Comprehensive Cyber Security Risk Management

Dr Linda Wilbanks

Towson University

Lwilbanks@Towson.edu

WHERE ARE YOUR RISKS?

Cyber Security Goal

- Goal = Ensure that the confidentiality, integrity, availability and accountability of the organization's resources (tangible and intangible) are maintained at an acceptable level.

- Risk = Threat x Vulnerability x Impact

- Risk management does NOT eliminate risks

- Not all risks are created equal or should be treated the same

- Identify the risks, determine the appropriate actions

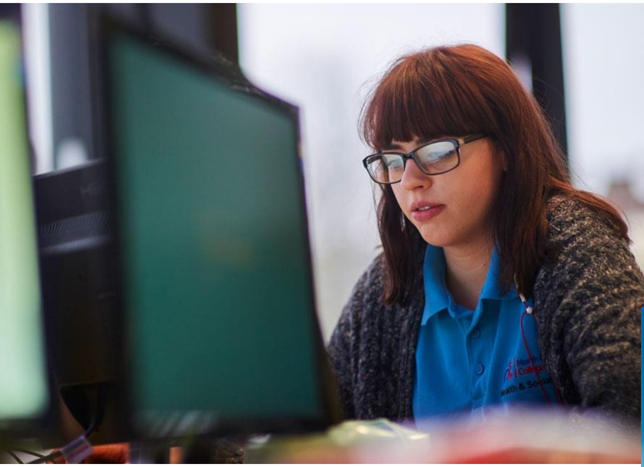
RISK Components

- Losses occur when a **Threat EXPLOITS a Vulnerability**
- **Threat** – any activity that represents a possible danger
- **Vulnerability** – a weakness in the system
- **Loss** – results in a compromise to business functions or assets that adversely affects the business
  - Compromise of business functions – activities a business performs, can result in a loss of revenue
  - Compromise of business assets – anything of measurable value, tangible and intangible
  - Driver of business costs

Threat

- A **threat** is any circumstance or event with the potential to adversely impact organizational operations and assets, individuals, or other organizations through an information system via unauthorized access, destruction, disclosure, or modification of information and/or denial of service.

