

Vulnerabilities

The Food That Hacker Eat



OLD REPUBLIC INSURANCE GROUP

Today's
ALTA Insights
Featured
Sponsor



About Me

Career Path



22 Years

IT Audit Group

CPA

CISA

CISSP



11 Years

State CISO



2 Years

CISO

Family



Fun



Outdoors

Fishing
Biking
Nordic Skiing



Travel

Family Vacations
Wine Trips



Arts

Concerts
Theatre
MN Orchestra

It's Brutal Out There



Being Secure May Not Be Good Enough



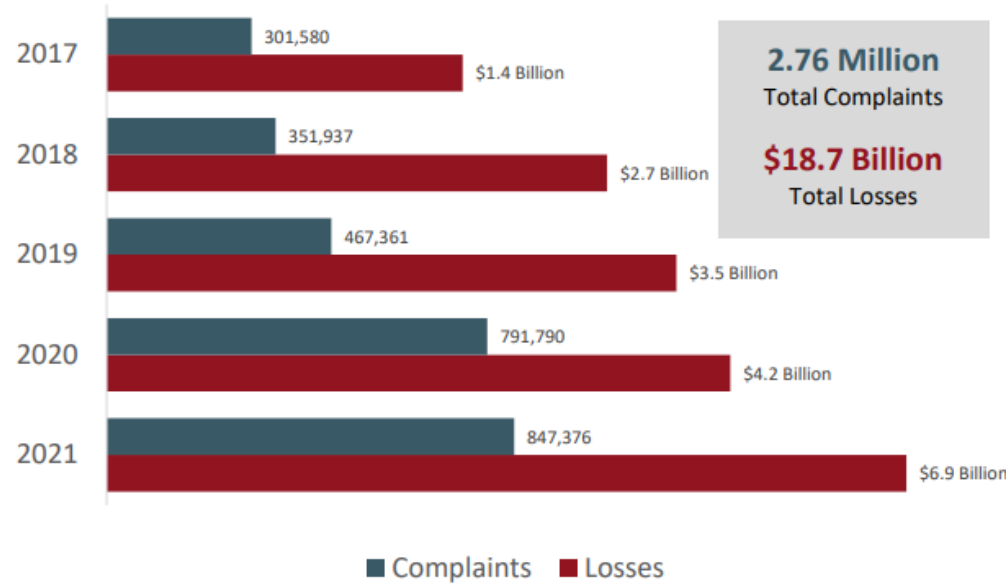
In March 2022, Deputy National Security Advisor Ann Neuberger issued a warning to United States corporations about nation-sponsored hacker groups

*“Russia recently disclosed that it will be attempting to compromise United States corporations, so there is no reason to believe that things will get easier. We need to prepare for even more sophisticated phishing attacks and business email compromise schemes. We also should expect the flood of critical vulnerabilities to continue, along with cascading effects from vendor security breaches. Collectively, these **changes in the threat landscape mean that we will need to be more than just secure, we also will need to be resilient.** Validating the efficacy of our data backups, business continuity and disaster recovery plans will be vital.”*

