

Keeping Data Secure for Remote Workers

By Allison Davis, Senior Manager

Where are you working right now? There's a good chance you're on a laptop in a coffee shop or a hotel, or multi-tasking at a conference. There's an even greater chance you're doing something work-related — accessing email, reviewing reports, or completing reconciliations. If you are working remotely, it's likely your employees and coworkers are, too. So how do you secure remote workers and the devices they use to access your resources?

Remote work is becoming extremely popular as it can reduce overhead costs, minimize employee burnout from travel and commuting, and increase efficiency, effectiveness, and employee satisfaction. But granting your user base the freedom to work where and when they want does not negate the need for controls. In fact, remote work may create new challenges as your network becomes decentralized.

With strategic planning, however, you can create a remote working environment that supports your organization while maintaining the security of your systems and data. Here are four steps to follow.

1. Identify the need and extent of access. You cannot manage what you cannot measure, so start by defining the who, what, and how of your remote working environment.

- **Who** needs to be working remotely? Is it the entire user base or a select group?
- **What** are they accessing? Are they accessing internal network resources, cloud-based applications, or internal and client data?
- **How** are they accessing it? Are they accessing internal resources via VPN or cloud-based solutions? Are workers using personal devices, or are all devices

Remote workers and the devices they use become an extension of your network.

owned by the organization? Are they using laptops, workstations, mobile devices, or a combination of these?

2. Define acceptable use policies for the identified resources. Because your organization likely allows personal devices to access business resources, it's imperative to define these areas:

- Who owns the devices, the data accessed and created, and the installed applications?
- What responsibilities do remote workers have? Consider [password](#), anti-malware, patching, encryption, and physical security requirements.
- What restrictions are in place for data storage and device synchronization? Many devices back up automatically. If an employee uses a personal computer for work purposes, business data may inadvertently be included in personal backups.
- What are the procedures if a device is lost or stolen? Can the data be wiped remotely? Do employees know who to notify and the timeframe for notification?
- What are the procedures to ensure data is removed properly from a device if an employee leaves or if a device is sold, sent for repair by a third party, transferred to another individual, or discarded?

3. Configure controls to support your policies for securing the applications and data that can be accessed, and the systems that they are accessed on.

Many remote workers use remote access and cloud-based applications. Using your inventory of applications, first ensure that each system is properly secured. Enable strong password parameters and conservative lockout settings and configure multi-factor authentication for all remote access and high-risk, externally-accessible applications. This is a non-negotiable control!

Next, set retention periods to limit the impact if data or systems are compromised. With the nature of remote work, large amounts of data are often stored in the cloud for ease of access. However, is all this data truly needed? Consider this question when evaluating the potential

impact if any of these systems are compromised. Establish a retention period for data and a process for deleting or removing it when it is no longer needed.

Finally, secure devices that will access the resources. Remote workers and the devices they use become an extension of your network. Even if the devices are employee-owned, you now are responsible for securing them to protect the data and systems they access.

Centralize and enforce these controls:

- Install anti-malware protection on all devices and ensure the definition files are updated regularly.
- Apply patches and updates to operating systems and applications.
- Enforce password-protected screen savers and inactivity timeouts to protect users when they walk away from the device.
- Configure encryption to protect any data stored locally on the device.
- Enable the ability to remotely wipe a lost or stolen device.
- Create a guest network to segment work-related traffic from guest and family member activity, if possible.

If existing management systems cannot support remote devices, you may need a more robust mobile device management solution. These solutions often provide enhanced controls for data storage and syncing.

4. Train your user base. Once employees are remote, the way you manage controls changes, and the layers you have at your physical office may no longer apply. Your employees need to be aware of the risks associated with remote work. Talk to your employees about current threats, the risks of using public Wi-Fi, and the heightened threat of malware when using computers for both business and personal use.

Employees want to work remotely for various reasons, and organizations can no longer avoid this shift in the workplace. Instead of shying away from this change, embrace it by compensating for the risks with strong controls.

About the Author

Allison Davis, Senior Manager

CapinTech
adavis@capincrouse.com
o 505.50.CAPIN ext. 2008

Throughout her time as an information systems auditor and senior manager, Allison has provided information security assessment and consulting services primarily for nonprofit organizations, financial institutions, and health facilities. In addition to these services, she has provided clients with consulting services in risk assessment and policy development engagements.

About CapinTech

CapinTech, a CapinCrouse company, provides information security services, including cybersecurity assessments, consulting, and training services, to nonprofit organizations, financial institutions, medical entities, professional services firms, and other organizations. Each year the firm performs hundreds of assessments, consulting, and speaking engagements with a team of experienced professionals retaining numerous certifications, including CPA, CISSP, CISM, CISA, CITP, CGMA, and CTGA. Each engagement is tailored to fit the unique needs of the organization, and information and reports are presented in a clear, concise manner intended for an audience with varying information systems (IS) knowledge. More information is available at capintech.com.

About CapinCrouse

As a national full-service CPA and consulting firm devoted to serving nonprofit organizations, CapinCrouse provides professional solutions to organizations whose outcomes are measured in lives changed. Since 1972, the firm has served domestic and international outreach organizations, universities and seminaries, foundations, media ministries, rescue missions, relief and development organizations, churches and denominations, and many others by providing support in the key areas of financial integrity and security. With a network of offices across the nation, CapinCrouse has the resources of a large firm and the personal touch of a local firm. Learn more at capincrouse.com.

CapinCrouse is an independent member of the BDO Alliance USA.



© 2019 Capin Technology LLC