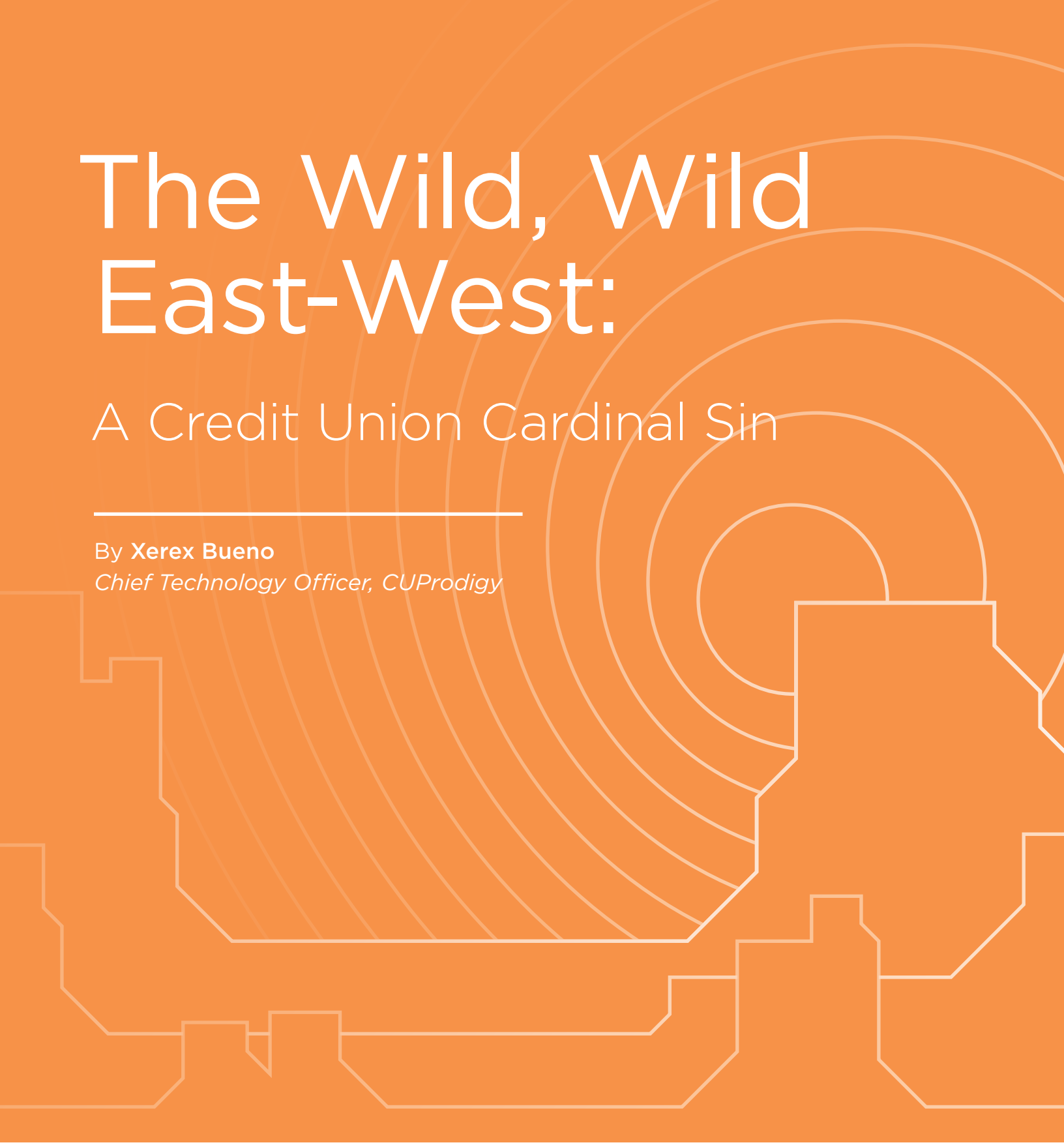
The Wild, Wild East-West:

