The IT Service & Technical Support Community

Good Practices in Remote Support

by

Roy Atkinson
Senior Writer/Analyst, HDI

UBM TechWeb

The *2012 HDI Desktop Support Practices & Salary Report* tells us that about 91 percent of desktop support organizations are using remote control tools to provide support. According to Jenny Rains, HDI's research analyst, "about three-quarters of the industry is providing support using remote support technology."[1]

Fundamental things we want to know about remote support are:

- Why use remote support?
- How effective is it?
- Who within the organization provides remote support?
- What about confidentiality and privacy?
- Which, if any, good practices are emerging?

Obviously, remote control ("shadowing") tools have become one of the key pieces of support technology. With ticket counts on the rise and management striving to control costs, remote connection and control software promise to cut down or even eliminate the time desktop support/field service technicians spend traveling to and from the customer's location. Often, a customer's computer can be quickly restored to full function by the addition of a patch or upgrade, a change in configuration, or an adjustment in the user and group settings, but the customer may not have the rights and permissions necessary to make the changes, may not know where to get required software, may not be aware that they need the software or adjustments, or may simply require some "hand-holding" to get through the process. In addition, "40 percent of support centers have at least some staff working virtually, and an additional ten percent are planning to implement this practice in the next twelve months."[2] Some estimates say that mobile workers of all types will make up nearly three-quarters of the workforce by 2013.[3] Working at a distance from colleagues and customers increases to value of being able to share a screen and perform operations on a distant computer.

Putting remote support technology in the hands of support center and desktop support staff makes a difference in terms of:

- Faster time to resolution, as phone tag and data gathering steps are eliminated, and more issues are resolved at first contact;
- Higher TSR (technical support representative) productivity, as support engineers can work directly on the system, see exactly what's happening, and not need to recreate customer environments on lab computers;
- Better root cause analysis, as engineers can see defects exactly as they present themselves at customer sites;
- Training as a by-product of support, as customers watch, learn, and duplicate expert resolution processes; and
- Higher customer satisfaction and loyalty as a natural side effect of faster, more accurate, and more transparent resolutions.[4]

[1] Jenny Rains, "**Providing Remote Support to Customers**," HDI Research Corner report (November 2011), p. 1.

[2] Jenny Rains, *2011 HDI Support Center Practices & Salary Report* (HDI, 2011), p. 68.

[3] IDC, "**How to Equip Your Company For the New Mobile Workforce**."

[4] D.B. Kay & Associates, "**Show, Don't Tell: Remote Support Best Practices and Benefits**."

Having access to others' computers, whether within the organization or outside of it, is fraught with both compliance and ethics questions for the support center. In the day-to-day pressure to get people back to work quickly, it may become easy to overlook some of the finer points of providing remote support. Support center managers, desktop support technicians, and support center analysts alike should be aware of all the considerations.

Consider, for example, a comptroller or other member of the finance team who is having serious issues with Excel. In order to solve the problem, an analyst or technician will probably need to connect to the comptroller's computer remotely *while the comptroller is logged in and the problematic workbook is open.* The workbook may very well contain sensitive, confidential data. The same can be said about connecting to computers in human resources, legal, product development, and many other departments or groups within a company. Likewise, educational institutions may wrestle with giving support analysts access to computers containing examination questions, admissions and financial aid information, and other sensitive data; the same is true for hospitals, law firms, tax accountants, stock brokerages, and so on.

We can discuss the need to safeguard the confidentiality of information from three perspectives:

- Technology
- Process
- People

Technology

Remote connection/control software varies. Some products can also be used for collaborative screen sharing, and are not restricted to purely technical support uses. Essentially, there are three major types:

- **Administrator-to-client:** In this model, administrative software running on a technician's computer (or on a server) can connect to a client that resides on a customer's computer, giving the administrator full view and control as if she/he were present at the client machine. In some cases, the client software can be "pushed" to the customer's machine over a network if it has not been previously installed.
- **Web-based:** The customer opens a webpage and shares his/her screen with a technician who "picks up" the connection based on information provided by the customer.
- **Appliance:** Hardware-based, centralized control over remote sessions.

