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

CYBERSECURITY FOR SMALL BUSINESSES

Celia Paulsen
CyberSecurity Awareness
10/26/2016

The NIST Mission

"To promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life."

Cost of an incident

- In 2013, the average total cost of a single incident was **$82,000** for North American small businesses. ***
- Average of **$2.4 million** for a targeted attack on a large enterprise. ***
- Total cost of cyber crime in the U.S. = **$24-140 billion** **

** McAfee, 2013 Economic Impact Report
*** Kaspersky Labs, Global Corporate IT Security Risks: 2013

Why Small Businesses?

- In 2013, nearly **one-third** (31%) of all cyber attacks targeted businesses with **fewer than 250 employees***

- **41 percent** of targeted attacks were aimed at businesses with **1-500 employees** (increase of 61% from 2012) *

* Symantec 2014 Threat Report

WHAT IS INFORMATION/CYBERSECURITY?

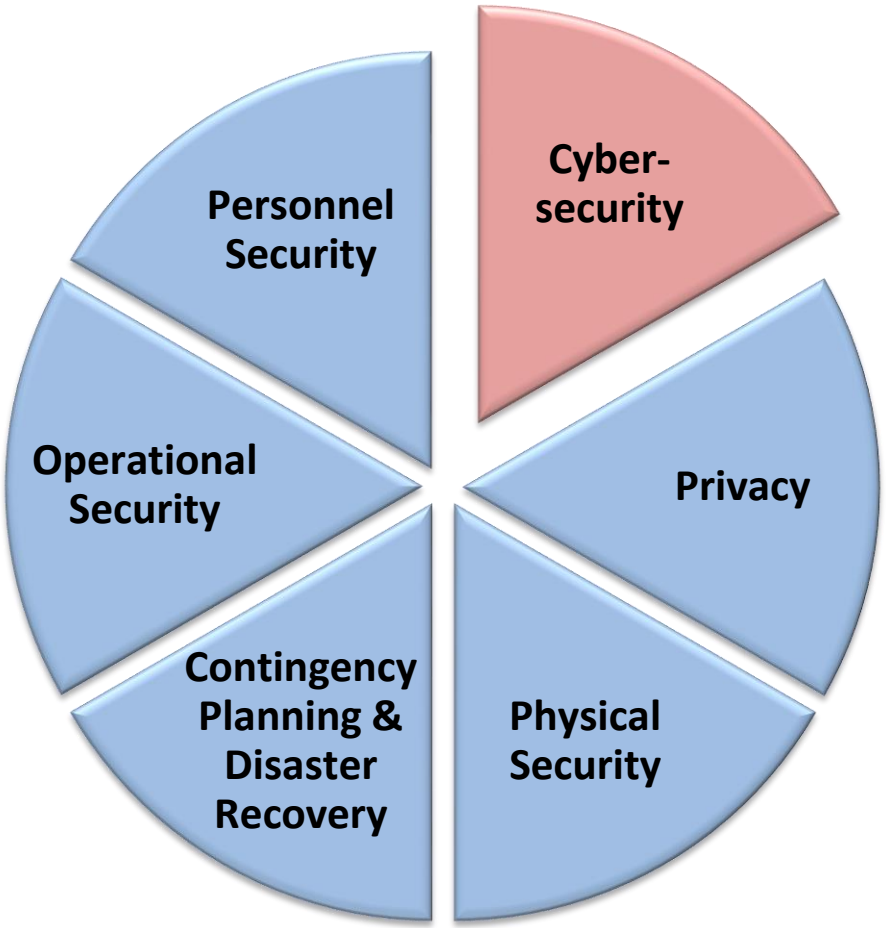
What is Information/cybersecurity?

Information Security - The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

Cybersecurity – The ability to protect or defend the use of cyberspace from cyber attacks.

"Glossary of Key Information Security Terms", NIST IR 7298

What is Information Security?



What is Information and an Information System?

- **Information**
  - Email
  - Invoices
  - Payroll
  - Employee Data
  - Client Data
  - Proprietary Info
  - Etc.

- **Information System**

  Any integrated set of information technology and people's activities for collecting , storing, processing and delivering information

What is Information Security?

