# cyberIdaho Financial Innovation Lab

# Emerging Technology Advisory Committee Report

## Rapidly Growing Cybercrime in Idaho Makes the Creation of a Specialized Cyber and Financial Crime Response Structure Necessary


## Executive Summary

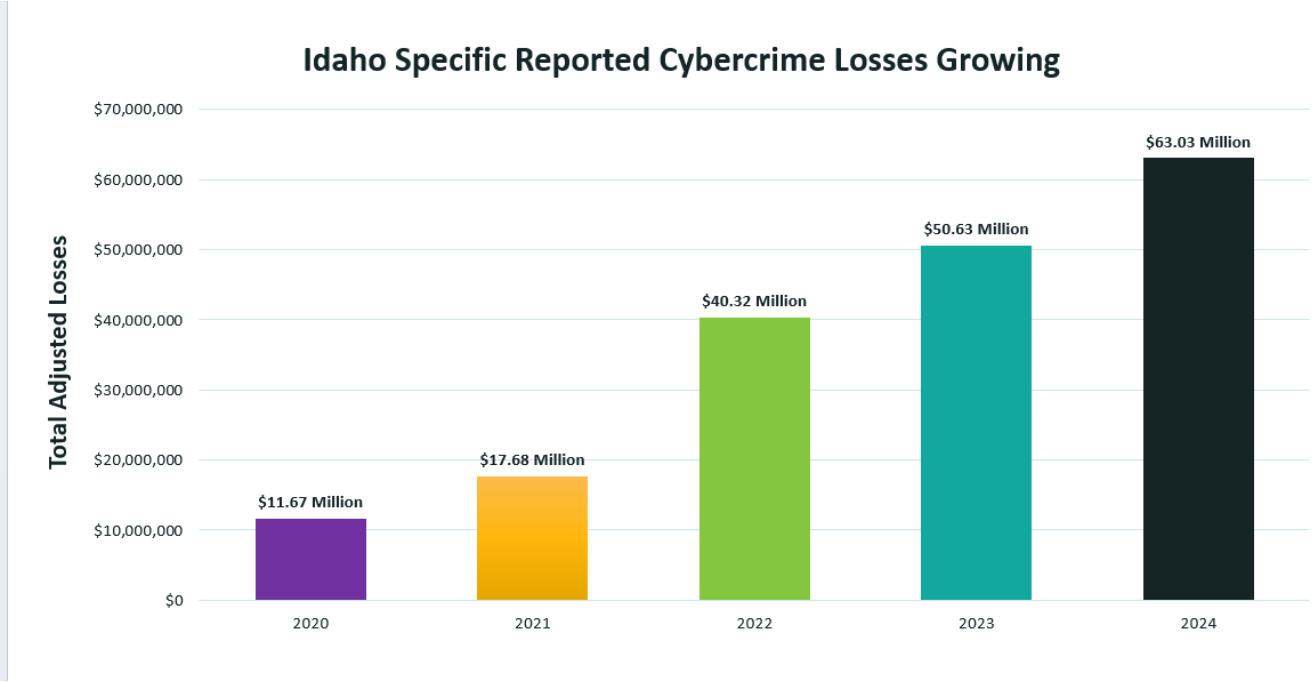
Increasing access and reliance on the internet/digital services is leading to a proliferation in cybercrime against Idahoans that requires the development of a specialized Idaho cyber and financial crime response structure that can better protect the financial health of Idaho's citizens and business community. **Known cybercrime losses increased to over $16.6 billion in 2025 with known Idaho cybercrime losses growing over 440% since 2020, which is 145% above the national average.** Various factors ranging from the digitization of society and the borderless nature of the internet to finite federal government capabilities, limited cyber/financial crime expertise, lack of access to key investigative tools, and outdated investigative/legal structures makes the creation of a specialized Idaho cyber and financial crime response structure essential to protecting Idahoans from surging cybercrime threats.

