



Achilles' 3 Fatal Business Mistakes (or How to Protect Your Heel)

Achilles, an ancient Greek superhero -- half human, half god -- was in the business of war.

During a recent 60 Minutes interview, I was asked off camera to name the Achilles' heel of an entire country's security infrastructure. The interviewer wanted a checklist of the nation's greatest weaknesses. The country happened to be New Zealand, a forward-thinking nation smart enough to take preventative steps to avoid the data loss and identity theft problems we face in the States. The question was revealing, as was the metaphor they applied to the discussion.

Achilles, an ancient Greek superhero -- half human, half god -- was in the business of war. His only human quality (and therefore his only exploitable weakness) was his heel, which when pierced by a Trojan arrow brought Achilles to the ground, defeated. From this Greek myth, the Achilles' heel has come to symbolize a deadly weakness in spite of overall strength; a weakness that can potentially lead to downfall. As I formulated my thoughts in regard to New Zealand, I realized that the same weaknesses are almost universal -- applying equally well to nations, corporations and individuals.

For starters, let's assume your business is strong, maybe even profitable in these tough economic times. In the spirit of Sun Tzu and The Art of War, you've dug in your forces, preparing for a lengthy battle: you've reduced costs, maximized your workforce, and focused on your most profitable strategies. As your competitors suffocate under market pressure, you breathe stronger as a result of the exercise. But like Achilles, your survival through adversity blinds you and even conditions you to ignore pending threats. You begin to think that your overall strength translates into an absence of weaknesses; and in general, you might be right. But Achilles didn't die because of his overall strength, which was significant; he died because he ignored critical details. What details are you and your company ignoring?

Information, like Achilles himself, is power. **And maintaining control and ownership of your information is quite possibly the most threatening Achilles' heel any data-reliant business faces.** Companies that don't actively take control of their data are prime targets for identity theft, social engineering, data breach, corporate espionage, and social media exploitation. Regardless of your title, you have a great deal to learn from Achilles' mistakes, and a significant opportunity to protect your own corporate heel.

Achilles 3 Fatal Mistakes and How to Avoid Them

Admit Your Vulnerabilities. Achilles forgot that he was human, failing to take inventory of his weakness in spite of superior strength. Though his faults were limited -- a small tendon at the base of his foot -- his failure to protect himself in the right spots proved fatal. When protecting data, it is imperative to understand that your greatest vulnerabilities lie with the people inside of your company. No matter how secure your computer systems, no matter how much physical security you deploy, humans will always be your weakest link. The more technological security you implement, the quicker data thieves will be to attempt to socially engineer those inside your company (or pose as an insider) to capture your data. Admitting vulnerabilities doesn't have to be a public, embarrassing act. It can be as simple as a quiet conversation with yourself and key players about where your business is ignoring risk.

The three greatest human vulnerabilities tend to be: 1. Unawareness of the risks posed by data loss, 2. Lack of emotional connection to the importance of data privacy (personally in professionally) and it's affect on profitability, and 3. Misunderstanding that in a world where information is power, it's no longer about whom you trust, but how you trust. These symptoms suggest that your privacy training has either been non-existent or dry, overly technical, policy related and lacking a strong "what's-in-it-for-me" link between the individuals in your organization and the data they protect every day.

If this is true inside of your business, rethink your training from this perspective: your audience members (employees) are individuals with their own identity concerns, not just assets of the company who can be forced to follow a privacy policy that they don't even pretend to understand. By tapping into their personal vulnerabilities regarding private information (protecting their own Social Security Number, etc.), you can develop a framework and a language for training them to protect sensitive corporate information. Like in martial arts, where you channel your opponent's energy to your favor, use your employee's humanness to your advantage. Pinpoint these vulnerabilities and shine the light of education on them.

Fight Prevention Paralysis. One of the most unfortunate and destructive character traits among humans is our hesitation to prevent problems. It is human nature to invest time to prevent tragedy only after we've experienced the pain that results from inaction. We hop on the treadmill and order from the healthy menu only after our heart screams for attention. We install a home security system only after we've been robbed. Pain motivates action, but the damage is usually done. You can bet that had he the chance to do it all over again, Achilles would slap a piece of armor around his heel (just like TJMAXX would encrypt their wireless networks and AT&T would secure their iPad data).

Prevention doesn't get the proper attention because its connection to the bottom line is initially harder to see. You are, in essence, eliminating a cost to your business that doesn't yet exist (the costs of a future data breach: restoring and monitoring customer credit, brand damage, stock depreciation, legal costs, etc.). This seems counterintuitive when you could be eliminating costs that already exist. But here is the flaw in that method of thinking: the cost of prevention is a tiny fraction of the cost of recovery. When you prevent disaster, you get a huge return on your investment (should a breach ever occur). Statistics say that a breach will occur inside of your organization, which means that by failing to invest in prevention you are consciously denying your organization a highly profitable investment. Why would you insure your business against low percentage risks (fire), but turn the other way when confronted with a risk that has already affected 80% of businesses (data breach) and has an almost guaranteed double digit ROI? It is your responsibility to demonstrate how the numbers work; spend small amounts of money preventing, or vast sums of time and money recovering.

Harden the Riskiest Targets. Once you have admitted to and cataloged your vulnerabilities and allocated the resources to protect them, it is time to focus on those solutions with the greatest return on your investment. A constant problem in business is knowing how to see clearly through information overexposure and pick the right projects. Just think of how much stronger Achilles would have been had he placed armor over his heel (which was human) rather than his chest (which was immortal). There is no financially responsible way to lower your risk to zero, so you have to make the right choices. Most businesses will gain the greatest security by focusing on the following targets first:

1. **Bulletproof Your People.** Most fraud is still committed the old-fashioned way - by manipulating trusting, unsuspecting people inside of your organization. Train your people for what they are: the first line of defense against fraud. Begin by preventing identity theft among your staff and then bridge this personal knowledge into the world of professional data privacy.
2. **Protect Your Mobile Data.** Laptops, smart phones and portable drives are the most common sources of severe data theft. The solution to this very powerful and ubiquitous form of computing is a quilt-work of security, including password strengthening, data transport limitations, access-level privileges, whole disk and wireless encryption, VPN and firewall configuration, physical locking and human decision making (e.g., don't leave it unattended the next time you get coffee at your corporate conference).
3. **Prevent Insider Theft:** Perform thorough background checks, reference verification and personality assessment to weed out dishonest employees before they join your organization. Implement an ongoing "honesty meter" for your employees that ensures they haven't picked up bad or illegal habits since joining your company.
4. **Classify Your Data.** Develop a system of classification that includes public, internal, confidential and top secret levels, along with secure destruction and storage guidelines. This classification system should be applicable both to physical and digital documents.
5. **Anticipate the Clouds.** Cloud computing (when you store your data on other people's servers), is quickly becoming a major threat to the security of organizational data. Whether an employee is posting sensitive corporate info on their Facebook page (which Facebook has the right to distribute as they see fit) or you are storing customer data in a poorly protected, non-compliant server farm, you will ultimately be held responsible when that data is breached. You must be aware of who owns that data, today and in the future, when your storage company is bought out or goes bankrupt.