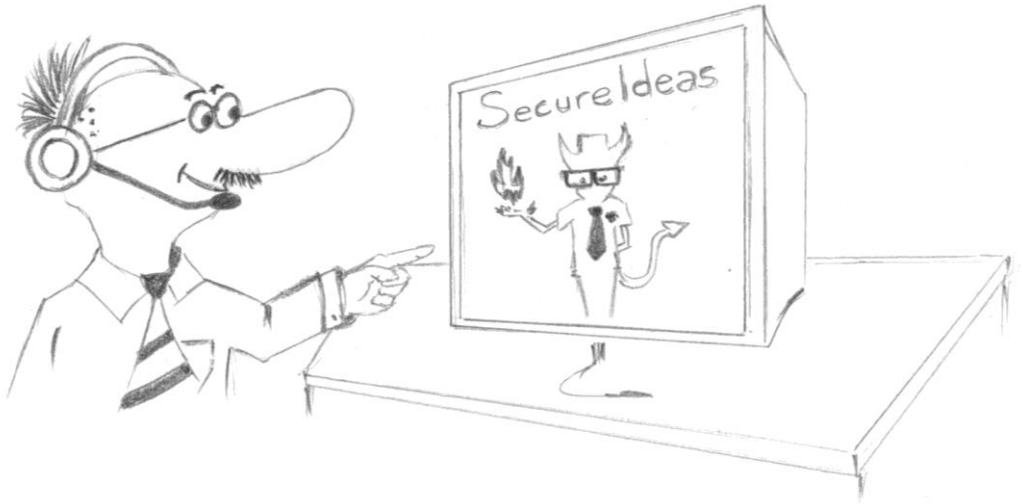
Secure Ideas
professionally evil®

The CISO's Myopia



Copyright © 2026 Secure Ideas LLC

Jordan Bonagura

Senior Security Consultant at Secure Ideas

- Located in FL
- Originally from Brazil
- jordan.bonagura@secureideas.com

Over 20 Years of Industry Experience

- Penetration Tester and Security Consulting
- College professor
- Worked on encryption of satellite communication
- Worked on police crime-solving unit

Other Items of Interest

- Be a father
- Simpson's lover
- Used to be a CISO...





Copyright © 2026 Secure Ideas LLC

Bill McCauley

Senior Security Consultant Secure Ideas, LLC

- I've been with Secure Ideas since 2018
- I am in a *remote* office location near DFW
- bill@secureideas.com

Over 20 Years of Industry Experience

- DoD Healthcare System Administration
- NERC / CIP Compliance Coordinator
- Solution Architect for custom compliance software
- Penetration Testing, Security Consulting, Ed & Training

Other Items of Interest

- Veteran
- Mini-Farm (dogs, cats, kids, chickens, ~~cows~~)
- Snowboarding
- Scarborough Renaissance Festival









Copyright © 2026 Secure Ideas LLC

Agenda



- Information Value
- Chronic Myopia
- The Constructive Process
- Pseudo-Security
- Examples
- What is necessary?

Copyright © 2026 Secure Ideas LLC

Information Value

- Let's reflect on the **importance of your company data.**



Copyright © 2026 Secure Ideas LLC

Information Value

- Now, imagine **what if** you need to manage your company **without your data**.





Copyright © 2026 Secure Ideas LLC

Information Value

- Even worse, imagine **if your data falls into wrong hands.**





Copyright © 2026 Secure Ideas LLC

Information Value

- So, **knowing** that your information is so important, **do you take care of it?**



Copyright © 2026 Secure Ideas LLC

Information Value

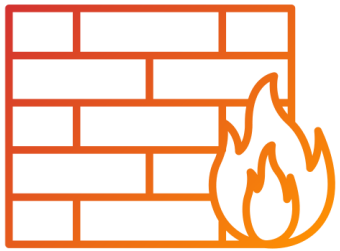
- I know that you are thinking, **but we take care of it, we have controls!**

Physical Controls



Locks!

Logical Controls



Firewall, IDS/IPS, A.V. etc

Services



Policies and Standards



Lockpicking Tools



Criminals



Users

She couldn't access her Facebook account at work anymore…

Copyright © 2026 Secure Ideas LLC

Information Value

- We also have a **CISO!**
  - Seeking solutions for security triad – aka C.I.A.
  - Enterprise risk management.
  - Understanding, mitigating and trying to stay ahead of a wide range of risks
    - (cyber, physical, operational and reputational).
  - People Management