A Credit Union Cardinal Sin

By **Xerex Bueno**
Chief Technology Officer, CUProdigy



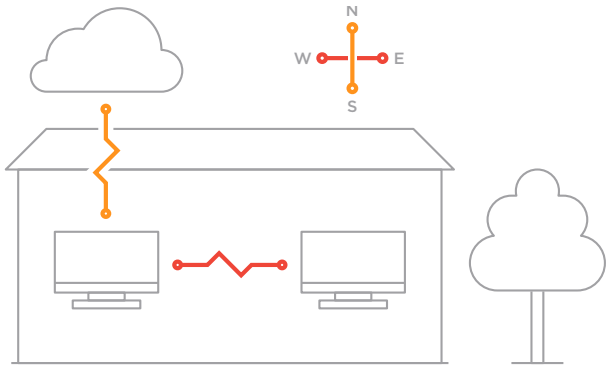
CUProdigy™

East-west traffic occurs when devices communicate with each other without leaving your credit union network

PLEASE, DON'T BE A MERE NORTH-SOUTH CREDIT UNION.

Why? It's not enough. It's fractional security, at best. Regardless of asset size, your credit union likely has a computer network supporting the distribution of information inside, as well as outside, your credit union. This vital network traffic includes member data, transactions, email messages, web commerce and file transfers. Moreover, this network traffic is categorized into two types based upon the cardinal directions of *north-south* and *east-west*. Ignoring east-west traffic can be deadly. In fact, Dictionary.com defines a *cardinal sin* as an unforgivable error or misjudgment.

North-south traffic is traffic that leaves and/or enters your network. A common example of this type of traffic is when you access a website. In this example, your traffic leaves your computer headed north (outward) to the Internet and then returns south (inward) back to your computer. North-south traffic that travels between employees in a branch office and a data center hosting an external system is a credit union example.



The other type of network traffic is east-west traffic. This traffic is where machines and devices communicate with each other – without leaving your credit union network. This traffic is the internal, lateral traffic from machine to machine. An example of this type of traffic is when you print a document to a networked printer. Here, the traffic leaves your computer and goes directly to the printer without escaping your network. Another example of east-west traffic is an application server, which provides your credit union employees access to data that lives on a separate database server inside your network. An in-house implementation of a core system would typically fall into this east-west category.

So why explore the cardinal differentiation in network traffic? One is volume. East-west network traffic makes up more than 75% of all traffic occurring on a typical network. Most of your credit union network traffic is moving from machine to machine and server to server on the inside. The other is security. East-west network traffic presents unique information security challenges that can be difficult to address within your credit union walls. Once inside, a threat can be hard to stop. Picture dominoes arranged in a nice, neat line. When one goes, they all go. Ugh. It's time to update the resume.

Of course, malware threats are not new and most credit unions are aware of them in the north-south setting. North-south threats are what credit unions tackle. They do this through installing properly configured and actively managed traditional firewalls. Such firewalls protect their member data from unauthorized access or theft from external threats. That's nice, but lacking. East-west traffic needs protection too and it's more difficult to secure; there is no real cost effective solution. Wide-open east-west traffic can leave a credit union vulnerable to attack from inside, as well as any threats from the outside that bypassed the firewall. A successful malicious attack on one server can spread without restraint to others. To prevent this domino effect and the need to dust off the resume, credit unions need to secure north-south and east-west traffic. Ignoring east-west traffic is a cardinal sin.

East-west network traffic makes up more than 75% of all traffic occurring on a typical network

Yet, you might ask how a north-south threat could bypass a firewall? That's a great question. Frankly, next-generation malware continues to evolve and is increasingly difficult to detect and stop. It's a game of cat and mouse between information security companies and cyber criminals. Moreover, depending on the threat, malware can discreetly hide within encrypted traffic that traditional firewalls can miss. A threat-miss can cause havoc in a network and leave significant damage. This is why protecting your east-west traffic is so important. East-west protection is designed to isolate and prevent the spread of a threat. Think of east-west protection as a circuit breaker, or a "man-trap" for armed and dangerous code.

