Digital Security in Sensitive Contexts

by David Cross

David is the VP of Information Technology for his organization and the author of 'Mondays in the Middle East: The Lighter Side of Arabian Nights' (2006) and is a contributor to 'The Desert Is Alive: Streams of Living Water from Muscat to Marrakech', edited by David Lundy, Gary Corwin & Gail Martin (2007).

Abstract

Sharing the Good News in sensitive contexts presents unique challenges that dramatically heighten the tension felt over data security. This article will present a contrast between the old model of data security that many of us are familiar with that is vulnerability-centric in its nature and a new model which is threat-centric in nature. The main objective with the vulnerability-centric model is to plug every known vulnerability to all software and operating systems. The assumption is that this will keep the bad guys out.

A better approach to data security is threat-centric data security. The success of this approach depends on the successful identification of the threat actors involved and adequate protection against the specific threats those threat actors bring. This creates a 'right-sized' approach to security which makes the task of applying appropriate security measures more reasonable for people who may not be especially technical in nature. The end result of this approach is enhanced security for people on the field.

The Old Model

Today's connected world presents challenges never seen before by those sharing the Good News. With a bit of levity, for example, twenty-five or thirty years ago, you would have readily allowed your child to sit on your laptop, but that is a costly prospect today. In the 1980's, a permanent marker was very useful in making a bold point on a tablet, but today's tablets are forever divorced from permanent ink. In the 1990's, phones had no IQ at all so we called them neither smart nor dumb. At that time, someone who Skyped simply hadn't run spell-check on WordPerfect 5.1.

Today's technology scene is a different world, indeed, and it has myriad challenges that simply didn't exist for Christian workers back then. Along the way, however, we've done our best to keep pace with the changes in technology. In those days, we paid large sums of money to purchase software that was really half-baked and we became part of the developers' test environment. We discovered bugs and vulnerabilities through our ordinary work by generating the infamous Blue Screen of Death (Windows) or Kernel Panic (Mac/Linux). We reported those bugs back to

the developers through support calls and they fixed them so that we found different bugs that would then be reported and fixed and the cycle went on.

We assuaged our concerns about wasting $299 on Microsoft Office by enabling automatic updates that would ensure that all of the holes poked in our system would be automatically patched...eventually. We installed antivirus programs to protect our floppy disks, added a healthy dose of prayer and hoped for the best. In fact, for most people this strategy of data security hasn't changed over the past 20 years. Patches + Antivirus + Prayer = Hope. Unfortunately, it is a vain hope that eventually software developers will patch all of the holes so that we will no longer have security issues.

The Futility of Focusing on Vulnerabilities

Some years ago, I was traveling through Illinois and I had taken roads off the beaten track to enjoy a bit of the scenery on a route I'd never taken before. As you'd probably guess, I got lost at one point and stopped at a gas station to ask for directions. Keep in mind, this was in the days when navigation consisted of a map and a good sense of direction.

I asked a gentleman the simple question, 'How do I get to Highway 41?' He responded with a straight face, 'Oh, Highway 41? You can't get there from here.' In a moment, his dry humour broke into laughter and relieved me that I hadn't stopped at the one place in the universe where I couldn't navigate to Highway 41.

When the task of patching all vulnerabilities is extrapolated out, the natural conclusion is, 'You can't get there from here.' The notion of patching all vulnerabilities assumes that at some point, all software and hardware will simultaneously become perfect and all future technological advances in that software and hardware will similarly be perfect. Only then can our devices truly be secure. Of course, this is a fanciful notion that is better suited to Alice in Wonderland than today's world. In other words, it will never happen.

Consider the following list from Security Magazine of 24 simple steps you are expected to do when traveling overseas:
http://www.securitymagazine.com/articles/85271-checklist-24-steps-for-data-security-while-traveling-abroad.

The list is filled with common advice but it is daunting to consider that each of those steps must be taken for every trip when traveling overseas. In fact, as helpful as lists like this are, they can lead to insecure practices because they are so overwhelming. Average, non-technical people see a list like this and they throw their hands up in resignation thinking, 'Well, I certainly can't do all of this, so I'm just going to wing it and hope for the best.' To really achieve greater security, we need a more focused approach on the vulnerabilities you encounter in your specific cross-

cultural context, not just a blanket list that is expected to cover all threats in all locations at all times.

A New Approach: Threat-centric Security

I want to present a new approach to data security that is more balanced and a bit more realistic. This approach, plainly put, is centred around the threats that individuals face. This threat-centric approach is dependent on a reasonable assessment of your threat context. With this reasonable assessment of your threat context and a threat-centric mindset, there are key actions you can take to simply increase your security.

The main thrust of a threat-centric approach to security is to understand the threats to your security and align your defences to those threats. Although there are threats that are common to all people in the digital world, not all threats apply to all people or for all situations. For example, certain threats apply to all people such as the threat of malware invading your devices or the simple threat of theft of those devices. Protecting against those threats forms a baseline in our security defences. Those actions are the minimum that would be acceptable no matter where you are in the world. Keep in mind, travellers are at a particularly high risk of exposure to 'opportunistic criminals', those who are simply trying to benefit from pickpocketing, for example.

On the other hand, certain ministry contexts, especially for those in ministry to Muslims or Hindus, might be actively hostile toward Christian ministry rather than passively tolerant of Christian ministry. These contexts present different threat actors and different threats to digital security. For example, some of the threat actors that make these situations unique could be:

- Governments who are hostile to the work of the Gospel
- Curious neighbours who want to know what Christian workers are doing
- Hostile militaristic groups who are actively searching for Christian workers
- Hostile individuals who take it on themselves as vigilantes to oppose the work of the Gospel.

