BloomCON Speakers

Speaker	Title	Abstract
Brian Martin	Charting a Path to the Ultimate Job	You've got a shiny new diploma or you've got a cubical you're tired of looking at. In both cases, you need to get a new job, but how? And what can you do if the job you really want is out of reach? How do you get from where you are, point A, to where you want to be, point X? We start with real job descriptions on the market currently and review requirements then walk through charting a path to several destinations from several starting point to provide the inexperienced job hunter with a methodology and strategy to landing the perfect job.
Nathan Cooper Joe Oriel	Getting Started with Web App Pentesting	This workshop is about getting started with Web App Pentesting. Starting with why we test, tools, methodology, and a few basic exploits. In the end attendees will at very good starting point to break into the web app security testing arena. We will also be providing a ton of resources to help build there skills from zero to hero.
Kristy Li Ayesha Rivzi Natalie Martinez Renee Xu	Security, Privacy, and Forensics in the Application Development of Logros	Logros is a web service that helps its users organize a project interactively from beginning to end.
Amber Welch	Breaking Into Tech from the Humanities	If you regret choosing a humanities degree and have tech FOMO, hope is not lost. Switching to a tech career from a language, arts, philosophy, or other "fluffy" background might be intimidating, but is achievable. This talk covers how to target a new career path, prepare for the switch, strategize career progression, and manage industry bias against humanities majors and tech newcomers. Some examples are specific to women, but the concepts apply to all. The discussion dives into anxiety-inducing topics such as finding a crossover entry point, the pros and cons of incremental career moves vs. one big leap, using your current job to prep for the next move, repackaging your humanities experience into tech terms, and avoiding the job hopping stigma during rapid changes. Bonus: get your daily dose of schadenfreude through personal examples of career mistakes and bad ideas.
Ben Tice	Make Buzzwords Great Again	The goal of the talk is to provide students and professionals with a practical, grounded (hype free) understanding of how the data mining process, "big data" technologies, and machine learning algorithms can be used in Security and Digital-Forensics/Incident-Response (DFIR). The talk will explain the concepts and how each applies to security and DFIR, then go into

		practical examples of data visualization, anomaly detection, classification, and link/graph analysis. Each example will tie to a specific challenge in security such as alert triage, log review, detecting unusual behavior, and hunting for lateral movement.
Chris Silvers Kris Silvers	Capture the Fail: Avoiding Pitfalls When Running your CTF	Is it possible to contribute to the security community without dropping an 0 day or coding the next nmap? How about running a CTF? Kris and Chris Silvers, creators of the OSINT CTF, share some lessons learned along their journey. They've run into some interesting problems — like their scoring engine's exploitable vulnerabilities to targets changing their attack surface mid-competition — and met them all head-on. Laugh along and learn something as they walk through their toughest challenges and how they handled them.
Daniel Pany	Red Teaming From a Blue Teamer's Perspective	Ever wonder how a red team is able to perform some of their sneaky tactics, techniques, and procedures (TTP), such as during a Collegiate Cyber Defense Competition (CCDC) or by a real-life threat group? I am no red teamer, but I was asked to set up a virtual cyber defense competition to help Bloomsburg students practice for CCDC, and I had to make the blue team systems intentionally vulnerable. In this presentation, I'll walk through different routes a red teamer might take to initially compromise my blue team systems, escalate privileges, maintain persistence, and achieve all of their objectives.
John Riley	Stings in Executables	In this talk we discuss how strings occur in executables (mostly in PE format) and the problems and limitations of doing string searches.
Michael Sitler	The Evolution of a Ransomware and a Look Ahead at Emerging Cyber Threats	Hospitals across the United Kingdom are crippled. Power distributers throughout Europe experience wide-spread system outages. The world's largest shipping conglomerate comes to a halt. City governments in the United States resort to pen and paper after being taken completely offline. What do all of these stories have in common? Ransomware. In this session, we will discuss the evolution of ransomware and look ahead at emerging cyber threats.
Alex Muentz	Your cybersecurity career – getting in, staying in and making mistakes	Cybersecurity is a booming job market right now. What makes someone good for this career? What are employers looking for? What types of skill sets and experience are good to develop? What does it take to convince an employer that you can do the work even if you don't have the experience?
Bill Barnes	CIS Controls – First 5 CIS Controls – Where do you start when you don't know	About 6 months ago, I got a call from a brand new Information Security Manager at a place that never had any focus on Information Security before, and he asked me "my opinion and any guidance on where to start". I introduced him to the CIS (Center for Internet Security) Controls, and specifically the first 5 CIS controls (aka "the critical security controls"). This is not specifically a compliance framework, however, this is a great place to get started if you have compliance framework requirements (they link!), and it has been my opinion that