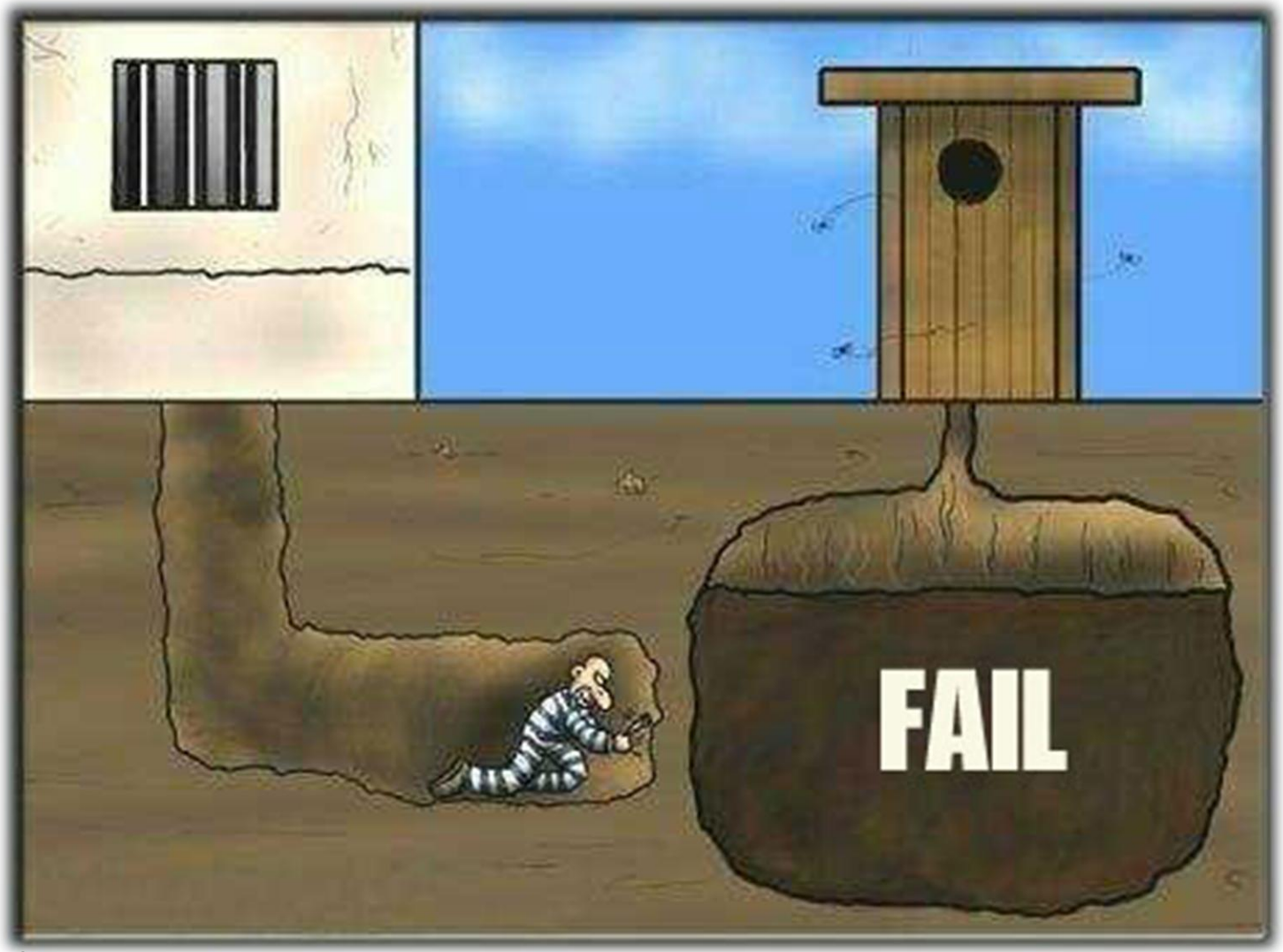




Copyright © 2026 Secure Ideas LLC

The Chronic Myopia

- So, now, was the **problem solved?**



Copyright © 2026 Secure Ideas LLC

The Chronic Myopia



The **constructive process** by which companies **continue** to develop and structure their security policies **still uses an "in-box" view.**

