leaders.