FRSECURE®

INFOSEC REPORT 2023

TL;
DR

FRSECURE

Report & data analysis by:

FRSecure CTO, Oscar Minks

NEED TO GET IN TOUCH?

6550 York Ave S #500, Edina, MN 55435

(877) 767-1891

hello@frsecure.com

Incident Response: CSIRT@frsecure.com

TABLE OF CONTENTS

FRSECURE

INTRODUCTION

Hello, and welcome to the first-ever FRSecure Information Security Report! As we march forward in our mission to fix a broken industry, we believe that providing the public with this data set and analysis is a critical step in increasing awareness and understanding.

About the Data

The data in this report is derived from nearly **400 validated security assessments and 55 incident response engagements** that were completed in the year 2022. Within these engagements, we've anonymized all the information, logged data on controls, incident root causes, exploits, and more. The result is a combination of analysis, interpretation, and related suggestions.

Objective

This data should be used to understand the current ecosphere of information security. See this as a lens into the eyes of the attacker, but more importantly, let's understand how those attacks can be prevented.

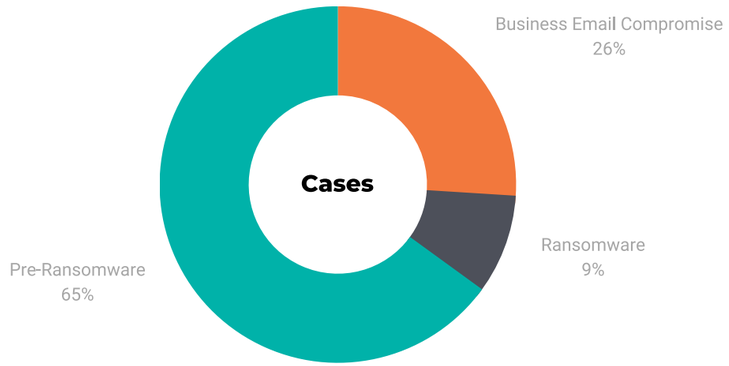
Purpose

The current state of our industry can feel overwhelming and daunting at times. I hope that this report will help provide clarity, a sense of normalcy, and a level of understanding that can be used as a powerful tool to aid in the maturation of each organization and person's information security posture.

We explore where we are winning, where we are improving, and where we are falling behind. We must also understand that our world evolves rapidly, and the data from this study will be used to improve further our assessment frameworks, understanding, guidance, and support of each other.

DIGITAL FORENSICS AND IR ANALYSIS

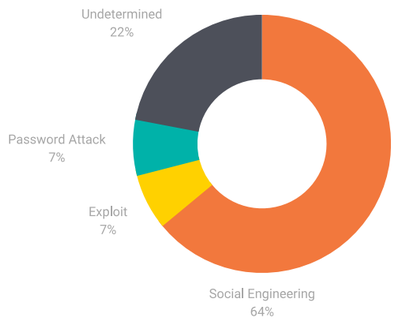
⚠ 2022 INCIDENT OVERVIEW



In the following pages, we will dive into these types of engagements to understand what events led to the compromise and more importantly, what can be done to decrease your organization's chance of being victimized.

Business Email Compromise

BEC ROOT CAUSE



- **68% of organizations** have deployed proper malicious code protections for all applicable transmission methods.
- **80% of organizations** test users periodically on their susceptibility to common attack vectors like downloading dangerous files and following malicious links in emails, documents, or web pages.
- However, **only 58% of organizations** mandate security awareness training for all employees and contractors regularly.

