2024 TOP THREATS IN THE PUBLIC SECTOR

What federal, state, and local governments can expect from cybersecurity and fraud threats this year.

Criminals are relentless. They exploit any opportunity to gain access to government funding. **Here are our predictions for the Top Threats** – based on recent findings and statistics – that will escalate and proliferate **throughout 2024**, creating numerous issues for government agencies.

1. Fraud-as-a-Service

Fraud-as-a-service (FaaS)– a service on the dark web which helps criminals commit fraud. In addition to selling social security numbers, credit card numbers, and health information, FaaS sites also sell **pre-packaged synthetic IDs individually or in bulk** that can produce hundreds of online activities in seconds. **Government agencies should be aware of FaaS** to protect constituent information.

The **threat of FaaS is growing**. Just as the software-as-a-service market is booming, with a **projected Compound Annual Growth Rate of 19.7% between 2022 and 2029** according to Fortune Business Insights, so too is the **FaaS market.**[1]

Tools and services for hire: In 2023, researchers discovered Styx, a **darknet marketplace selling illegal techniques for committing fraud**, such as money laundering, distributed denial-of-service (DDoS), bypassing two-factor authentication (2FA), fake or stolen IDs and other personal data, renting malware, using cash-out services, email and telephone flooding, identity lookup, and much more.[2]

MITIGATION STRATEGY: Leverage an identity verification workflow with behavioral biometrics to mitigate FaaS risk.

2. Account Takeover Fueled by Synthetic Identities

Fraudsters use personal information from several different individuals to create **brand-new synthetic identities**—a type of fraud that's fast-growing–**government agencies are at risk** as it's hard to detect synthetic identities.

Account takeover attacks **increased 354% year-over-year in 2023**, and **22% of U.S. adults have been victims** of account takeover (24M households).[3]

Precisely how much money is lost to synthetic identity theft isn't fully known — **estimates range from $20 to $40 billion** and growing. But fraudsters know **government agencies, financial institutions, insurance companies, retail stores, and e-commerce sites have not sufficiently upgraded their verification systems** to detect and prevent synthetic identity fraudsters before it's too late.[4]

MITIGATION STRATEGY: Ensure identity composition and risk elements are front and center in your workflow.

3. (Artificially) Intelligent Fraudsters

Fraudsters are accessing machine learning, generative Artificial Intelligence (AI), predictive analytics, and other intelligent solutions to make them faster, smarter, and commit crime on massive, real-time scale.

In a June 2023 survey of 650 cybersecurity experts, **three out of four experts polled noted a rise in cyberattacks over the past year**, with **85% attributing this rise to bad actors using generative AI**. In 2022, consumers reported **losing $8.8 billion to fraud**, up more than 40%.[5]

Generative AI is **enabling fraudsters to save time by automating** the previously complex process of stitching together fake, synthetic identities that interact like humans across thousands of digital touchpoints, **fooling agencies and constituents** into thinking they are legitimate.[6]

MITIGATION STRATEGY: Utilize both behavioral and device risk intelligence to reduce synthetic identities and their impact.

4. Serious Cyberthreats

The **cyberthreat landscape keeps evolving. The MOVEit Transfer file management program attack** is the **largest hack of 2023**, and in recent history. Experts say it has **spawned over 600 breaches** and is not done yet, but the full impact of the attack is still being examined. **Government agencies were impacted.**

At least **60 million individuals have been affected**, though the true number is thought to be far higher, and U.S.-based agencies and organizations account for **83.9% of known MOVEit victims**.[7]

The **estimated total cost of the MOVEit mass-hacks so far is $9,923,771,385**. The number is based on IBM data, which found the average data breach last year cost $165, coupled with the number of individuals confirmed to have been impacted.[7]

A report by security analysis firm Censys, which analyzed **1,400 MOVEit servers** that were openly accessible on the internet, found that **15.96% of hosts were associated with the healthcare sector**, 8.92% were linked to information technology organizations and **7.5% were attributed to government** and military entities.[7]

MITIGATION STRATEGY: Add back-end investigative solutions to maintain program integrity and reduce improper access and payments when traditional identity verification doesn't catch the fraudster using stolen information.

