A CYBERSECURITY FRAMEWORK FOR THE SMBs

Why, What & How

State Designated as Florida's Principal Provider of Business Assistance [§ 288.001, Fla. Stat.]

Florida SBDC at FGCU
Helping Businesses
Grow & Succeed

Introduction

"There are only two types of companies: Those that have been hacked and those that will be. Even that is merging into one category: Those that have been hacked and will be again"

Robert Mueller

"Terrorism does remain the FBI's top priority, but in the not too-distant-future we anticipate that the cyberthreat will pose the greatest threat to our country." 2012

Introduction

Over 70% of SMBs experience cybersecurity attacks in 2018!

83% of SMBs don't have a cybersecurity plan

60% of business go out of business within 6 months of a cybersecurity attack

Over 30% of SMBs say *"They have NO IDEA how to defend against a cybersecurity attack."*

What do they mean, *"No idea"*?

Introduction – But There's Hope

There are two types of companies – those that have been hacked and those that don't know they've been hacked"

Dmitri Alperovitch, 2011

"I've since modified that phrase. The first two companies still exit, but now there's a third type that's able to successfully defend itself against intrusion"

2019

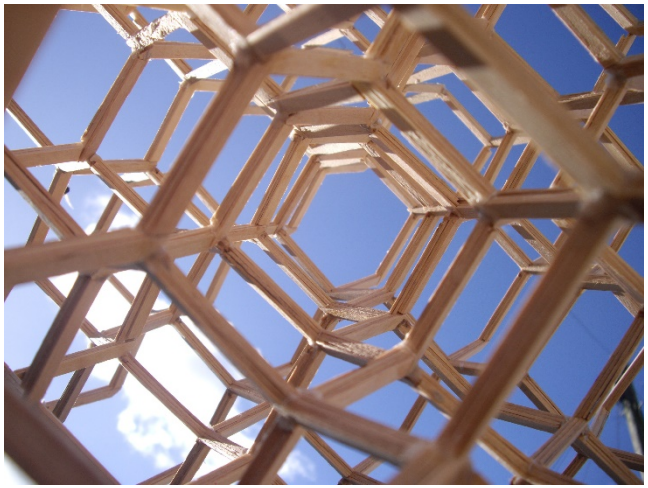
A CYBERSECURITY FRAMEWORK FOR THE SMBs

- I. What is a Framework
- II. Why a Cybersecurity Framework
- III. Which one
- IV. The NIST Cybersecurity Framework

I. What is a Framework

When we talk about a 'business framework' we mean a:

- Structure
- Way of looking at things
- Way of conceptualizing
- Paradigm



I. What is a Framework

It's a framework, not a prescriptive standard

- Common Language
- Adaptable
- Collaboration Opportunities
- Ability to Demonstrate Due Care
- Easily Maintain Compliance
- Secure Supply Chain
- Cost Efficiency

This slide is straight from NIST!

Compliance ≠ Secure

I. What is a Framework

A Framework is NOT a

Policy, Procedure +/or Compliance Manual

II. Why a Framework

Which field would it be easier to have an organized game of football on?

II. Without a Cybersecurity Framework

It's like:

How do you know when you made first down? Scored?

II. Why a cybersecurity Framework

II. Why a cybersecurity Framework

Without a framework, organizations use the 'Numbers Games' to handle cybersecurity

