Title: ITIL Service Management - Bible For Managing Information ... (Finance, Banking, Insurance)
Content Type: Article
Creator: Jody Pellerin

Operating in the highly regulated banking and financial industry, awash in rules for engaging in business, you must also remain accessible to your customers while maintaining the tightest information security. ITIL information security management provides a framework to support both compliance and security while still efficiently taking care of your customers.

Astute financial institutions such as [*Client* names] turned to [*Company Name*] to help them implement and maintain information security without slowing down business.

Doing Business in Cyberia

Given enough time, a determined thief can break through nearly any security. The online world is still trying to catch up. One of the biggest threats right now is High Roller, where the perpetrators identify and target only large consumer and corporate accounts. The Wall Street Journal explains how it happens:

Operation High Roller is characterized by extensive automation. The compromised employee computer interacts with a server controlled by criminals and much of the processing of transactions is done on the criminal's server, which makes it easier to hide and bypass corporate security software. All of the instances that involved High Roller malware could bypass complex authentication including so-called two factor authentication that use smartcard readers to generate a one-time password.

In other words, you need to not only fortify your defenses but be able to quickly identify when and where those defenses have been breached.

Consult the Bible of ITIL®

ITIL service management is a framework to guide effective, efficient, and secure computing practices. All C2 Innovations solutions are ITIL compliant plus we offer training in using ITIL in your information security strategy. This same level of protection is also recommended by the FFIEC in a 2011 supplement responding to the growing sophistication of cybercrime.

ITIL, while not strictly a standard, still offers recommendations to protect information using a layered approach. Multiple tools are chosen to provide compliant and safe authentication, building integrity through digital signatures and hashing. While each individual tool may have a weakness that can be exploited by malware, another tool is also in place that can bolster that weakness and bolster the system from attack.

But the protection does not stop there. In the event the data is compromised, a truly secure system will detect and respond to the threat in real time. Files that have been changed are marked to show unauthorized incursions and changes. This same capability is used to ensure that original files, in their entirety, have arrived at the transfer destination without change.

Serving Your Customer

Title: ITIL Service Management - Bible For Managing Information ... (Finance, Banking, Insurance)
Content Type: Article
Creator: Jody Pellerin

It may seem that all these additional ITIL information security management practices will take time away from serving your customers and allowing them access to their accounts. On the contrary, these solutions help you find the sweet spot at the intersection of high security and high access. Being safe doesn't have to mean bogging the system down with endless challenge questions, difficult password policies, or other complex identification practices.

Instead, your customers can enjoy the same level of service you have always given them with the assurance that their data is as safe as you can make it. [*Company Name*] stands ready to help you make it happen.

Call one of our specialists to learn more.