Report of the JMU Faculty Senate IT Security Task Force

February 26, 2015

Members of the Task Force:

- Dr. Tim Louwers (Chair), Professor of Accounting (present member of the JMU Faculty Senate) is a Certified Information Systems Auditor who has written article on a wide range of accounting, auditing, and technology-related topics.
- Dr. M. Hossain Heydari, Professor of Computer Science (present member of the JMU Faculty Senate) serves as the Director of JMU's Graduate Information Security Program, and has teaching and research experience in telecommunications and networking security.
- Dr. Edna Reid, Associate Professor of Intelligence Analysis, came to JMU after a number of years as an intelligence analyst at the FBI. Her research interests focus on cyber intelligence (strategic analysis of cyber threat environment), and she is conducting research in cyber intelligence tradecraft and designing new methodologies for analyzing cyber environment, cyber threat actors, and cyber deception.
- Dr. Tammy Castle, Associate Professor of Justice Studies (past member of the Faculty Senate) has a primary teaching and research focus in crime and criminology.
- Dr. Michael Kirkpatrick, Assistant Professor of Computer Science, has primary teaching and research interests in access control, operating systems, and computer security.

The Task Force met with JMU IT Security (Dale Hulvey, Assistant Vice-President for Information Technology; Darlene Quackenbush, Information Security Officer; Gary Flynn, Lead Security Engineer; and Jack Knight, Associate University Counsel and Virginia Assistant Attorney General) for two hours on Friday, February 20, 2015, in response to the information security breach disclosed in December 2014. A candid discussion of the breach took place, but confidentiality was requested due to the nature of the ongoing investigation involving federal law enforcement, as well as a private consulting firm (Mandiant) specializing in these types of investigations (paid for by JMU's cyber security insurance policy).

The breach started with a compromised employee account (perhaps through "phishing") that allowed outsiders unauthorized access to JMU network/system resources. Specifically, there is evidence that outsiders used a compromised e-ID and password to access a text file containing confidential employee information consisting of name, social security number, health ID#, and address, as well as other non-sensitive information that does not pose a threat to faculty and staff information security. Almost 2800 faculty and staff members were affected; however, no dependent information was contained in the file. Also note that there is no evidence that other critical and sensitive systems, such as Payroll Services computers, were affected or accessed. All those affected, including those no longer at JMU, have been contacted. Faculty and staff not receiving notification were not affected.

The Task Force asked very pointed questions about the breach specifically and JMU's IT Security practices in general, and left the meeting with the belief that JMU's IT Security follows best practices for information security and is pro-active in response to perceived or real threats to the University's information security. Upon discovery of the breach, JMU's IT Security quickly initiated an appropriate protocol to limit its impact, and they have since taken proactive steps to reduce the likelihood of similar breaches in the future.

In a subsequent meeting, the Task Force discussed the following issues:

- The Task Force believes that although JMU's IT Security response and notification were timely, clearer communication might have prevented misinterpretation by the JMU community. A faculty liaison or liaisons might provide useful feedback should future incident occur.
- JMU's cyber security insurance policy covers one year of credit monitoring for affected employees. Because of the recent Anthem breach, most JMU employees will receive an additional year of coverage. There may be some current and former employees not covered by Anthem who will not receive additional coverage. The Task Force noted that the benefits of the credit monitoring service are limited and that there has been no evidence that the information has been used to anyone's detriment. On the other hand, there is nothing to prevent the hackers from using the data at some point in the future beyond the covered period.
- The task force discussed the importance of cybersecurity education for members of the JMU community, including a CFI Flashpoint presentation and/or a presentation at the May Symposium.
- Given the access that faculty and staff have to confidential student and employee information, there is a consensus among task force members that faculty and staff members who fall prey to a "phishing" scheme should be required to complete relevant training as soon as possible. Task force members suggested immediately suspending IT privileges until the employee commits to the training; failure to complete the training within a limited time frame (such as two weeks) would result in suspension of IT privileges until the training is completed.