II. Why a Cybersecurity Framework

Number Game #1

Number of Solutions

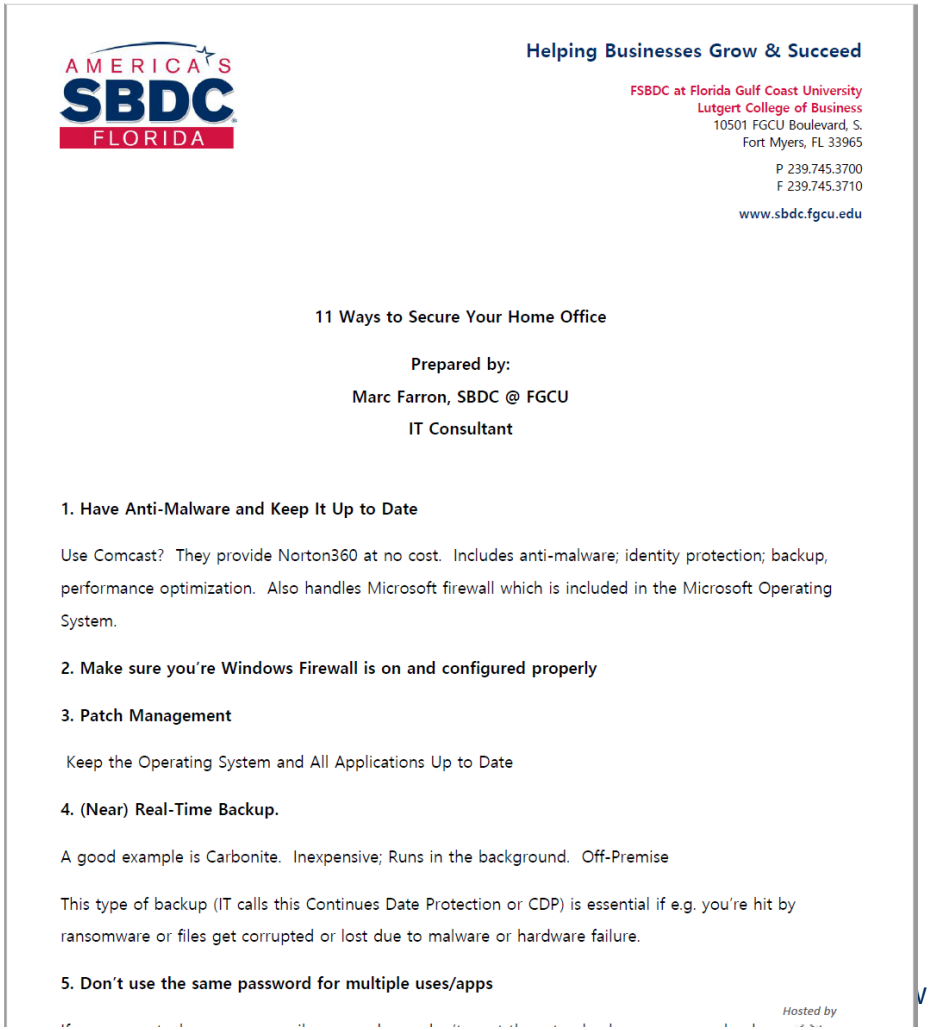
- ✓ Anti-Virus
- ✓ Anti-Spam
- ✓ Firewall
- ✓ Password Manager
- ✓ Security Appliance
- ✓ Penetration Testing
- ✓ Staff Training
- ✓ Etc.
- ✓ Etc.

II. Why a Cybersecurity Framework

Number Game #2
Number of Tasks

- ✓ Keep your AV up-to-date
- ✓ Keep all your software recent
- ✓ Change your passwords every 3 months
- ✓ Keep passwords at least 15 characters long
- ✓ Don't open unknown attachments
- ✓ Etc.
- ✓ Etc.

II. Why a Cybersecurity Framework



AMERICA'S SBDC FLORIDA

Helping Businesses Grow & Succeed

FSBDC at Florida Gulf Coast University
Lutgert College of Business
10501 FGCU Boulevard, S.
Fort Myers, FL 33965

P 239.745.3700
F 239.745.3710

www.sbdc.fgcu.edu

11 Ways to Secure Your Home Office

Prepared by:

Marc Farron, SBDC @ FGCU

IT Consultant

1. Have Anti-Malware and Keep It Up to Date

Use Comcast? They provide Norton360 at no cost. Includes anti-malware; identity protection; backup, performance optimization. Also handles Microsoft firewall which is included in the Microsoft Operating System.

2. Make sure you're Windows Firewall is on and configured properly

3. Patch Management

Keep the Operating System and All Applications Up to Date

4. (Near) Real-Time Backup.

