The BusinessEdge Inside Technology

November 29, 2013

Cyber Security: How Much is Enough?

by Neil Rerup

"What should I do to make my company secure?" is a critical question in a business landscape replete with hackers, attackers, and in-house security imperfections.

The best answer varies by organization, the sensitivity of its data and infrastructure, as well as the business requirements (including budget constraints). Quite simply, a mom and pop printing shop requires a lower level of IT security than a health care provider managing medical records while processing credit card transactions, which in turn, requires somewhat less of a defense than a critical utility installation.

Determining the right level of cybersecurity for your company and the necessary actions to achieve that state of IT protection is a strategic balancing of factors; however, company leaders face myths, rumors, varying "expert opinions" and a plethora of expensive solutions touted as absolute necessities by salespeople disguised as unbiased cybersecurity analysts.

> "...in the cybersecurity field there is no such thing as "Industry Best Practice" solutions. What this phrase really means is "I don't want to take the time to understand your business requirements so just do as I say and don't question me."
>
> – Neil Rerup
> Author,
> CyberPeril

In reality, any business leader can discover the right level of IT security by first understanding that cyber threats fall into these categories:

1. Motivated hackers
2. Competitors
3. Criminal organizations
4. Nation states
5. Internal source, such as a disgruntled employee (this is the number one threat)

Consider that most incidents, according to some studies between 75 and 90 percent are of this internal sort, but it's important to be aware of and address the others, too.

Concurrent with identifying and estimating the most likely risks, your business requirements analyses will include identifying what assets (and responsibilities) must be protected. These fall within defined categories, with some crossovers, such as intellectual property, customer (or client or patient) data, company processes,

Continued on next page

Continued from previous page

infrastructure, and firm data not falling within these categories — but nonetheless important and needing IT protection.

With your list of assets and responsibilities needing protection in hand and a thoughtful consideration of the most likely threats specific to your company, the final step is to consider the cybersecurity resources available to counter the threats and provide protection. Every company has three tools to wage and win the cybersecurity battle, better known as the three P's of IT security: processes, people and products. It is the strategic balancing of these tools within the parameters of a budget that will define the optimal cybersecurity solution for your company.

In practice, it is your knowledge of the workings of the company that will frame this solution matrix. For instance, one security goal of a small company might be to know who is accessing what information. Simply adding a log-in requirement is an easy and practical solution that surely fits within any budget while achieving the business requirements. A more complex organization, such as a utility, might have hundreds of servers that instead require an automatic monitoring solution, which is more expensive from a capital expenditure standpoint but a lower cost from a sustainment and operations perspective. The message is that your optimal solution will be defined by balancing people, processes, and products in a combination that fits within the budget.

This framework will enable any business leader to determine the right level of IT security for a specific circumstance. However, there are four pitfalls that can derail even the best plans. The good news is that if you know about them, you can bypass these challenges that have caused security turbulence for your less well-planning competitors.

1. **Security for security's sake.** Keep your business requirements at the forefront of your analyses. If your solution goes far beyond meeting those requirements, you are wasting resources.

2. **Trying to do it all at once.** Know your time frame for meeting those requirements. If your business strategy calls for entering a new market in three years, the cybersecurity solution for that market does not demand an in-place solution in six months.

3. **Bigger or more expensive does not mean better.** Cyber-security vendors are masters of showmanship, but do not become mesmerized by the spectacular technology. Most often, the best solution is nothing more than changing a process.

4. **Conflicts between IT Management and cybersecurity.** Be certain that conflicts between IT management and cybersecurity management are resolved at the executive level by the leader responsible for the overall strategy.

As a final bit of counsel, be aware that in the cybersecurity field there is no such thing as "Industry Best Practice" solutions. What this phrase really means is "I don't want to take the time to understand your business requirements so just do as I say and don't question me." As a now-prepared strategy decision maker for your company, you know that every solution must be focused on meeting your company's specific business requirements. Anything else is a waste of your time, energy and resources. ■

About the Author

Neil Rerup, an enterprise security strategist and founder of Enterprise Cyber Security Architects, helps companies and governments efficiently and effectively achieve their business requirements in the cybersecurity arena. Neil, a 12 year veteran of the cybersecurity wars, is the author of the upcoming CyberPeril (Sutton Hart 2013). Interested readers can contact Neil at nrerup@enterprisecybersecurity.com and can get additional information by visiting www. neilrerup.com.