# *Addressing Insider Threats, Cyber Attacks & Data Security*

Like all financial institutions, the reality of insider threats represents a serious security concern to banks. Whether it's an employee who unknowingly opens a phishing email or a contractor with access to privileged areas of a corporate network, insider threats are particularly insidious because they often remain undetected for an extended period of time.

Banks of course represent a highly attractive target given the significant amount of highly sensitive data that they house. And consequently, they have invested heavily in their security infrastructure over the years to ensure the integrity of their customer's data. In response to a more hardened perimeter, hackers have resorted to more sophisticated and targeted attacks such as spear phishing. Last year, in fact, the US Secret Service issued a warning in which they noted that they were seeing a "significant increase in the frequency, sophistication, and fraud losses" associated with these new attacks.

For financial institutions in particular, many spear phishing attacks take the form of Business E-mail Compromises, or BEC scams, in which the attacker attempts to impersonate a legitimate, usually high-level employee in an attempt to extort the user credentials from another employee. While these scams are nothing new, they have grown in sophistication, with hackers leveraging social media and professional networking sites such as LinkedIn, to identify those insiders that are to become targets. BEC scams can run the gamut from simple email spoofing of an email address to more complicated malware attacks in which they attempt to take control of a bank's entire email system.

One emerging standard that is proving highly effective against spear phishing is adding Domain-based Message Authentication, Reporting, and Conformance (DMARC) to your e-mail delivery systems.

The DMARC standard is designed to help with spear phishing by identifying and blocking, based on policy, the treatment of these types of e-mails that appear to be from trusted and even internal e-mail delivery domains. The most valuable aspect of DMARC is the feedback and the visibility it provides into both your authorized e-mail systems as well as all the failure reports generated by those campaigns initiating and trying to deliver spoofed e-mails. With this knowledge, you can improve your understanding and subsequent blocking of spoofed emails, reducing the chance of their success.

At Easy Solutions, we believe that a layered approach to security is the most effective way to identify and mitigate these and other types of threats. To this end, we have developed a full portfolio of products and services oriented to helping customers identify fraud at the earliest stages – from mobile fraud protection and authentication to transaction risk monitoring to our DMARC Compass solution, which allows organizations to identify different authentication failures in their email platform, proactively detecting targeted attacks and preventing these attacks from spreading so that attempts to compromise corporate 'insiders' are recognized at the earliest point in the fraud lifecycle.

**Daniel Ingevaldson**
Chief Technology Officer

EASYSOLUTIONS

## Contact Info

***www.easysol.net***
***866-524-4782***

**Daniel Ingevaldson** is Easy Solutions' Chief Technology Officer. With over 15 years of experience protecting some of the world's biggest organizations from next-generation threats, Daniel is our guru when it comes to developing fresh approaches to online security and fraud. As our CTO, he defines and executes the strategies for researching and creating the next phase of Total Fraud Protection® products. Daniel was co-founder of Endgame Systems, Inc., a startup focused on building advanced network security technology for United States government clients.