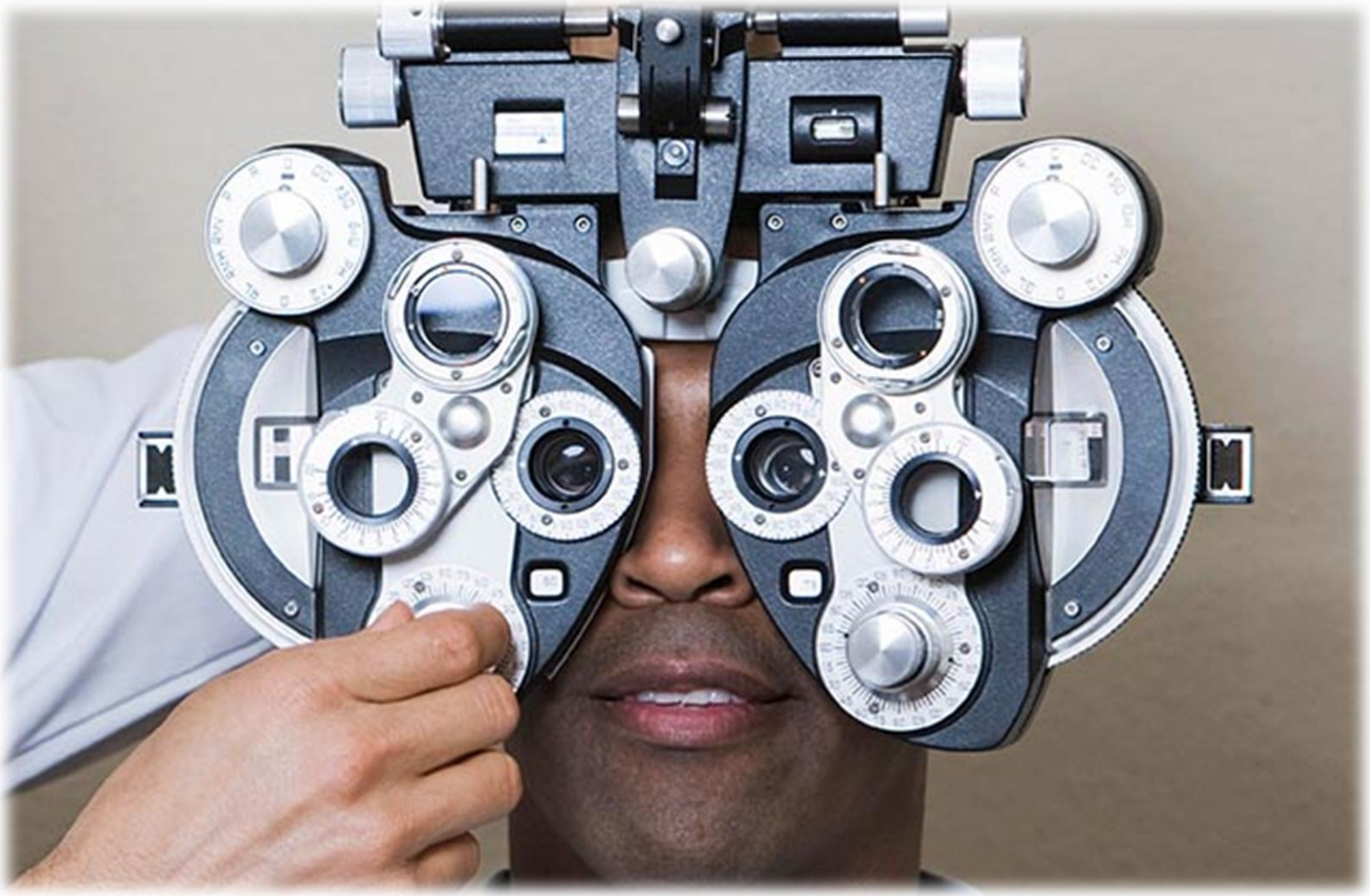
It is an **internal perspective** and, therefore, **limited in scope.**

This "approach" **was not, is not, and is unlikely to be** sufficient to cover the full range of vulnerabilities.

Copyright © 2026 Secure Ideas LLC

The Chronic Myopia – An Eye Exam

- Let's check, any **similarity** between the following scenes?



