Building a business case for Mainframe Security - Detailed Abstract

Submitted by: Meenu Gupta,CISA,CISM,CISSP,CIPP

Date: 04/28/2010

Mainframe security sounds more like two words that don't belong together then a topic that must be taken seriously. We all believe mainframes to be inherently secure. After all, how many of us have heard about mainframes being involved in those famous privacy breaches and hacks? Even the NIST controls don't talk much about Mainframe security. So what's the evidence to suggest anything but the fact that Mainframes are built secure?

One has to wonder whether this perception is due to blissful ignorance or based on some solid evidence?

After all, one rarely hears about mainframe involvement in major security breaches. Take for example the T.J. Maxx hacking case, one of the largest data breach by far. In 2007, retailer T.J. Maxx announced the discovery of a "computer system's breach' and the suspected loss of millions of credit card records. As the world would learn later, the breach involved over 45 million customer records and went on for a number of years undetected.

The exact chronology and nature of the breach was never made public (understandably), however, this is what went down on the internet as people conjectured and debated:

From internet posts, 2007:

""It's not clear when information was deleted, it's not clear who had access to what, and it's not clear whether the data kept in all these files was encrypted, so it's very hard to know how big this was". Deepak Taneja, CEO, Avesco

"Numerous companies still have not secured data for various reasons, some of them technical, " said Payment Card Industry (PCI) certified auditor Nigel Tranter. "Encrypting data on a mainframe is difficult, for example."

" a. How many run z/OS with 3 consecutive bad passwords = revocation of account (or some similar low number)? b. How many have a challenge system that must be passed before the account can be re-activated, and includes mandatory change of password". Steven Thompson

The writer goes on to say…

"...but where does it say that a mainframe was specifically the portal through which the cracking took place?"

This last statement goes right in to the heart of the debate. Mainframes are seemingly fortified so what happens inside a mainframe no one knows. But that's not enough assurance to be able to conclude that nothing bad happened.

In the last 40 years, since the advent of mainframe computers, security paradigm has changed dramatically. With the inclusion of Privacy Considerations into the discipline of Information Security, the new paradigm forces us to deal with risks that apply to any and all computing platforms including the mainframes. Later on we will see what some of these risks are.

So with more than 10000+ mainframes still processing data around the world, the topic of mainframe security could hardly be ignored. It should also not be ignored because mainframes process some of our most sensitive data including our Tax records, our Health records, and our Credit card records.

So what are we doing to protect it? That's a question those Compliance Officer should ask of themselves who are responsible for meeting the regulatory compliance with laws such as the FISMA, GLBA, and HIPAA.

Hopefully they already realize that security in not just about the technology but also about the integration of technology with processes and humans. The proverbial security crack is really almost always at the seams, otherwise known as "integration points". And with mainframes integrating with the web services, there are many integration points to consider.

The topic of mainframe security has also been addressed in a recent research study conducted by the Stevens Institute of Technology. The study concludes that "…the Enterprise (mainframe) Computing suffers from the same risks as the mid-range or mini-rage computing does, especially in today's web-centric computing environment".

As mainframes have become a major component of SOA (Service-Oriented Architecture) architecture due to their vast storage of data that has been collected over the year, they became exposed to malware and vulnerabilities as related to the HTTP, HTML and SOAP protocols. The introduction of Web services on the mainframe has had a significant impact on security.

For those, who are still not convinced about the need to focus on the mainframe security, the following list of vulnerabilities may help:

- Disclosure of privileged information
- Loss of physical assets
- Loss of intellectual property
- Loss of competitive advantage
- Loss of customer confidence
- Violation of regulatory requirements

- Disruption of the computer infrastructure resulting in the inability to perform critical business functions
- Use of the computer systems as a launching pad for malicious activity against other entities (and the potential to be held liable for their damages)

Source: www.isaca.org (z/os security audit/assurance program)

More often than not, Enterprise Computing relies on a reactive security model and attempts to control the mainframe security risks with piecemeal solutions. Having a full view of what mainframe security currently looks like will certainly help visualize the "To be" state and will help organizations meet their regulatory requirements and keep our data secure.

As organizations get a deeper look at the mainframe components and their various security requirements, the need to view the mainframe security systematically becomes apparent. This presentation will highlight those security requirements from a study that was recently conducted by the Stevens Institute of Technology.