

Don't Let Data and Business Assets Slip Out the Back Door

An Interview with CenturyLink Security Expert Bob Schroeder

Businesses of all sizes face the moving target of always changing security threats, but SMBs don't have the IT resources that larger organizations have to focus on the latest dangers. As CenturyLink Director of Product Management Bob Schroeder points out, there's not a textbook that tells business owners how much security is enough, but in this interview, he gives you the next best thing: a "CliffsNotes" for keeping your data protected.

Q Every day it seems like there's a new security risk to worry about. How can SMBs be sure they're protected?

A On one extreme, you might think you're protected and yet your assets, your intellectual property, your trade secrets—anything that's of value to you—could be going out the back door. You could be losing valuable information about your business, or more importantly, you could be exposing valuable information about your customers, your suppliers and friends of the business and putting it at risk. That's a very real problem in every network, from the end user all the way up to the enterprise level.

On the other extreme, you could over protect your network and pay more than you need to. When is enough, enough? With security, the question is "How much can I afford?" It's always a trade-off, and some smaller businesses don't have the resources to invest in the security they need. They wait until they have an emergency and then react—which often ends up costing more.

Q Where are businesses most likely to be vulnerable—are there some common blind spots?

A A common vulnerability is the connection between your private network, including devices—PCs, laptops, smart phones, etc.—and the outside world. The minute you create that connection by, let's say, giving an employee a laptop with a Wi-Fi card, you create a potential vulnerability where an unsuspected bridge may exist between the public Wi-Fi network and your private network.

We've seen these problem at large businesses, too. Even companies that have spent hundreds of thousands of dollars on security can lose sight of where the public and private networks came together and inadvertently put valuable data at risk.

If that can happen at a major enterprise with all of their high-end security measures, you can be sure it can happen to small and medium-sized businesses. Take, for instance, the example of a restaurant that processes hundreds of credit card transactions each day. They think they're protected because they bought their point-of-service (POS) terminals from a well-known manufacturer that guaranteed their terminals were safe and secure. But maybe it's not as thoroughly protected as they thought, exposing their systems to risk. Hackers are smart—they'll find those vulnerabilities and steal customers' credit card data or other valuable information.



When enterprises make mistakes, it costs them lots of money and lots of customers, but they usually stay in business. They survive. That small restaurant that accidentally had one POS with a vulnerability is not nearly as likely to survive.

Q What proactive steps can you take to prevent a breach like that from happening?

A Well, first you have to make security a priority. Every business—no matter how big or small—has to be cognizant, observant and diligent about how they use the Internet and how they protect their network. That begins with understanding your points of exposure and what you have that someone could find valuable.

Here's a typical scenario: You're reviewing your son's homework, which is on a thumb drive he shared with a friend. Unfortunately, the friend's computer was contaminated, and there's a virus on the drive. Now you've got the virus on your laptop, and all of a sudden, you're propagating the virus to everyone you e-mail. Not only are you creating risk for your business, but you are also potentially generating unnecessary virus traffic across the network and affecting many networks.

It's bad user behavior that feeds the mess. So what do you do? You put policies in place that take into account human error. So when I give that infected drive to my co-worker it isn't allowed to contaminate the network. You should also have policies that govern recreational Internet surfing on corporate-owned assets. Many Internet sites are prone to bad behavior and attract hackers that plant viruses. When you visit one of those sites you can infect your computer with a virus, worm or software that can steal valuable information.

Q What are some of the specific security protections that all businesses should put in place?

A An obvious first step is anti-virus protections, which you must keep up to date. Another basic step you should take is to install a firewall between your network and the Internet. A firewall will prevent unwanted traffic from entering or leaving your network. The problem is, the majority of malicious activity over the Internet is increasingly sophisticated and may be able to bypass simple firewall protection.

For additional protection, you can add an Intrusion Detection and Prevention system (IDPS) alongside your firewall. IDPS appliances are constantly monitoring for known attack patterns or vectors, which are ways hackers use to enter your network. IDPS systems will alert you immediately if you're under attack—or possibly even shut down an attack.

I could list more security measures, but the key is to begin by asking yourself what you're protecting. Once you figure that out, you can create a security policy that articulates how you will address potential vulnerabilities and what you would do if you are attacked. You should also consider bringing in outside expertise to help you identify your vulnerabilities across your network and computer systems and develop a comprehensive security plan.

Q Businesses have mobile employees who access the company network from home and on the road. How can they make mobile computing secure?