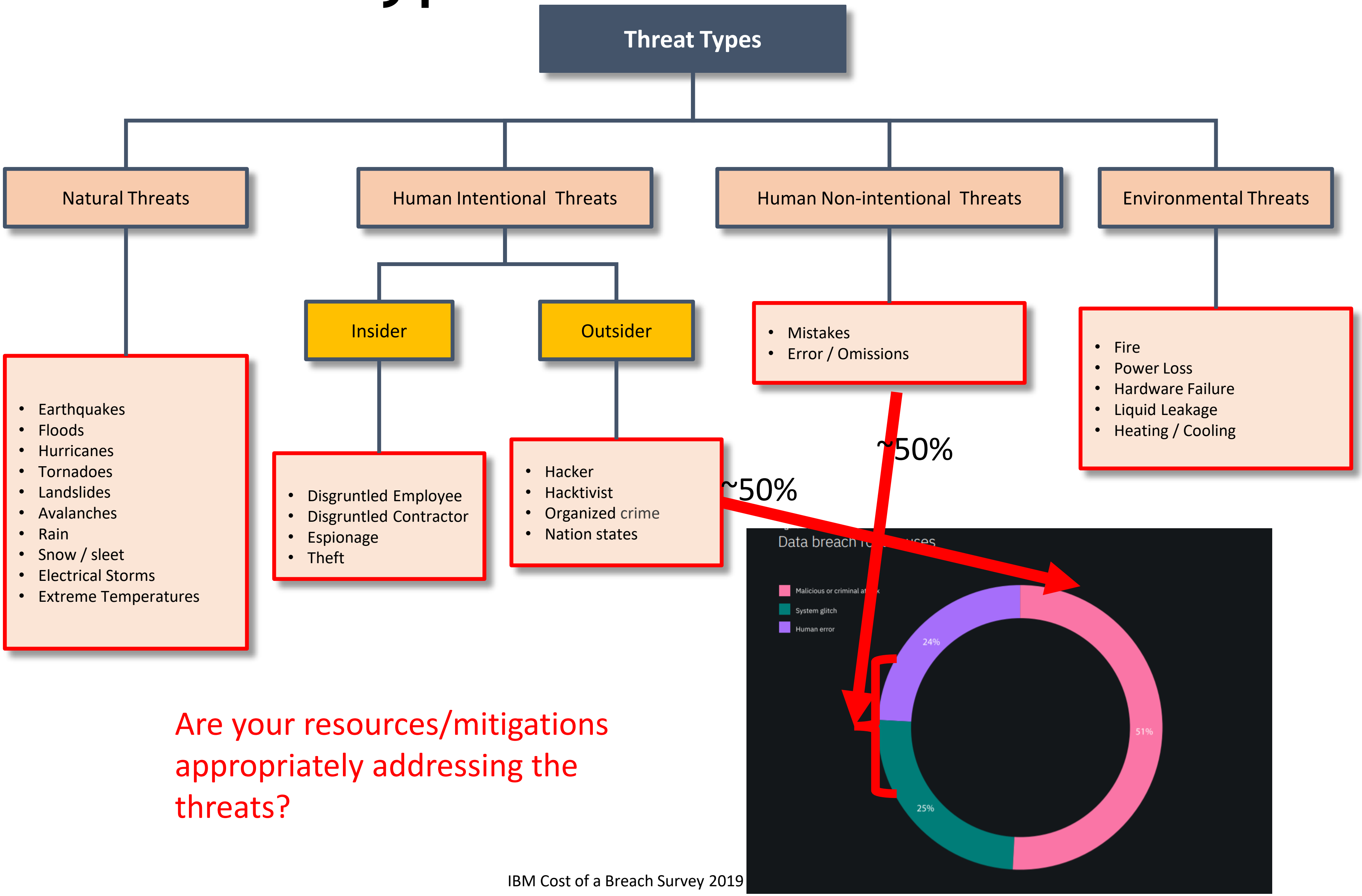
Cyber Threats Are EVERYWHERE



Nature of Threats:

- **Threats cannot be eliminated**
- Threats are always present
- You can reduce the PROBABILITY for a threat to occur by reducing the vulnerability
- You can reduce the IMPACT of a threat
- You cannot affect the threat

Threat Types



Threat Types
Natural Threats
Human Intentional Threats
Human Non-intentional Threats
Environmental Threats
Insider
Outsider
~50%
~50%
Data breach ro[illegible]uses
Malicious or criminal at[illegible]k
System glitch
Human error
24%
51%
25%

- Earthquakes
- Floods
- Hurricanes
- Tornadoes
- Landslides
- Avalanches
- Rain
- Snow / sleet
- Electrical Storms
- Extreme Temperatures

- Disgruntled Employee
- Disgruntled Contractor
- Espionage
- Theft

- Hacker
- Hacktivist
- Organized crime
- Nation states

- Mistakes
- Error / Omissions

- Fire
- Power Loss
- Hardware Failure
- Liquid Leakage
- Heating / Cooling

Are your resources/mitigations appropriately addressing the threats?

IBM Cost of a Breach Survey 2019

The Vulnerabilities:

Vulnerability - weakness in an information system, system security procedures, internal controls or implementation that could be exploited or triggered by a threat source.

Vulnerability examples:

- Unpatched systems
- Out of date systems/software
- Employees
- Location

The Impact/Loss From A Breach:

- The average total cost of a data breach increased by 10%
- $180 = The cost per personally identifiable information record
- $4.62m = average cost of a ransomware breach
- Compromised credentials responsible for 20% of breaches.
- Remote working (due to Covid-19 pandemic) increased the average cost of a data breach by $1.07m.

OKAY – SO WHAT?

