Addressing Insider Threats, Cyber Attacks & Data Security

Banks would do well to follow best practices with a defense-in-depth strategy. This covers several layers of security with examples such as policies, procedures and awareness in the first layer. End-user security awareness is an important piece of your security puzzle because many attack types go after the end user (called social engineering) to succeed.

Next is defending the perimeter with a firewall and related tools to block intrusions. Follow that with internal network protection, individual computers, protecting applications and protection of the data itself with tools such as encryption. Your human resources are the weakest link and unfortunately, no amount of hardware or software can completely prevent the actions of a single user lacking security awareness from clicking on something they shouldn't.

The leading cause of data breaches is phishing or spear phishing and these threats are skyrocketing. Cybercriminals are getting better, users are sharing more information through social media, and some anti-phishing solutions' threat intelligence is not adequate. Users should be considered the first line of defense in any security infrastructure, and so organizations should implement a robust training program that will heighten users' sensitivity to phishing attempts and other exploits.

The danger point is the window of opportunity the cybercriminals are all too familiar with. Cybercriminals know there is a time lag between the time vulnerabilities are discovered and the time organizations get around to correcting the vulnerability. The criminals know to attack swiftly while defenses are down and the chance of detection is low.

According to a recent information security study, it takes organizations an average of 176 days to remediate known vulnerabilities. However, it only takes cybercriminals an average of 7 days to exploit known vulnerabilities. During the 169-day delta between vulnerability remediation and cybercriminal exploitation, your defense in depth layers may be at the mercy of your end user's level of security awareness education. On top of this, we have been seeing a window of several days before anti-malware providers can detect the newest malware strains.

KnowBe4 has become the world's most popular integrated Security Awareness Training and Simulated Phishing platform. Well over 2,500 enterprise accounts are using it, 25% of which are financial institutions. Based on KnowBe4's Chief Hacking Officer, Kevin Mitnick's 30+ year unique first-hand hacking experience, you now have a powerful tool to better manage the urgent IT security problems of social engineering, spear phishing and ransomware attacks.

Stu Sjouwerman
CEO

KnowBe4
Human error. Conquered.

Contact Info
www.knowbe4.com
Phone: 855-KNOWBE4 (566-9234)

Stu Sjouwerman (pronounced "shower-man") is the founder and CEO of KnowBe4, LLC, which hosts the world's most popular integrated Security Awareness Training and Simulated Phishing platform. A data security expert with more than 30 years in the IT industry, Sjouwerman was the co-founder of Inc. 500 company Sunbelt Software, a multiple award-winning anti-malware software company. Realizing that the human element of security was being seriously neglected, Sjouwerman decided to help organizations manage the problem of cybercrime social engineering tactics through new school security awareness training. KnowBe4, services over 2500 organizations in a variety of industries, including highly-regulated fields such as healthcare, finance, energy, government and insurance and is experiencing explosive yearly growth of 300%. Sjouwerman is the author of four books, with his latest being "Cyberheist: The Biggest Financial Threat Facing American Businesses."