

Finding a Balance between Security and Convenience

There are instances when security can be inconvenient, as well as convenient. For example the recent FFIEC requirement for multi-factor authentication is, in some instances, placing a burden on bank customers when they have to prove their identity. This is clearly inconvenient. However, if you consider that strong authentication allows customers to do banking from home instead of going to a branch, it is clear that multi-factor authentication affords convenience. That is the explicit role of information security, to enable us to do things with information that we couldn't or shouldn't do otherwise. Another example would be sharing Microsoft Office documents over e-mail. E-mail allows us to transmit documents in near real-time to other parties, and the quality of the document remains intact compared to other alternative methods, such as faxing. However, SecureWorks is tracking and protects against three zero-day vulnerabilities in Microsoft Office that allow a hacker to embed malicious software in a word document and take control of any machine that opens the document. Security can help us here as well, by inspecting all documents before they are opened either in a network gateway or desktop. This way, we can continue to share information making us more cost effective and increase the quality of our services.

The best security plan is one that is as transparent to customers, employees, and system and network administrators, as possible. This means security is part of the culture and environment where we and our customers can operate and know that we are protected. Making security the responsibility of everyone gives ownership of the problem and lets users and customers feel like they are taking steps to secure themselves. In this environment, organizations make better decisions due to better access to readily available information. This means we need to build security into the information infrastructure from end to end in order to protect banks from external and internal threats. Data security specifically resolves the gold standard of authentication, authorization and auditing (They all start with au which is the atomic symbol for gold).

With over 1,600 clients, SecureWorks has become the largest managed security services provider safeguarding more financial institutions than any other vendor. SecureWorks provides the most effective security services by leveraging its integrated security management platform, advanced security research, and 100 percent GIAC certified experts. By providing a full breadth of security services, SecureWorks can offer fully-managed, co-managed or self-service security solutions to meet the needs of Fortune 100 companies with large security teams as well as smaller companies with no security expertise. In addition, SecureWorks has helped companies pass over 1,400 compliance audits by providing comprehensive and straight-forward board and examination reports. SecureWorks won SC Magazine's 2006 MSSP of the Year and Best Intrusion Prevention awards, Frost & Sullivan's 2006 Entrepreneurial Company of the Year award and was named to the Inc 500 and Deloitte & Touche lists of fastest-growing companies for the past two years.

Secureworks works to protect against threats via a risk management process that includes prevention, detection and response. Risk management helps drive processes that determine what the threat is to the data you are trying to share. Prevention is done through a proactive process, one which is developed through learning about assets, vulnerabilities, exploits and adversaries before you are attacked and by putting countermeasures in place to keep you protected. Detection and response is critical to make certain that if an incident occurs we can keep your data safeguarded with the appropriate response.

SecureWorks designs and implements security services around the philosophy that "information security should not get in the way of the business and secondarily, you should not let anyone else get in the way of the business."



Jon Ramsey
Chief Technology Officer

Jon Ramsey is Chief Technology Officer at SecureWorks in Atlanta, GA. Ramsey has 10 years of hands-on experience at every level: system administrator, software engineer, analyst, security penetration specialist and senior engineer. Prior to joining SecureWorks, Ramsey was a member of the Computer Emergency Response Team (CERT), and worked for Siemens International and the University of Pittsburgh. Ramsey earned a Master's degree in software engineering from Carnegie Mellon University and a BS in computer science from the University of Pittsburgh. He is a member of IEEE and the Association for Computing Machinery (ACM). SecureWorks is the credit union movement's leading provider of affordable Intrusion Prevention and security services.



Contact Info:

<http://www.secureworks.com>