Copyright © 2026 Secure Ideas LLC







The Constructive Process

- "in-box" view **= tunnel vision.**





Copyright © 2026 Secure Ideas LLC

The Constructive Process

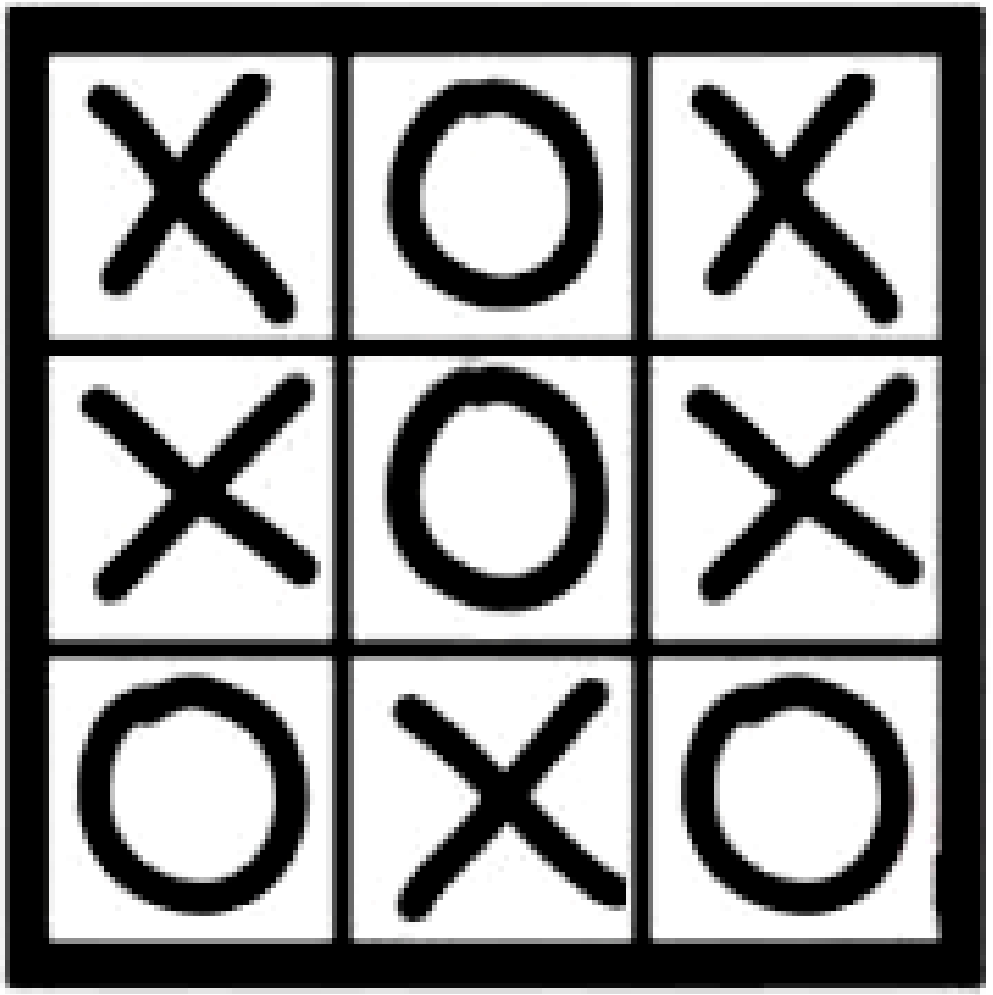
- #FAIL



Copyright © 2026 Secure Ideas LLC

The Constructive Process

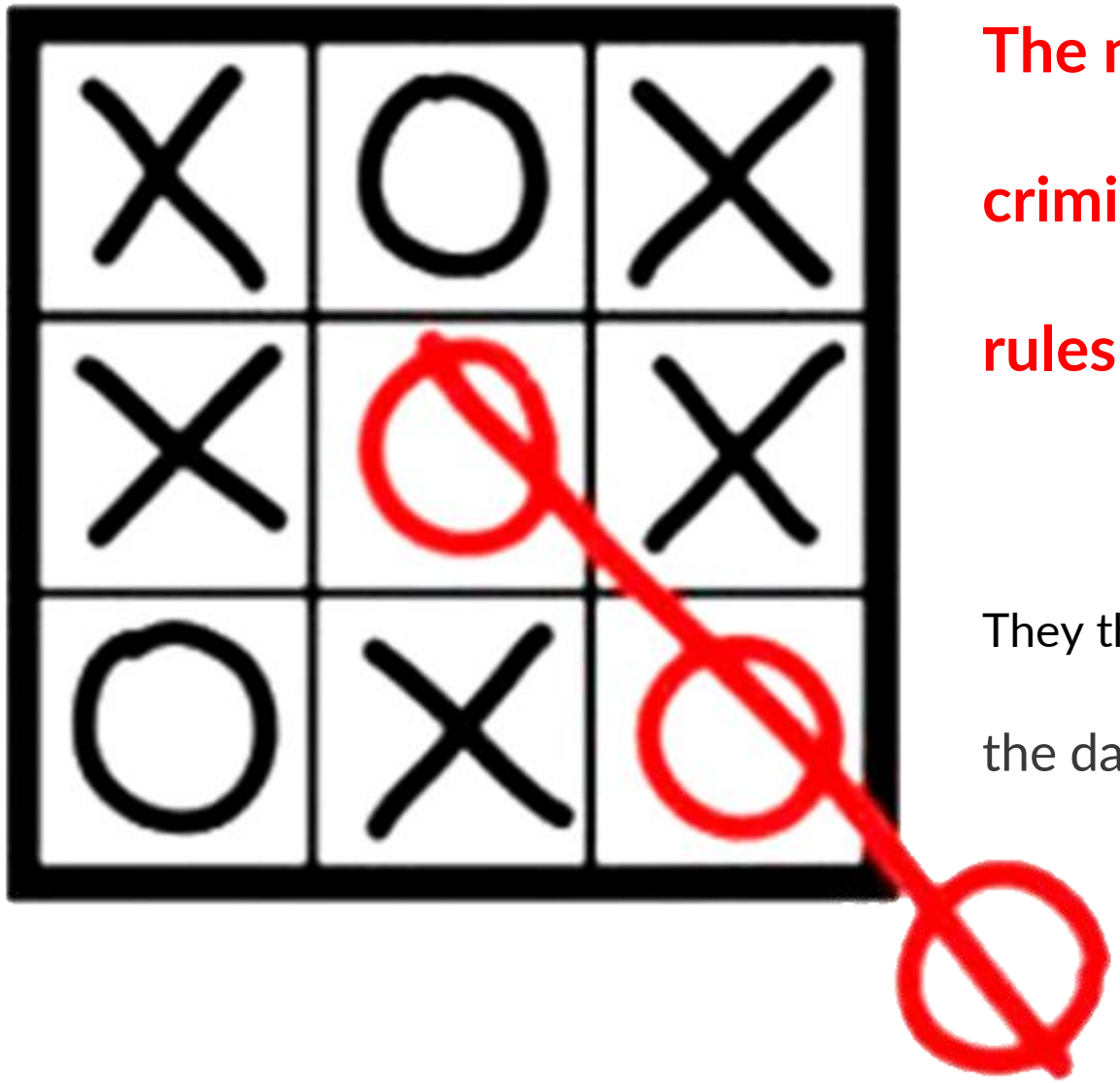
- Let's check… **Can you win?**



Copyright © 2026 Secure Ideas LLC

The Constructive Process

- **Breaking News!!!**



The myopia ignores that criminals do not follow your rules and policies.

They think differently and, at the end of the day, **it's many against few.**

Copyright © 2026 Secure Ideas LLC

The Constructive Process – How the criminals think?



