DEFEND YOUR ORG (or at least try to)

Izdihar

whoami

Izdihar Sulaiman

Husband, Father, Co-founder (cyber673), Avid CTF Player

Principal Consultant @ Swarmnetics 👨🏽‍💻

Placed 🥇/🥈/🥉 at CyberBattle CTF (Brunei) 8 out of 9 times

CVE-2022-40317 (lonely XSS CVE)

CISSP, GXPN, OSEP, OSWE, OSCP, OSWA, OSWP, CRT, CPSA, BSCP, eMAPT...

=> izdiwho.com <=

cyber673

Reality Check

- 60% of SMEs close within 6 months of a cyberattack
- Average breach costs for SMEs: $108,000+
- Most successful attacks exploit known vulnerabilities
- Perfect security doesn't exist, but neither does the perfect crime

Today's Goal: Understand practical implementations of NIST CSF 2.0 principles

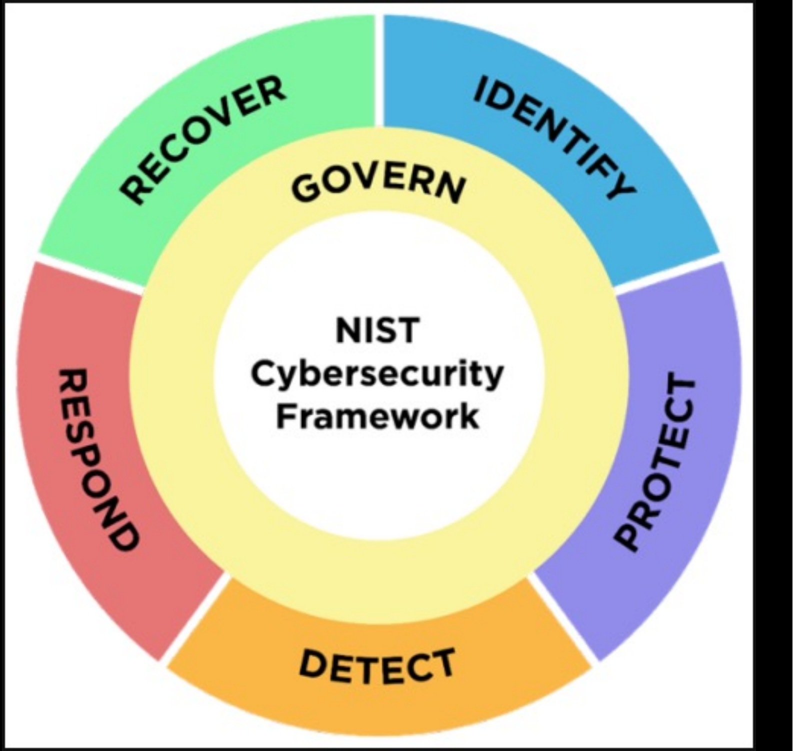
WHY NIST CSF 2.0 FOR SMEs?

- Framework designed to be flexible and scalable
- Provides common language for security discussions
- Adaptable to organizations of any size
- Maps to other frameworks and regulations
- Focuses on outcomes, not specific technologies
- New 2.0 version emphasizes governance and supply chain

NIST CSF

The Six Core Functions:

- GOVERN - How do we manage cybersecurity risk?
- IDENTIFY - What assets need protection?
- PROTECT - What safeguards are needed?
- DETECT - How do we identify incidents?
- RESPOND - How do we contain impacts?
- RECOVER - How do we restore capabilities?



GOVERN - MANAGE CYBERSECURITY RISK

Key Concepts:

- Establishing cybersecurity roles and responsibilities
- Determining risk tolerance
- Creating policies and processes
- Risk-informed decision making
- Resource allocation

SME Implementation Focus:

- Start with clear ownership of security tasks
- Define what risks you will and won't accept
- Develop simple, usable policies

IDENTIFY - KNOW WHAT YOU HAVE

Key Concepts:

- Asset management
- Business environment understanding
- Risk assessment
- Supply chain risk management

SME Implementation Focus:

- Know what you have (hardware, software, data)
- Prioritize based on business impact
- Focus on highest-risk vendors

PROTECT - BUILD BASIC DEFENSES

Key Concepts:

- Identity management and access control
- Awareness and training
- Data security
- Information protection
- Maintenance and protective technology

SME Implementation Focus:

- Multi-factor authentication everywhere possible
- Principle of least privilege
- Basic security awareness training
- Automated updates where possible

DETECT - NOTICE WHAT'S WRONG

Key Concepts:

- Continuous monitoring
- Anomalies and events detection
- Security monitoring process
- Detection process improvement

SME Implementation Focus:

- Centralized logging of critical systems
- Focus on quality over quantity of alerts
- Regular review of detection capabilities

RESPOND - HAVE A PLAN

Key Concepts:

- Response planning
- Communications
- Analysis
- Mitigation
- Improvements

SME Implementation Focus:

- Simple, actionable response plan
- Clear roles and responsibilities
- Communication templates ready to use
- Focus on containing damage quickly

RECOVER - GET BACK TO NORMAL

Core Activities:

- Backup and restoration
- Improvement planning
- Communications

Practical Implementation:

- Automated nightly database backups
- Weekly code repository backups
- Monthly test restoration to staging
- Document recovery steps for each critical service

COMMON SME SECURITY MYTHS

- "We're too small to be a target"
- "We can't afford good security"
- "We'll just buy a tool to fix everything"
- "Our cloud provider handles all security"
- "We've never been hacked, so we're secure"

Reality: Attackers target vulnerability, not size

cyber673

TOP 5 SME SECURITY CONTROLS

Based on BHIS Survival Guide & NIST Recommendations:

- Multi-factor authentication on all accounts
- Regular, tested backups using 3-2-1 rule
- Endpoint protection with automated updates
- Network segmentation (even if simple)
- Security awareness training for all staff

THE TECHNOLOGY TRAP

Common Mistake: Focusing on tools over fundamentals

Better Approach:

- Start with governance and risk understanding
- Define processes before selecting tools
- Choose tools that fit your organization's capabilities
- Free and open-source tools can be highly effective
- Build capacity over time

MEASURING SECURITY MATURITY

Simple Metrics for SMEs:

- % of systems with security controls implemented
- % of staff trained on security basics
- Time to detect security incidents
- Time to recover from disruptions
- Number of security events resolved

Focus on improvement over perfection

IMPLEMENTATION ROADMAP

Phase 1: Foundation
(1-3 months)

- Assign security responsibilities
- Inventory critical assets
- Implement MFA and basic access controls
- Create simple backup strategy

Phase 2: Maturity
(3-6 months)

- Develop basic security policies
- Implement monitoring for critical systems
- Conduct staff awareness training
- Create incident response plan

Phase 3: Optimization
(6+ months)

- Regular risk assessment process
- Continuous monitoring improvements
- Tabletop exercises for incidents
- Supply chain security assessment

RESOURCES / REFERENCES

- https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf
- https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1300.pdf
- https://learn.cisecurity.org/defining-reasonable-security
- https://www.blackhillsinfosec.com/prompt-zine/prompt-issue-infosec-survival-guide-third-volume/
- https://learnsecurity.amazon.com/en/index.html

KEY TAKEAWAYS

Remember:

- Security is about risk management, not elimination
- Start with governance and fundamentals
- Focus on high-impact, low-cost controls first
- Build security into processes, not as an afterthought
- Measure and improve continuously
- Perfect security doesn't exist, but good enough security does

Q&A

THANK YOU