VIEWS & VISIONS

A publication of Bowles Rice LLP

Summer 2015

Bowles Rice Information Security: Where Do We Stand?

Scott Ball, Technology Director
Bowles Rice LLP

Scott Ball is Bowles Rice's Information and Technology Director. He is responsible for overseeing all aspects of the firm's technology, including computers, video and telephone systems, security and disaster recovery/business continuity.

Scott joined Bowles Rice in February 1992 as a technologist, providing helpdesk support and training. He has served as administrator of UNIX, Linux, Windows and Novell systems and SQL Server and Informix databases. He also has provided Intranet and Internet support and administration, and is experienced in HTML, ASP, VBScript, Visual Basic and Crystal Reports.

He is a 1991 honors graduate of Marshall University with a bachelor of science degree in computer science. Prior to joining Bowles Rice, Scott taught adult education courses for the Putnam County Board of Education.

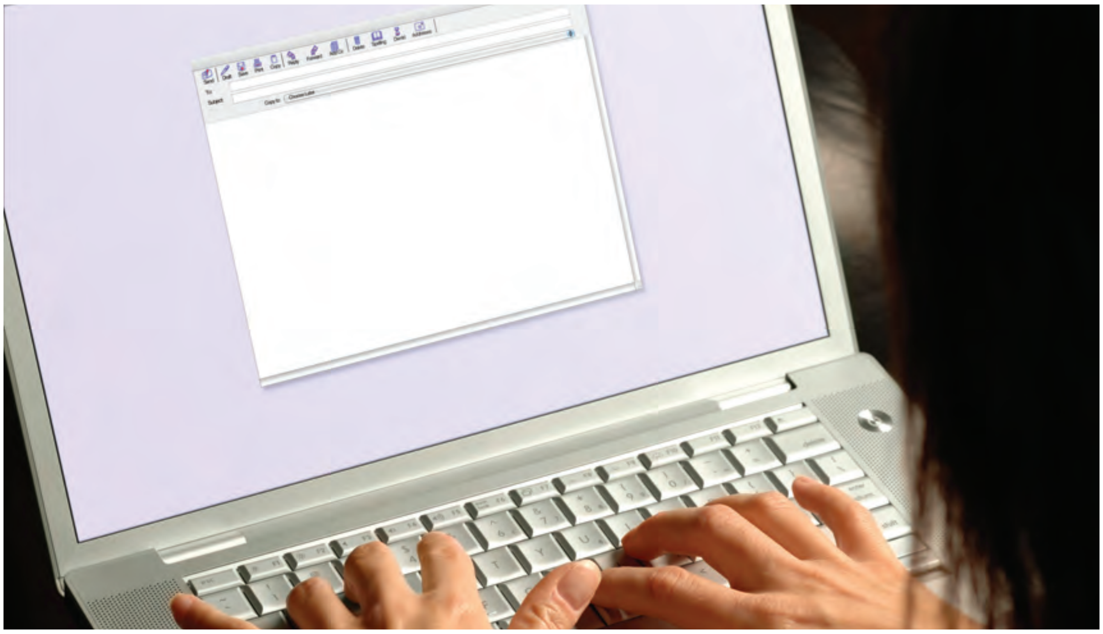
Headlines in recent months blare with data breaches and security worries. Oftentimes, those administering the breached systems have followed all recommended guidelines and procedures, yet their systems were still compromised. Recognizing the challenges we face, Bowles Rice continues to take a proactive stance on security and privacy. We strive to provide high-quality, highly secure services that meet the expectations of our clients. When asked by our clients to provide our current position on security or how we are responding to an ongoing security threat, we must be able to provide accurate answers that meet their requirements and expectations. Compliance failure could have a negative impact for both the client and Bowles Rice.

To that end, 2015 is an important year for Bowles Rice in the area of security. A Network Security Engineer has been hired. Our team is evaluating new tools to enhance security in email communication. We are continuing to train our users in the area of security.

The addition of a Network Security Engineer allows us to focus greater attention on the security of our systems and data. It allows us to have full-time focus on current threats, evaluate and implement mitigation and response strategies, and take appropriate and timely action when needed. This will help ensure best practices in security are in place and maintained across all locations and systems. It also helps ensure software and operating system updates are thoroughly tested and installed in a timely manner across all systems and offices.

One of the greatest challenges businesses face is the use of social engineering to entice a user to make a decision that could have great impact on a system or business, such as clicking on a link in a very well-prepared, yet fake, email. Studies show the best way to overcome these challenges is to provide appropriate security-related end-user training. While it is important to have proper protection in place for our systems, such as firewalls, virus detection systems, logging, penetration testing, etc., proper security awareness training remains at the top of the must-do list.

Another obstacle all businesses face is the ability to provide a secure environment while providing



ease of use for end users. Far too often, users would rather sacrifice security and safety for convenience. It's convenient to use a basic, consumer file-sharing solution over a secure enterprise solution, for example. Fortunately, more enterprise tools are coming to market that provide the necessary security – such as encryption in transit and at rest, along with convenience. We continue to explore such solutions.

Email is inherently insecure by nature as the body of an e-mail is clear, readable text. The ability to encrypt an email helps overcome this issue. We have the ability to provide secure email communication through Transport Layer Security (TLS). Our mail server is opportunistic TLS capable and will automatically use TLS when the recipient's mail server is also opportunistic TLS capable. While the TLS scenario is not always available, over the coming months we will strengthen our position by implementing a tool to provide ad-hoc secure, fully encrypted email communication.

Another important area of consideration is user access and authentication to our systems. The standard password, the password that many users love to hate, has outlived its usefulness in many cases. Two-factor or multi-factor authentication are becoming more prevalent through tokens, SMS messages and smartphone apps. Biometrics are also gaining momentum with many mobile devices or laptops providing voice recognition and fingerprint authentication. We are investigating how we can bring these types of authentication into our environment. Further, we are implementing full disk encryption (FDE) on all of our laptops as another layer of data security.

Mobile devices are also an area of concern. Before adopting a Bring Your Own Device (BYOD) policy, we had to have a way to manage the devices our users would purchase. A Mobile Device Management (MDM) system provides the necessary means of managing mobile devices. Before we allow any information to sync between our systems and a device, the device must be added to our MDM with no exceptions.

Handling our devices in this manner allows us to know exactly what is connected to our system, as well as provide a means of properly wiping a device in an emergency. Each mobile device in our MDM is encrypted as part of the setup for this system.

What does the future hold? Unfortunately, more of the same. We do not anticipate these challenges will go away anytime soon. We will only see more attempts to socially engineer a user, exploit a system and destroy data. We must continually take steps to prepare for what is happening and what will happen. Zero-day attacks, which exploit a previously unknown vulnerability that has not been patched, remain a constant threat, for example.

It is important to evaluate who has access to our systems and who is in our systems. An Intrusion Detection System (IDS) and regular monitoring of our systems are key to heading off potential threats and exploits. Other key components include a strong password policy and a review of who has access to the files in our systems.

Finally, we must also position ourselves for expanded use of cloud services. As vendors drive more of their products to the cloud, we must ensure we maintain the level of security we have with our on-premises deployments. Encrypted communication between on-premises data centers and cloud deployments, data encryption for at-rest data, user identity and access, bandwidth and proper monitoring of systems are just a few of the areas that must be considered. V