A If you offer remote access to your employees you need to take precautions to ensure those connections don't open your network to



unauthorized users. A relatively simple way to protect your network is to equip your users with secure access via a Virtual Private Network (VPN). It provides you with the tools to authorize network users and provides auditing and reporting so that you can control user access to network resources. The VPN provides built-in encryption via IP Security (IPSec) or Secure Sockets Layer (SSL) technology standards. VPN solutions are commonplace today and every business, large or small, should ensure their network is protected with this technology.

Q Data encryption seems like another simple step that businesses could take to protect their mobile data. Is encryption automatic on most laptops?

A It should be automatic, but only a small percentage of today's laptops encrypt data. Although encryption software is sophisticated, all the end user has to worry about is a password—it's relatively easy, inexpensive and thorough. The unfortunate reality is that most businesses don't use encryption because they don't want to invest the money and they don't like the nuisance.

Q Should SMBs consider using software as a service (SaaS) as part of their security policy?

A That's a great question. Smart SMBs are beginning to move to the SaaS model because it can provide simplicity, convenience and cost savings. A SaaS model also provides a sound business continuity strategy in the event of a disaster.

I'll give you a specific example of the benefits of SaaS. Steve is the owner of a small business near my home, and he had laptops for his 10 or so employees. Instead of purchasing and installing software, he invested in cloud-based software applications through a SaaS provider—which came in handy recently when someone broke into his

small shop and stole all his laptops. The next day, he was able to replace the laptops and get himself and his employees back online. His business really didn't miss a beat. All of his customer data and software applications were in the network—he just needed Internet access to the cloud.

Q How can you ensure that your business stays up and running if and when a security breach occurs?

A The first thing is to have a written plan to get back in business quickly after an attack. In other words, you need to know how you'll get immediate access to computers, data and the Internet. You may need to have expert resources available that can help you understand how the attack was performed and prevent the exposure when you come back online. You need to practice how you will implement your plan should the need arise. The next step—which really cannot be emphasized enough—is to back up your data on a regular basis, preferably to a location physically removed from your main office with a network-based storage service.

Q What are a few of the key questions SMBs should ask before they invest in new security measures?

A Businesses should look at security investments the same way you might look at any major investment. That is, you need to think about your priorities in terms of what you need to spend your money on right now, as well as how much you can afford to spend. Above all, you want to be sure that your security investments deliver what they promise—that they actually make your business more secure.

Business Continuity:

1. Make a plan.
2. Back up data.
3. Test plan regularly.



Q How do you know when you've spent enough to make your business secure?

A When is enough, enough? The truth is that when it comes to security, there's no such thing as "enough." The more critical question is how much can you afford. Unfortunately, that makes it tempting to do nothing, to spend little or nothing and just wait until you have a problem, and then react to the intrusion. That's a risky strategy, to say the least. It can be very difficult and expensive to correct the network vulnerability and restore lost business.

Q At what point does it make sense to have a third party help you manage your security?

A Once you've taken the basic step of installing anti-virus protections, encryption and a firewall, and you begin to need more sophisticated security measures, you should think about bringing in help. When you get to the point of spending money on vulnerability scanning, VPNs and Intrusion Detection and Prevention, you may be able to save time and actually save money as well by bringing in professional assistance.

The last thing you want to do is to devote a lot of your own time and energy to security, only to find out you didn't invest in the right protections, or you paid too much or you didn't follow up with the necessary updates to make your investments worthwhile. Experts can help you avoid those problems.

Q What should you look for in potential service providers, either for individual solutions or for managed security services?

A Finding a reliable vendor can be a challenge, because security is not tangible and often you don't know you're vulnerable until after an attack happens. The first thing you can do is look for a trusted provider with a proven record of accomplishment. Ask around to find out which providers are trusted by businesses like yours. Also, make sure you choose a vendor that will provide you with monthly reports that will show you how many viruses your security system has quarantined and how many intrusions have been stopped.

And, finally, contact other businesses that have used that provider. Check the references to be sure those businesses have not suffered attacks and have been pleased with the overall level of service and support they've received.



Robert L. Schroeder
Director of Product Management,
CenturyLink Communications Company

Bob Schroeder has 20 years of experience in the communications industry and works directly with customers and account managers to customize data security solutions for businesses of all sizes. Bob is currently leading the product development program for CenturyLink Next Generation WAN, VoIP, Cloud Computing, SaaS, Ethernet and Data Protection Services. He was also responsible for the development and launch of CenturyLink Networking, a family of private MPLS services.