Confidentiality

Unauthorized Access, Disclosure

Integrity

Unauthorized Modification, Use

Availability

Disruption, Destruction

CYBERSECURITY IS GOOD FOR BUSINESS

Customer Service

- **Customers want their private information protected and respected**
- **Customers need to have confidence in you to continue doing business with you**
- **Customers expect their data will be kept safe and accounted for by you**

Just as you have your expectations of how those that you trade with will protect YOUR information

(Remember – in general, you are the custodian of the data entrusted to your care – you are NOT the owner of that data)

Legal Protection

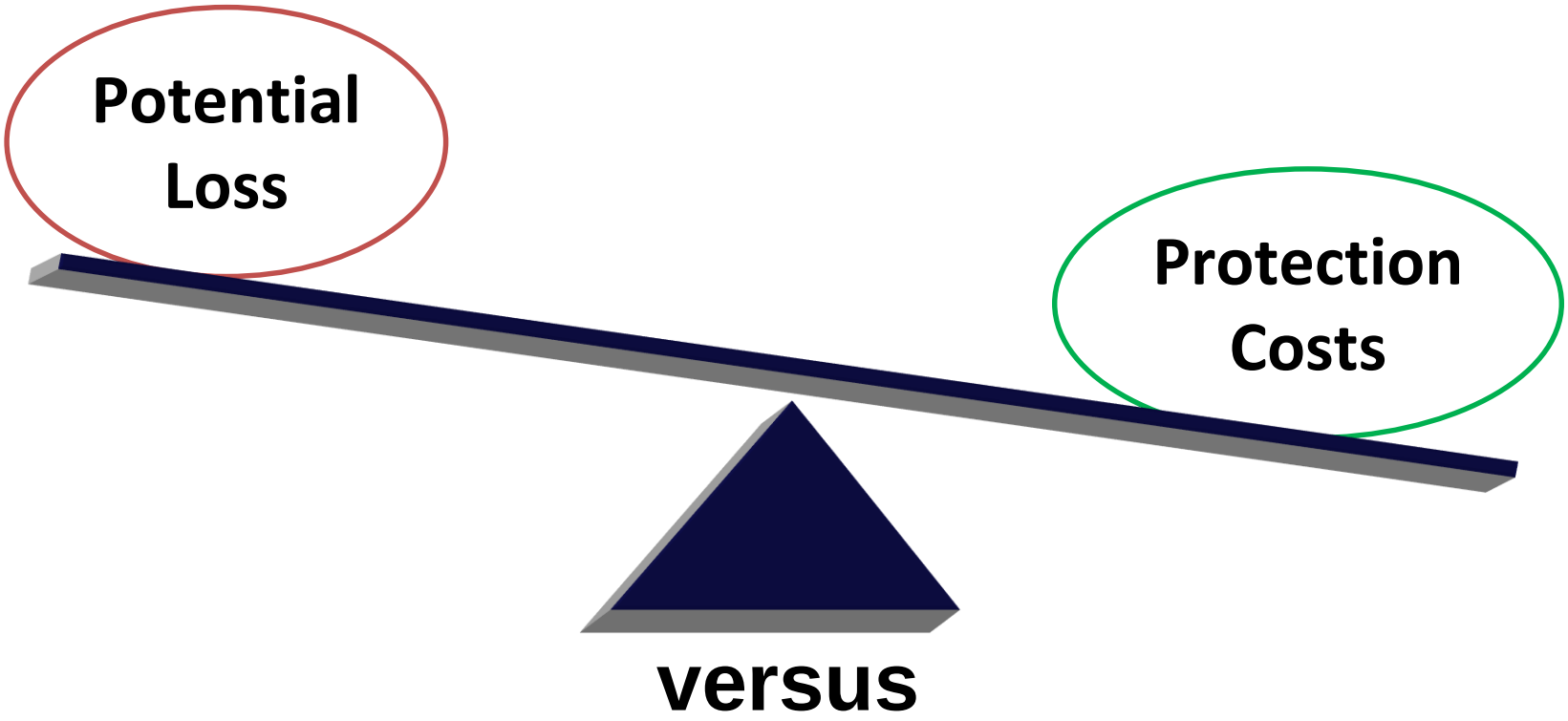
Taking steps to ensure that your customer or employee data does not fall into the wrong hands (i.e., demonstrating due diligence) provides protection against liability

What's at risk when you DON'T implement information security / cybersecurity?