Now, let's examine some examples on securing credit union east-west traffic. Take the example above where a credit union has an application server that needs to communicate with a database server. For the application server and database server to communicate, they typically require a set of communication ports. This is the channel to move data back and forth. First, next-generation firewall technology leverages security policies that only allow specific traffic to move across those ports between those servers. All other traffic is blocked. Second, because the specific type of traffic is known to be database in nature, additional scrutiny filters in the security policies inspect the network traffic for any signs of malware and other threats. Identified threats or irregular traffic are blocked. These blocked threats can also trigger alert notifications for an immediate response. It's a concept of compartmentalizing credit union servers to achieve isolation.

Let's combine north-south security with east-west security. To do so, let's take another example that is relevant for most credit unions. Home banking and mobile banking systems travel across the Internet and such traffic is typically encrypted. Encryption is great for protecting member data, but it can also hide malware. Advanced firewall technology allows deep inspection of encrypted north-south traffic tied to member facing systems, such as home banking, mobile banking, email, and web. In short, a credit union with next-generation firewall technology can identify advanced malware and other malicious threats before they enter the credit union's network. Only once traffic is vetted to be threat-free will it continue into the credit union's network. And once it's

into the credit union's network, the east-west traffic pattern takes over. Again, the same inspections occur ensuring that traffic is free of any malware and other damaging threats, and that member data is protected.

Having this level of control and visibility into network traffic is a benefit that cybersecurity minded credit unions should embrace. As threats continue to evolve, so must a credit union's approach to security. Layered security and concepts like "circuit breaker" isolation are paramount to providing solid protection around your member data. So what should a security minded CEO, CFO, or CIO do? A credit union should secure not only their north-south traffic, but also their critical east-west traffic. Next-generation firewall technology does exactly this and is a prudent step toward protecting member data.

Yet, this type of cybersecurity can be expensive. Next-gen firewalls with north-south and east-west capability will require a minimum investment of $50K, and can go up from there based upon credit union size and complexity. That also doesn't count the installation or the salary required to maintain these state-of-the-art firewalls. Then, if that's not enough cash outlay, firewalls should be replaced every three years. Between hardware, software licenses, and staff, the total three-year cost could be in the range of $200,000 to $300,000. That same security minded CEO, CFO, or CIO now has sticker shock, and unfortunately, many credit unions simply cannot afford it.

Next-gen firewalls with north-south and east-west capability will require a minimum investment of $50K

While great cybersecurity isn't cheap, it can be done more affordably through a CUSO. An investment in next-generation firewalls can be leveraged across multiple credit unions to create economies of scale. This is where CUProdigy can help. Our cloud solution is designed and built, not as a product, but as a solution. We fully understand what credit unions require from both a security and cost standpoint. CUProdigy's approach to next-generation firewall technology will help protect your credit union servers and member data from north-south and east-west threats at a reasonable price. CUProdigy can help increase your credit union's security posture without adding significant cost or being burdened with managing an advanced security platform. In short, cybersecurity minded CEOs, CFOs, and CIOs no longer have to choose between next-generation protection of member data and ROA.

Our cloud solution is designed and built, not as a product, but as a solution.

Xerex Bueno has worked several years in the credit union industry, created public and private cloud strategies, and has been a member of the U.S. Army Cyber Network Defense team.

CUProdigy is a CUSO that blends the combined power of an adaptable, user-friendly, and modern core architecture, with full-service cloud managed services. The CUProdigy community exists to empower our credit union owners to participate in the direction, evolution, and design of our innovative products and services.

www.CUProdigy.com
(801) 335-5084
elevate@CUProdigy.com

CUProdigy™