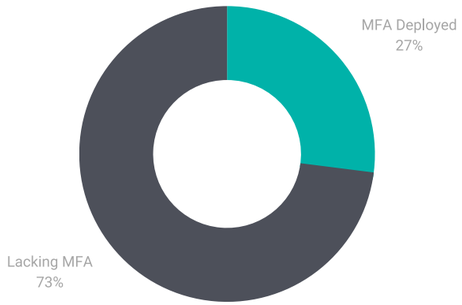
Safeguards should be put in place wherever possible to prevent these malicious emails from reaching your user's inbox in the first place and minimize the potential for damage if they do. Email gateway systems have come a long way in inspecting links and attachments, but as our analysis suggests, they are not infallible. Attackers continue to find ways to circumvent these controls and reach the users' mailboxes anyway.

Training, education, and buy-in are key! I encourage you to build a security program that arms your team with the knowledge to prevent this type of attack.

MFA should also be properly deployed to prevent the usage of credential sets harvested during a successful social engineering campaign.

MFA

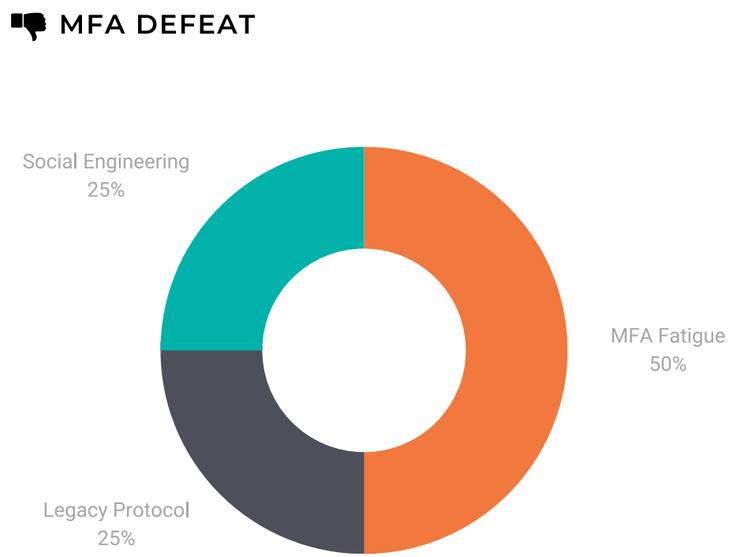
Of the fourteen business email compromise cases we worked, only four organizations had fully implemented multi-factor authentication controls. MFA is an essential part of any defense to prevent unauthorized access to your network and email system.



- **70% of organizations** protect administrative login pages with multi-factor authentication.
- **60% of organizations** protect general-user login pages with multi-factor authentication.

MFA DEFEAT

50% of our BEC incidents where MFA was properly deployed were the result of MFA fatigue attacks (the user is tricked into approving the MFA notification).



MFA Recommendations

FRSecure recommends that you consider the usage of hardware security key devices or the usage of a widely trusted authenticator application.

MFA should be deployed to all accounts in the tenant. Ensure that service accounts are configured to prevent public access unless required. If they are required – implement MFA.

While this section is focused on BEC, it should be noted that this logic can and should be applied to all log-on systems and especially any publicly available systems without exception.

FRSECURE

BEC COMPROMISE PAYLOAD

- **86% of these fraudulent ACH requests** were unsuccessful, and our assessment data helps us understand why.
- **92% of organizations** require dual control for all financial transactions exceeding a designated dollar amount.
- **68% of financial accounts** are monitored and balanced daily.
- **In 43% of BEC cases**, we observed continued phishing targeting internal users, external clients, and often both.
- In **ALL** cases, data ex-filtration was successful.

Logging

The root cause for **22% of our BEC investigations** was undetermined.

In all of these examples, insufficient logging capabilities limited our investigation efforts and ultimately prevented us from determining the root cause. A minimum of 12 months of logs should be stored for all critical systems and infrastructure if possible.

A proper SIEM implementation will also allow you to normalize your environment and develop alerts based on anomalies.

- **90% of network time** is synchronized with NTP on all devices (e.g., servers, firewalls, switches, workstations).

Our assessment data reveals that most organizations are logging security-related events on critical systems, but a significant population is still struggling with correlation, management, and review of those logs.

