Enterprise security

The price of protection vs. the price of none **Interviewed by Jason Lloyd**

In this era of digital dependence, risk to a company's infrastructure abounds from all sides, including from within. Enterprise security is a topic that simply cannot be ignored. Security infrastructures can be costly investments, but when compared to the alternative, they are sensible investments.

Security is a broad topic that receives nearly limitless research and development resources. Several professional organizations manage the amount of knowledge contained with the topic. One organization, the ISC(2), created The Common Body of Knowledge, which consists of 10 unique domains that cover various facets of enterprise security.

They are access control systems and methodology; telecommunications and network security; security management practices; applications and systems development security; cryptography, security architecture and models; operations security; business continuity planning and disaster recovery planning; law, investigations and ethics; and physical security.

Controls on investment, in the form of a well-designed plan, must be put into place before spending and attempts to secure an enterprise ensue.

Return on investment can be difficult to calculate but can be put into perspective with this question: What would be the impact on a business if the IT infrastructure (including trade secrets, financial data, etc.) were available to the public? The impact would be directly proportional to the return on investment. If the impact would be minimal, then return on investment would likely be low; if the impact would be high, then so would return on investment.

"When in doubt, a good security firm can perform a security assessment," says Ron Plew, vice president and CIO of Perpetual Technologies. "That third party provides an objective set of eyes and can often provide criticism and recommendations, and generate action that would be difficult or impossible for employees."

Smart Business spoke with Plew about enterprise security.

Ron Plew
Vice president, CIO
Perpetual Technologies

How can a company tell if it is vulnerable?

Certain vulnerabilities are easy to discover — an unlocked door, for example. Vulnerabilities are not always this obvious. There are freely available tools for checking servers, applications and hardware for vulnerabilities.

These tools simplify the discovery process. Server logs should be periodically checked by a knowledgeable administrator. Logs can provide a good amount of information to the trained eye.

A good security firm can help a company create and implement ongoing operations security practices. Strong operations security practices will ensure that a company is pro-active as vulnerabilities appear.

How can a business improve its security systems?

Improvement requires an established baseline. You have to know where you stand in order to improve. This baseline is established through a security assessment. It is essential to critically analyze the entire security spectrum when determining this baseline. The process of performing the security assessment will expose vulnerabilities and weaknesses in security systems and policies. Details of implementation remain.

In the absence of a security assessment, do not underestimate the insider threat, which is the largest source of risk to any business. A well-enforced security policy can help mitigate this risk.

How does one domain affect overall enterprise security?

Security domains operate in cooperation. The common analogy is a knight's armor. In battle, when vulnerability is discovered, it is only a matter of time before the knight falls and the entire suit is useless. All domains applicable to a business's enterprise security are equally important.

In certain security domains, countermeasures can be implemented that minimize the effect of vulnerabilities. Depending on the impact of penetration at various points in the security domain, countermeasures may prove economically feasible.

How much security is enough?

It is easy to spend thousands of dollars while trying to address security issues on the fly. Avoid doing this, as you may end up wasting time and money on insignificant or irrelevant items.

Instead, perform a security assessment and a risk analysis, and create a deployment plan. The resulting documents will provide instruments that can measure success. Without the proper instruments, it will be difficult to determine how much security is enough.

When all of the items identified in the security assessment and risk analysis have been addressed, there may be enough security. A post-implementation audit will help verify this.

A word of caution: Do not become comfortable after implementation. As technology evolves, new security threats — which will continue to appear — must be addressed. Security policy coupled with continuous monitoring and review will help assure a secure business.

RON PLEW is vice president and CIO of Perpetual Technologies. Reach him at rplew@perptech.com or (317) 824-0393.

Insights Technology is brought to you by Perpetual Technologies Inc.