Since Idaho currently lacks the organizational structure and capacity to address rising cybercrime it should look to build a specialized structure that accounts for the investigative and prosecutorial gaps cybercriminals take advantage of to harm Idaho businesses and steal the hard-earned money of Idahoans, especially seniors. To accomplish this goal Idaho should develop a strategy that designates a lead state investigative agency and prosecutor's office for cyber and financial crimes, helps acquire necessary technological tools for addressing cybercrime, identifies key investigator/prosecutor trainings to improve essential skills and expertise, and establishes a cybercrime prevention workforce/recruitment pipeline to assist in the fight against cybercriminals for the benefit of all Idahoans.


[1] [2]

## Cybercrime Financial Losses in Idaho are Increasing Dramatically

Cybercrime financial losses are proliferating in Idaho as more Idahoans rely on the internet to interact with others and conduct financial transactions. The combination of approximately 88% of Idahoans having access to the internet, over 70% of Americans using social media, nearly 90% of Americans using financial technology, and over 80% of Americans regularly using text/messaging applications creates the perfect environment for cybercriminals to target Idahoans in the digital age.[3] [4] [5] [6] COVID-19 acted as a catalyst to this trend as more people began using digital technology and internet connectivity for work, school, shopping, dating, communication, and entertainment.[7] Criminals are adapting to this change in behavior by developing industrialized cybercrime operations to target Americans and Idahoans, which is highlighted in the Federal Bureau of Investigations (FBI) Internet Crimes Complaint Center's (IC3) metrics that shows known cybercrime losses growing over 295% since 2020 nationally with Idaho's losses increasing significantly more during the same time period (see the chart below highlighting Idaho's nearly 440% growth in known cybercrime losses since 2020).[8]




Bad actors find cybercrime increasingly attractive overall because it is profitable, highly scalable, enables global targeting, and there is a lower risk of being held accountable, which means that Idaho can expect cybercrime to continue to grow against its citizens. Cybercrime is expected to cost $10.5 trillion globally in 2025 with illicit actors earning nearly $1.5 trillion in profits.[9] These profits combined with the ability for cybercriminals to target potential victims anywhere in the world and scale their attacks via automation, cybercrime-as-a-service kits/services, and botnets means that cybercrime is becoming more accessible and easier than ever to conduct.[10] Furthermore, cybercriminals are able to protect themselves by carrying out operations in geographic regions outside the reach of U.S. law enforcement and by using privacy preserving technologies such as virtual private networks (VPNs), proxies, and private browser tools (e.g., The Onion Router/TOR) that make criminal attribution difficult.[11] [12]

All of these factors showcase that bad actors are adapting and reaping many benefits from cybercrime that will lead to additional losses for Idahoans unless an effective cyber and financial crime response structure is built.

## Finite Federal Resources, Outdated Strategies, Lack of Specialization, & Absence of a State Structure Enable Cybercrime to Grow in Idaho

The need to secure growing digital critical infrastructure, defend Americans from global cybercriminal activity, and adapt to new emerging financial technologies (that enable bad actors to move money faster, more opaquely, and globally) is overwhelming federal authorities and making it essential for Idaho to build its own cybercrime response structure that adopts a "freeze and seize" strategy to better protect Idahoans. Due to resource constraints federal agencies prioritize cases that have either large dollar values or meet national security priorities, which means many Idaho cases are not meaningfully investigated.[13] Additionally, cybercriminals are increasingly using cryptocurrency and digital payment apps to hide their identities and move money quickly making recovery extremely difficult.[14] This makes the implementation of a "freeze and seize" strategy that places a freeze on reported cybercrime assets so they can be investigated for potential seizure before criminals (who often cannot be identified or are outside the reach of U.S. law enforcement) can take possession of the assets vital to better protecting Idahoans.[15] This approach emphasizes the recovery of stolen funds given that

attribution, arrest, and prosecution of cybercriminals may prove impossible. Suspects often are in countries where there are no extradition treaties foreclosing the likelihood of arrest and prosecution. Victims prioritize the recovery of their stolen funds, but many prosecutors are uninterested in investigations that will not lead to prosecutions and do not consider the recovery of stolen funds to be a priority.