- **76% of security-related events** on critical systems are consistently and sufficiently logged.
- **64% leverage group policy** to enforce specific logging and auditing of important events.
- **60% of organizations** have a separate, isolated logging system that is employed to collect and protect log files.
- **47% of logs from critical systems** are aggregated and correlated to enable the identification of events that span multiple systems.
- **38% of organizations** have defined and implemented a formal standard for logging, monitoring, and alerting on events and potential incidents.

BONUS TIP

Throughout our investigations, PowerShell-based attacks are regularly observed **(20% of cases in 2022)**. A gap we continually observe in engagements is a lack of proper PowerShell logging. We recommend you ensure PowerShell script block logging is enforced via GPO, and that those logs are retained.

The Defense: Normalize Your Environment

Regularly review all connected devices with access to your environment and investigate any unapproved devices promptly.

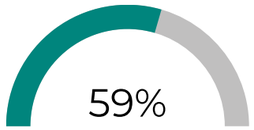
- **63% of organizations** require access controls for mobile devices.
- **69% of software applications** within the organization are inventoried.

If you discover a compromised user in your environment, don't assume they are the only victim.

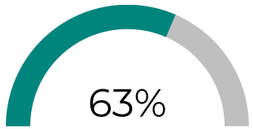
FRSECURE

MOBILE DEVICE MANAGEMENT

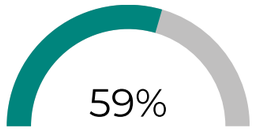
As more and more organizations adopt bring-your-own-device (BYOD) policies, this risk continues to grow. FRSecure recommends that organizations lacking in this area act now.



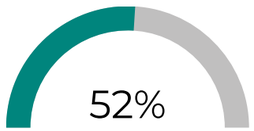
Have a mobile device security policy applying to all mobile devices used by the organization.



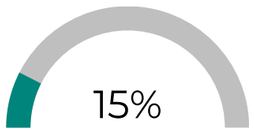
Organizations require access controls for mobile devices.



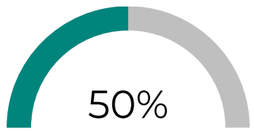
List remote disable, wipe, and account lockout as documented mobile device requirements.



Have an MDM solution enforcing control for mobile devices accessing private data.



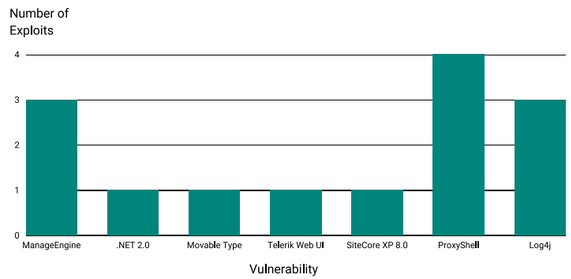
Mobile devices employ anti-malware protection.

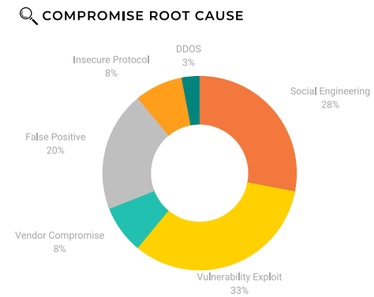


Have mobile computing guidelines or procedures handling device security.*

Ensure that security policies are defined and applied to all mobile devices that can access the organization's assets. Review current acceptable use policies.

RANSOMWARE AND INTERNAL COMPROMISE





Application Exploits

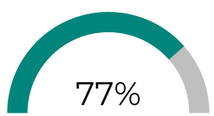
32% of all ransomware and internal compromise cases and **24% of all cases** were the result of a vulnerability exploit.

Another key finding: only one vulnerability exploit was the result of a vulnerability published in the last 12 months. All others had been published the previous year or before. One even dated back to 2017.