Regardless of the type your organization chooses, security should be a high priority. A remote support session that is not secure is a big opportunity for a "man-in-the-middle attack."[5] The protocol used to make and continue the connection should be secure, and should comply with requirements such as PCI DSS, HIPAA, SOX, and any other industry-specific requirements. All remote connections should be automatically logged so that audits can be performed.

Process

There should be a standard procedure for connecting to any computer for remote support. Many remote control products have a feature that alerts the end-user when a connection is made, and can require acceptance by that end-user before the connection is completed. Where this feature exists, it should be enabled so that customers/end users always know when connections are made and have the right to delay or refuse them. If your organization uses a remote control product that does not offer this feature, written (email will suffice) or verbal (phone) permission should always be obtained from the customer/end user for a *specific connection*. (In other words, just because you have my permission to connect to my computer today, that does not mean you have it again tomorrow. If you need to connect again, you need to ask again.)

People

At the very least, each analyst and technician should receive training about the importance of following procedures when using remote control tools, and should be asked to sign a code of ethics attesting to their agreement to act in an honest and professional manner. There should be appropriate consequences (up to and including termination) for violating the code and/or failing to follow proper procedure.[6] Staff members are being entrusted with "the keys to the kingdom" and need to understand the gravity of this trust.

As with any rule, there are exceptions, however rare. Suppose, for example, an end user's computer is infected with a virus or malware that is attempting to propagate across your organization's network. If repeated attempts to reach the end user fail and a network administration remedy is not readily available, the best (i.e., fastest) solution may be to shut the machine down via remote control until a technician can address the issue. In such emergencies, a supervisor or manager should be consulted to make the decision to access the computer and issue the command. An analyst or technician should not make the decision unilaterally, and the steps leading up to the decision to access the remote computer without permission should be documented. Cases like this should be reviewed to see if there was another solution, and whether existing procedures or remote control product features need to be changed.

[5] Click **here** for a definition of "man-in-the-middle attack."

[6] One example is the **USENIX/LOPSA/LISA Code of Ethics**, which, though originally intended for system administrators, is also used for analysts and technicians.

Safe and Successful Remote Support

Once appropriate and secure remote control tools are in use in your organization, don't forget the importance of ongoing education and awareness. Make sure that new end users/customers understand that remote control is an option, that they have ultimate control over when and how it is used, and that new analysts and technicians understand the proper procedures for remote control.

There are many benefits to remote support, perhaps the greatest of which is *the ability to show customers/end users how to do something, and vice versa*. Every remote connection is a teaching opportunity, and it can work in both directions. Imagine a customer saying, "Well, our group has found that it's better to do it this way…" and showing a technician how people actually use a given tool or perform an operation.

Work with your information security staff to make sure they have the ability to audit remote support sessions and make recommendations. Remember, "just because you *can* doesn't mean you *should*." Because of the cost benefits and ease of remote support, organizations may be tempted to use it as the default method of working with end users. In some cases, it may be better to have a technician visit in person to attend to the issue at hand, answer questions, and make personal contact. Even the most honest of end users is wary of being "spied on" and may resist the idea of remote control. Be clear about the benefits to them and make sure they understand their level of control.

About the Author

Roy Atkinson is HDI's senior writer/analyst. He is a certified HDI Support Center Manager and a veteran of both small business and enterprise consulting, service, and support. In addition, he has both frontline and management experience. Roy was a member of the conference faculty for the HDI 2012 Conference & Expo and is known for his social media presence, especially on the topic of customer service. He also serves as the chapter advisor for the HDI Northern New England local chapter.

About HDI

HDI, a UBM TechWeb company, is the leading professional association and certification body for technical service and support professionals. Serving a community of over 110,000 members, followers, customers, solution providers, and contributors, HDI hosts industry conferences and events, produces comprehensive publications and research, and connects solution providers with practitioners, all while certifying and training thousands of professionals each year.