IBM Cost of a Breach Survey 2021

Use the Data To Determine Actions:

- Cost of a breach is going up. PII loss is expensive.
  - Possible expense mitigation – cyber insurance
  - Identify PII location – remove unneeded, additional defense
- Ransomware is usually successful through phishing
  - Possible mitigation = Employee training
  - Additional infrastructure
- Credentials are an issue
  - Review, change, increase access controls
- Remote work, home networks and computers

USE this risk information in structuring the cyber security

Life of a Data Breach:

- 287 Days average time to identify and contain a breach
- 2 years to recover

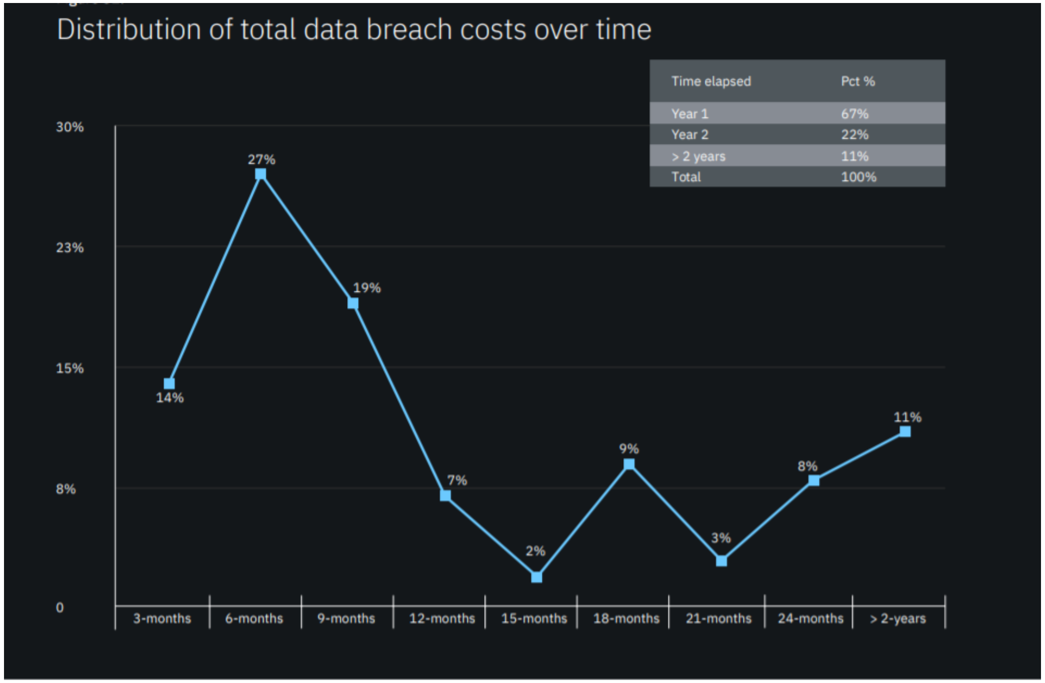
Do you plan for

a 2 year incident

Recovery in vulnerability

management, resources,

and financial??



Distribution of total data breach costs over time

Time elapsed	Pct %
Year 1	67%
Year 2	22%
> 2 years	11%
Total	100%

IBM Cost of a Breach Survey 2019, 2021

Risk Management Considerations:

- Comprehensive asset management, hardware and software. What do you have? No matter how inconsequential.
- Contractor risk management – access control, networks. No matter how obscure.
- Age of systems, hardware and software – old = vulnerable
- Faster identification of breaches = less damage
- More automation, possible AI = faster identification

Thinking Outside the Box

Think outside the box for security, look at all options regardless how probable.

- Attackers tend to be people who look at a system differently then the rest of us.
- They think outside the box, or they see the box as part of the system.

