Sponsor Testimony: House Bill 368
Representative Brian Baldridge, 90th House District
House Criminal Justice Committee

Chairman Lang, Vice Chair Plummer, Ranking Member Leland and Members of the House Criminal Justice Committee, thank you for allowing me to provide sponsor testimony in favor of House Bill 368, the Ohio Computer Crimes Act. The intent of this legislation is to reduce the frequency of cyber-crimes by updating and modernizing Ohio's computer crimes laws. This legislation is a follow-up to Senate Bill 220, enacted in the 132nd General Assembly, which provided an affirmative defense from civil action for businesses who proactively invest in a cybersecurity program.

I was made aware of the need to enact this legislation after meeting with my local credit union, headquartered in Portsmouth, OH, and the Scioto County Prosecutor. The CEO of the credit union, shared with us that a disgruntled former employee was caught attempting to break into their computer network, which holds the personal, identifiable information of their members. After a conversation with a local FBI agent, they were told the FBI is reluctant to spend resources prosecuting cases in which the attempted theft was prevented. Prosecution of cybercriminals at the county level is also a challenge because current Ohio law is damages-based, meaning the value of the impacted computer-related items determines the severity of the penalty.

The damages-based model is not reflective of the harm caused to businesses such as my local credit union during an attempted breach. To help Ohio prosecutors swiftly prosecute cybercriminals without trying to prove and calculate damages using limited and outdated statutes, House Bill 368 recognizes new categories of cybercrime and extends a variety of stricter charges for prosecutors to pursue. Of note, "computer contaminant" will be replaced by a general "malware" or "malicious software" definition that will not require us to keep up with the rapidly changing tools that can be used by a criminal to commit a hack.

Other key components of the legislation include making electronic data theft and electronic data tampering felonies of the third degree. An example of electronic data tampering would be a cybercriminal intercepting email exchanges between individuals and altering the messages in order to steal money or information. Electronic data theft would be more aligned with a person using a phishing e-mail to gain access to a computer network and stealing personal information. If that information is then disclosed without authorization on the Dark Web for example, the result would be a felony of the third degree.

Those negatively impacted by a breach, will be able to bring a civil action against a person convicted of violating the law and may receive compensatory damages, attorney fees or other equitable relief. There

is protection in the bill for “white hat” or ethical hackers, who are paid to test the security of a company’s firewall system. CyberOhio, a subsidiary of InnovateOhio, was helpful in making me aware of the need to include these protections in the bill.

As H.B. 368 moves through the legislative process, I look forward to hearing from interested parties on ways we can make improvements while ensuring bad actors are prosecuted. I want to thank my former aide, Bill White, for helping draft this legislation, as well as those that have been involved in the IP process.

I am happy to answer any questions.