Office of Attorney General
Daniel Cameron

Cyber Security for Public and Private Agencies

Before the Budget Review Subcommittee on General Government,
Finance, and Personnel & Public Retirement

Attorney General
DANIEL CAMERON

Office of Attorney General
Daniel Cameron

- Chris Lewis, Commissioner, Office of Consumer Protection
- Matt Cocanougher, Assistant Attorney General, Office of Consumer Protection
- Matt Hedden, Director of Special Victims Unit, Department of Criminal Investigations
- Blake Christopher, Deputy General Counsel & Director of Legal Policy

Consumer Protection: Data Breach Notices

- KRS 365.732
  - Applies to both private companies and state agencies
  - It requires notice to individuals when a breach involving personally identifiable information has occurred; however, it does not require notification to the Attorney General
- KRS 61.933
  - Requires notice to the Attorney General (along with other agencies) if a public agency or third party that collects, maintains, or stores personal information on behalf of the agency suffers a data breach.

Consumer Protection: Frequency of Cyber Security Attacks

- From 2018 to present, our Office has received 358 data breach notices under KRS 61.933

Year	Data Breach Notices Received
2018	121
2019	30
2020	83
2021	75
2022	49

Consumer Protection: Frequency of Cyber Security Attacks

- The vast majority of data breach notices we receive under KRS 61.933 are breaches that are not intentional cyber attacks

Year	Data Breach Notices Related to Cyber Security Attacks
2018	5
2019	7
2020	15
2021	20
2022	5

Consumer Protection: Ransomware Reported Under KRS 61.933

- Ransomware attacks against state agencies or third parties contracting with state agencies are rare

Year	Data Breach Notices Citing Ransomware
2018	0
2019	0
2020	2
2021	2
2022	1

Consumer Protection: Costs to Agencies

- Most Data Breaches
  - Most agencies report that they do not incur substantial costs
  - However, agencies note that staff time is required to investigate the breach and to complete the notice form
  - Staff time is also required to train employees and update policies related to breaches
- Ransomware
  - Agencies facing ransomware typically must hire outside firms to investigate the breach and ensure compliance with notice statutes
  - If an agency determines that misuse of personal information has occurred, or is likely to occur, it may also incur costs for providing credit monitoring services to individuals whose personal information was compromised

Consumer Protection: Conclusion

- Our Office receives a notice and reviews it to ensure that agencies are taking the proper steps in response to the breach
- Independent of our review of the notice, our Office also investigates the data breach
  - Since 2018, our Office has entered into 12 multi-state settlement agreements with private companies involving data security practices
  - Our Office has recovered over $5 million in monetary damages from these agreements

Criminal: Network Intrusions

- Ransomware
  - Used in completely opportunistic attacks affecting individuals' home computers as well as targeted strikes against organizations;
  - Attempted with little risk or cost to the adversary involved;
  - Successful with no reliance on having to monetize stolen data;
  - Deployed across numerous devices in organizations to inflict bigger impacts and thus command bigger ransoms;
  - Accounted for 39% of malware-related breaches in 2018 and 68.5% in 2021; and
  - Spreads through clicking on a malicious link or through gaining access to systems via weak password/unsecured Remote Desktop Protocol

The ongoing telecommuting model may be contributing to the threat against data systems as employees are utilizing credentials over non-supervised home networks