Cyber and financial crimes are inextricably linked and require specialized knowledge/skills and dedicated structures that Idaho currently does not possess to protect potential victims.[16] [17] Cybercrime investigators should possess a mix of financial and cyber technical/analytic skills that include digital forensics, forensic accounting, malware analysis, financial payment and trading data analysis, network security skills, corporate legal structure expertise, and deep knowledge of financial operations and regulatory requirements. These are specialized skillsets that need to be recruited, developed, and cultivated to properly investigate and prosecute cybercrime for the benefit of Idaho citizens and businesses.

Moreover, to be effective these skillsets need to be organized into a specialized cyber and financial crime response structure where they can work in unison to address increasingly complex cases involving financial fraud, business email compromise, investment scams, tech support scams, data breaches, ransomware attacks, identity theft, and many other cybercrimes. Unlike many other states, Idaho currently lacks a cyber and financial crime response structure that can handle these types of cases efficiently and effectively for its citizens and businesses.

## Cybercrime Financial Losses Will Continue to Accelerate in Idaho as Cybercriminals Organize and Incorporate Emerging Technologies into their Operations

Criminals are creating industrialized organized cybercrime structures and using new digital technologies that will ensure financial losses rise significantly for Idahoans unless Idaho builds a cyber and financial crime response structure that can properly investigate cybercrime, provide necessary technical support/assistance, and take appropriate legal actions. Cybercriminals are creating corporate-like structures and professionalizing the cybercrime industry to attack Americans and Idahoans at scale.[18] The combination of cybercrime groups such as Fin7, LockBit, and Blackcat (ALPHV) and cyber/financial crime compounds like KK Park are bringing structure to cyber and financial crime operations that will lead to a substantial increase in victim losses unless Idaho builds an organized response to properly protect its citizens and businesses.

Cybercriminals are often early adopters of new emerging technologies and methods for exchanging financial value because they know law enforcement/oversight authorities will be a step behind and need to adapt. As more people become dependent on the internet for their everyday lives cybercriminals are now using artificial intelligence (AI) solutions to target victims at scale with automated and personalized phishing/social engineering attacks, deepfakes, AI malware attacks, synthetic identities, and other types of attacks that add to the industrialized nature of their crimes.[19]

Bad actors are also incorporating new methods for exchanging value into their operations via cryptocurrency/digital assets that enables them to move illicit profits quickly and in a pseudonymous manner, which makes it difficult to track and seize these assets without necessary training, resources, and expertise.[20] As cybercrime organizations and criminals adapt and become more specialized it is essential that Idaho build its own specialized structure that possesses the necessary expertise and authorities to adapt and frustrate cybercrime operations against Idahoans.

Since Idaho currently lacks the organization and specialized expertise to address growing cybercrime it is likely to continue to see cybercrime losses grow higher than the national average due to its large senior population. Americans and Idahoans aged 60 and over are the number one age group for cybercrime losses and often face unique challenges such as cognitive decline, social isolation, and financial insecurity, making them prime targets for bad actors.[21] Research also shows that 22.7% of Idaho's population is aged 60 or over ranking it in the top three states for growth in this category during the last decade making Idaho a target-rich environment for cybercriminals and a big problem for state authorities.[22] [23]

These facts point to the need for Idaho to establish a specialized cyber and financial crime response structure with statewide jurisdiction to combat cybercrime. Currently, Idaho victims do not have a reliable means of recovering stolen assets or even effectively reporting cybercrimes. Additionally, Idaho law enforcement agencies and prosecutors generally lack the training and expertise to investigate and handle these types of crimes. This makes it vital for Idaho to create a structure that consists of knowledgeable investigators, enables timely communication between law enforcement/oversight agencies and financial institutions, and possesses seasoned prosecutors who can understand and apply key legal processes to implement a "freeze and seize" strategy to protect Idaho citizens and businesses from the growing cybercrime threat they face.

