Transforming How
Texas Government
Serves Texans

Data Security: Best Practices for the Remote Workforce

Texas Department of Information Resources

June 2023

Authors

John W Kovacevich, Texas A&M University at Galveston

Jeff Krempin, Texas Parks & Wildlife Department

Suresh Sundararajan, Texas Department of Transportation

Monica Smoot, Texas Department of Information Resources

Table of Contents

Introduction

Remote working has become a necessity for organizations of all sizes to ensure business continuity, and to recruit and retain talent. The spring of 2020, with the beginning of the COVID-19 pandemic, was a great example of the need for business continuity and workforce management processes, and without remote working options, it would have been impossible for organizations to continue and sustain their business operations.

From an IT management perspective, enabling and maintaining remote working for workforces has many challenges, with enhancing security without impeding performance and productivity being the most significant challenge. However, the benefits of remote work would be diminished if the organization is not able to ensure seamless access to services, applications, and resources.

Remote working options present additional challenges from a data security perspective, as well. Just as an onsite office worker must be diligent when it comes to cybersecurity awareness, a remote worker must also defend against any number of information security threats while conducting their day-to-day business.

Additionally, there may be added risks employees are not always aware of. For example, when employees use unsecured networks and devices to perform their jobs, such as free Wi-Fi networks, they leave gaps in cybersecurity for criminals to exploit. An organization’s designated Data Management Officer can work with the Information Security Officer, or other security analyst, to develop the necessary data security policies and procedures to protect and ensure the integrity of the organization’s data and to prevent any misuse or loss of that data.

Security Risks

Without diligent adherence to cybersecurity best practices, remote workers risk exposing an organization’s data and information to parties not authorized to access it. A data breach occurs when a thief or hacker is able to access the data of an organization without receiving the proper authorization. Files containing confidential, sensitive, or even public information can be highly sought-after targets, particularly because that information can be correlated together to discover the identity of each person.

Employees must be aware of the possibility of external threats that may compromise data security while working remotely. Just some of those threats are listed in the section below.

External Threats

Malware Activity: With malware, or malicious software, a hacker can accomplish any number of things—from taking over a computer system to controlling a network, to providing backdoor access and more. Malware can also be used specifically to steal personal information.

Ransomware: Ransomware is a type of malware in which cyber criminals lock or block users’ access to their own data or devices. Hackers typically seize control of a machine then threaten to delete, destroy, or publish data unless their ransom demand is paid. This threat is often spread through phishing emails containing malicious attachments that infect a device and then encrypt files or even entire devices. Ransomware attacks may use other social engineering or drive-by downloading techniques, such as links sending victims to spoofed websites that install malicious material onto their machines without the person’s knowledge.

Phishing: In a phishing attack, the attacker sends a fraudulent message that creates a sense of urgency or appeals to the victim’s curiosity to entice them to either click on a malicious link or provide private information via a form.

Spear-Phishing: With a spear-phishing attack, the victim is specifically targeted, and the attacker often performs extensive research ahead of time. Once the attacker knows how to manipulate the victim, they launch the attack, phishing for information, credentials, or sensitive data.

Baiting: A baiting attack attempts to draw in a victim by promising something that appeals to their sense of curiosity or greed. This lures the target into installing or clicking on something that ends up putting malware onto their system.

Scareware: Scareware bombards a target with fake threats or false alarms in the hopes that their natural inclination to protect themselves or something they value drives them to taking the desired action. One of the more common types is using realistic-looking banners warning that their computer may be infected with a virus or some other kind of malware.

Pretexting: In an attack that uses pretexting, the attacker lies to the victim regarding their identity. After they have gained the target’s trust, the attacker tricks them into handing over sensitive information.

Quid Pro Quo: In a quid pro quo attack, the attacker pretends to provide something to the victim in exchange for information or a specific action. For example, the attacker may pretend to be someone from tech support and then convince the target to enter commands or download software that installs malware onto their system.

Rogue: With a rogue attack, the victim is tricked into paying to have malware removed from their system. The malware is not taken off the system, but the victim still ends up paying the attacker.

Vishing: Vishing, short for voice phishing, uses a conversation over the phone to get financial or personal information from the target. They often hide their identity using spoofing, which changes their caller ID. As with other social engineering tactics, the attacker tries to gain the individual's trust or uses fear to get them to divulge valuable information.

