

### *Protecting Member Data at Rest and in Motion*

When it comes to security threats to credit union data, there are two separate security perspectives at play. The first one is, how is my credit union most likely to be affected? In my experience, the greatest threats to an individual credit union are most likely to come from internal sources. Employees who are disgruntled or desperate for cash can often find ways to cleverly circumvent technical solutions and get key information out of the credit union. Even though new threats are constantly emerging, ultimately it is the old fashioned non-technical components that often hold the biggest threat for an individual credit union.

The second question is, how is the credit union system most likely to be affected? In this regards, the high tech hacker threats still remain a critical concern because their attack methods are constantly evolving and improving. A multi-layered technical defense system from the perimeter down to the desktop is essential. While there is no silver bullet for securing sensitive credit union systems, a 'defense in depth' strategy that addresses technology, personnel and operations is the best course that any credit union can chart.

Solutions that prevent data leakage in a technical manner, firewalls & virtual private networks (VPNs) are some of the most important technical solutions that credit unions can deploy to effectively protect valuable member data from both hackers and disgruntled employees. Good hiring policies, ongoing employee training and social engineering testing are key to mitigating the human elements. Again, the overriding consideration is to combine well designed and maintained technical defenses along with non-technical approaches so that the credit union can successfully combat and neutralize both threats.

Ongoing Operations helps make credit unions more secure and protect member data by not adding to the situation. In our world class data centers, each and every credit union is isolated and all credit union data is fully encrypted with credit union defined encryption keys. Every solution requires the credit union's passwords and dual controls so that one person doesn't weaken the system.

In addition to these stringent measures protecting data at rest, OGO's VPN solutions encrypt and protect data in transit at all times. As a preferred partner and certified provider of Blue Ridge/Secure Virtual Ethernet Service (SVES), we are completely confident that credit union data in transit is secure. SVES utilizes the ubiquitous availability of the Internet and time-tested Ethernet to create a powerfully secure any-office-to-any-office high performance VPN. The SVES infrastructure creates 100% secure interoffice links able to carry data, VoIP, and video simultaneously.



**Kirk Drake**  
CEO



#### Contact Info

[www.ongoingoperations.com](http://www.ongoingoperations.com)

**Kirk Drake** is founder and CEO of Ongoing Operations and brings more than 15 years of experience in the Financial Services and Information Technology industries. After spending significant time leading Credit Union IT Departments and consulting on disaster recovery and business continuity issues, Kirk ventured into CUSO development in 2005. Leading a collaborative effort with 9 credit unions to the successful launch of a national CUSO, Kirk brings hands-on experience with launching multi-owned CUSOs, raising capital, and developing companies that leverage team work, collaborative values, and entrepreneurial spirit. Ongoing Operations now works with over 60 credit unions and is owned by 17 credit unions and a CUSO.