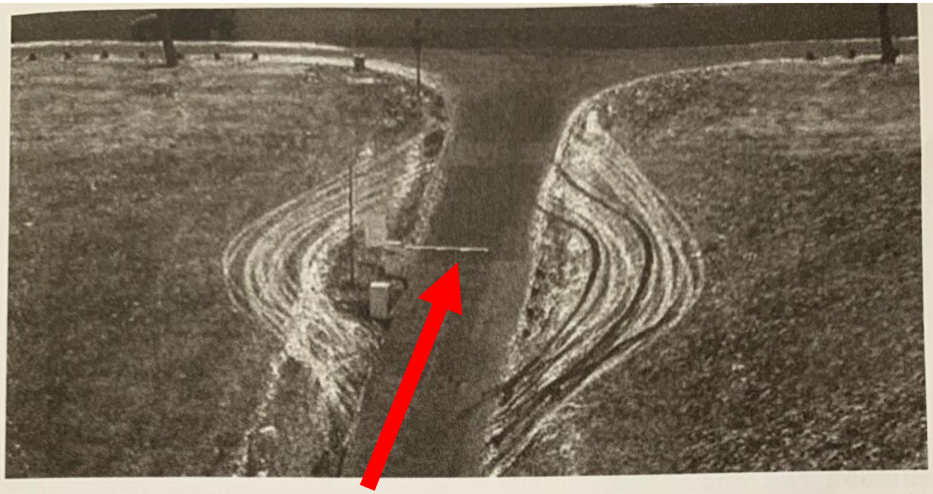


Figure 1: Cars avoiding a security guard rail

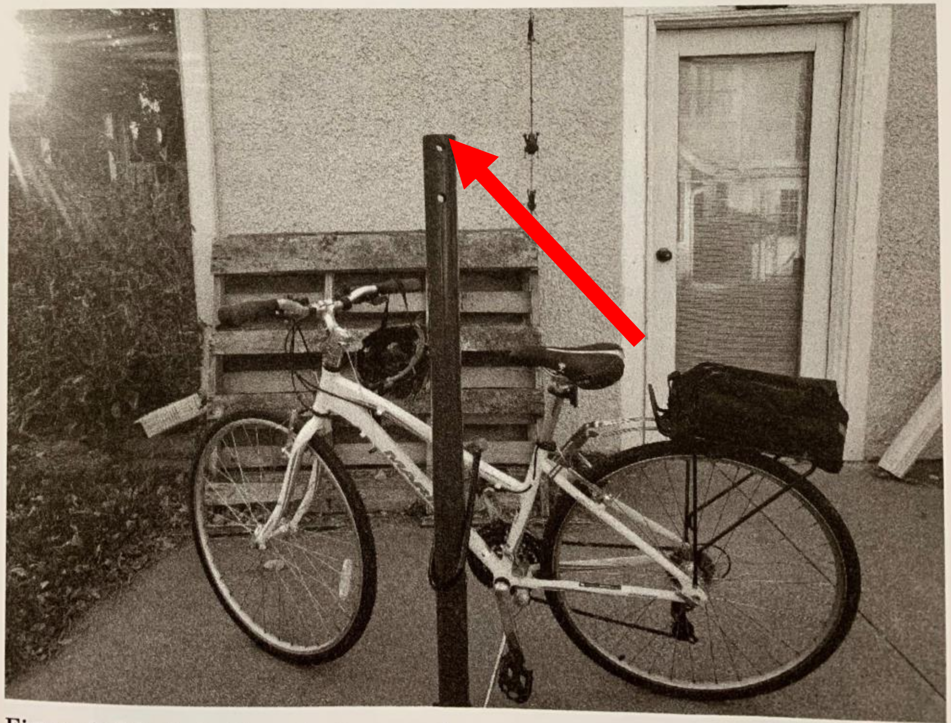


Figure 2: Bike locked to a short, open pole

Understanding the Hackers

- Feb 23, 2020 The 2020 Hacker Report
- By Hackerone

- **What are you protecting?**
- **Where are your access controls the strongest?**
- **Have you considered external hackers for assistance?**

WHAT IS YOUR FAVORITE KIND OF PLATFORM OR PRODUCT TO HACK?