Mail Theft: Even before the internet, identity thieves were busy taking people's personal information and using it for their benefit. A common method was, and continues to be, mail theft. In this kind of attack, the thief grabs the target's credit card or other information from their mailbox. They then try to use it to make purchases—or sell it to another thief for a quick profit.

Internal Threats – Risky Behavior

In addition to these external threats, employees must also be aware of their own behaviors or choices that may compromise data security while working remotely.

Weak Passwords: One of the biggest threats to companies' remote workforces is the ongoing use of weak, insecure, or recycled passwords and login credentials. Failure to use secure passwords negates cybersecurity software and tools like firewalls and virtual private networks (VPNs).

Hackers can now use software to help them crack account passwords and access sensitive corporate information. For example, they can compile vast lists of common passwords to access accounts or write code that uses multiple password variants to guess login combinations successfully. Another common approach is to use passwords they know someone has used for one account, such as a personal email or social networking site, to try and access their corporate accounts.

Personal Devices: One of the most significant security risks of remote working is using personal devices to connect to corporate networks and systems. These devices often do not have the same level of cybersecurity protections as a corporate computer or laptop. Personal smartphones often do not use encryption to protect personal data, and home printers can leave security gaps that can be exploited by hackers.

Some people use their mobile phones to log in to sites automatically, without having to enter their username or password. If someone gets ahold of your mobile phone, they may be able to access these same sites, especially if they do not need to enter a password or use biometric verification, such as a fingerprint or facial scan.

Use of Public Networks: Corporate Wi-Fi networks are typically secure because they are protected by secure firewalls that monitor and block malicious traffic. However, remote-based employees may connect to corporate networks and systems from unsecured Wi-Fi networks.

Anytime an employee uses a computer or mobile device on a public network, they may be vulnerable to a hacker that can eavesdrop on communications within the network. This is a particularly prevalent issue at places like coffee shops, department stores, or airports where anybody can get onto the network, often without a password.

Additionally, most people routinely update their smartphone firmware or antivirus software but rarely do so on their home routers. This can leave their home network vulnerable to a data breach that, in turn, risks the security of the organization's data.

Unsecure Browsing: In most cases, the websites people visit are safe. They are protected by security measures that prevent hackers from gaining access to the information you enter. The protection often involves encrypting the data that gets entered. However, if employees use websites that are not as well-known, they may be putting themselves at risk. Even if the website's designer had good intentions, the website itself may have been compromised by a hacker.

Dark Web Marketplaces: The dark web consists of a network of websites hidden from regular internet users. When someone visits the dark web, they can use software to hide who they are, as well as what they are doing while connected. This makes the dark web an ideal place for thieves, hackers, and others looking to defraud users.

Data Sharing: Remote-based workers are likely to use file-sharing services to send documents and other files to their colleagues. These files, when stored on corporate networks, are likely to be protected through encryption. However, when shared remotely, the same level of security may not apply. Sharing sensitive information through file-sharing tools can leave data vulnerable to being intercepted or stolen by hackers — especially while data is in transit. The loss of sensitive corporate data can result in security events like data theft, identity fraud, and ransomware attacks.

Work Environment Awareness: Just as confidential or sensitive information must not be left unsecured in the office work area where anyone may gain access it, the same clean desk policy should be employed at the remote work location. Working remotely in a public location makes it easier to be observed without one's knowledge. "Shoulder surfing" is a way for those with bad intentions to steal protected data by watching their victims while on their devices or when working with paper records. Carrying confidential or sensitive paperwork or documents to unsecured public locations provides opportunities for paper records to fall into the hands of unauthorized users, resulting in a data breach. Remote workers should take care to ensure any paper documents in their possession are kept in a secure environment or location to mitigate this risk and should avoid viewing confidential or sensitive data and information on their devices while in public locations.

Procedures for protecting confidential or sensitive data that remote staff may print out should be covered in any information security training session. Failure to shred or safely dispose of any sensitive documents and safeguarding organization information per your organization's data retention policies will compromise data security.