A good example is Carbonite. Inexpensive; Runs in the background. Off-Premise

This type of backup (IT calls this Continues Date Protection or CDP) is essential if e.g. you're hit by ransomware or files get corrupted or lost due to malware or hardware failure.

5. Don't use the same password for multiple uses/apps

Hosted by

Even I got into the #s game!

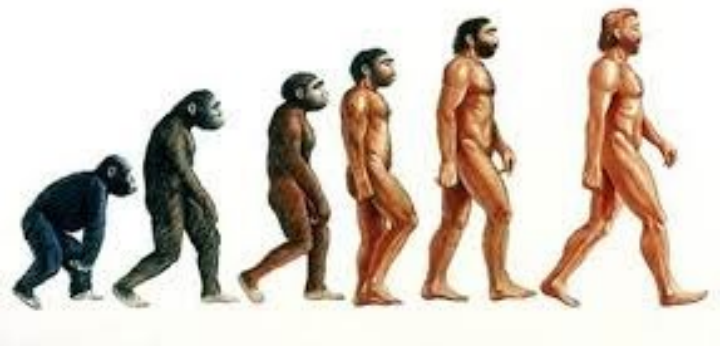
II. Without a Cybersecurity Framework

The Problem: You don't know if you have enough or the right solutions and tasks….When's enough?

The 'Point Solution' approach is insufficient.

II. Without a Cybersecurity Framework

Without a framework, organizations don't know if they're getting better or worse at cybersecurity.



Maturity Model

How do you map out and measure improving over the months and years…count how many more devices or solutions you have & use?

III. Which Cybersecurity Framework

III. Which Cybersecurity Framework

Abbreviation	Full Name
NIST	National Institute of Standards and Technology
COBIT	Control Objectives for Information & Related Technologies
ISO/IEC Standards	ISO/IEC Standards
COSO	Committee of Sponsoring Organizations of the Treadway Commission
NERC	North American Electric Reliability Corporation
TY CYBER	Technical Committee on CyberSecurity
HITRUST CSF	Health Information Trust Alliance

...and this is just some of them (:

III. Which Cybersecurity Framework

The answer is

NIST: National Institute of Standards and Technology

Why NIST

It is actionable— focusing on the five core functions

It leverages industry standards and best practices

It helps organizations focus and prioritize their cyber-related investment decisions

It can help reduce legal risk with evidence of your organization's good faith efforts to manage cybersecurity risks

It's flexible—and allows SMBs in different industries and of various sizes to adapt the Framework and make it work for them.

III. Which Cybersecurity Framework… The NIST Cybersecurity Framework

NIST was 1901 to establish as the "…national standards and measurements laboratory"

National Electrical Safety Standards Codes

Radio broadcasting standards to set airwave usage

III. Which Cybersecurity Framework… The NIST Cybersecurity Framework

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

In February, 2013, President Obama passed an Executive Order that included efforts developing a framework for reducing risks to critical infrastructure.

NIST was tasked to develop this Framework

In 2016 NIST published "Small Business Information Security: The Fundamentals"

III. Which Cybersecurity Framework… The NIST Cybersecurity Framework

It is the standard for larger organizations

Organizations	SMBs	Enterprises; Governments; Nations
# of employees	1 – 500	1,000 ->
Heard of, interested in, want to or have deployed the NIST Framework	Never	Always