## Keys to Addressing Growing Cybercrime in Idaho: A Statewide Cyber & Financial Crime Structure, Training, Educational Pipelines, & Tools

The tremendous success illicit actors are having in profiting from the industrialized cybercrime structures they have built is making it critical for Idaho to develop a well-organized and dynamic cyber and financial crime response structure. This structure should integrate vital cyber and financial skills/capabilities, authorities, and missions throughout the state to counter surging cybercrime in Idaho affecting its citizens and businesses. To create a functional and effective cyber and financial crime structure Idaho should take the following steps:

**Create a Specialized Statewide Cyber & Financial Crime Investigative Unit** – Successfully protecting victims from cyber and financial crime is about speed and specialized knowledge. Recovery of assets requires an almost immediate series of actions (e.g., asset tracing, freeze letters, search warrants, and subpoenas etc.) from state authorities to stop bad actors attempting to move stolen funds from financial entities. Unit staffing should include investigators with specialized knowledge and backgrounds in either cyber or financial crime (or both) who are able to work together to take swift action against illicit activity.

Various Idaho agencies and departments are well positioned to house a specialized cyber and financial crime response structure including the Idaho Department of Finance (IDOF), Idaho Attorney General's Office (ID AG), and Idaho State Police (ISP). The IDOF Securities Bureau already successfully runs a Financial Crimes and Intelligence Unit with specialized knowledge and integral relationships with financial institutions that could make them a good choice for a structure, especially if they are granted law enforcement status similar to the Idaho Lottery Commission (Idaho Code section 67-7410). The ID AG could also be a potential fit if granted jurisdiction similar to their Internet Crimes Against Children authorities (Idaho Code section 67-1410). Another potential fit could be ISP since they already have statewide jurisdiction and preexisting relationships with local law enforcement and prosecutors. Lastly, some type of joint hybrid structure between these investigative entities could be a potential solution.

**Designate a Lead Cyber & Financial Crime Prosecutor's Unit Statewide** – The ID AG seems perfectly placed to potentially handle statewide prosecutions for cyber and financial crime cases due to their cyber expertise and statewide jurisdiction of Internet Crimes Against Children (ICAC). Specialization in cybercrime is a valuable skill that the ID AG already possesses, and they also have access to more resources than most county prosecutors. Some other options could be the formation of a specialized Cyber and Financial Crime County Prosecutors Council (CFCCP) or a hybrid model that combines resources from the ID AG and CFCCP, but these models risk becoming overly complex, convoluted, and ineffective.

Since speed and know-how are essential in cybercrime cases, a streamlined and focused prosecutorial unit with statewide jurisdiction and authorities is necessary for any successful cyber and financial crime structure in Idaho.

**Budget for Specialized Cyber, Emerging Technology, & Financial Crime Training–** Agencies involved in Idaho's cyber and financial crime structure should use a portion of their budget to enhance the knowledge of their investigators and prosecutors by sending them to targeted trainings focusing on cybersecurity/crime, new emerging technologies (e.g., AI or blockchain etc.), and novel financial crime methodologies and protection strategies. Since cyber and financial crime are constantly evolving it is important for stakeholders to obtain the knowledge and training they require to successfully adapt and fulfill their mission of protecting Idaho from cybercrime.

**Develop a Cyber & Financial Crime Educational & Recruitment Pipeline** – Cybersecurity and financial crime will continue to be key issues for the foreseeable future, so it is important to build educational/training programs for students and citizens to gain the specialized knowledge and skills they need to help in the fight against cyber and financial crime. Idaho should create dedicated cyber and financial crime college/legal programs, provide students/trainees with access to key investigative tools (e.g., blockchain analytic or link analysis tools etc.), and develop internship and fellowship programs that provide the necessary skills, capacity, and knowledge to produce the next generation of cyber and financial crime fighters that can better protect Idaho from growing cybercrime threats.