There are **no rules** ,or rather, there are, but **not for those who want to break it…**

Laws, policies, rules, all of this belong to the companies, but **not for those who want to break it…**

they really don't care…

Copyright © 2026 Secure Ideas LLC

Pseudo-Security

- Supported by **your own policies**, many become prisoners of **pseudo-security.**



Copyright © 2026 Secure Ideas LLC

Pseudo-Security



Constructive Process

- “In-box” View
  - Pseudo-Security
    - 

Copyright © 2026 Secure Ideas LLC

Pseudo-Security

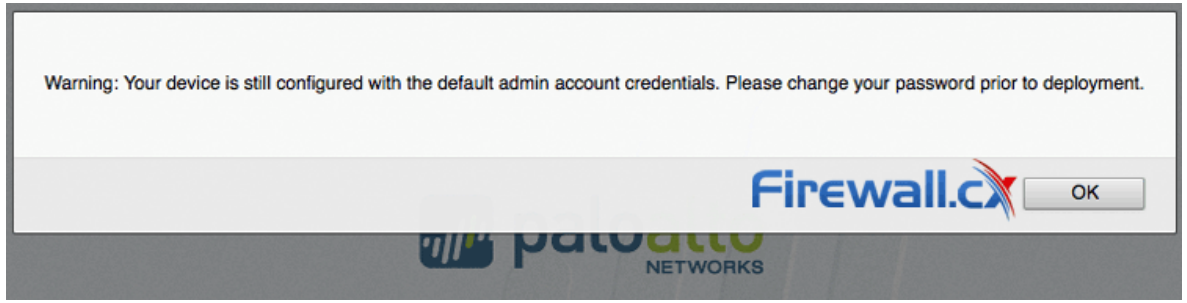
- **Still spending a lot of money and getting hacked?** Let's check why…