Best Practices

Data Management and Information Security Officers should work together to ensure data and cybersecurity best practices address the unique challenges faced by remote workers. Each of the measures described below provides an extra layer of security for your remote work environment. By implementing them, and providing training to both management and staff, you can be sure that your data is safe and secure.

1. Enable Encryption

Encryption is a tool designed to ensure the confidentiality and privacy of the data on your devices. Encryption mitigates the risks posed by a lost or stolen device. So even if a criminal were to gain physical access to any remote employees' devices, the data on it would still be protected from unauthorized access. Enabling encryption is simple and you can encrypt your device (including portable storage devices) using products such as BitLocker for Windows and FileVault for macOS. It is highly recommended to use a key management solution for IT administrators to manage encryption keys to devices, to assist in recovering a drive if needed.

2. Install Antivirus and Anti-Malware Software

Antivirus and anti-malware software are required not just for security but also for regulatory compliance. Antivirus and anti-malware solutions provide a layer of protection where it is most needed, i.e., the users, who when in a rush or too busy, tend to engage in risky behaviors that the IT team advises against. Be sure to choose the right antivirus that meets your business needs and that they are installed on all devices.

3. Ensure All Operating Systems and Applications Are Up To Date

Software updates and patches are regularly released to improve the functionality, usability, or performance of the software. More importantly, patches often fix security vulnerabilities. Many ransomware attacks are preventable by ensuring updates and patches are installed timely. If you delay updating your software, cybercriminals can use the known and yet unpatched vulnerabilities to hack into your system, install malware, or steal data.

4. Enforce a Strong Password Policy

The use of weak passwords is an open invitation to cyber-attacks. To safeguard user accounts from cyber-attacks, organizations need to enforce a strong password policy that helps create good password hygiene. Ensure that your password policy checks for length and complexity, disables automatic login, and enables automatic lock.

5. Use Mobile Device Management (MDM)

One of the key challenges of securing remote access is the difficulty of ensuring that the devices get the same level of security when they are remote as they would when in the office. This is where Mobile Device Management (MDM) solutions help. MDM solutions allow organizations to monitor and manage devices wherever they are located.

With MDM solutions your organization can easily install and configure applications, push updates, and manage mobile devices such as laptops, tablets, and mobile phones easily. It simplifies and enhances the security of portable devices, mitigating much of the risks associated with remote access. On employee-owned mobile devices, it is a best practice to segment personal data from organizational data. Work profiles provide a separation of work applications and data, allowing organizations to control security policies and applications on employee-owned devices.

6. Use Virtual Private Networks (VPN)

When employees work remotely, they may use public Wi-Fi at airports, hotels, or other public spaces. Therefore, organizations need to ensure that no one intercepts or snoops in while employees are accessing the company resources from public Wi-Fi.

Virtual Private Networks (VPN) not only give secure access to your office network but also ensure its security. VPNs allow employees to easily access company resources using any high-speed internet connection enabling them to work efficiently while keeping their connection secure. VPN is a must for any organization that allows remote work but especially for those that depend on sales and services teams who work in the field and may often use unsecured public connections.

7. Use Two-Factor Authentication

Two-factor authentication (2FA) provides excellent security, is relatively easy to implement, and comes at no extra cost. It is a type of multi-factor authentication, in which your username/password pair needs to be supplemented with another method such as an OTP (one-time-password) to verify your identity. This additional step required for logging in to your accounts adds an extra layer of security, making it difficult for hackers to gain access to your accounts.

8. Avoid Using Remote Desktop Protocol (RDP)

Remote Desktop Protocol (RDP) is a protocol used for creating remote desktop sessions. When remote employees access their office desktop from their mobile device, it is commonly done using RDP. However, RDP is prone to vulnerabilities that can compromise your internal network. RDP sessions have been known to be vulnerable to security attacks. They are also susceptible to credential harvesting, remote code execution, and can be even used to directly drop malware on the computer. Therefore, it is highly recommended to avoid using the remote desktop protocol.

If it is unavoidable and you have to use it, then you should take the following precautions:

- Do not expose RDP to the internet.
- Direct all activities through a secure connection.
- Instead of direct RDP connection, force RDP sessions through a Remote Desktop Gateway.
- Restrict who can use RDP and what they can access.