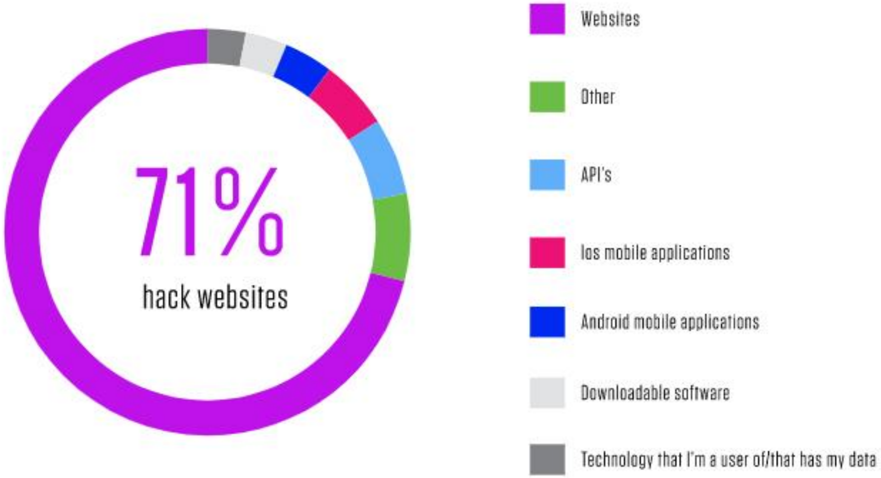


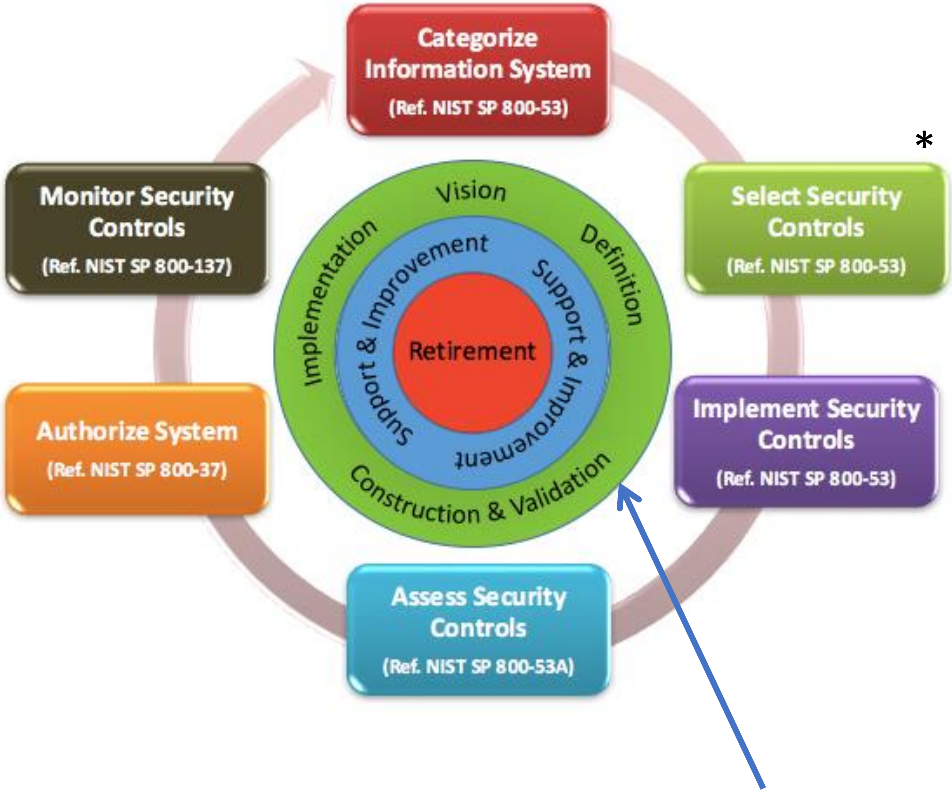
Figure 13: What is your favorite kind of platform or product to hack?