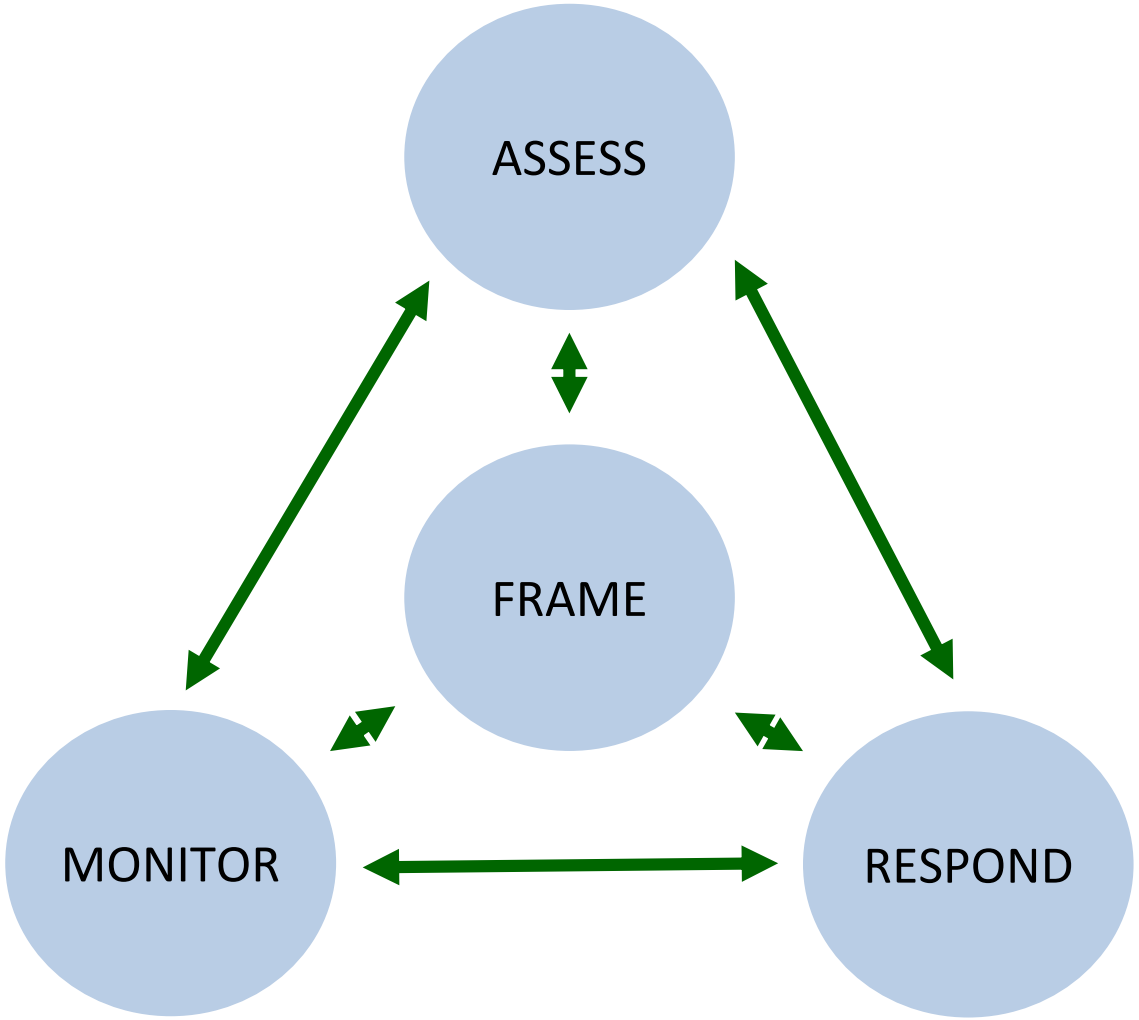
- Decreased productivity
- Increased labor costs
- Legal liability
- Loss of confidence
- Adverse reputation
- Your Business!
- Your personal assets!

WHERE CAN WE START?

What is Risk Management?



"FARM" – The Risk Management Process



NIST SP 800-39, *Managing Information Security Risk*

Where Can We Start? – FRAME

- **Do you know what information you need to run your business?**
- **Do you know where the information is?**
- **Do you know which types of information are the most important?**
- **Do you know who has access to your sensitive business information?**