		following all of the CIS Top 20 Controls will dramatically improve an organizations security posture, and continue to move you towards your security goals.
Aaron Young	Retro Video Game Reversing	Retro video game reversing workshop covering Atari and others.
Brendan Munro Joe Kirwin	The emperor's old clothes: visualizing ssdeep	We were excited to review and potentially implement ssdeep for some fuzzy-hashing in a project we are working on. So we read the paper, then the papers referenced by it, then anything else we could find on it… nobody said why the rolling-hash algorithm works, where it came from and whether it is optimal or can be improved upon!
Stephen Larson	POS systems: The Good News and the Bad News	POS systems are supposed to follow the Payment Card Industry Data Security Standard (PCI DSS), an information security standard for organizations that handle branded credit cards from the major card schemes. The PCI Security Standards Council sets standards that cover technical and operational system components included in or connected to cardholder data. One of the standards is to protect card holder data, which includes encrypting the card holder data at rest and in transit. This talk will discuss a project in which three POS systems used in restaurants and a catering company were examined to ensure they are compliant with PCI DSS, and deliver both the resulting good news and the bad news.
Korey Young	Phishing Github users with old blog posts	Blog posts can be "post it and forget about it" for an organization. But what happens when a website that is linked to in a blog post gets abandoned, and becomes available for purchase? Now, an attacker can get control of the abandoned domain and use it for phishing. "Hey user, click this link in this company blog post".
Benjamin Brown	More Than Tor: Shining a Light on Different Corners of the Dark Web	When the terms darknet or dark web are invoked it is almost always in reference to the Tor network, but what about the other extant darknet frameworks? A true understanding of the dark web would be impossible and misleading if it only included the Tor network. In this talk I will expand the field of view to include frameworks such as Freenet, I2P, and OpenBazaar. We'll take a quick look at the origins and technical underpinnings of these darknets as well as their actors and offerings. I will also discuss the differentiators that set these networks apart from Tor and highlight why they too should be included in modeling our knowledge of the dark web. Audience members will walk away with a fuller understanding of the internet's hidden corners, the goals of its users, and the technologies that help keep them in the dark.
Sean Goodwin	No One Secures it Alone: Engaging your staff in the fight against cyber criminals	So you think you can stop the attackers? Guess what? You can't, at least not alone. Even the best coders, hackers, or computer geeks don't stand a chance protecting their company alone. The soft-skills required for running a successful and engaging security program are too often overlooked.

Larry Snyder	Human Error is not a Security Failure	A long-standing cybersecurity mantra is that humans are the weakest link in any cybersecurity program. This talk will examine this mantra and discuss an alternative understanding of human errors. Humans interact with nearly every piece of technology within an organization. Human-technology interaction is a normal part of every computer operations and by extension a regular part of business operations. These interactions manifest themselves in many different forms including; system and software development, system deployment, network administration, and end-user activities. The high rate of these day-to-day interactions tends to mistakenly lead individuals to see a causal relationship between humans, technology and security incidents.
Diane Barrett	TBD	
Philip Polstra	ARM Assembly Workshop	Intro to Assembly on the ARM platform. The BeagleBone family of boards will be used.
Adam Creasy	Drone Workshop	
Michael Daugherty	Cybercriminals, Politicians, and Bureaucrats: What could possibly go wrong?	The early years of his entering and fighting Washington, DC, are recorded in his book, "The Devil Inside the Beltway". In so doing, he has become the only litigant to challenge the basic authority that underlies more than 200 enforcement actions relating to cybersecurity and online privacy that the FTC has brought over the past 15 years. Every one of the 200+ litigants before him – including some of the largest companies in the world – have settled with the FTC, creating an unquestioned and untested belief that the FTC has broad authority to regulate in these areas. On June 6, 2018, he prevailed. In so doing, he toppled key pillars of the FTC's cybersecurity and online privacy edifice, successfully exposing and challenging The Administrative State. Mike is committed to our Founding Fathers' principles regarding the separation of powers, so he demands fair notice, due process and accountability. Mike seeks to educate and demonstrate how these principles are sorely lacking in DC today.