CYBEROhio
An InnovateOhio Initiative

Proponent Testimony: HB 368
Senate Judiciary Committee, November 11, 2020
Kirk Herath
Vice President, Assoc. General Counsel & Chief Privacy Officer, Nationwide Insurance Companies (Retired)
Chair, CyberOhio Advisory Board

Chairman Eklund, Vice Chair Manning, Ranking Member Thomas, and members of the Senate Judiciary Committee, thank you for allowing me to provide testimony in support of House Bill 368. My name is Kirk Herath and I just recently retired as Vice President, Associate General Counsel, and Chief Privacy Officer at Nationwide Insurance Companies. I also have the privilege of serving as the Chair of the CyberOhio Advisory Board, which is under Lt. Governor Husted's InnovateOhio office.

I want to take a moment to give you some background information on CyberOhio and our role helping to improve Ohio's cyber-related laws. CyberOhio was created in 2016 by then Attorney General DeWine to help Ohio businesses defend against cybersecurity threats. The goal of CyberOhio is to help foster a legal, technical, and collaborative cybersecurity environment to help Ohioans and Ohio businesses thrive. The initiative has an advisory board made up of industry experts from across the state. We now provide guidance and technical expertise to InnovateOhio and Lt. Governor Husted on cyber-related affairs.

CyberOhio staff and advisory board members worked tirelessly on Senate Bill 220, known the Data Protection Act, enacted in the 132nd General Assembly, which provided an affirmative defense from civil action for businesses who proactively invest in a cybersecurity program. This was CyberOhio's first piece of legislation and put Ohio on the map as a leader in helping businesses adopt proper cybersecurity frameworks to keep Ohioans' data safe. Numerous other states are now exploring similar legislation and Senator Portman is even considering a similar proposal in Congress.

With the passage of the Data Protection Act, the next step was to ensure that Ohio is equipped to handle the ever-changing threats in cyber space. Ohio was one of the first states to address computer crimes, but the law has not been updated since the early 2000s. Like I just mentioned, cybercrime is always changing, and cybercriminals are always coming up with new ways to steal or manipulate data. This is why we began our work with the Ohio Credit Union League and various other organizations to ensure that Ohio is equipped with the laws to combat cybercrime.

As you are aware, the intent of this legislation is to give prosecutors the necessary, modernized tools to combat cybercriminals. The bill's sponsor, Representative Baldridge, recently testified on why he sought to introduce this legislation because of a

network breach to a local credit union in his district. Since you have already heard this story, I won't repeat those details.

The key difference between existing law and HB 368, is that this bill moves Ohio away from a damages-based model to one that criminalizes actions, such as electronic data tampering and electronic data theft. The legislation also updates definitions to account for rapidly changing computer crimes, so that Ohio is not always attempting to define the next computer-related crime fad, such as ransomware.

I want to take a few minutes to highlight the differences in penalties that exist in current law versus what is being created in HB 368. Existing law contains two offenses that cover computer-related crimes: (1) criminal mischief and (2) unauthorized use of a computer. The proposed bill would eliminate these two offenses and replace them with six computer-specific crimes.

Currently, a person commits criminal mischief by either impairing computer function, hacking, altering, damaging, modifying, or introducing a "computer contaminant" into a computer, system, network, software, or program. Criminal mischief is damages-based, meaning the value of the impacted computer-related items determines the severity of the penalty. This ranges from a first-degree misdemeanor for losses under $1000 to fourth-degree felony for losses greater than $10,000.

This bill would remove such provisions related to criminal mischief from ORC and replace them with:

1. Electronic computer service interference
    - An example would be a distributed denial of service attack or DDos attack, where a network is purposely overwhelmed with traffic so that it crashes.

2. Electronic data tampering
    - An example would be a common man-in-the-middle attack, where a cybercriminal intercepts email exchanges between individuals and alters the messages to steal money or information

3. Electronic data manipulation
    - An example would be some sort of "hacktivist" group introducing malware into a computer system in order to cause disruption and chaos.

Additionally, under currently law, unauthorized use of property occurs when a person accesses a computer, system, or network without consent. The statute also contains enhanced penalty provisions if the victim is elderly or disabled. Like criminal mischief, unauthorized use of property is also damages-based, ranging from a first-degree misdemeanor to a second-degree felony, depending on the amount of damages that can be proven.

CYBEROhio
An InnovateOhio Initiative

This bill would limit the existing prohibition under unauthorized use of property and create a number of new prohibitions:

4. Computer trespass
    - An example would be a former employee using old credentials to access a computer network to snoop around or steal information. Does this sound familiar? Because this is likely what the person who accessed the credit union in Representative Baldridge's district would have beeen charged with.

5. Electronic data theft
    - An example would be using a basic phishing email to gain access to a computer network and steal personal information.

6. Unauthorized data disclosure
    - An example would be some kind of data breach where stolen information is posted or sold online.

Finally, the legislation would introduce and define "malware" into ORC, a much more appropriate and up-to-date term that reflects today's malicious software variants like viruses and ransomware.

We believe that it is important to move away from a damages-based, because it is very difficult to show or prove how much something is or was worth at the time of the criminal act, especially when dealing with company data and networks. These new provisions under the bill would eliminate this and simply criminalize the actions themselves. The bad actors get punished, regardless of what or how much of what they stole or damaged. It would even allow prosecutors to go after cybercriminals for the act of attempting to steal any data.

Additionally, these new provisions can be mixed and matched to give prosecutors a flexible group of tools to use at their disposal. It would eliminate barriers for law enforcement and create a clear path to defend against diverse cybercriminals.

I also want to note the inclusion of a new "white-hat" provision that protects Cybersecurity professionals authorized to test and seek out weaknesses and vulnerabilities in computer networks. Several of the CyberOhio Advisory Board members brought this item to our attention as they operate in the space. These individuals are essential for testing and assessing networks, but like in all industries, errors can occur, and their actions can sometimes unintentionally damage networks. This provision simply protects them from criminal liability, if they have the proper authorization. Individuals and businesses can still be civilly held accountable for any unintentional damages under negligence law.

CYBEROhio
An InnovateOhio Initiative

As I mentioned earlier, the CyberOhio Advisory Board is made up of industry experts across Ohio, and all agree that this legislation is necessary to help keep Ohio safe and secure. We are excited to see Ohio continually moving in a direction to ensure Ohioans' digital security.

Thank you for your time and I am happy to answer any questions.