9. Implement Identity and Access Management

Identity and Access Management (IAM) secures an organization’s resources by allowing organizations to easily manage access rights, privileges, and digital identities. In addition to managing how users gain digital identities and permissions granted to those identities, IAM also validates the hardware and software of the device requesting access.

IAM ensures the correct level of access to IT resources in complex business environments using risk-based authentication, artificial intelligence, and machine learning. IAM allows the application of role-based access to control access to critical IT resources and to regulate access to systems, applications, and networks from a single platform.

Considering today's threat landscape, username and password combination isn't enough to secure your resources during remote access by users. If organizations want to maintain elevated security standards or rigorous compliance requirements, Identity and Access management is absolutely necessary.

10. Conduct Security Audits and Risk Assessments

Regular security audits and risk assessments help identify, analyze, and evaluate vulnerabilities and associated risks. Organizations can either include remote services and remote work as part of a company-wide IT security audit or conduct a separate audit specifically for remote services.

Remote services audits should have a special focus on the following:

- Logins to both cloud and on-premises resources
- VPN logins
- User activity on cloud solutions such as SharePoint, OneDrive, Microsoft Teams, etc.
- Group membership and permission changes
- Use of network ports and VPN connections
- Port scans and failed login attempts
- RDP sessions, if in use
- Configurations of all critical resources

Use the data gathered to create a baseline or to benchmark normal use. This will help flag suspicious activity when there are spikes or anomalies in user activity or network traffic. Document the results of the audits and make changes as and when necessary to accommodate changes in processes, new technologies, etc.

12. Provide Organization-issued equipment

Employers should consider supplying staff with laptops and other mobile devices that are managed by the organization. Hard drives would be encrypted, administrative privileges would be restricted, only approved software would be installed, critical patches and updates would be applied regularly, scans for malware would be done on a schedule, and devices would have approved virus protection. Requiring staff to do business on equipment provided and managed by the organization would add a much-needed layer of security for remote users.

11. Employee Education

Finally, the best defense against any attack is for organizations to educate employees on best practices. We know by now that technology alone isn't sufficient to protect organizations from cyber threats. There is no security system that can protect a business 100% on its own. Data shows that human errors, social attacks, and phishing are responsible for a large number of cyberattacks. Effective protection of an organization's data requires focusing on the weakest point in the security system, i. e. the users. A well-informed person is better equipped to handle a phishing attempt or social engineering situation that could lead to a data breach.

While remote work offers many advantages, it adds new security challenges that traditional office environments don’t usually experience. As more organizations transition to remote work, the security threats they face increase. Educating and informing users on the risks and safety protocols associated with new technologies is the organization’s responsibility. Therefore, it is essential any data and cybersecurity training include topics specifically addressing the additional challenges and threats impacting remote working.

Effective IT security comprises a security-conscious culture supplemented by the right technologies and tools that work together to mitigate security risks. To create such a culture, organizations need to provide regular security awareness training to their employees highlighting the risks of remote work, keep them engaged, and communicate expectations and the importance of their role in the organization’s data and information security. Creating this culture is a long and difficult process but the resources invested will be well worth it. A security-conscious culture enables a sustainable security system that contributes to a strong overall defense in protecting the organization’s data and information.

References

Fortinet
https://www. fortinet. com/resources/cyberglossary/cybersecurity

CMSWIRE
https://www. cmswire. com/information-management/6-ways-to-keep-employer-data-secure-when-working-remotely/

OT Group
https://www. otgroup. ca/en-ca/remote-worker-technologies

Phoenix NAP
https://phoenixnap. com/blog/secure-remote-access-best-practices#:~:text=Most%20commonly%2C%20remote%20workers%20will,Secure%20Sockets%20Layer%20(SSL)

World Wide Technology
https://www.wwt.com/article/have-zero-trust?utm_campaign=infosec_article_zerotrust_us_emea_ps_2_search&utm_source=google&utm_medium=cpc&utm_content=static_stock&gclid=EAIaIQobChMI26Oh2qCZ-QIVARXUAR0nNgrtEAAYAyAAEgI9H_D_BwE

Hitachi Solutions
https://global. hitachi-solutions. com/blog/working-remotely-security-tips/

Expert Insights
https://expertinsights. com/insights/what-is-security-awareness-training-and-why-is-it-important/