Use a Risk Management Framework

- Provides a structured, consistent, flexible process for managing risk.
- Provides guidelines for determining the appropriate risk mitigation supporting organizational mission/business processes.
- Balances key mission/business goals and organizational priorities with security requirements and policy guidance.
- Facilitates the development of cost-effective information security solutions to commensurate with strategic goals, mission/business process, and overall tolerance for risk.
- Provides processes for continuous monitoring.
- Applicable to both new development and legacy information systems.

EXAMPLE - Cyber Risk Management Framework (CRMF)

- Continually evaluating the organization's risk posture and maintaining situational awareness of its cyber security posture
- Understanding the state and maturity of an agency's cyber security program
- Evaluating cyber security programs at key vulnerability points: people, processes, and technology
- Maintaining a focus on the security program lifecycle
- Addressing the key functions (governance, risk, management, compliance, operations) of a security program



System Development Life Cycle

https://www.nist.gov/cyberframework

Where is Risk Quantification?

What are you measuring?
How are you using the metrics?

✓Software Development
✓Software Testing
✓System Monitoring
✓Training

? Risk Management

How Can You Measure a System’s Cyber Risk????

? How big the system is (# components)

? How much data the system processes

? How much money the system processes

? What is the age of the HW & SW

? Mission criticality

? POAMS

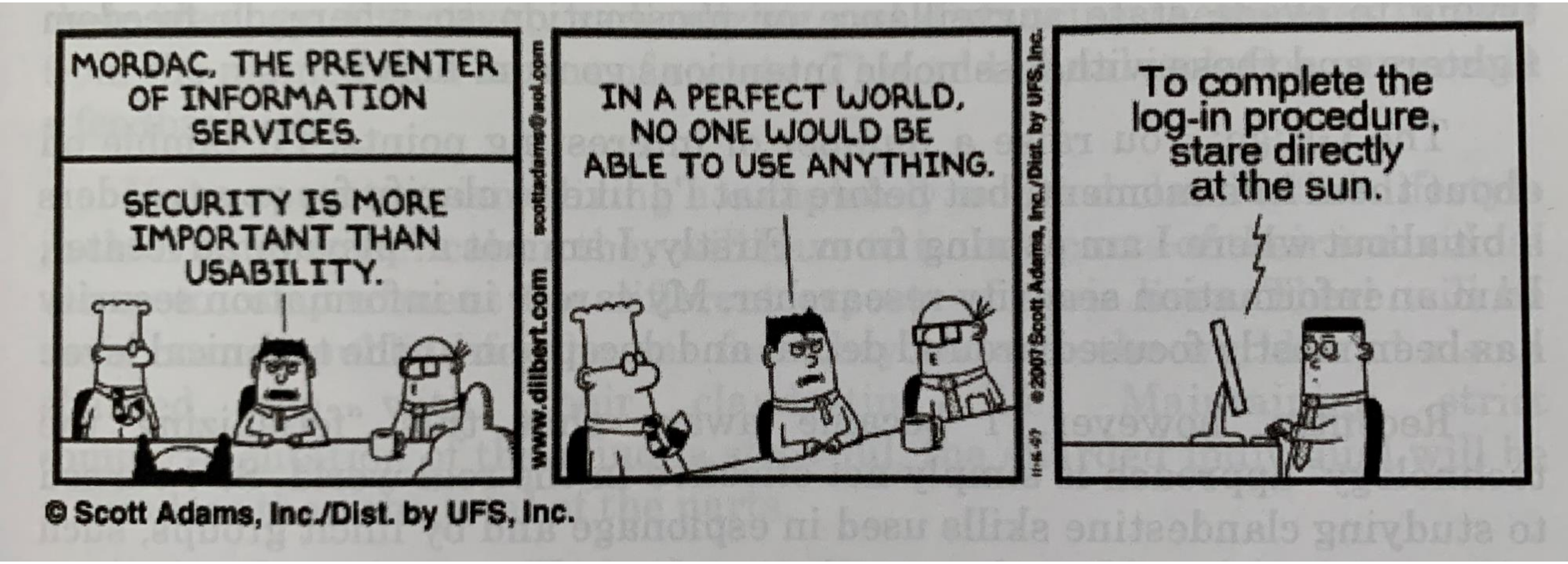
POAM = vulnerability

RISKS =
Plan of Action & Milestones (POAM)