-- 2022 IT Security Risk Assessment Report

Another Year Like No Other

Complaints and Losses over the Last Five Years

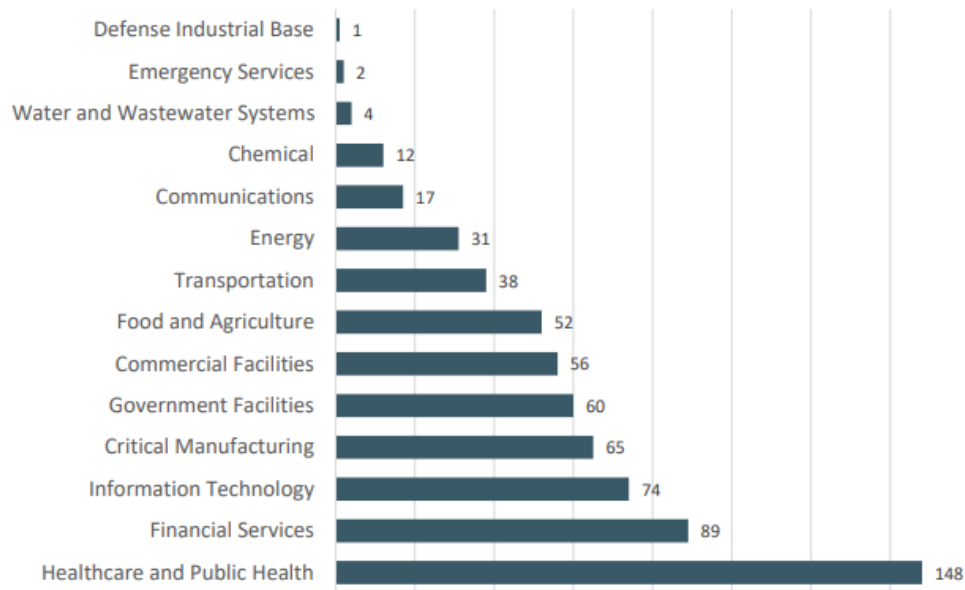


Source: FBI's 2021 INTERNET CRIME REPORT

Role	Driver
Attacker	Money to be made by cyber crime
Attacker	Inflict economic punishment
Attacker	Time to create new attack vectors
Attacker	Only need to be right once
Defender	Increasing IT complexity
Defender	More sophisticated attack vectors
Defender	Old technology that is hard to secure
Defender	Many silos of IT to manage and defend
Defender	Insatiable desire for more technology
Defender	Need to be right 100% of the time
Defender	Rising regulatory bar

Ransomware

Infrastructure Sectors Victimized by Ransomware



Source: FBI's 2021 INTERNET CRIME REPORT

Top Ransomware Variants Victimizing Critical Infrastructure
2021 Incidents



Russian threat actors are responsible for the top three ransomware variants



Vulnerabilities: The Food That Hackers Eat

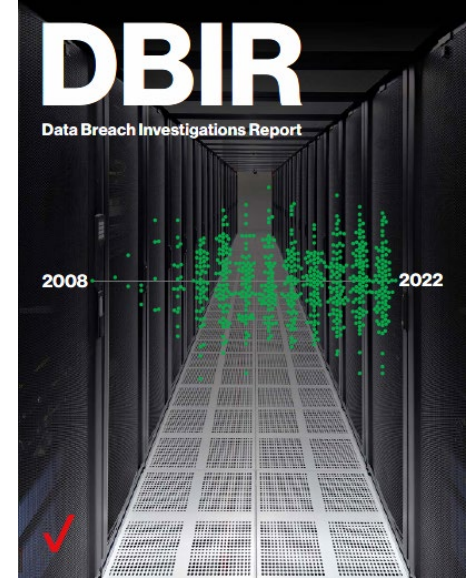
Goal

**Find and fix
vulnerabilities
before they
get found and
exploited**



Time is of the Essence

90%	Hacks perpetrated by external actors (North America)
3	Actions to compromise (Phish, Downloader, Ransomware)
>50%	Breaches discovered through actor disclosure



**More Threats
More Targeted
More Sophisticated**

Vulnerability Management Building Blocks



People

IT Security
(Finders)
IT Operations
(Fixers)



