When Programs Collide - A Panel Discussion on the Competing Interests of Analytics and Security

Jacob Young  
*Bradley University*, jayoung@bradley.edu

David Biros  
*Oklahoma State University*, david.biros@okstate.edu

Ryan Schuetzler  
*University of Nebraska at Omaha*, rschuetzler@unomaha.edu

Paul R. Stephens  
*Bradley University*, prs@bradley.edu

Tyler J. Smith  
*Bradley University*, tjsmith3@bradley.edu

See next page for additional authors

Follow this and additional works at: [https://aisel.aisnet.org/mwais2019](https://aisel.aisnet.org/mwais2019)
When Programs Collide – A Panel Discussion on the Competing Interests of Analytics and Security

Jacob A. Young*  
Bradley University  
jayoung@bradley.edu

David P. Biros  
Oklahoma State University  
david.biros@okstate.edu

Ryan M. Schuetzler  
University of Nebraska-Omaha  
rschuetzler@unomaha.edu

Paul R. Stephens  
Bradley University  
prs@bradley.edu

Tyler J. Smith  
Bradley University  
tjsmith3@bradley.edu

Rhonda A. Syler  
University of Arkansas  
rsyler@walton.uark.edu

Shawn H. Zheng  
Bradley University  
hzheng@bradley.edu

* corresponding author

ABSTRACT (REQUIRED)

The increasing demand for business analytics and cybersecurity professionals provides an exciting job outlook for graduates of information systems programs. However, the rapid proliferation of devices and systems that has spurred this trend has created a challenging ethical dilemma for those responsible for educating future generations of IT professionals. Many firms are collecting and storing as much data as possible in the hopes that technology might uncover useful insights in the future. This results in an ever-increasing challenge for those charged with protecting organizational assets and exerts pressure on executives seeking an analytical edge to remain profitable in a hyper-competitive marketplace. With this dilemma in mind, the panel will search for a delicate balance between unleashing the power of analytics and securing the sensitive data it consumes.

Keywords (Required)
analytics, privacy, security, IS education

INTRODUCTION

The increasing demand for business analytics and cybersecurity professionals provides an exciting job outlook for graduates of information systems programs. However, the rapid proliferation of devices and systems that has spurred this trend has created a challenging ethical dilemma for those responsible for educating future generations of IT professionals. Despite daily headlines of data breaches and governmental inquiries into questionable behavior by some of the world’s most recognizable companies, the appetite for data is not slowing. Many firms are collecting and storing as much data as possible in the hopes that technology might uncover useful insights in the future.

This results in an ever-increasing challenge for those charged with protecting organizational assets and exerts pressure on executives seeking an analytical edge to remain profitable in a hyper-competitive marketplace. For example, even well-intentioned organizations might attempt to anonymize sensitive customer data, only to find out later that it was trivial for analytics to attribute the data to individuals. Others might rely too heavily on the promise of analytics, resulting in biased or incorrect interpretations. With this dilemma in mind, the panel will search for a delicate balance between unleashing the power of analytics and securing the sensitive data it consumes.
Potential questions the panel might explore consist of:

1. Is collecting everything ethical?
2. How do we train our students to recognize the difference between what we can do and what we should do when it comes to business analytics?
3. How can analytics professionals remain mindful of the privacy and security implications of big data?
4. How can analysts recognize and mitigate their own bias, especially when interpreting results?
5. How can organizations better communicate to consumers what data is being generated and how it is collected or stored?
6. How can security professionals help organizations resist the temptation to exploit the power of analytics to gain a competitive edge if it means putting the privacy of individuals and the organization’s reputation on the line?
7. Should the analytics profession adopt the pro-social principles of “white hat” security professionals?
8. How can analytics assist security professionals in protecting organizational assets?

REFERENCES