Assessing Your Threat Context

Understanding the different threat environments is the first step to appropriately identify the right security actions to protect against the threats in your environment. There are several reasons that this approach of self-analysis makes sense. First, you are the person who has the most to gain or lose in getting an accurate self-assessment. It's appropriate for you to have ownership of your own security. With that responsibility comes the watchfulness for any changes that may happen in your security context. If something substantial changes such as government unrest in your host country, you have the full authority and responsibility to make the

necessary changes in your digital security. Second, you know your situation best. You know, for example, if the curious questions of neighbours is a dramatic change that might indicate a higher level of scrutiny.

Questions to ask yourself to assess your threat context:

- What digital assets do I have? It's helpful to list all of your digital assets so that you know what you are protecting. For example, your Kindle might seem harmless enough, but if it contains books about ministry that would be offensive to a host government, it is an important asset to guard.
- Who might benefit from my digital assets? For example, opportunistic criminals might benefit from stealing your iPhone whereas a hostile group might benefit from the contacts and connections in your Facebook account.
- How are those assets at risk? This is an important point of self-assessment that will help you recognize when your security context changes. For example, if your city is dealing with a rash of burglaries of the homes of expats, your assets are at increased risk. This would indicate a change in your security context.

Regularly asking yourself these three questions will help you establish your initial threat context and detect any changes to your threat context. You might choose to re-assess your threat context every six months or whenever your security environment changes. These changes might include:

- Changes in political climate in your host country.
- Changes in scrutiny on Christian ministry that you hear of in your area.
- Changes in the curiosity of neighbours or strangers you might repeatedly see.
- Specific threats made to you, your family or team.

Practical Steps to Securing Your Data

After coming to a better understanding of threat-centric security and accurately assessing your threat context, you can now begin to apply digital defences appropriate to your context. Again, the whole point of this approach is to have security defences that are just right for your context. You can think of this as the Goldilocks principle – not too big, not too small, just right. Security is always at odds with convenience. A twenty-character password of random numbers, letters and symbols such as 'pEgG1@Qzww4M68r$mw*V' is much more secure than 'pa$$w0rd', but it's also less convenient to memorize and type than pa$$w0rd. Also, if you forget such a long, complex password, it could put your data at risk because there is no back door to get around good encryption. So, it can be dangerous to apply too much security and it is dangerous to apply too little security. You need a solution that is just right, like Goldilocks.

As mentioned before, there are certain security steps that everyone should take because it is common sense in today's world. I will call these the baseline security steps. Here are some tips for baseline protection:

1. Guarded Watchfulness

Some of the most common threats to digital security are not technological threats at all. Rather, they are exploits of your social media presence or social engineering itself. Serious care should be given as to how much information is shared on social media applications and limited unless the information is really necessary. Additionally, vigilance to keep you and your family from accidentally sharing too much information through prying questions. The example often given is the way grandma gave her social security number to an imposter calling on the phone and a new line of credit was opened in her name without her knowledge. Well, it's not just happening to grandma and these threats come through your clicks, not just phone calls.

2. Vendor Supported, Current on Updates (Devices and Software)

Not using a supported device means that security updates are not being created for the device, which leaves the device vulnerable to malware. Malware, or malicious software is one of the common ways that devices are compromised by opportunistic criminals. Unpatched security vulnerabilities in the operating system and key applications are the primary way that malware is able to gain a foothold on the device. Keeping up to date on security patches is foundational to a baseline defence.

3. Anti-Malware Software

Using a supported and updated device and software sometimes isn't enough, and malware can still infect your device. Using an anti-malware solution to detect and remove malicious software will add another layer of security.

4. Appropriate Access Control

Using quality passwords for critical accounts will make it much more difficult for it to be guessed or 'brute-forced'. Making use of a password manager will allow you use these qualities passwords without resorting to writing them down in an insecure manner. Finally, enabling what is called 'Two Factor Authentication' will add a very strong layer of defensibility.

On the other hand, if you have identified that your security context includes people like curious neighbours, there are some further steps you can take. Your goal at this point is to keep the level of scrutiny low. This can be done using three sets of steps when it comes to handling sensitive information.

4.1. Reduce

Assume everything you put on a computer is impossible to get rid of. With that assumption, ask yourself, 'Is there a legitimate reason that I need this digitally? If I need it digitally, am I limiting where it goes as best as possible?' A strategy worth considering is one that more and more people are adopting which is downgrading to a 'dumbphone' instead of continuing to use a smartphone. If you can meet your mobile needs for calling and texting without the frills of GPS, Facebook, an Internet browser, etc., this is a real option.

4.2. Protect

If you are interested in specifics, a full strategy is available of which device encryption is a part. Feel free to contact the author for more information (send an email to the editor and he'll connect you: seedbed.editor@sent.com).

4.3. Detect

Just as we need to exercise situational awareness from a physical security perspective, the same applies digitally. We need to exercise online situational awareness.

Conclusion

Finally, if you are under more intense scrutiny from hostile groups or governments, there are further protections to consider. Since you are already under a much higher level of scrutiny, the goal is to reduce the scrutiny as much as possible. This would entail using all three of the previously described steps (Reduce, Protect & Detect), but also specific steps to make yourself a more difficult target to compromise. If you are interested in specifics, feel free to contact the author.

In the end, it must be recognised that there is no perfect, risk-free security system. That being the case, the most successful approach to security will be one that people can understand and one they can apply, namely, a Goldilocks approach to security that is not too much, not too little, but just right. A threat-centric approach to security is solid foundation for an approach that can be understood and easily used.