III. Which Cybersecurity Framework… The NIST Cybersecurity Framework

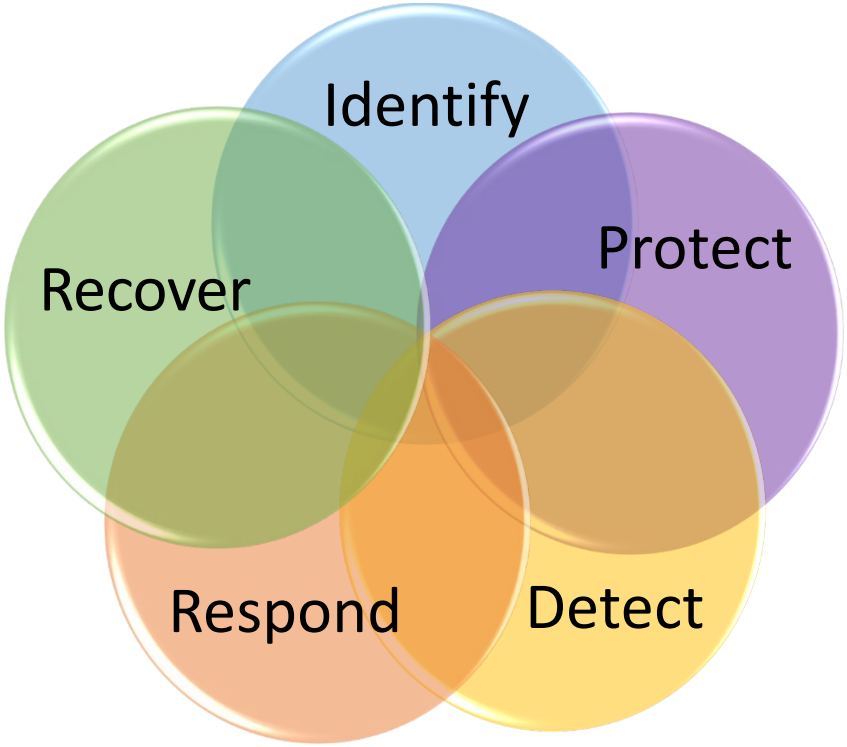
The only problem is…

…it's too 'much' in its current form for SMBs.

III. NIST: The Five Functions

The Five Functions

III. NIST: The Five Functions



Here they are again (:

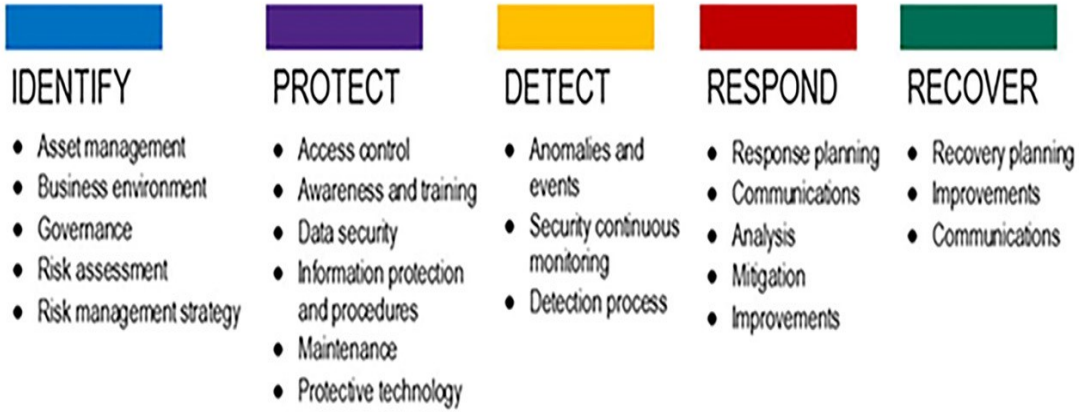
III. Introducing the NIST Framework

There are Five Functions

Which are divided into Categories

Which are divided into sub-categories

These three pieces – Functions, Categories and Sub-Categories are what NIST call "The Core"



NIST

III. Before we start with NIST

Let's start off by saying,

"Security is all about managing risk"

III. Risk Management

Risk = The Cost of the impact X The Likelihood of the impact occurring

There are 4 ways you can manage risk:

1. Accept it
2. Mitigate it
3. Transfer it
4. Ignore it

Risk Management
So What Are the Threats

Top 5 Cybercrimes/Trends -- SMB

Ransomware

Supply Chain Attacks/Business Email Compromise (BEC)