Criminal: Anatomy of a Hack

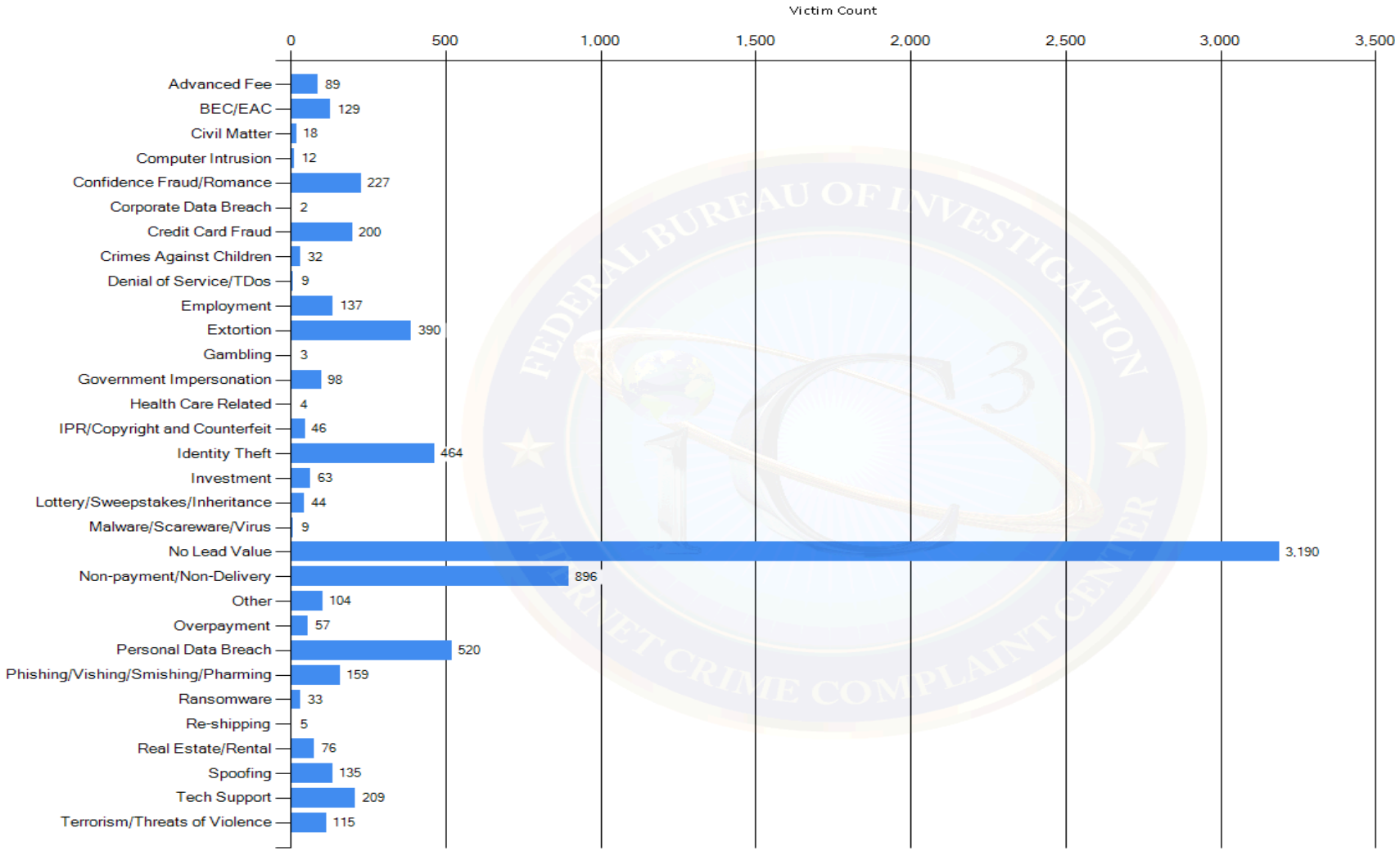
Initial Compromise:

- Webserver SQL Injection (almost always used)
- Spear phishing
- Botnet already on your network (cost $100-$1000)
- Insider (e.g., paid an employee to launch malware)
- Router attack

