The Growing Consequences of Security Breaches

Over the last few decades, I have watched the balance between the white hats and black hats change back and forth many times. However, the balance has never been as skewed as it is today. Companies have invested heavily in "front gate" defenses and ignored everything else, punishing organizations in almost all industries. The damage to companies like Target and Sony mounts into the billions, ranging from PR battles to lost sales and ultimately, civil liability.

For years we've been shouting from the rooftops about the need to invest in security proactively and thoughtfully. As the costs become clearer—and higher—business owners are realizing the need to take action. However, the challenges of implementing meaningful, appropriate security are also increasing:

- The threats we face are significantly more sophisticated than they have been in the past. Attackers are probing for weakness and blending together many techniques with devastating results.
- Compliance is king. Many compliance standards and mandates overlap and conflict; yet failure to comply can incur substantial liability in many different forms. Reconciling this is difficult.
- Technologists lack confidence in solutions offered by third party providers, this is based on a lack of experience with the products, as well as unimpressive performance. The result is a lack of trust in the tools and their results.
- Security is necessarily becoming more integrated with overall solutions; businesses understand that we are beyond the days of simply patching systems and protecting the front door.

You Must Step Up: Static investments in security are no longer enough. With very rare exceptions, your organization MUST be more concerned about security than you are right now. Tools are important, but a good process and dedicated team are needed to make them useful.

Five Common Security Issues: There are in all likelihood some critical commonalities between organizations that suffer breaches, and your organization. Very common issues include:

1. **You're Sold Insecure Equipment:** Almost every piece of technology or equipment you buy is much less secure than it should be? Why? Because a secure product is difficult for a sales team to demo and difficult for a new customer to get started with. Factory settings are NOT secure, and we rarely find customers have done more than change the default password—if even that.
2. **Your Internal Systems are More Open Than You Think:** During multiple recent visits with a large technology enterprise, we watched as employees would fail to lock their workstations before leaving their desks. Because the company had invested so much in building security, they did not protect their data center assets from their employees' desktops. The result was a huge attack vector, easily exploited by anyone who could get their hands on the shirt and building entry card of a janitor or security guard, or even just be invited into the facility for a meeting.
3. **Your Security Tools May Actually Enable Hackers and Attackers:** Simplistic security tools such as an "all defaults" Intrusion Prevention System make it easy for an attacker to understand what they're blocking—and what they're not blocking. Good security is cross-cutting and multi-layered. In defending our clients, we use the obvious things like Intrusion Prevention and DDoS prevention to detect people poking around the outside edges. We use other things too, like web server security modules and OS lockdown modes that will detect unusual behavior and either notify us or intervene. As a result, we can find—and block—the attacks others miss.
4. **Your Team Is Too Comfortable:** Buying some expensive tools and investing in a cloud provider that says security is important to them is no reason to breathe easy. Attackers are always in attack mode and so you must never be comfortable. We are living through the Cold War of Information Security, and mutually assured destruction is not a reasonable defense.
5. **You Aren't Managing the Signal To Noise Ratio:** In a sophisticated security system, you capture and surface a potentially enormous amount of data. As Target learned, successfully capturing an ongoing attack is not enough if the news is lost in the noise. You need tools that will help you correlate data from a variety of entirely different systems in search of the information you need. If you are looking at everything without the right tools to sort the chaos, you might as well not be looking at all.

While we're just scratching the surface with this list, fixing these vulnerabilities before they become problems is critical. Importantly, it is also attainable. While not a magic bullet, a step-by-step plan for continuous protection improvement should be a must for your organization in these dangerous times.

How Should You Defend Yourself?

Unfortunately, there are dozens of things you should be focused on when it comes to defending your organization against attack. But let's address the core focus areas common in all robust security programs:

1. **Make everyone align around security:** Security is a discipline, not a practice. Disciplines span your key IT process areas including network/system administration, software development, configuration management, backups, monitoring, etc). Even non-IT areas must be on the same page—facilities, procurement and human resources have been attack vectors for some of the most devastating attacks in the last five years. With threats accelerating on nearly a daily basis, your organization must build a security-conscious culture, and you must have a dedicated team that works to align all process areas around security. Through a comprehensive, mindful security discipline, results can be achieved without dictating security mandates that squeeze revenue.
2. **Ask Questions of your Colocation and Cloud Vendors:** Cloud and data center providers and their salespeople are frequently more than willing to misrepresent the quality of the security systems and protocols offered on behalf of their customers. Some have security officials who are badly overmatched. Security and compliance is an area you MUST knowledgeably question your providers.
3. **Trust Your Tools or Get Rid Of Them:** Organizations invest heavily in security and then when warning signs appear they do NOTHING about it. At all. Target's massive credit card info breach happened after a $1.6 million investment in a malware detection tool and their security specialists (offshore resource) saw it happening. They alerted corporate security and NOTHING happened. If you can't trust the tools you are using, try harder or get rid of them.
4. **Learn How To Correlate Data To Find Information**: Sometimes noise is noise, but sometimes it is a threat. It's a bit of an art to listen to what everything is telling you. The common approach is to funnel as much information into security/event correlation tools that cost tens of thousands of dollars (or more). We utilize automated correlation and filtering of key events across everything we log. This

is why people buy big expensive security products, but they don’t work well at automatically detecting. We use cheap tools to look for very narrow things that have a high probability of being interesting. The same user failing to log in on a handful of servers in a row is a signal and should be investigated immediately.

5. **Invest In Resources, Not Just Tools:** Security tools are primarily designed to create data. Log files need reviewed. User access needs reviewed periodically. Configuration needs validated constantly. In fact, there are hundreds of controls that need followed and tended to. This requires professionals who understand the threats and who have the work ethic and diligence required to keep on track.

The bottom line is that no piece of equipment or single action is going to protect you. A blend of intelligence and elbow grease is required. A respect for the silent army attacking you is also essential. Thousands of attackers dedicate their lives to getting into your network. Defending against that requires an investment of money and time. It requires dogged, detail-oriented professionals doing work that is far less glamorous and intriguing. Anything less is a distraction.