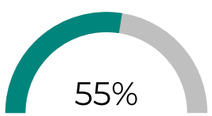
How Do We Manage These Vulnerabilities?

Asset Management

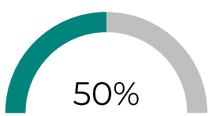
Once a comprehensive inventory approach is established, we can now be confident that we are including all assets in our vulnerability management program.



Maintain a complete inventory of assets for technical vulnerability management.



Critical business assets and their dependencies have been identified.



A complete, up-to-date, and detailed inventory of all cloud services is maintained.

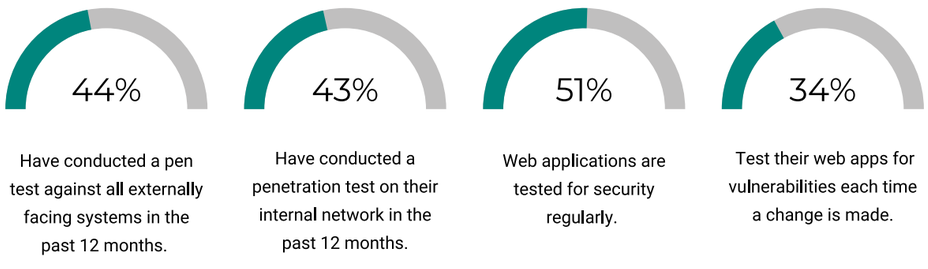
Vulnerability Management

At a minimum, organizations should be scanning quarterly. It is our stance that monthly or continual scans should be the ideal state for all organizations.

Most organizations had no critical or high-severity vulnerabilities on externally accessible systems.

- **86% of organizations** had no critical severity (CVSS 10) vulnerabilities on systems exposed to the internet.
- **82% had no high-severity (CVSS 7-9) vulnerabilities** on systems exposed to the internet.

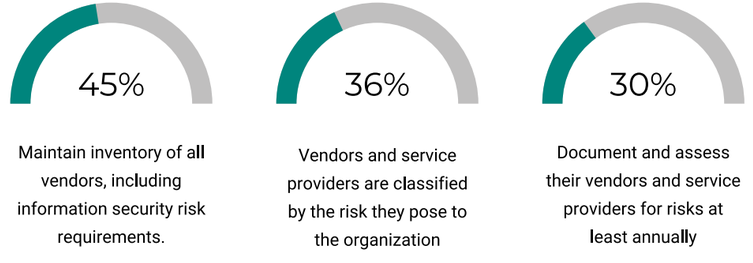
Penetration Testing



Completing internal network, external network, and web application penetration tests identifies vulnerabilities and risks that may not be discovered through scanning alone.

Vendor Risk Management

Three engagements were the result of a compromised vendor.



Engage Your IR Provider Early

Early detection and prompt knowledgeable response are critical opportunities in our defense mechanisms.

100% of the ransomware investigations confirmed the point of ingress was due to vulnerability exploitation, and dwell times ranged from **15 hours to 9 months**. In **80% of all ransomware cases from 2022**, backups were damaged as part of the encryption process.

Backup Strategy

While we can report that most organizations have an effective backup strategy, and most have an off-site storage procedure in place, many still have network connectivity to the backup location.

- **91% of organizations** have an effective backup strategy.
- **85% of organizations** store those backups in a remote facility to avoid physical disaster.

Backups should also be tested. Today, **just over half of all organizations** are periodically testing and validating backup data.

Backups were periodically tested and validated in **59% of organizations** assessed.

False Positives

Reporting early is key to defending. If these had been true positives, the likelihood of significant impact would have been greatly reduced.

You can even measure some key IR-related metrics in these situations.

- How quickly did we detect?
- How quickly did we report?
- What was the turn-around time of our IR partner?
- Did everyone involved truly understand their responsibilities?

IR PREPAREDNESS

Insurance is not a plan, and you're doing it wrong.

