Employers are managing myriad risks and challenges posed by the coronavirus pandemic and its containment efforts. With the corresponding surge in telecommuting, data security must be a priority among them.

In the face of a global pandemic and stay-at-home orders by state and local governments, all employees who can telecommute are telecommuting. Working from home during these trying times is essential company policy. However, the sharp and unanticipated rise in telework—implemented without advance notice or opportunity to plan accordingly—carries a corresponding increase in cybersecurity threats. Employers are grappling with many challenges in the wake of an unprecedented public health emergency. Managing the risks of data breaches and other cyberattacks are among the most critical.

Cybersecurity has been a steadily growing concern in recent years, and data breaches have wreaked havoc on companies that have fallen prey, disrupting operations and threatening classwide liability when employee or customer information is compromised. But the onset of the coronavirus pandemic and the corresponding exponential increase in telecommuting presents a ripe opportunity for data hackers. This is especially true given that the typical home office will have far fewer cybersecurity protections than the onsite work environment.

Employers that have implemented telecommuting as an emergency measure in response to the pandemic have had little chance to put the proper protocols in place to protect their data—to develop written data security policies, train employees in remote cybersecurity best practices, and prepare for the spike in IT demand. Protection. Rigorous data security measures are essential to minimize risk and safeguard company data, systems, employees, and customers. As the workforce settles into stay-at-home mode for the foreseeable future, there are numerous protective measures that employers can implement to ensure data security in the telecommuting environment:

- Restrict employees from conducting company business and logging on to internal systems over an unsecured network. Require them to access company data through a virtual private network (VPN) or other secure connection. Increase the organization’s VPN connections to meet demand, or triage employee VPN access by need.
- Ensure that the organization’s remote computers are equipped with the most current firewalls and encryption software services and that security patches are continually updated.
- Consider which employees need remote access to company systems and data, and provide only the access needed to carry out their specific duties. Consider, too, whether it may simply be unduly risky for employees who require access to highly confidential company, client, or employee information to work remotely in a less secure environment. This is particularly true for employers in healthcare, banking, and similarly data-sensitive and highly regulated industries.
- Restrict employees’ use of company laptops to home use only.
- Confirm that employees accessing the network from their own computers and devices are maintaining up-to-date antivirus and malware protections.
- Ensure that your IT department retains the ability to access, control, and delete information from cell phones, laptops, or any other employee-owned equipment through which they transact company business and access network data.
Implement strict password protection policies with multifactor authentication. Emphasize to employees the importance of robust passwords in deterring cyber-attacks.

Alert employees about "phishing" attempts and how to detect them. (Already, a rash of coronavirus-related email scams have been unleashed, at a time when employees are particularly susceptible.) A useful resource: the Federal Trade Commission’s guidance on How to Recognize and Avoid Phishing Scams.

Make sure that IT has the resources needed to provide ramped-up support and increased security monitoring during this critical high-demand period.

Provide a 24-hour IT hotline for employees to report data security lapses or suspicious incidents.

**Prevention.** No organization is immune from cyberattacks. Every employer, large and small, has sensitive data of interest to hackers—employee social security numbers, direct deposit account information, and other valuable information—and employers have a legal obligation to protect this data. Preparedness is key:

- Require employees to sign formal telecommuting agreements affirming their compliance with data security protocols and clearly outlining the consequences of a failure to do so.
- Conduct online employee training on data security, including avoiding risks and reporting vulnerabilities or suspected breaches.
- Perform a risk assessment to "stress" your IT systems and identify vulnerabilities.
- Review your data breach insurance policy to ensure that it continues to meet coverage needs in this heightened risk environment.
- Review vendor contracts involving third-party access to your organization’s sensitive data to ensure that they contain appropriate indemnity protections.
- Assess the security and resilience of your data backup systems (including whether the system is securely located off-site, in the event the company’s main site is compromised), and act promptly to remedy deficiencies.
- Stay abreast of ever-changing legal and regulatory developments impacting your organization’s obligation to secure employee and customer data. It is vital, well in advance of a breach incident, to identify the myriad statutes and regulations that apply to your organization, location, and industry, along with the obligations imposed by each.
- Determine what type of notice your organization will be required to provide to those affected by the breach, and draft notice templates for ready use.
- Draft a formal data breach incident plan that will serve as the organization’s roadmap for responding to a data breach. The plan should identify the internal and external team members who will be involved, and their roles, as well as a communications and media strategy. Review and update the plan in keeping with changes to the organization, the risk environment, and the law.

**Response.** An organization that does experience a data breach, despite preventive measures, must be prepared to act immediately. A rapid response will be critical to minimize the damage, as well as to ensure compliance with data breach laws.

Activate your data breach incident plan. Notify law enforcement. Consult with cybersecurity professionals to locate and isolate the source of the breach, diagnose the nature and scope of the damage, and ensure that the breach is not ongoing, the cyberintruder’s access is cut off, and any malware is removed. Issue prompt notice, in accordance with legal and ethical requirements, to individuals whose data has been compromised. Support employees and others personally affected by the breach by providing ID theft protection, credit monitoring, and other supports.

**MainStory:** Covid19 PracticeTip Privacy Safety GCNNews