# FIR RISK NEWS

## VERIZON DBIR + U.S. NATIONAL INITIATIVES!

**INSIDE**

**TOP FINDS THIS MONTH**

**Verizon DBIR**

**Secure by Design**

**U.S. Cybersecurity Posture & Strategy**

**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


# 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**.

The annual Verizon DBIR, featured below, is a must read for Leaders and Teams focused on cybersecurity, attacker trends and successes!

The U.S. Cybersecurity posture is a first of it's kind report and provides useful details of the current posture of the United States and the latest plan to continue to improve. Organizations need to be aware of this first line of defense from our Nation's agencies whose mission is to protect America, our Organizations and Individuals from threat actors.

# Verizon DBIR


In my experience, the **DBIR team** has delivered consistently the most **comprehensive research on data breach and incidents** for 20 years now! Today's newsletter is a brief recap of charts and trends I found most interesting from a financially motived fraud perspective.

**DBIR HIGHLIGHTS:**

**Adversaries follow the path of least resistance:** Path of least resistance for adversaries are known vulnerabilities! CISA Known Exploited Vulnerabilities (KEV) catalog, shows it takes on average 55 days to remediate 1/2 of known vulnerabilities! DBIR reported it takes 5 days for vulnerabilities to be exploited causing a 50 day head start on average for adversaries to take advantage!

**Social Engineering is a path of least resistance:** DBIR reported it takes less than 60 seconds for users to fall for phishing emails to click and enter data requested! Pretexting aka Business Email Compromise (BEC) made up nearly a quarter (24%) of Financial actor motive goal actions over the past 2 years. The human element makes it easy for the adversary to succeed.

**Ransomware & Extortion continue to trend up:** Extortion occurs when the adversary steals sensitive information and threatens to leak that information publicly unless the victim makes a payment to prevent disclosure. Ransomware is a type of malware which prevents you from accessing your device and the data stored on it, usually by encrypting your files. A criminal group will then demand a ransom in exchange for decryption.

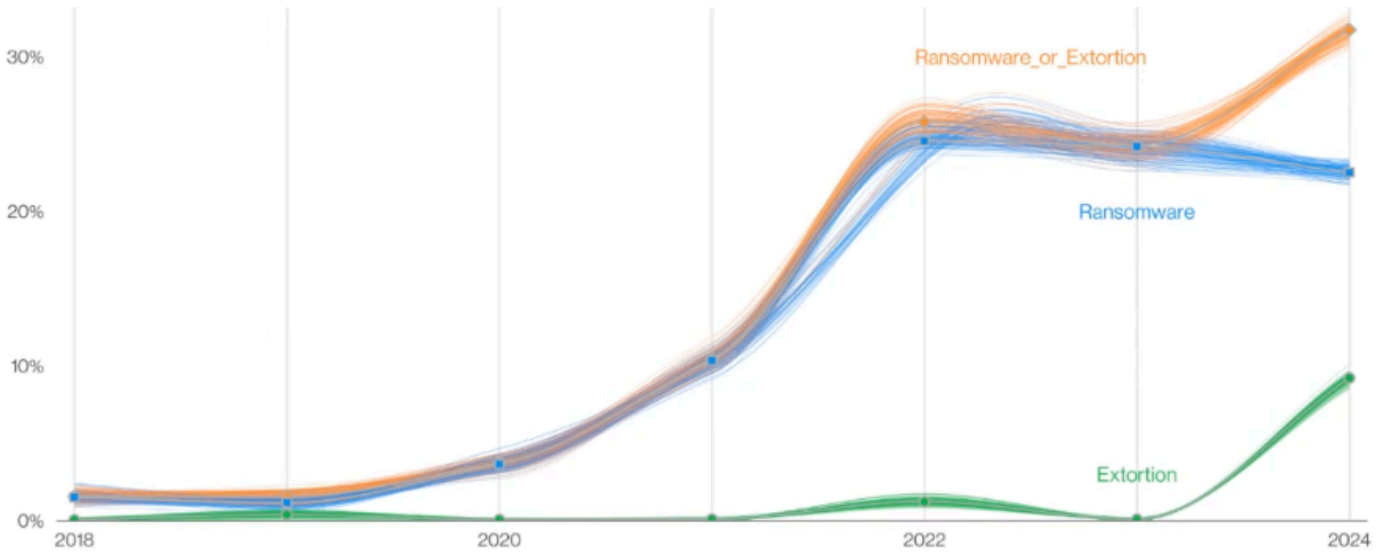


**Figure 7.** Ransomware and Extortion breaches over time

Verizon DBIR 2024 Figure 7

## "Ransomware & Extortion pay $50,000 on average"

***-VERIZON DBIR 2024***

**Comparison 2018 DBIR to 2024:** Purely by the numbers, 2018 saw 53,308 incidents and 2,216 breaches reported. 2024 saw 30,458 incidents and 10,626 breaches.

Incidents data **decreased 43%** where Breaches have **increased by 380%**. 2018, Breaches represented 4% of all reported data and in 2024, now represent 26%!