Business Process Analysis

Exercise 1 – Identifying and prioritizing your organization's information types

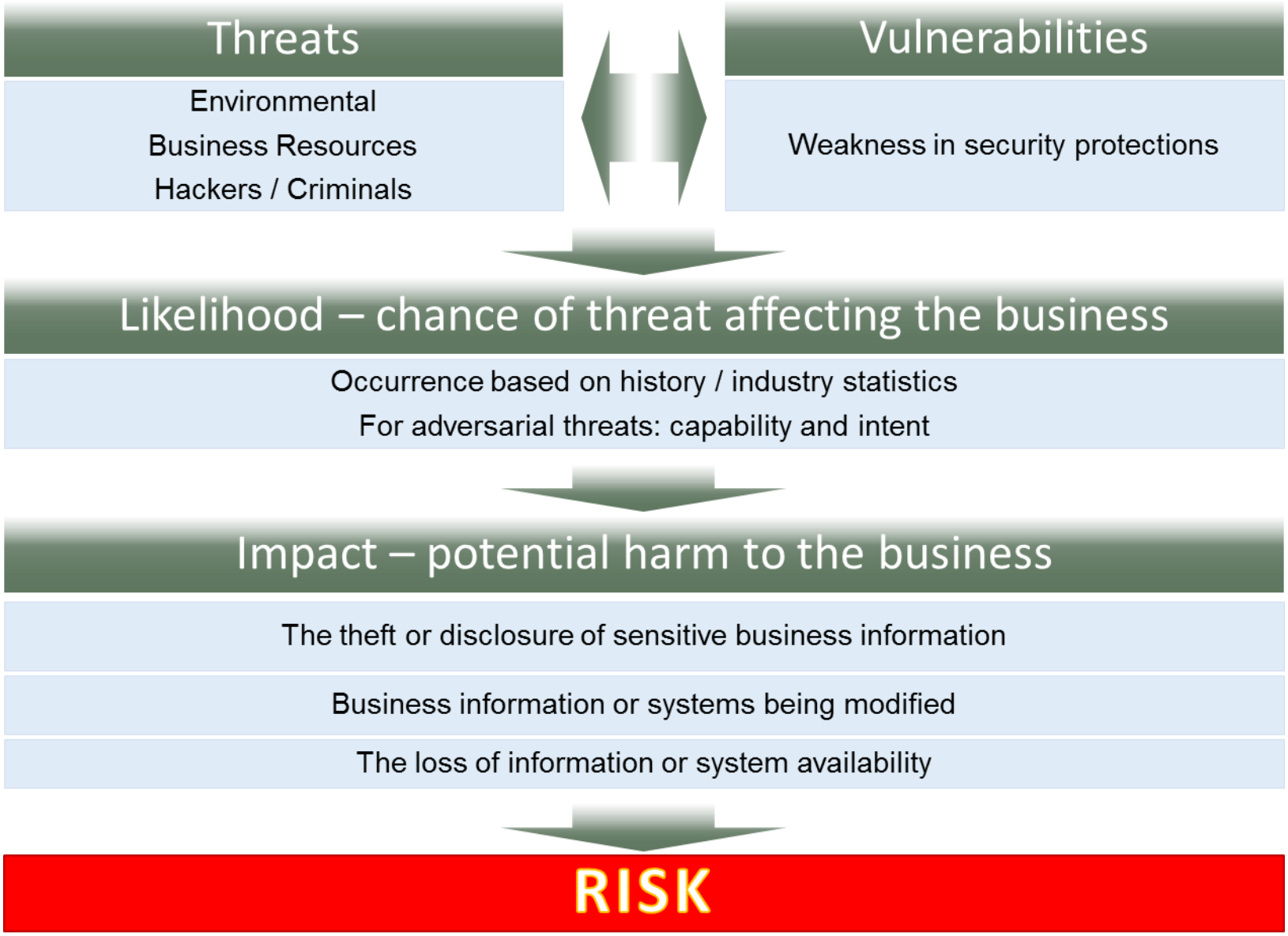
	Type of Information	Type of Information	Type of Information
	Employee PII		…
Cost of revelation (Confidentiality)	*$$*		
Cost to verify information (Integrity)	*$$$*		
Cost of lost access (Availability)	*$$$*		
Legal costs (Fines, Penalties, Notification)	*$$*		
Repair Costs	*$*		
…			
Impact Score	***7***		

Exercise 2 - Develop an Inventory

1. What systems (technology / people / organizations) “touch” your information?
2. Add the information type scores or use the highest score
3. Consider any constraints (e.g. FIPS 199)

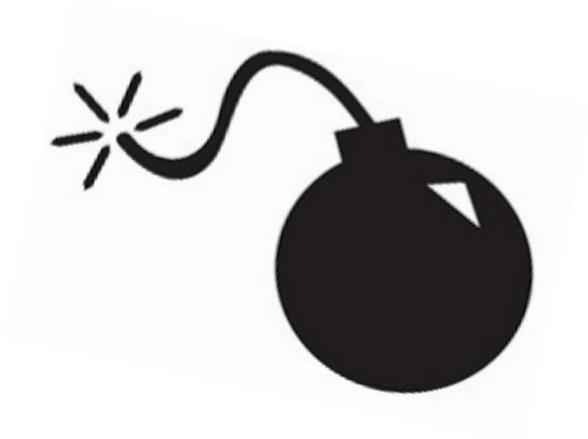
	Description (make, model, serial number, service ID, etc.)	**Location**	**Type of Information** (from Exercise 1)	**Impact Score**
1	*J. Smith’s Cell Phone (“Blue Box”, #555-555-5555)*	*Mobile, BW Network*	*Employee PII; Calendar; email; …*	***7 (Moderate)***
2				
3				
4				
…				

ASSESS THE RISK


Threats
Environmental
Business Resources
Hackers / Criminals
Vulnerabilities
Weakness in security protections
Likelihood – chance of threat affecting the business
Occurrence based on history / industry statistics
For adversarial threats: capability and intent
Impact – potential harm to the business
The theft or disclosure of sensitive business information
Business information or systems being modified
The loss of information or system availability
RISK

What is a Threat?