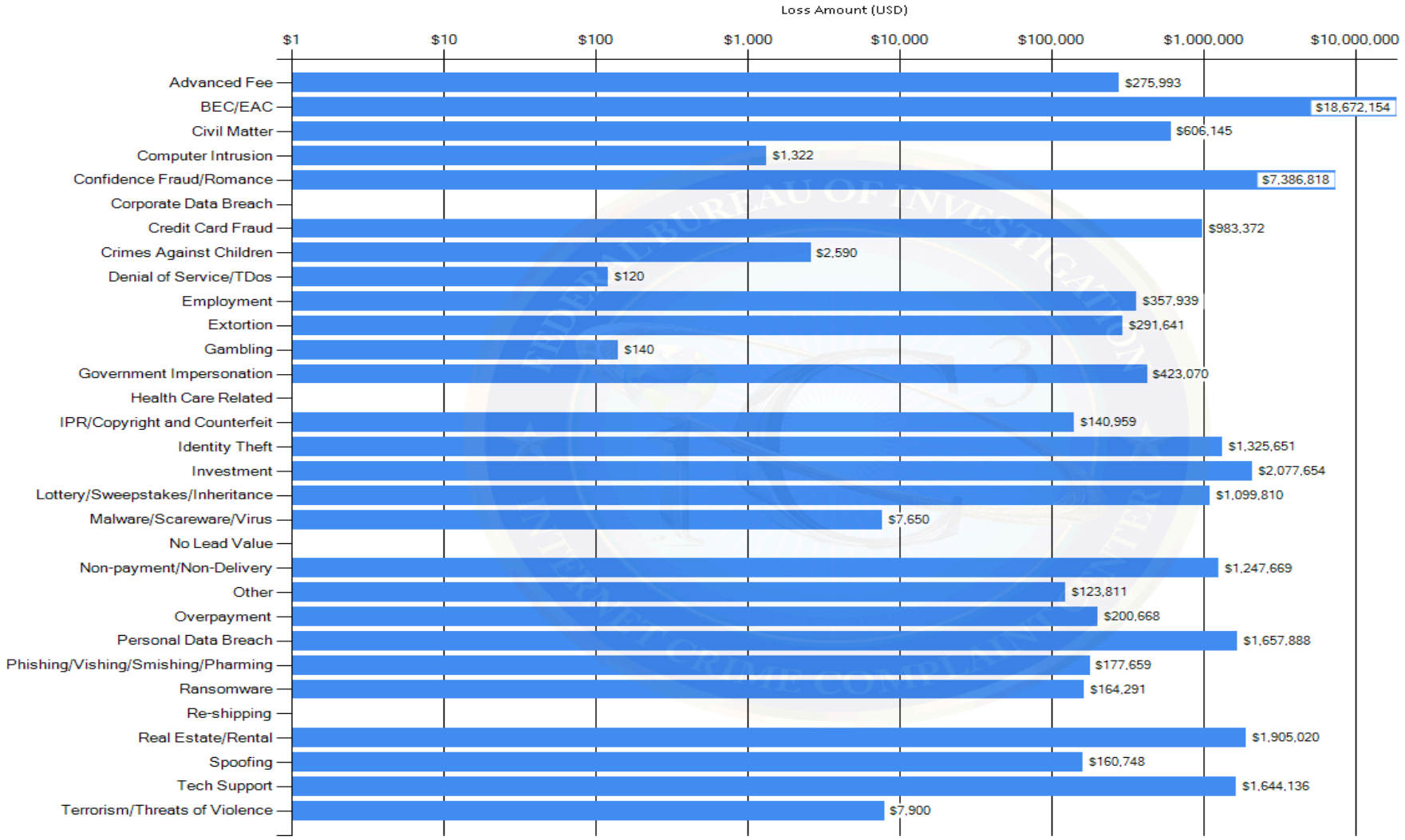
Criminal: Statistics

By Victim Loss			
Crime Type	**Loss**	**Crime Type**	**Loss**
BEC/EAC	$1,866,642,107	Overpayment	$51,039,922
Confidence Fraud/Romance	$600,249,821	Ransomware	**$29,157,405
Investment	$336,469,000	Health Care Related	$29,042,515
Non-Payment/Non-Delivery	$265,011,249	Civil Matter	$24,915,958
Identity Theft	$219,484,699	Misrepresentation	$19,707,242
Spoofing	$216,513,728	Malware/Scareware/Virus	$6,904,054
Real Estate/Rental	$213,196,082	Harassment/Threats Violence	$6,547,449
Personal Data Breach	$194,473,055	IPR/Copyright/Counterfeit	$5,910,617
Tech Support	$146,477,709	Charity	$4,428,766
Credit Card Fraud	$129,820,792	Gambling	$3,961,508
Corporate Data Breach	$128,916,648	Re-shipping	$3,095,265
Government Impersonation	$109,938,030	Crimes Against Children	$660,044
Other	$101,523,082	Denial of Service/TDos	$512,127
Advanced Fee	$83,215,405	Hacktivist	$50
Extortion	$70,935,939	Terrorism	$0
Employment	$62,314,015		
Lottery/Sweepstakes/Inheritance	$61,111,319		
Phishing/Vishing/Smishing/Pharming	$54,241,075		