Tools

Vulnerability
Scanners



Process

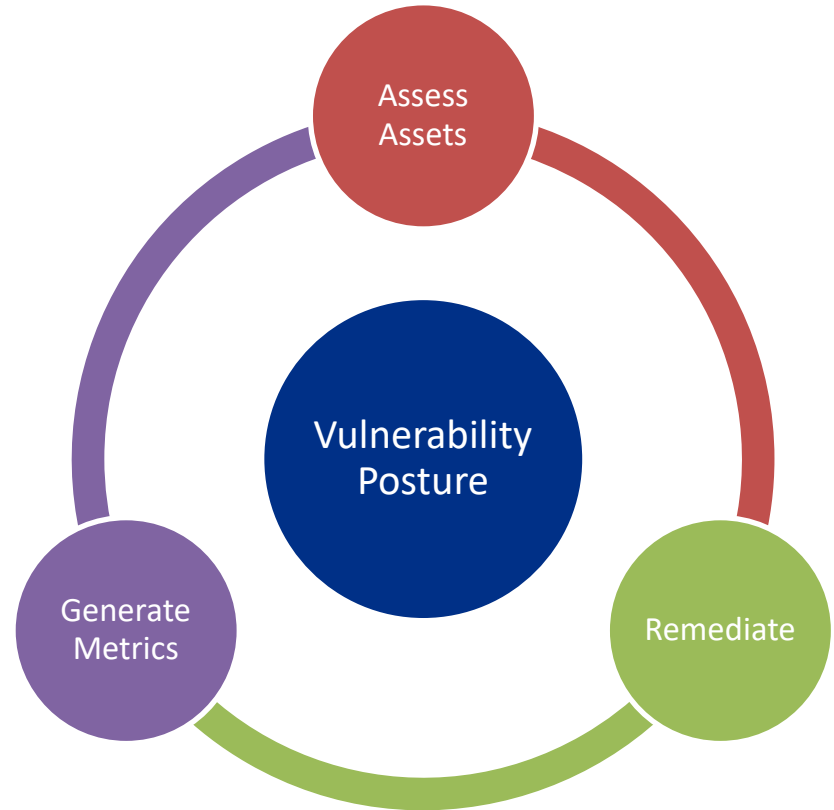
Scan Frequency
Remediation
Timeliness

A Continuous Process

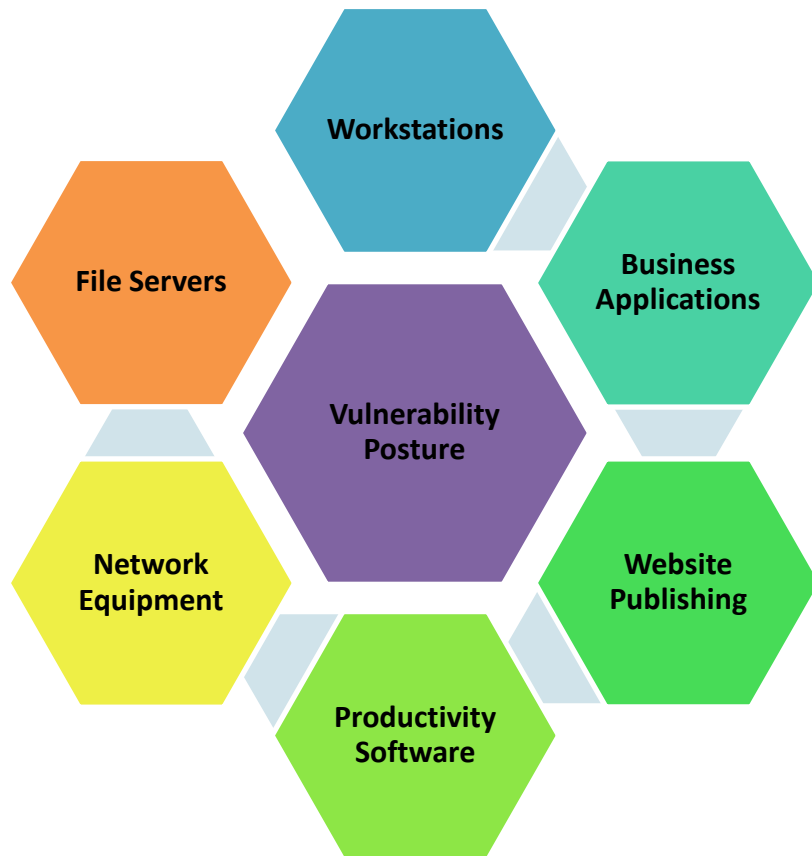
There will always be a massive inventory of vulnerabilities

The art of VM involves

- Understanding the inventory
- Prioritizing remediation
- Closely monitoring enterprise-wide risk metrics



Tip #1: Actively Manage Your IT Footprint



No software is immune from exploitable vulnerabilities

- Patch frequently
- Consider using auto update features in software, especially web browsers

Tip #2: Scan, If You Can

Free and Open-Source
Assessment Tools

Low Cost

Commercial
Vulnerability Scanners

Expensive

Coverage: Everything
Scan Type: Credentialed
Timeliness: As frequently as possible

Poll Question

How frequently do you scan your technology environment for exploitable vulnerabilities?