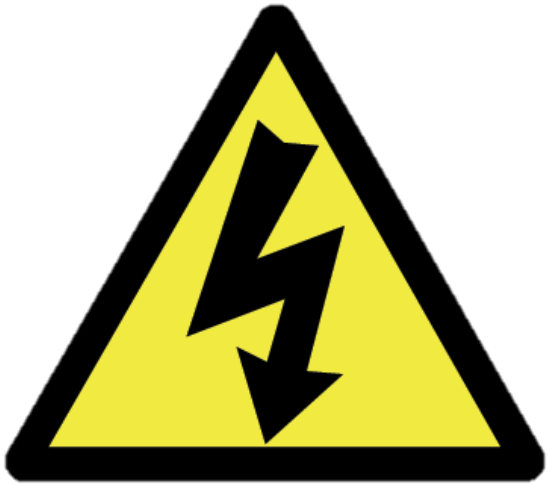
- **A threat is a circumstance or event with the potential to adversely impact business assets**
- **A threat may be:**
  - Hostile / intentional
  - Accidental / unintentional
  - Active (requires action) or passive
  - Physical, cyber, human, or “act of God”



Physical Threats

- **Disasters**
  - Fire (natural or man-made)
  - Flooding (natural or man-made, e.g, from burst pipes)
  - Hurricane, tornado, earthquake (natural, locality-based)

- **Business Resource Threats**
  - Network/communications failure
  - Equipment (hardware) failure
  - Application (software) failure
  - Supply chain disruption



Hostile Threats

- **Who are they and what do they want?**
  - Money
  - Politics / Hacktivism / Revenge
  - Fun / Boredom

- **What are they after?**
  - Money
  - Business information
  - Personally Identifiable Information (PII)
  - Your computing resources (for use in botnet)
  - Access to your customers' / suppliers' systems

Hostile Attack Vectors

- SPAM
- Spoofing
- Snooping
- Ransomware
- Insider threats
- Social engineering
- Phishing & Spear Phishing
- Theft of information (data) and resources
- Malware (Malicious code – viruses, worms, etc.)

Exercise 3 – Identify threats to your business

	Info Type / Technology	Info Type / Technology	…
	Customer PII on J. Smith's Cell Phone		
Confidentiality			
Theft	*High*		
Accidental Disclosure	*Mod*		
Integrity			
Accidental alteration	*Mod*		
Intentional alteration	*Low*		
Availability			
Accidental destruction (fire, water, user error)	*Low* *(Have off-site backups)*		
…			
Overall Likelihood	*High*		

WHERE ARE SMALL BUSINESSES VULNERABLE?

Recent Events

- **Healthcare service provider Newkirk Products:** Hackers accessed a server affecting up to 3.3 million people (August)
- **Tidewater Community College:** Employee received a request from a fake TCC email address requesting employee W-2 information. At least 16 employees have reported false tax returns filed under their SSN. (March)
- **Systema Software:** During a system upgrade, data storage was set up improperly and customer data, including that of multiple insurance companies, was made publically available on the internet for 75 days. (March)
- **Austrian-based aerospace parts manufacturer FACC**: accounting department was the target of cyber fraud resulting in the direct theft of €50 million (January)

https://www.identityforce.com/blog/2016-data-breaches

Case Study – Online Banking

- **Green Ford Sales Inc.**
  - Malware distributed via malicious websites and phishing emails.
  - At 1pm, hacker logged in to banking account, created nine new employees, transferred $63,000 to them.
  - At 7:45am the next day, business owner discovered the transfers and called his bank.
  - Bank was able to freeze the funds in six of the nine cases, but three had already withdrawn the money.
  - Business lost $22,000.

http://www.wsj.com/articles/SB10001424052702304567604576454173706460768

Case Study – Insider Threat

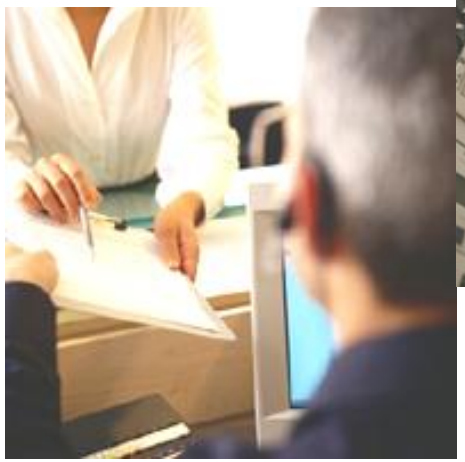
- **80'sTees.com**
  - Notified by Discover that cardholders using his site had experienced suspicious transactions on their accounts
  - Company stopped collecting credit card data, brought in a forensic examiner and contacted the Secret Service
    - Found no evidence of an intrusion
  - Visa and MasterCard complained about fraudulent charges
  - Source of breach was determined to be a former senior executive
  - Cost = $200,000, not including lost sales

http://www.cnbc.com/id/101971980

Common Cybersecurity Vulnerabilities

Where are you vulnerable to the threats?