Fireless Malware Attacks

Cryptojacking

Regulations now effect ALL Companies -- GDPR

I. Identify

DON'T CHANGE ANYTHING

Review and Note Where Your Company is at with all the other Functions, Categories and (perhaps) Subcategories

This will develop your company's (what NIST calls) Profile

Then you can decide your next steps

I. Identify

- Take an Inventory of Your
  - Data/Information
  - Hardware
  - Software
- Develop Organizational Chart
- Detail Cybersecurity Roles and Responsibilities
- Resilience Requirements to Run the Business

I. Identify

- Legal and regulatory requirements regarding cybersecurity
- Threats, both internal and external are researched
- Potential business impacts and likelihoods are identified
- Threats, vulnerabilities, likelihoods, and impacts are used to determine risk
- Organizational risk tolerance is determined and clearly expressed

II. Protect

- Password Management
  - Length/Time
  - 2 Factor Authentication
  - Limit employee access to data and information (Policy of Least Privilege)
  - Individual user accounts for each employee
  - Ensure employee that leave the business no longer have access
  - Provide only temporary logins to vendors
  - Change the administrative password that came with devices

II. Protect

- Spam filtering
- Web filtering
- Encryption of sensitive information
  - At Rest
  - In Transit
- Dispose of old computers and media safely

II. Protect

- Patching/Updates
- Software and hardware firewalls
- Securing connected home offices
- Installing an Intrusion Detection / Prevention System (IDPS). -- analyzes network traffic at more detailed level, providing a greater level of protection. (Optional)

II. Protect

- Background Checks
- Session lock feature included with operating systems is used
- Secure your wireless access point
  - If your business provides wireless internet access to customers, ensure that it is separated from your business network
- VPNs for connecting to unknown networks
- Near Continuous Backup
- Journaling

II. Protect

- Train employees
  - Immediately when hired & at least annually
  - Pay attention to the people you work with and around
  - Be careful of email attachments and web links
  - Do not connect personal or untrusted storage devices or hardware into your computer
  - Watch for harmful pop-ups
  - Have a Procedure & Policy Statement that is reviewed and signed by all employees (Sample Provided)
  - Policies and procedures for information security

III. Detect

Cyberattacks are taking a shorter time to activate (< 3 minutes)

…and a longer time to detect (> 7 months)

III. Detect

- Install and update
  - Anti-virus
  - Spyware
  - other –malware programs
- Monitor
  - Network
  - Physical Environment
  - People
- Continuously improve detection practices
- Log Management (Optional)

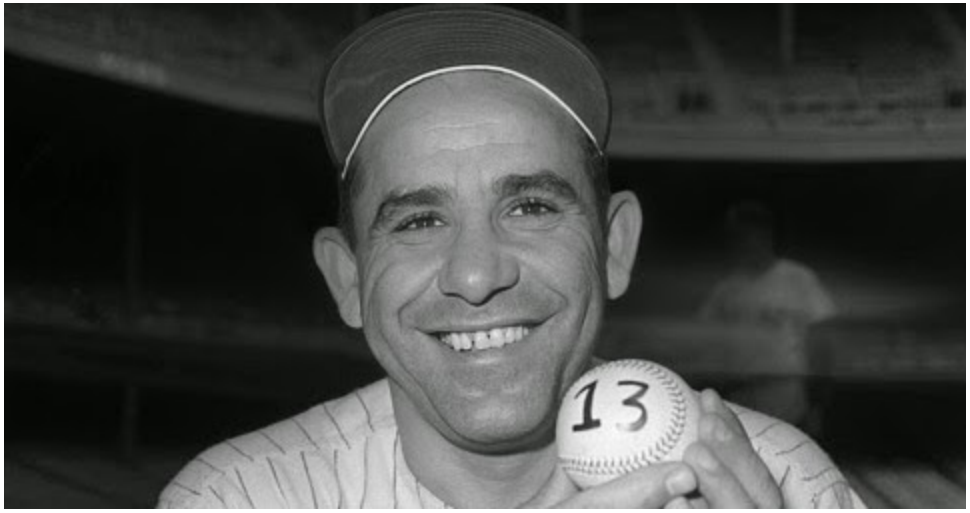
III. Detect

- Mysterious email
  - Unusual password activity
  - Locked out for no reason
  - Received notice your password has been changed
- Slower than normal network
- Mysterious Popups
- Missing Information
- Website
  - Alerts
  - Increased traffic
  - Down