- A. Daily
- B. Weekly
- C. Quarterly
- D. Never – it only happens to the other guy

Tip #3: Keep Abreast of Threats

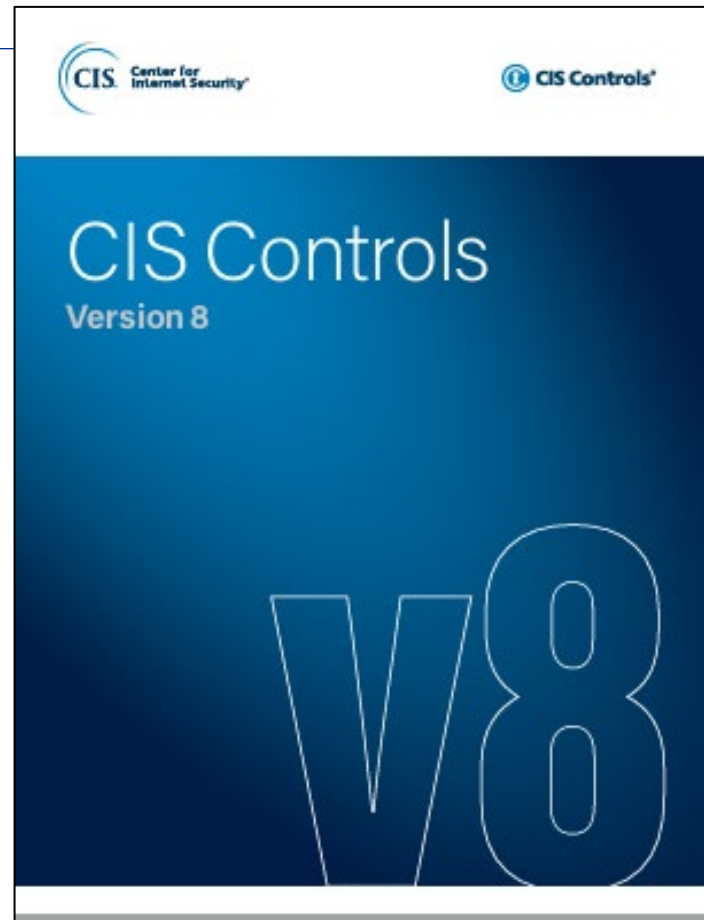
-  The Hacker News - Cybersecurity News and Analysis
-  FS-ISAC
-  The VERIS Framework
-  CSO | Security news, features and analysis about prevention, p...
-  Infosecurity Magazine - Information Security & IT Security Ne...
-  Dark Reading | Security | Protect The Business
-  Threatpost | The first stop for security news
-  BleepingComputer.com - Technology news and support
-  IT Security News and Cybersecurity News - IT Security Guru
-  Cybersecurity News | Information Security News
-  Krebs on Security – In-depth security news and investigation
-  Homepage - The Record by Recorded Future
-  Law360

Tip #4: Practice Defense in Depth

Assess your controls against industry best practices

Tasty morsels for hackers

- Unmitigated vulnerabilities
- Simple passwords without MFA
- Ability to install software on workstations



Tip #5: Know When to Fold Em

Cyber has become a high-risk big kid's game

Leverage IT vendors who are up to the task

- Email and messaging services
- Endpoint detection and response
- Security monitoring
- Continuous vulnerability scanning



Tip #6: Prepare for Rough Seas

Ransomware is now a major risk

Your survival will be predicated by having robust plans

- “Air-gapped” copy of all data needed to restore operations
- Disaster recovery procedures that are regularly exercised



“In today’s high-risk environment, it is no longer good enough to just be secure. Organizations also need to be resilient.”

Thank You

A wide-angle photograph of a sunset over a body of water. The sun is a large, bright yellow orb in the center of the horizon, casting a long, shimmering reflection down the water. In the background, a long pier extends from the right side towards the center, with a small lighthouse on its left end. Several streetlights are visible along the pier. The water is dark with gentle ripples, and some rocks are visible in the foreground on the right.

**I am Looking Forward to
Our Journey Together!**