- Unsupported / unpatched hardware and software
- Ineffective / nonexistent policies & procedures
- Separation of personal and business activities
- New technologies / Internet of things
- Lack of oversight & training
- Loose enforcement
- Weak passwords
- Mobile Devices
- Suppliers



DEVELOP A SECURITY STRATEGY

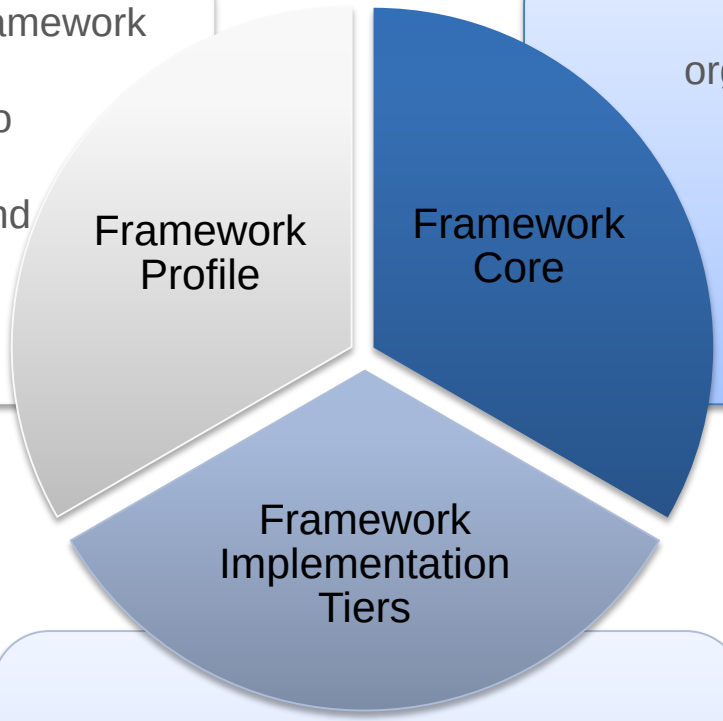
The Cybersecurity Framework Is for Organizations…

- Of any size, in any sector in (and outside of) the critical infrastructure
- That already have a mature cyber risk management and cybersecurity program
- That don't yet have a cyber risk management or cybersecurity program
- With a mission of helping keep up-to-date on managing risk and facing business or societal threats

Cybersecurity Framework Components

Aligns industry standards and best practices to the Framework Core in a particular implementation scenario