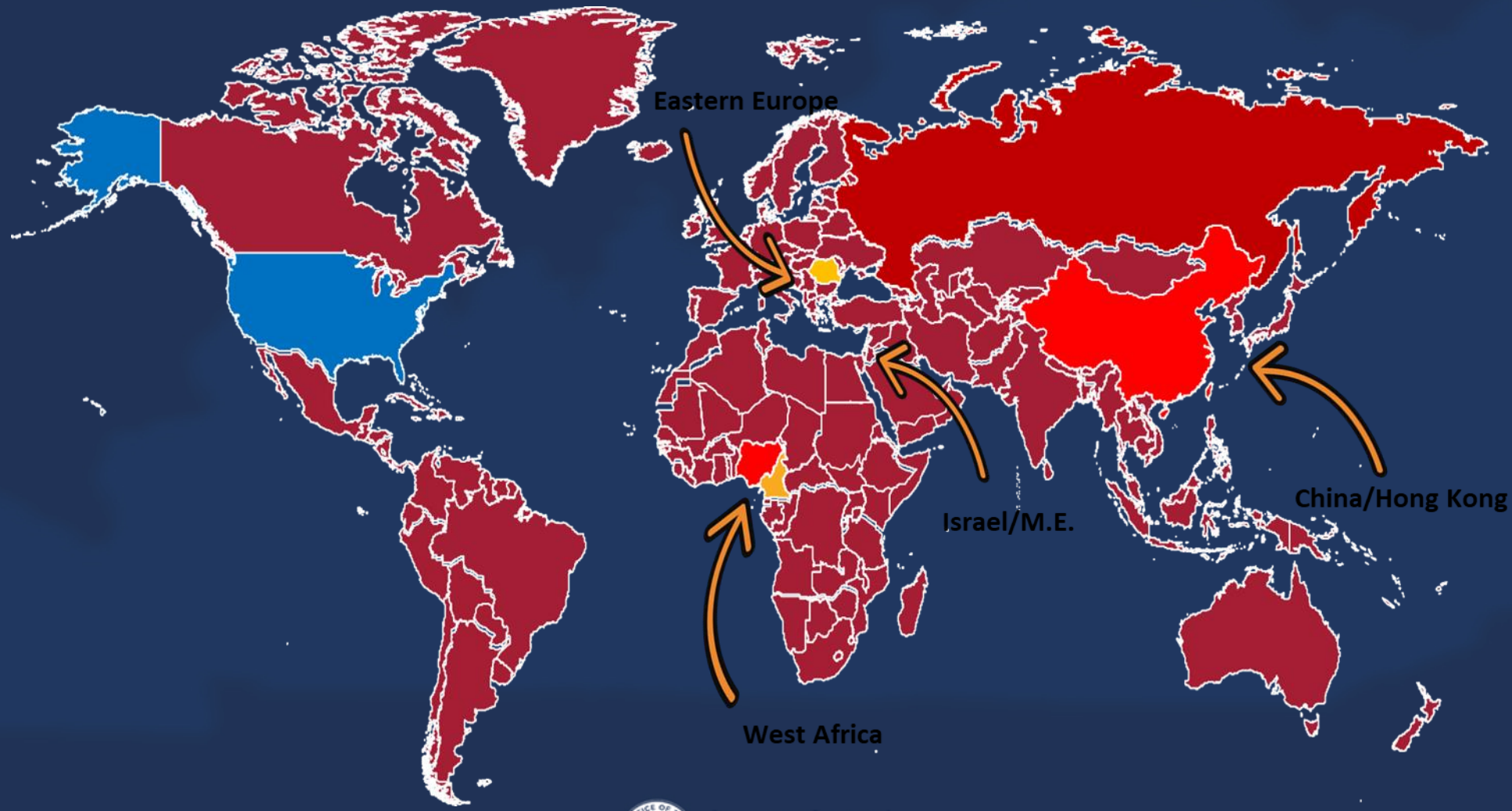
Kentucky 2021 - Crime Type by Victim Count



Kentucky 2021 - Crime Type by Victim Loss



Criminal: **Global** Participants



Attorney General
DANIEL CAMERON

Questions?