5. Worries About Windows

Ransomware is becoming a bigger and bigger problem for government agencies and companies by the day. The U.S. government is looking at **cryptocurrency sanctions in large part to combat ransomware**. This type of attack has been at the center of **major national data breach incidents**. And now, there's a report on how this critical problem **links back to Windows**, where users have in recent years been the **primary ransomware attacks target**.

Google's VirusTotal service study revealed that **95% of ransomware malware identified by its systems targets Windows**. Specifically, **93.28%** of ransomware detected were Windows executables (exe.file), and **2%** Windows dynamic link libraries.[8]

Criminals use exe.file in phishing schemes as it directly installs a program or malware to the system when the user clicks its icon.[9]

MITIGATION STRATEGY: Establish, adopt, and enforce agency-wide policies to promote awareness. Implement a device risk mitigation workflow.

6. A Cashless Society

Cashless cards for payment government services are under attack by fraudsters, particularly those **employing Electronic Benefits Transfer (EBT) card skimmers** – an activity that is draining millions of dollars from those most in need. **Food and Nutrition Services (FNS), Administration for Children and Family (ACF) and individual Supplemental Nutrition Assistance Program (SNAP)/Temporary Assistance for Needy Families (TANF) agencies have issued numerous client education materials** aimed at informing genuinely needy and vulnerable participants about skimming and other digital payment risks.

Fair Isaac Corporation (FICO) saw a **368% increase in compromised cards in 2022**. One state has long struggled with this issue, providing numbers related to the depth of this problem: **$84 million in anticipated 2023 losses**.[10]

For **every $1 value of lost benefits through fraud, it actually costs SNAP agencies $3.85** based on additional costs related to labor and administrative activities. This is **up from $3.72 in 2022**. For SNAP agencies that have more **multi-program responsibility and an above average level of mobile-based applications**, every **$1 value of SNAP benefits lost through fraud is actually $4.05**.[11]

MITIGATION STRATEGY: Educate recipients on secure pin numbers to prevent easy guessing by bots. Employ investigative solutions to maintain program integrity. Implement insider threat workflows and monitoring to minimize payment fraud.

7. Nefarious Elder Fraud

Elder fraud, also called **elder financial abuse or elder financial exploitation**, is defined as the **misappropriation or abuse of financial control in a relationship** where there is an expectation of trust, resulting in **harm to the elderly victim**. More than **333,000 scams and financial abuse cases targeting the elderly** are reported to authorities every year, and most experts agree that's barely scratching the surface. **Agencies providing services to the elderly should work to educate their constituents** about fraud schemes targeting services and to be wary.

More than **1 in 10 elderly people in the U.S. fell victim to elder fraud** in the last year, and over **7.8 million incidents of elder fraud occur every year** in total, with an **average loss per case of $30,192**.[12]

In 2022, **total losses reported** to the Internet Crime Complaint Center by elderly victims **increased 84% from 2021**.[13]

An estimated **$28.3 billion is lost to elder fraud scams each year**, according to an AARP Study. The study said many of the scams that account for this incredible loss go unreported, and the **FBI is now urging anyone who encounters suspicious activity online to disengage and report the conduct to law enforcement**.[14]

MITIGATION STRATEGY: Implement behavioral biometrics to mitigate elder fraud. Provide education to constituents about the risk of elder financial exploitation tactics and schemes.

8. Digital IDs at Risk

A **digital identity**, or online identity, is a **person's digital representation**. It contains unique vital information, such as **account names, browsing data, and even medical history**. But unlike a physical ID card, there **are currently limited applications or sign-up processes** to get a digital identity. **Everyone who uses the internet in any capacity** has some form of digital identity, and this includes **government services.**

More **than half (54%) of fraudulent activities were found online, followed by mobile spam calls (18%)**. This alarming data highlights the risks of digitization, where **scammers move away from traditional methods of breaching data**.[15]

67% of all identity theft fraud victims experience a total digital takeover, which means if someone has 10 or 12 logins to places like Facebook, Pinterest, their bank, credit card, etc., **criminals can become familiar with all of their personally identifiable information**.[16]

In 2022, **40 million consumers lost a total of $43 billion to identity theft**. These bad actors are **pretending to be you**, accessing your accounts and spending your money.[17]

MITIGATION STRATEGY: Encourage constituents/recipients to change passwords frequently and monitor breach notifications. Implement a workflow designed to detect and manage compromised credentials.

