FIR RISK NEWS

RANSOMWARE, OSINT, AND CYBER INSURANCE!

INSIDE

TOP FINDS THIS MONTH

Ransomware

Open Source Intelligence

Cyber Insurance

FIR RISK NEWS
Every month, we bring to you new sources and cybersecurity news for your review

FIR RISK INSIGHTS
We will bold in RED key takeaways to consider for your business

Q1 2024

FIR

FRAUD INTELLIGENCE REPORT
EMPOWERING BUSINESSES TO OUTSMART FRAUD

APRIL 2024 EDITION

FIR RISK ADVISORY LLC

Top finds this month

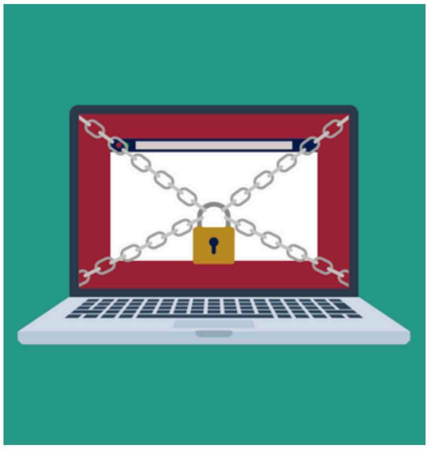
- By Bruce Bird, Principal, FIR Risk Advisory, LLC

FIR Quarterly, our flagship fraud intelligence report, is designed to keep business leaders informed of the digital fraud landscape. We include insights throughout the report to highlight must read content. We published our first edition on April 24 and have made this report available for FREE, download **here**.

Ransomware trends in 2024 are revealing continued momentum but law enforcement is taking a bit out of the top ransomware groups!

RANSOMWARE

The Information Technology- Information Sharing and Analysis Center (***IT-ISAC***) has been tracking Ransomware incidents and trends since 2021, and in 2023, the IT-ISAC recorded a total of 2,905 ransomware attacks globally along with identifying 18 new ransomware groups in 2023!



Key Trends and Takeaways for 2023:

- **Ransomware-as-a-Service (RaaS)** is a cybercriminal business model where threat actors rent or purchase ransomware software and services from developers, allowing them to carry out attacks without the need for having sophisticated technical skills of their own.
- There is **an increase in data extortion schemes** with ransomware groups skipping the encryption process altogether.
- Ransomware actors continue **to target third-party vendors t**o gain access to mission-critical systems and data.
- There is a notable trend in Ransomware actors **abusing remote management tools and legitimate software** to gain initial access and evade detection.
- 2023 saw a trend in the **exploitation of zero-day vulnerabilities** (MOVEit, GoAnywhere, Citrix devices, PaperCut, etc.) and deployment of custom tooling by ransomware actors.

TOP 5 Ransomware Attacks by Country

- United States of America - [1565 Attacks] - [53.9%]
- United Kingdom - [167 Attacks] - [5.7%]
- Canada - [137 Attacks] - [4.7%]
- Germany - [97 Attacks] - [3.3%]
- France - [88 Attacks] - [3.0%]

TOP 5 Ransomware Attacks Against Critical Infrastructure Globally 2023

- Critical Manufacturing Sector - [468 Attacks] - [15.5%]
- Commercial Facilities Sector - [398 Attacks] - [13.1%]
- Financial Services Sector - [375 Attacks] - [12.4%]
- Healthcare and Public Health Sector - [299 Attacks] - [9.9%]
- Information Technology Sector- [283 Attacks] - [9.3%]

In 2024, the overarching prevalence of ransomware in the cyber threat landscape is anticipated to persist. This enduring trend is underscored by the continual emergence of new ransomware groups, coupled with the adept utilization of tools and services by these threat actors. **As long as the likelihood of a payday is high, and the risk of getting caught is low, ransomware will remain a threat.**

PREVENTING RANSOMWARE EVENTS IN THE FIRST PLACE

Mitigating malware and ransomware attacks guidance issued by the *National Cyber Security Centre*, provides actions to help organizations prevent a malware infection, and also steps to take if you're already infected. You should adopt a 'defense-in-depth' approach. **This means using layers of defense with several mitigations at each layer.** You'll have more opportunities to detect malware, and then stop it before it causes real harm to your organization.

Action 1: make regular backups! Ensure that your cloud service protects previous versions of the backup from being immediately deleted and allows you to restore to them.

Action 2: prevent malware from being delivered and spreading to devices! Use mail filtering (in combination with spam filtering) to block malicious emails and remove executable attachments; block known-malicious websites; actively inspecting content using signatures to block known malicious code.

Action 3: prevent malware from running on devices! Consider whether enterprise antivirus or anti-malware products are necessary, keep software up to date; provide security education and awareness training to your people; configure host-based and network firewalls, disallowing inbound connections by default.

Action 4: prepare for an incident! Ensure incident management playbooks and supporting resources are available; ***Exercise your incident management plan;*** what processes need to be followed to restore servers and files from your backup solution; how you would continue to operate critical business services; revise plans based on lessons learned!