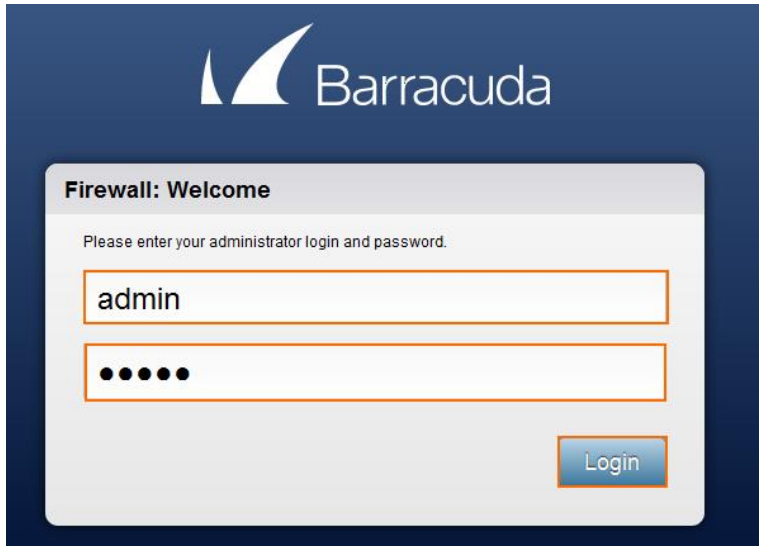


Copyright © 2026 Secure Ideas LLC

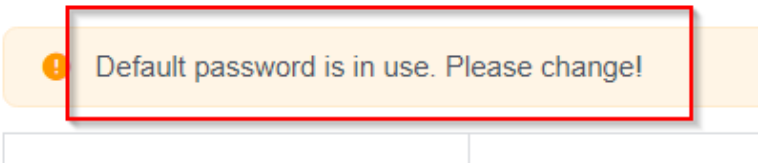
Examples

- Default Credentials





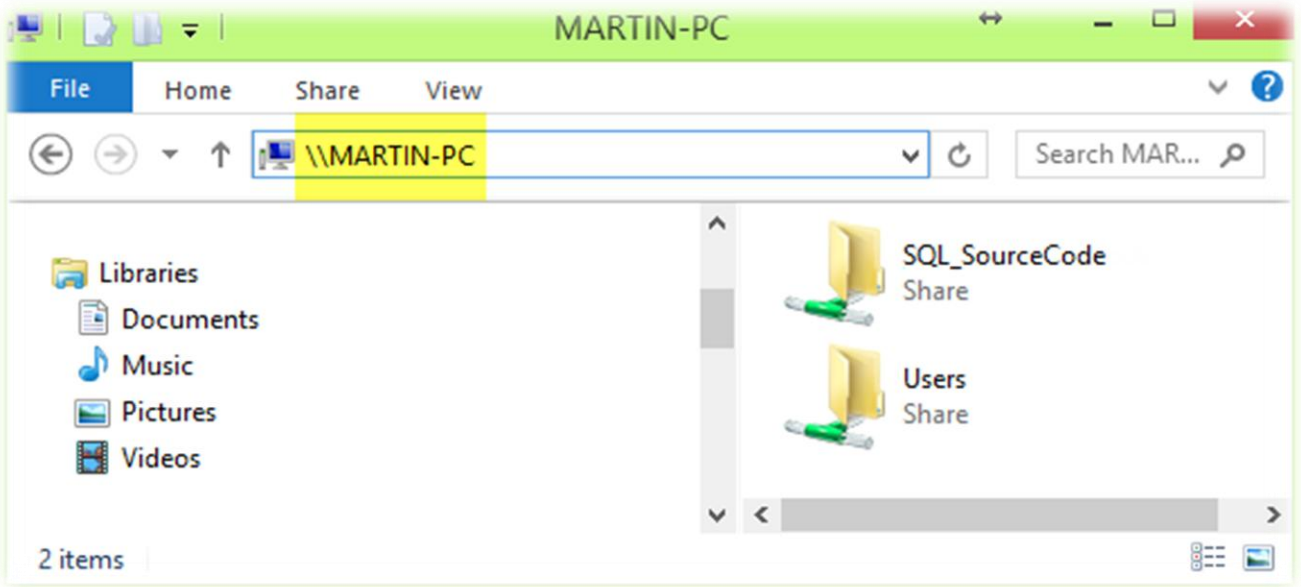


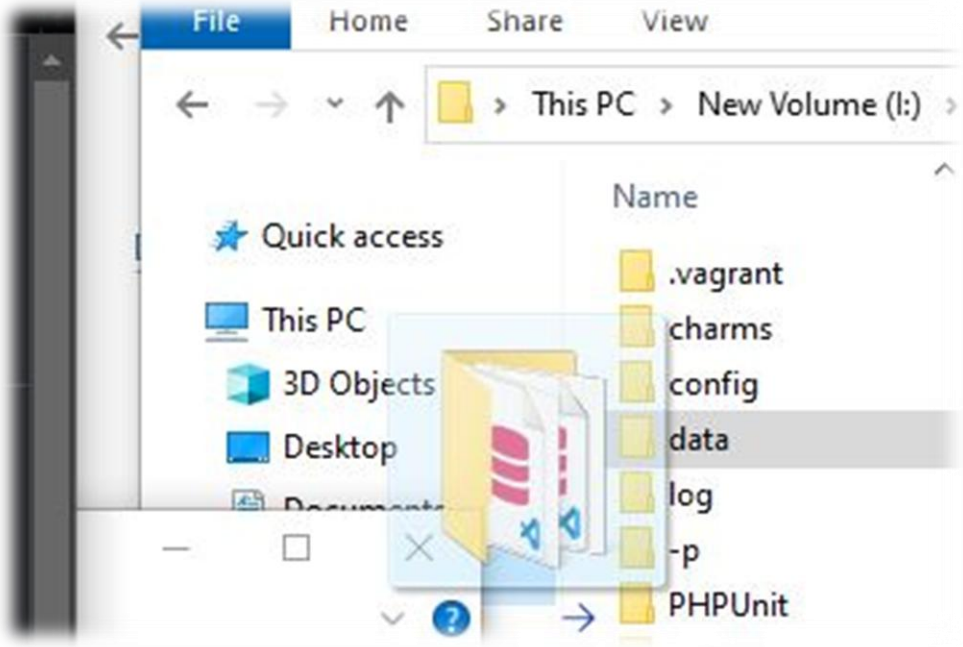


Copyright © 2026 Secure Ideas LLC

Examples

- File Shares Containing Sensitive Data

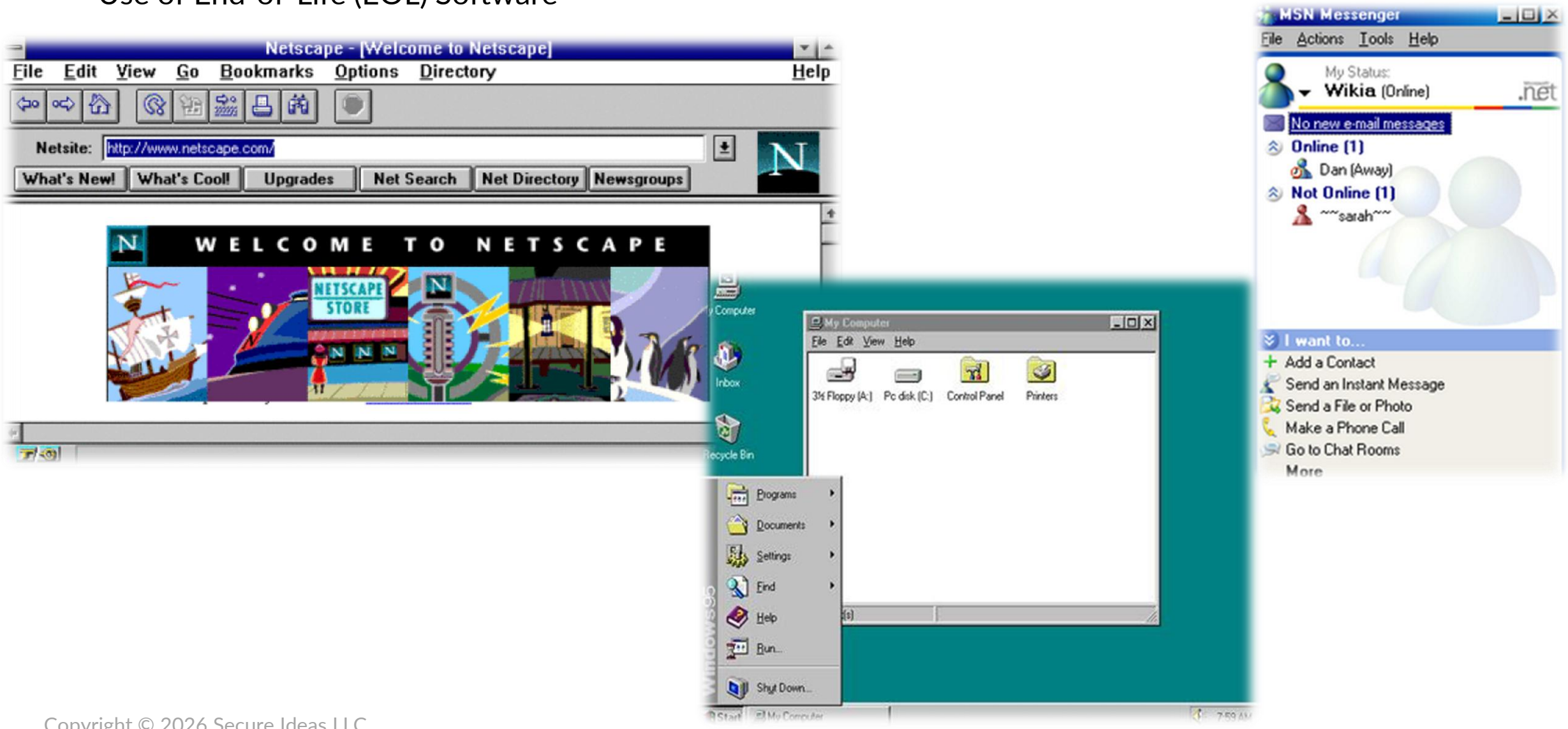




Copyright © 2026 Secure Ideas LLC

Examples

- Use of End-of-Life (EOL) Software



Copyright © 2026 Secure Ideas LLC

What is necessary?

- Ok, I got it, so I need to review my EOL, File Shares and Default Credential, right?



Symptoms are not the same than root cause

No fuel!

Copyright © 2026 Secure Ideas LLC

What is necessary?