Supports prioritization and measurement while factoring in business needs

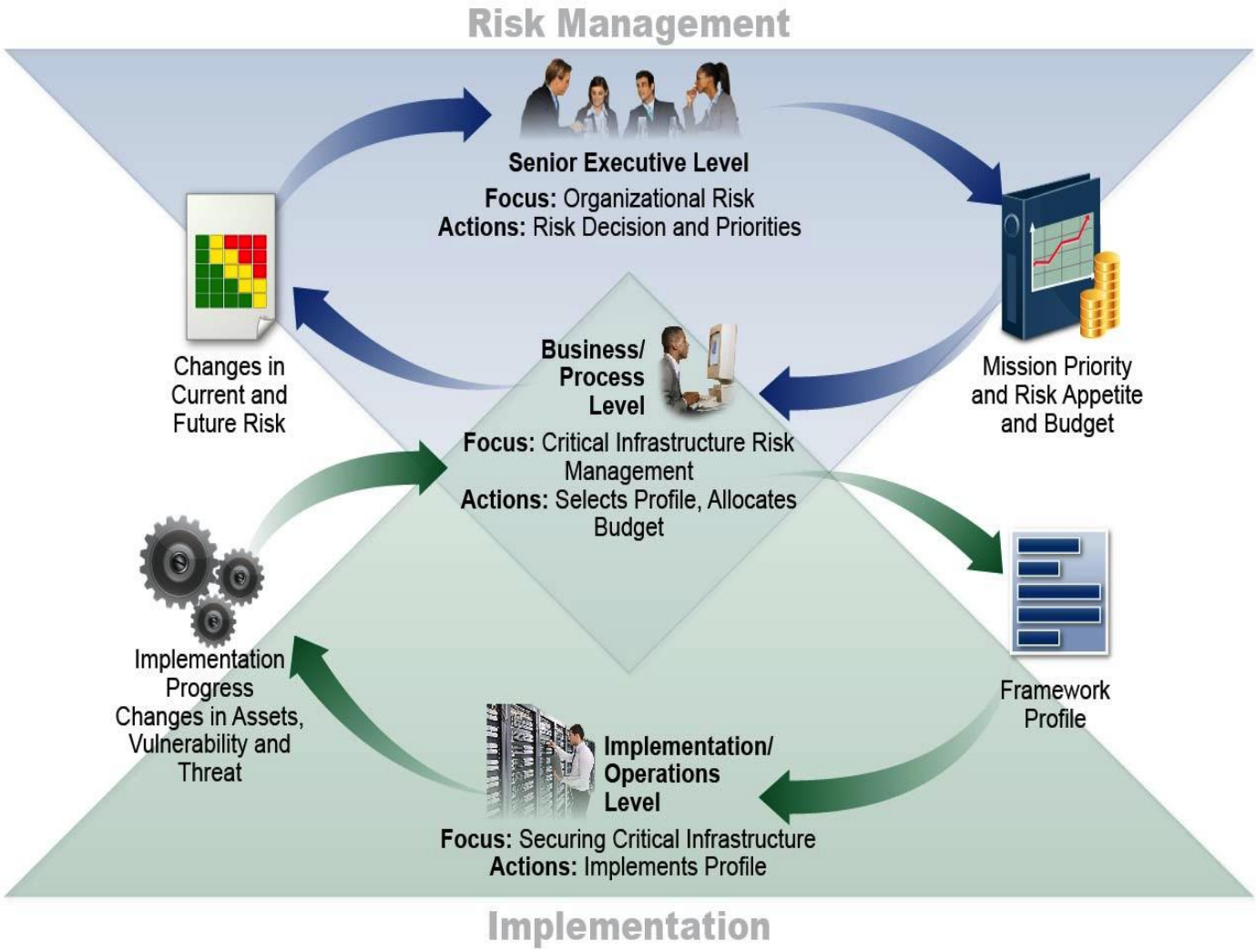


Cybersecurity activities and informative references, organized around particular outcomes

Enables communication of cyber risk across an organization

Describes how cybersecurity risk is managed by an organization and degree the risk management practices exhibit key characteristics

Supporting Risk Management with Framework



Taxonomy Value Proposition

Scientific classification follows a system of rules that standardizes the results, and groups successive categories into a hierarchy.

For example, the family to which lilies belong is classified as:

- **Kingdom:** Plantae
- **Phylum:** Magnoliophyta
- **Class:** Liliopsida
- **Order:** Liliales
- **Family:** Liliaceae
- **Genus:** .....
- **Species:** .....

Value Proposition

- Accurate communication
- Quickly categorize known
- Logically name unknown
- Inherent properties understood based on name

Core

What processes and assets need protection?

What safeguards are available?

What techniques can identify incidents?

What techniques can contain impacts of incidents?

What techniques can restore capabilities?

Function	Category	ID
Identify	Asset Management	**ID.AM**
	Business Environment	**ID.BE**
	Governance	**ID.GV**
	Risk Assessment	**ID.RA**
	Risk Management Strategy	**ID.RM**
Protect	Access Control	**PR.AC**
	Awareness and Training	**PR.AT**
	Data Security	**PR.DS**
	Information Protection Processes & Procedures	**PR.IP**
	Maintenance	**PR.MA**
	Protective Technology	**PR.PT**
Detect	Anomalies and Events	**DE.AE**
	Security Continuous Monitoring	**DE.CM**
	Detection Processes	**DE.DP**
Respond	Response Planning	**RS.RP**
	Communications	**RS.CO**
	Analysis	**RS.AN**
	Mitigation	**RS.MI**
	Improvements	**RS.IM**
Recover	Recovery Planning	**RC.RP**
	Improvements	**RC.IM**
	Communications	**RC.CO**

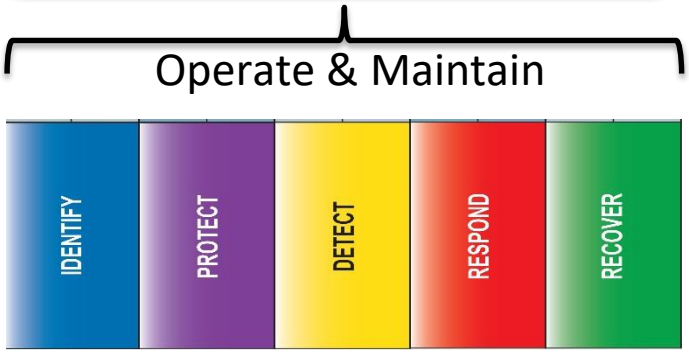
Where Should I Start?

(1) Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.

(2a) Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk

(2b) Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.

Framework Version 1.0, Section 3.2, Step 1: Prioritize and Scope. The organization identifies its business/mission objectives and high-level organizational priorities. With this information, the organization makes strategic decisions regarding cybersecurity implementations and determines the scope of systems and assets that support the selected business line or process. The Framework can be adapted to support the different business lines or processes within an organization, which may have different business needs and associated risk tolerance.