RANSOMWARE

Key Takeaways:

#1: FBI National Press Release, issued May 30, 2024, showcases the work of Operation Endgame, a multinational coordinated cyber operation to dismantle criminal infrastructure responsible for hundreds of millions of dollars in damages worldwide

#2: Healthcare and Public Health sector saw a 36% increase in ransomware attacks in Q1 of 2024 compared to the previous year.

#3: Adopt defense-in-depth approach to prevent malware infections!

OSINT: Open Source Intelligence

Transform intelligence analysis and production! That describes my mission very well for FIR Risk Advisory LLC, to improve the collection, interpretation, and distribution of open source fraud and cybersecurity intelligence to business leaders globally **to provide decision advantage**!

DID YOU KNOW: The U.S. Intelligence Community (IC) is a coalition of 18 agencies and organizations that work both independently and collaboratively to inform our national security decisions!   Download your copy of the ***OSINT Strategy***.

As the open source environment continues to expand and evolve at breakneck speed, the ability to extract actionable insights from vast amounts of open source data will only increase in importance. To advance the OSINT discipline, the IC will:

- streamline data acquisition,
- develop innovative technologies to collect and derive insight from open source data,
- strengthen the coordination of open source collection activities across the community,
- update and standardize OSINT tradecraft, and
- develop a highly skilled OSINT workforce.

GOALS FOR OSINT

Goal: Coordinate Open Source Data Acquisition and Expand Data Sharing
Expanding the accessibility of Publicly Available Information (PAI) and Commercially Available Information (CAI) will maximize the return on IC investment and increase the value of open source data and tools across all IC missions.

Goal: Establish Integrated Open Source Collection Management
The IC must establish a new and improved community-wide collection orchestration system that enables collective visibility on requirements and collection efforts.

Goal: Drive OSINT Innovation To Deliver New Capabilities
The OSINT community is already pioneering new uses of artificial intelligence, machine learning, and human language technologies for the OSINT mission. The IC must expand and accelerate these efforts to sustain a competitive edge. External partnerships will be vital to success in this domain.

Goal: Develop the Next-Generation OSINT Workforce and Tradecraft
The growth of generative artificial intelligence (GAI) presents both opportunities and risks for OSINT tradecraft. GAI can be a powerful tool to enable timely and insightful OSINT production.

CYBER INSURANCE MARKET UPDATE

The **National Association of Insurance Commissioners** produces a ton of interesting and actionable content, with Cybersecurity making the content list last fall with 2 interesting and useful reports.

First, the Report on the Cybersecurity Insurance Market presents lots of data and trends while discussing changes in the cybersecurity market and the reason for those changes. Second, The Current State of Cyber Insurance and Regulation in the Context of Investment Efficiency and Moral Hazard: A Literature Review was published in the Journal of Insurance Regulation and dives deep into the motivation of Managers' choices on information-security related investments for risk prevention and the desire to transfer risk through the purchase of cyber insurance, fueling the growth in the cyber insurance market. The authors make the argument for **the need of an optimal level of regulation to reduce cyber risk exposure of businesses and insurers**, as well as to protect consumers and the overall economy.

Both reports contain a wealth of cyber specific information, trends of cyber insurance, the economics of cyber risk and cybersecurity, the market reaction to cyberattacks, and trends in the Cybersecurity landscape. **NAIC Report Highlights:**

- U.S. cybersecurity Insurance market is the largest in the world, of roughly $9.7B in direct written premiums (DWP) for 2022, growing 41% YoY.
- The top 20 groups in cyber insurance market reported direct loss ratios in the range of 10.7% to 85.9% in 2022, averaging 44.6%, down from 66.4% in 2021.
- Chubb Ltd Grp; Fairfax Financial, and AXA Ins Grp hold the top 3 spots in the top 20 rankings from 2021 and 2022, accounting for 25% of cumulative market share.
- Cyberattacks and the use of ransomware continue to increase in 2022, prompting business to purchase cyber coverage and implement stronger cybersecurity controls.
- Cybercriminals have utilized ChatGPT and other AI platforms.

- Insurers continue to limit their exposure by implementing endorsements around security measures. **Upfront and annual cyber risk assessments are required**, and **known vulnerabilities in the National Vulnerabilities Database (NVD) must be patched within 30-45 days** without seeing your cyber coverage affected.

- Insurers continue implementing more restrictive coverage terms for certain cyber risks, including lower sub-limits and aggregate limits.