As fraud and cyber risks evolve and continue to grow, government agencies deserve the best line-of-sight into their populations to provide secure and frictionless service.

LexisNexis® Risk Solutions can help. Learn more about how our workflows can mitigate evolving cyber and fraud risk.

LexisNexis® RISK SOLUTIONS

Scan the QR code or call us at 1.888.216.3544

1 https://seon.io/resources/dictionary/fraud-as-a-service/
2 https://www.bleepingcomputer.com/news/security/new-dark-web-market-styx-focuses-on-financial-fraud-services/
3 https://spycloud.com/blog/2023-cybersecurity-industry-statistics-account-takeover-ransomware-data-breaches-bec-fraud/#:~:text=Account%20Takeover%20(ATO)%20Statistics%3A,account%20takeover%20(24M%20households)
4 https://legal.thomsonreuters.com/en/insights/articles/trends-in-synthetic-identity-fraud
5 https://www.forbes.com/sites/jeffkauflin/2023/09/18/how-ai-is-supercharging-financial-fraudand-making-it-harder-to-spot/?sh=1ca05fcd6073
6 https://www.securitymagazine.com/articles/100086-combatting-the-next-wave-of-ai-fraud#:~:text=Generative%20AI%20is%20enabling%20fraudsters,into%20thinking%20they%20are%20legitimate
7 https://techcrunch.com/2023/08/25/moveit-mass-hack-by-the-numbers/?guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAL8UtHgiuskJWcGQXaUsOhS9rGyFFyFsOCOhZ4qqPpGjdH-C2rx8Vi5DkGsMKtddBoOdXTGYgqAlEK6hQintfBx-FxwuQrnEOriYwwqa-nYFGQXKXUXHoT9erprvIOrIaXIcJQy2rh-yiwefKYnVbVrFl7vUgB7UsBq42di04TJDh&guccounter=2
8 https://www.theregister.com/2021/10/14/googles_virustotal_malware/
9 https://www.techtimes.com/articles/266728/20211015/windows-users-ransomware-attack-windows-ransomware-windows-microsoft-google-report.htm
10 https://risk.lexisnexis.com/insights-resources/article/electronic-benefit-transfer-ebt-card-skimming-a-deeper-look-at-the-issue
11 https://risk.lexisnexis.com/insights-resources/infographic/discover-fraud-cost-for-snap-and-ies-agencies
12 https://www.comparitech.com/blog/vpn-privacy/elder-fraud-by-state/#:~:text=Over%207.8%20million%20incidents%20of,Internet%20Crime%20Complaint%20Center%20(IC3)
13 https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3ElderFraudReport.pdf
14 https://www.cbsnews.com/news/fbi-warns-elder-fraud-crime-rates-rising-scammers-steal-billions-each-year/
15 https://asliri.id/blog/digital-identity-and-identity-fraud-explained/
16 https://www.fox13now.com/news/fox-13-investigates/shocking-data-shows-digital-identity-theft-is-on-the-rise
17 https://www.fox13now.com/news/fox-13-investigates/shocking-data-shows-digital-identity-theft-is-on-the-rise

About LexisNexis Risk Solutions
LexisNexis® Risk Solutions harnesses the power of data and advanced analytics to provide insights that help businesses and governmental entities reduce risk and improve decisions to benefit people around the globe. We provide data and technology solutions for a wide range of industries including insurance, financial services, healthcare and government. Headquartered in metro Atlanta, Georgia, we have o¬ices throughout the world and are part of RELX (LSE: REL/NYSE: RELX), a global provider of information-based analytics and decision tools for professional and business customers. For more information, please visit www.risk.lexisnexis.com and www.relx.com.