- **48% of organizations** assessed have defined a formal incident response plan.
- **30% of organizations** assessed are testing their incident response plan at least annually.

Cyber Insurance Policies and Providers

Only 68% of organizations have engaged their insurance provider pre-incident. A proactive consultation will allow you to select your breach counsel representative and to confirm the vendor(s) that will be used in the event of an incident.

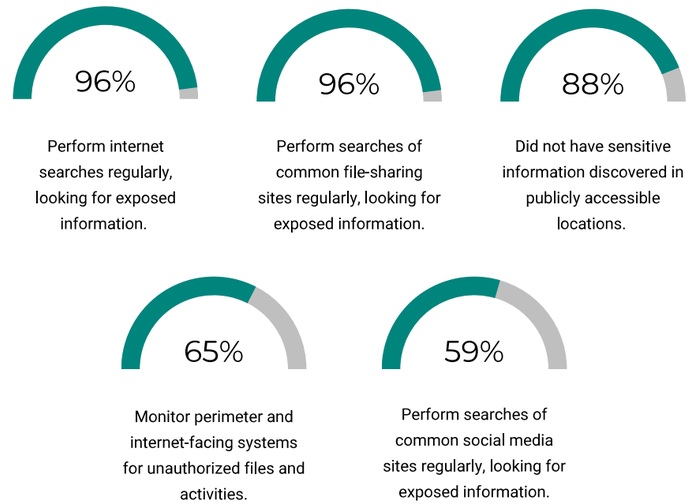
- **90% of organizations** observed have a cyber insurance policy.
- **68% of organizations** observed have obtained cyber insurance, selected breach counsel, and vendors (forensics firm, public relations firm, crisis management firm, etc.) are included in the organization's incident response plan.
- **22% of organizations** document how and when to notify insurers of cyber incidents.

Other Key Findings

44% of organizations configure egress filtering to only permit traffic that is specifically authorized for system functionality.

Identify and combat OSINT and recon techniques to supplement scanning
Email harvesting, leaked credential review, social media review, accidental information leakage.

- **96% search themselves online** and on file-sharing sites for leaked credential exposure.
- **Only 59% of organizations** are reviewing social media sites regularly.



TOP-DOWN APPROACH & SECURITY TRAINING

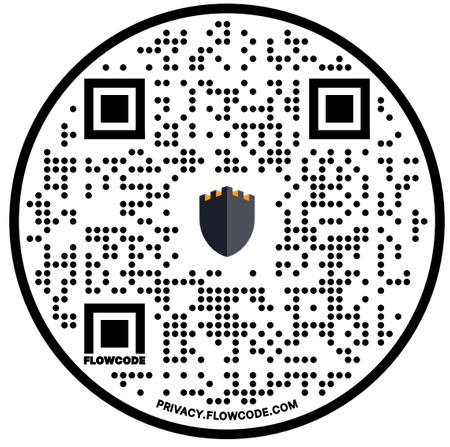
Organizations should work to develop training that focuses on leadership and privileged users in the environment. Your leaders have the most influence in an organization, and this can be used to promote and grow a culture that incubates security as a life skill.

Summary/Conclusions

- You can't secure what you don't know exists (inventory management).
- Get a better handle on your vulnerability management programs (scan frequently)!
- Logs, Logs, Logs (and normalize your environment)!
- MFA everything… but do it the right way (revolving access tokens)!
- IR Preparedness. Have an IR plan, and test the plan (it's not insurance)!
- Train, Train, Train – Develop a security-focused culture (from the top down)!
- Security is not easy (stop looking for easy buttons and do the work).

If there is anything at all in this report that you have questions about or need help with, don't hesitate to reach out to us. Part of FRSecure's mission is to be a resource for everyone in the industry, so we're always more than happy to help where we can.

Stay safe and happy hunting!



GET A COPY OF THIS REPORT TO SHARE

MORE RESOURCES

frsecure.com/resources