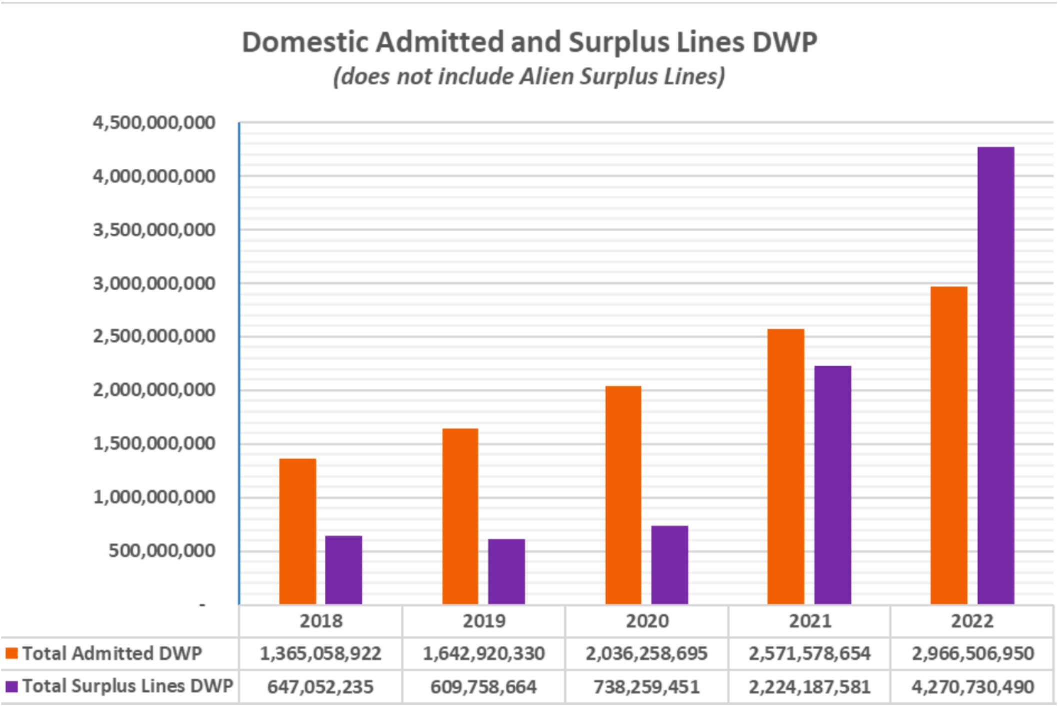
- Cyber events and losses usually cross state or country borders, meaning an insured will want to be sure which countries and territories the cyber insurance policy covers.

- Insureds are also **held accountable for their cyber hygiene** to receive coverage, including endorsements that reduce coverage if businesses do not patch known vulnerabilities in a timely manner.

CYBER INSURANCE

Key Takeaways:

1. Upfront and annual cyber risk assessments are required.
2. Patch known vulnerabilities in a timely manner.
3. Cyber Insurance is becoming harder to find!



	2018	2019	2020	2021	2022
🟧 Total Admitted DWP	1,365,058,922	1,642,920,330	2,036,258,695	2,571,578,654	2,966,506,950
🟪 Total Surplus Lines DWP	647,052,235	609,758,664	738,259,451	2,224,187,581	4,270,730,490

NAIC Report Figure 3: Direct written premium

Current State of Cyber Insurance and Regulation Highlights:

- **The economics of cyber risks and cybersecurity**: Reliance on digital transactions and containing extensive personal data are susceptible to cyber incidents. Cyberattacks cause substantial financial and reputational damage.

- **Cyber risk is difficult to quantify:** Due to the uncertainly regarding the severity, probability, and timing of cyberattacks. Since managers cannot easily justify the tangible costs to both the firm and its customers against intangible benefits, they may defer cybersecurity investment until a cyberattack occurs.

- **Market reaction to cyberattacks**: Managers are under pressure to produce earnings that meet expectations and may take excessive risks to maintain an upward trend in stock price, which may eventually destroy firm value, shareholder wealth, and image.

- **Role of Board governance for effective cyber risk management:** Empirical evidence shows that the involvement of an IT executive in senior management reduces the likelihood of experiencing cyberattacks. Strong corporate governance is necessary but not sufficient alone to achieve effective cyber risk management.

- **Cyber Insurance and the role of cyber insurers:** Firms resort to cyber insurance policies to manage cyber risk and hedge against potential losses. Obtaining cyber insurance can benefit the firm as upfront risk assessment and evaluation of how prepared a firm is to handle cyber attacks, as required by insurers.

- **Trends in cybersecurity landscape:** A substantial increase in the number of cyberattacks and ransomware makes cyber insurance a less attractive business for insurers. **Cyber insurance is becoming harder to find** and many companies have to spend more money to purchase cyber insurance for less coverage. The largest increases in cyberattacks are in the Netherlands, Ireland and the U.S., and Netherlands, Spain, and France experienced the largest increase in ransomware attacks.

Download **NAIC Report on the Cybersecurity Insurance Market** ***here***
Download **The Current State of Cyber Insurance and Regulation** ***here***

FIR

FIR RISK ADVISORY,LLC

— Fraud Intelligence Report —

Download your copy of FIR Quarterly from firriskadvisory.com for FREE!

DOWNLOAD FIR

Contact Us

Bruce Bird, Principal

Colorado, United States

970-689-2473 mobile

bbird@firriskadvisory.com

https://firriskadvisory.com/

Subscribe on LinkedIn