*Download* The VERIZON DBIR **here**

# DBIR INSIGHTS

## Key Takeaways:

#1: Attackers follow the path of least resistance, protect your business by ensuring high value assets and accounts don't offer an easy way to exploit them.

#2: Social Engineering continues to exploit human tendencies to trust and click- Educate your employees and partners to think before they click!

#3: Add protections to prevent malware infections!

# CISA driving Secure By Design Principles:


Just over 1 year ago, America's Cyber Defense Agency, CISA and 17 U.S. and international cybersecurity agencies released a whitepaper titled **"Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and Default."** This served as the launch of Secure By Design initiative, read the launch press release **here**.

The idea is to bake security into product development and centers on 3 key principles:

1. Take ownership for the security outcomes of the customers.
2. Embrace radical transparency.
3. Build the organizational structure to achieve these goals.

## What it Means to Be Secure by Design

"Secure by Design products are those where the security of the customers is a core business requirement, not just a technical feature. Secure by Design principles should be implemented during the design phase of a product's development lifecycle to dramatically reduce the number of exploitable flaws before they are introduced to the market for broad use or consumption.

Products should be secure to use out of the box, with secure configurations enabled by default and security features such as multi-factor authentication (MFA), logging, and single sign on (SSO) available at no additional cost." Read the Cybersecurity Best Practices Secure-by-design advisory **here.**

---

**"Every technology provider must take ownership at the executive level to ensure their products are secure by design."**

---

**Fast forward to today**, lots of progress is being made as evidenced by the latest updates from CISA:

**June 20, 2024**- Why SMBs Don't Deploy Single Sign On (SSO)

1. Small enterprises often opt for manual passwords and hands-on approaches over an SSO option.
2. Lack of technical know-how and awareness poses another significant barrier to SSO adoption.
3. Customers have varying degrees of satisfaction with the accuracy and completeness of support materials and instructions.

Manufacturers should recognize these unique challenges for their SMB customers and configure their settings to reduce operational friction and frustration.

**May 13, 2024**- published Categorically Unsafe Software blog post **here**

- "The bottom line is that a secure by design software development program necessitates formal efforts to eliminate entire classes of defect before the product ships rather than playing whack-a-mole with defects that appear on customer systems in production."

**May 09, 2024**- published The Top Four Things Tech Manufacturers can do to Bolster the Cybersecurity of Target-Rich, Cyber-Poor Organizations blog post here- the following four steps can guide software manufacturers to bolster the digital defenses of "target-rich, cyber-poor" organizations.

1. Take **CISA's Secure by Design pledge** to commit to building products that have security from the start and available out of the box.
2. Make it easy to use technology products securely for users of all skill level.
3. Contribute time and technical expertise to programs that support the cyber readiness of schools, municipalities, and non-profits.
4. Develop a program that offers tools or services to "target-rich, cyber-poor" organizations for free or at a discounted rate.

# Secure-by-Design INSIGHTS

## Key Takeaways:

1. Verify if your software vendors have signed and working to comply with the CISA Secure by Design guidelines as part of your Vendor Management program.
2. Require all your software vendors to sign the CISA's Secure by Design pledge, else begin looking to replace those vendors.
3. Support this effort by holding accountable the software manufacturer's your organization relies on!

# U.S. Cybersecurity Update

On May 7, 2024, the Office of the National Cyber Director (ONCD) released the **2024 Report on the Cybersecurity Posture of the United States.** I strongly recommend downloading and reading this report, it's very well written and is packed full of great content. There is far too much content to summarize in this newsletter, so I'm selectively condensing to give you the most compelling headlines.

**OVERVIEW:** The report content is organized by the following topics:

- Landscape of emerging technologies of an increasingly interconnected world.
- Cyber risk landscape and evolving vulnerabilities in our own defenses.
- Top Trends of 2023- Risks to Infrastructure (PRC threat unlike any America has previously faced), Ransomware, Supply Chain Exploitation, Commercial Spyware (allows malicious cyber actors to target victims with greater frequency), and Artificial Intelligence (one of most powerful technologies of our time).
- Current Efforts- Improving coordination and incident response, disrupting adversary activity, defending networks, strengthening cyber workforce, advancing software security, enabling a digital economy that empowers and protects consumers, investing in resilient next-generation technologies, managing risks to data security and privacy, enhancing security and resilience globally, and advancing a rights-respecting digital ecosystem.
- Future Outlook- 1. Rebalancing the responsibility to defend cyberspace away from end users and to the most capable and best-positioned actors. 2. Realigning incentives to favor long-term investments in future resilience.

The Administration has also released **Version 2 of the NCSIP**, which complements the findings of this report and outlines the next phase of action necessary to implement the President's Strategy and further improve U.S. national cybersecurity posture.

- The v2 plan fact sheet is available **here** for a quick overview. Read the full Implementation Plan **here.**
- The v2 plan is a full 64 pages containing 100 initiatives, check out my **LinkedIn FIR Risk Tuesday May 21, 2024 newsletter** that covers the most interesting aspects of the plan that is relevant to Corporations and Organizations as need to know information to stay informed on upcoming improvements in U.S. Cybersecurity protections.


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**