III. Detect

"You can observe a lot by just looking around"

Yogi Berra



IV. Respond

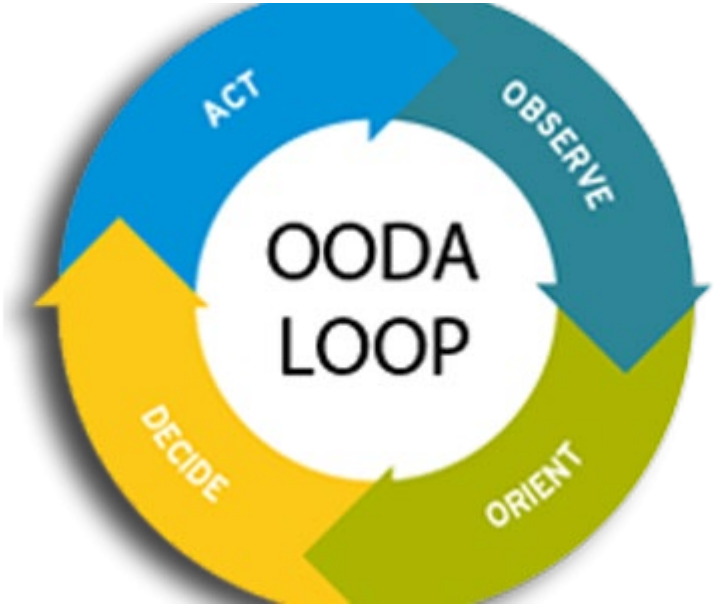
The RESPOND and RECOVER are the hardest and most perennially underprepared of the NIST Functions

IV. Respond

Respond

There's a Framework for that!!

THE OODA LOOP



Developed by the US Air Force for military campaigns in the 1950s

IV. Respond

Respond

....actually, more than one Framework

1. Preparation
2. Identification
3. Containment
4. Eradication
5. Recovery
6. Lessons Learned

Don Murdoch
Blue Team Handbook: Incident Response Edition

IV. Respond - Identify, Contain & Eliminate

- Have a designated Response Team that will be grouped emailed if an attack is detected.
  - Executives
  - Internal Staff
  - Vendors & Partners

- Mobilize the team
- Determine where & how the attack took place

IV. Respond - Identify, Contain & Eliminate

- Disconnect affected computer(s) from the network
- Utilize spares and backup to continue to capture operational data
- Switch to paper
- Plan to continue when system are down

Recover

- Public Relations Management
  - Repair Reputation
  - Manage the Story
- Address Legal and Regulatory Requirements
- Consider cyber insurance
- Recovery activities are communicated to internal and external stakeholders as well as executive and management teams
- Make improvements to processes / procedures / technologies

Sample Policy Statement

All employee personnel data will be protected from viewing or changing by unauthorized persons.

All computer users will have their own account and password.
Passwords are not to be shared with anyone!

All computer users will read and sign an access and use agreement
Information Types A, B, C, D, E, and F will be backed up regularly in accordance with their determined priority/criticality

Employees should be required to read the business's policies and sign a statement stating that they understand and will comply. Employees should receive annual training on the policies.

The Final Thought

Stop making cybersecurity a technology issue

…a constraining issue

And start making security a business enabling issue

To be successful or venture into new business you have to manage risk and compliance

The Final Thought

Get management & employees involved early and often:

Explain why

Get them involved in decision/selection processes

Work closely with HR, CFO, Department Heads

Q & A

Marc Farron
IT Consultant
Florida Gulf Coast University FSBDC
239.745.3705 or 239.745.3700
mfarron@FGCU.edu

sbdc.fgcu.edu