

## Accurate Risk Assessment

The Office of the Comptroller of the Currency (OCC) requires financial institutions to have a formal risk assessment program. A program needs to accurately identify where sensitive customer information is stored, who has access to the data, and how to speak to the security controls that are being utilized. The OCC also mandates that financial institutions must demonstrate that they have a mature risk assessment program that is accurate, consistent and repeatable. Accuracy is the name of the game. A saying that I like to use is that *risk is a constant while the variable is how accurately it is assessed*.

**Philip Alexander**

**August 9, 2007**

### Accuracy is King

I can't overstate the value of **accurate risk assessments**. Minimize the threats to your data, and your company is unknowingly accepting risk. While some will say that ignorance is bliss, in the case of data security, it can expose your company to a huge amount of liability. Unknown risks are not only undocumented, they also do not get remediated. If you don't know there are problems, most certainly you will not try to implement security measures to address them. And eventually, you will discover what risk your company is accepting. You will either suffer a security breach or fail a government audit. While certainly educational, neither scenario is particularly pleasant.

### The Sky is Falling

A common mistake is to overstate risk. This is sometimes due to a lack of expertise on the behalf of the assessor, or a somewhat irrational avoidance to risk. Keep in mind that there is no such thing as an absence of risk when it comes to handling sensitive electronic data. Overstating risk can lead to a Chicken Little syndrome. Reports that contain higher assessed risk levels will require the review and acceptance of more senior executives within your organization. If you continually bombard your executives with over inflated assessments, you run the possibility of diluting their attention from real risk. Overstating risk can also have a paralyzing effect on an organization as well. Managers may opt not to proceed with a particular project because of an over inflated risk assessment. Remember, sometimes the greatest risk is to miss out on a business opportunity.

Many organizations will also restate the same risks over and over again. As with overstating risk, regurgitating the same issues will have the same numbing effect on executive management. While an inherited risk is worth mentioning in the narrative of an assessment document, it doesn't necessarily have to be included in the actual risk rating of subsequent projects. The risk assessment should be on the delta, what's new, and not be rehashed old issues that have already been reviewed and accepted by appropriate levels of management.

### The Information Security Officer

There are many skills that are necessary in order to make an accurate assessment of risk in the realm of data security. Broad technical knowledge is required in order to understand how computer systems work. This knowledge is also necessary to accurately understand and articulate any weakness the systems may have, and its impact to data security. Without a technical background, an information security officer really does not know what he/she doesn't know.

For example, a fully qualified information security officer would need sufficient knowledge of firewalls and network protocols to understand the risks of allowing SSH traffic in to your network from a vendor's network. On the surface, this may sound very secure. SSH is an encrypted protocol so the data being transmitted between the two organizations would be protected. However, the same encryption would also allow the vendor to bypass any intrusion detection sensors that your

company may utilize. The only thing the sensors would see is the encrypted traffic or cipher-text. They wouldn't know if what is being transmitted is appropriate or not. SSH also has a capability known as **port forwarding** which enables any protocol to be tunneled through it. In essence, the vendor would be able to force any transport protocol through SSH, effectively bypassing your firewall and your intrusion detection sensors. SSH is also an interactive protocol which can give a user the ability to actually control a remote system.

To use SSH or any encrypted transport protocol securely between your company and a vendor:

- Have the transmission end at a DMZ at the edge of your network.
- Have an interior firewall that separates the DMZ from the rest of your company's internal network, thus protecting your other resources.
- Ensure that host-based intrusion detection is installed on the systems in the DMZ to which your vendor has been given access.
- Have the servers only accept inputs from expected protocols and turn off any unnecessary listening ports.
- Give your vendor the least privileged access that is necessary for them to perform their required duties.

There is more, but this is an article and not a book.

For the information security officer, an understanding of data privacy laws is also required because in many instances, it is the combination of certain data elements that presents the greatest risk to an organization. For example, the risks to a company are greatly increased when the data elements include both customer names along with other pieces of identifiable information such as their social security numbers. There are many data privacy laws that require disclosure in the event of a breach of sensitive data. It is also necessary to know that in most cases these laws have an exemption to their disclosure requirement if the data was encrypted. This exemption is not absolute and protection of the encryption keys themselves is an important consideration. As with the concept of least privileged access, if certain sensitive data elements aren't required, don't use them.

## **Deviations from Security Policy**

Remember that security policies are high level and were not handed down by Moses. A deviation from a policy doesn't necessarily mean that a given effort has a high level of risk. An accurate risk assessment needs to look at a situation on a comprehensive level in order to see if there are any compensating controls that would mitigate the risk introduced from the policy deviation. For example, many would say that a weak password would constitute a high risk. However, it is important to take into consideration what type of access is granted by the password. There's a huge difference between being given access to a large database that contains millions of customer records and a stand alone system that only stores marketing brochures.

The best decisions are always fully informed ones. The more accurate your risk assessments, the better decisions you'll make on whether they should be remediated or accepted as is.

*Philip Alexander is the author of the book [Information Security: A Manager's Guide to Thwarting Data Thieves and Hackers](#) published by Greenwood Publishing*