**Access to Necessary Investigative Technological Tools & Services** – As cyber and financial crime continues to evolve investigators and prosecutors will need access to key technological tools and services to help them fight AI enabled crime and to track and trace illicit financial activity and digital assets. Link analysis programs, blockchain analytic tools, custody services/solutions, automated forensic accounting tools, and others will be necessary to fight cyber and financial criminals. A successful cyber and financial crime response structure should also seek to leverage public-private partnerships to gain access to critical tools, services, and capabilities. Without these types of tools and services investigators and prosecutors will not be able to effectively investigate and prosecute bad actors or protect the Idaho citizens and businesses that depend on them.

The creation of a dynamic cyber and financial crime response structure in Idaho that possesses specialized knowledge and capabilities is essential for fighting increasingly organized cyber and financial crime operations that are stealing the hard-earned money of Idahoans and harming Idaho businesses. The adoption of these solutions will create an effective response structure for frustrating rapidly growing cybercrime in Idaho, while also providing the necessary resources, tools, talent, and knowledge necessary to better protect Idaho from cyber and financial crime now and in the future.

## Endnotes

[1] https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf (refers to $16.6 billion in financial losses mentioned in the callout box).

[2] https://www.ic3.gov/annualreport/reports (the percentage change metric in the callout box is from IC3's annual and state reports between the years 2020 - 2024).

[3] https://libraries.idaho.gov/digital-access-for-all-idahoans/digital-navigator-workbook/

[4] https://www.theglobalstatistics.com/united-states-social-media-statistics/

[5] https://plaid.com/the-fintech-effect-2021-mass-adoption/

[6] https://www.localproject.net/docs/texting-stats/

[7] https://pmc.ncbi.nlm.nih.gov/articles/PMC9222023/#:~:text=During%20the%20COVID%2D19%20pandemic%2C%20the%20significant%20increase%20in%20online,articles%20summarized%20in%20Table%201%20.

[8] https://www.ic3.gov/annualreport/reports

[9] https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

[10] https://www.fbi.gov/contact-us/field-offices/sanfrancisco/news/fbi-warns-of-increasing-threat-of-cyber-criminals-utilizing-artificial-intelligence

[11] https://www.thirdway.org/report/a-roadmap-to-strengthen-us-cyber-enforcement-where-do-we-go-from-here

[12] https://www.adfixus.com/post/digital-cloak-and-dagger-embracing-anonymity-for-a-new-online-era

[13] https://www.justice.gov/d9/pages/attachments/2022/07/19/ccr_0.pdf

[14] https://www.cyberdefensemagazine.com/why-do-hackers-love-cryptocurrency/

[15] https://federal-criminal.com/forfeiture-seizure/us-laws-on-seizing-proceeds-from-interstate-cybercrime/

[16] https://arctic-intelligence.com/insights/cybersecurity-and-financial-crime-merging-risk-assessments#:~:text=The%20convergence%20of%20cybersecurity%20and,attacks%20to%20fraudulent%20wire%20transfers.

[17] https://www.nga.org/wp-content/uploads/2020/05/Cyber-Crime_What-a-Governor-Can-Do.pdf

[18] https://www.cnbc.com/2019/05/05/heres-what-cybercriminals-do-during-the-workday.html

[19] https://www.fbi.gov/contact-us/field-offices/sanfrancisco/news/fbi-warns-of-increasing-threat-of-cyber-criminals-utilizing-artificial-intelligence

[20] https://www.cyberdefensemagazine.com/why-do-hackers-love-cryptocurrency/

[21] https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf

[22] https://www.neilsberg.com/insights/idaho-population-by-age/

[23] https://www.consumeraffairs.com/homeowners/elderly-population-by-state.html