- So, wait… Let's think…

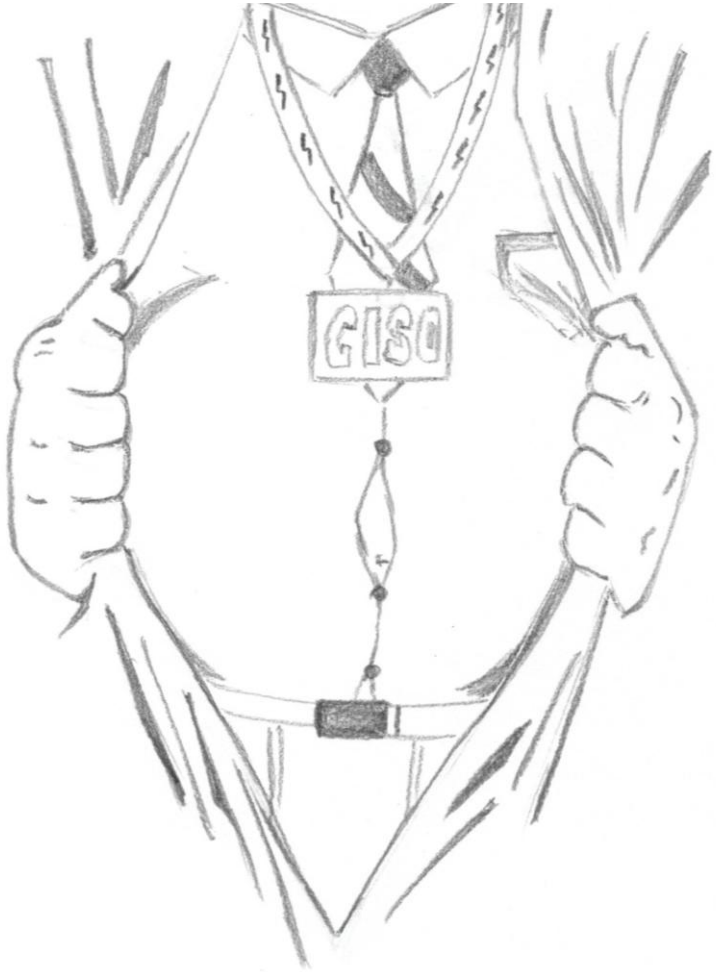


Copyright © 2026 Secure Ideas LLC

What is necessary?

- This is a mission for the **Super CISO**





Being a Super CISO means understanding that a superhero doesn't need to act on everything.

His most important quality is to have an open mind and be willing to ask for help and check to see what the market is already providing.

Copyright © 2026 Secure Ideas LLC

What is necessary?

- What is necessary?



An outside perspective.

Specialized professionals and companies can offer more **impartial, less biased views.**

Copyright © 2026 Secure Ideas LLC

What is necessary?

- An outside perspective



An "out-of-box" perspective to help alleviate problems rooted in the usual "in-box" view.

professionally evil®

Someone that doen't live the everyday situation...

Copyright © 2026 Secure Ideas LLC

What is necessary?

- Implementation Groups

IG1 “Cyber Hygiene”

- Essential protections for all organizations regardless of size or risk profile
- Sub-Controls for small, commercial off-the-shelf or home office software environments where sensitivity of the data is low

IG2

- Sub-Controls focused on helping security teams manage sensitive client or company information

IG3

- Sub-Controls that reduce the impact of zero-day attacks and targeted attacks from sophisticated adversaries

Copyright © 2026 Secure Ideas LLC

What is necessary?

- It's not about the "list"
  - Offense Informs Defense
  - Focus
  - Feasible
  - Measurable
  - Align





Copyright © 2026 Secure Ideas LLC

Additional Resources



- Additional Resources

CIS Critical Security Controls (https://www.cisecurity.org/controls/v8)

- **Establishing Essential Cyber Hygiene**
  - https://learn.cisecurity.org/Establishing-Essential-Cyber-Hygiene
- **CIS Controls Cloud Companion Guide**
  - https://www.cisecurity.org/insights/white-papers/cis-controls-v8-cloud-companion-guide
- **Guide to Enterprise Assets and Software**
  - https://www.cisecurity.org/insights/white-papers/guide-to-enterprise-assets-and-software
- **CIS Benchmarks List**
  - https://www.cisecurity.org/cis-benchmarks

Verizon DBIR:

- https://www.verizon.com/business/resources/Tdb/reports/2023-data-breach-investigations-report-dbir.pdf
- https://www.verizon.com/business/resources/reports/dbir/2023/summary-of-findings/
- https://www.verizon.com/business/resources/Ta13/reports/2024-dbir-data-breach-investigations-report.pdf
- https://www.verizon.com/business/resources/reports/dbir/2024/summary-of-findings/

Copyright © 2026 Secure Ideas LLC

Thank You!



jordan.bonagura@secureideas.com

bill@secureideas.com

Secure Ideas
professionally evil®

Copyright © 2026 Secure Ideas LLC