Mitigation types

- **Policies & procedures**
  - In writing (may be signed)
  - Processes
  - Automated where possible
- **Awareness & Training (employees, suppliers, customers)**
- **Information Technology**
  - Network
  - Computers
  - Mobile devices

DEVELOP A SECURITY STRATEGY

Prioritize Your Response

Impact	High	**Priority 3** – schedule a resolution. Focus on Respond and Recover solutions.	**Priority 1** – Implement immediate resolution. Focus on Detect and Protect solutions.
	Low	Address as Funds Allow	**Priority 2** – schedule a resolution. Focus on Detect and Protect solutions.
		Low	High
		Likelihood	

Scenario 1– Malware

- **A new employee accidentally clicks on a phishing link.**
  - **Identify**: What information do they have access to? What resources could be affected by an infestation of malware?
  - **Protect**: What protections do you have in place to prevent malware from being downloaded?
  - **Detect**: How would you detect the malware? How would you identify what the malware had done (e.g. corrupted data)?
  - **Respond**: How would you contain the malware?
  - **Recover**: How would you clean up the malware and restore any information that was corrupted.

Scenario 2 – Insider Threat

- **An employee's relative needs surgery and is desperate for money. They think they can get some by selling the information your business stores or uses.**
  - **Identify**: What information do they have access to? What information would be valuable to them?
  - **Protect**: What protections do you have in place to prevent them from accessing, removing, or selling your businesses information?
  - **Detect**: How would you detect this activity?
  - **Respond**: What would you do to contain this activity? Who would you contact?
  - **Recover**: What strategies does your business have to recover from such an event?

Write It Down!

- **Security Policy**
  - What do you want to protect (exercise 1)
  - To whom does it apply? (exercise 2)
  - What will be done to protect it?

- **Procedures** (the details)
  - Who, What, When, Where, How, How Often

Example Procedure Supporting a Policy

Policy: All computer users will have their own account and password.

Procedure:

1. Supervisor completes/signs account creation request form for new user and sends it to the system administrator [Note that the account request form would be part of the procedure];
2. System administrator creates new account with unique identifier;
3. System administrator assigns a temporary password to new account ;
4. System administrator notifies the new user of the unique account identifier and temporary password;
5. New user logs into the new account and is prompted to immediately change the password;
6. System administrator reviews user accounts monthly.

Monitor & Enforce

- **Begins with the first day at work**
  - Security policies and procedures (should be signed)
  - Security threats and cautions
  - Basic security “do’s and don’ts”

- **Continues with reminders and tools**
  - Regular auditing / monitoring for compliance
  - Track improvement
  - Rewards for good security
  - Periodic re-training – because people forget

WHEN YOU NEED HELP

When You Need Help – Cybercrime

- **If you are or think you are the victim of cybercrime, first report it to your local cybercrime unit**
  - local police, county police/sheriff, state police
- **Contact the local FBI office and/or your State or Local Fusion Center (DHS)**
- **File a complaint with the "Internet Crime Complaint Center" at www.ic3.gov**
- **Contact legal advisor, contractors, insurance, etc.**

Resources

- **NISTIR 7621 Rev. 1: Small Business Information Security: The Fundamentals**
  - http://csrc.nist.gov/publications/nistir/ir7621/nistir-7621.pdf
- **NIST Small Business Corner**
  - http://csrc.nist.gov/groups/SMA/sbc
- **Cybersecurity training for small businesses**
  - http://www.sba.gov/tools/sba-learning-center/training/cybersecurity-small-businesses
- **FCC cybersecurity advice for small business**
  - http://www.fcc.gov/cyberforsmallbiz

Resources

- **National Initiative For Cybersecurity Education**
  - http://www.nist.gov/nice
- **Stop.Think.Connect**
  - http://stopthinkconnect.org
- **National Cyber Security Alliance for small business, home users.**
  - http://www.staysafeonline.org
- **Federal Trade Commission – Identity Theft Information**
  - http://www.ftc.gov/bcp/edu/microsites/idtheft/

Resources

- **NIST Computer Security Resource Center**
  - http://csrc.nist.gov/

- **The *Framework for Improving Critical Infrastructure Cybersecurity* and related news and information**
  - www.nist.gov/cyberframework

For additional Framework info and help

cyberframework@nist.gov

Presenter

Celia Paulsen

Computer Security Division

Information Technology Laboratory MS8930

National Institute of Standards and Technology

Gaithersburg, MD 20899-8930

celia.paulsen@nist.gov

NIST SMALL BUSINESS CORNER:

http://csrc.nist.gov/groups/SMA/sbc/index.html