- A POAM is a **vulnerability*** that is scheduled to be fixed.
- If a system has a high number of POAMS = high vulnerability. Are there mitigations in place?
- If POAMS are past due = vulnerability was not corrected/mitigated on time. Are compensating controls still sufficient?
- POAMS are rated critical, high, moderate, low. Are the critical and high being addressed first?
- Does the ATO renewal take the risks associated with POAMS into account?

*vulnerability = weakness in the system that can be exploited

Usability vs. Security


MORDAC, THE PREVENTER OF INFORMATION SERVICES.
SECURITY IS MORE IMPORTANT THAN USABILITY.
scottadams@aol.com
www.dilbert.com
IN A PERFECT WORLD, NO ONE WOULD BE ABLE TO USE ANYTHING.
© 2007 Scott Adams, Inc./Dist. by UFS, Inc.
11-6-07
To complete the log-in procedure, stare directly at the sun.

© Scott Adams, Inc./Dist. by UFS, Inc.

✓Minimal risk

Cyber Risk Focused Future

- Keeping up in cyber security is challenging and can feel impossible
- As soon as you have a handle on major threats, new threats pop up
- To stay a head or just keep pace you need to:
  - Understand fundamental principles of a solid information security program
  - Understand threats, vulnerabilities
  - Identify Risks and Rank them

Wack A Risk

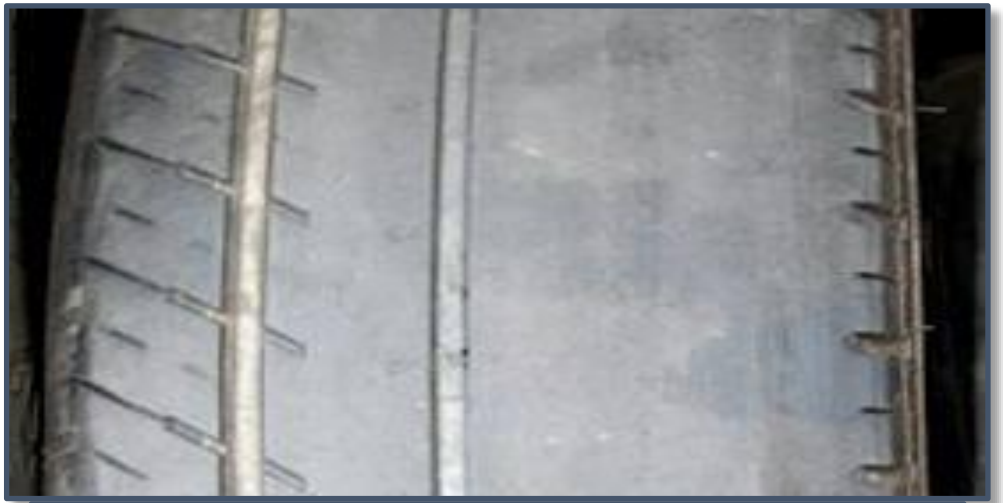
Summary

- Risk Management is a recognition that you cannot protect your company from everything.
- Threats and vulnerabilities are dynamic.
- A Framework/Structure is critical
- POAMS are vulnerabilities

© 2010 Kevin Spear kevin@kevinspear.com www.kevinspear.com

"This year, I resolve to stay away from unnecessary risks."

Risk Exercise –
How Much Risk Will You Accept?



WHAT IS THE THREAT?

WHAT IS THE VULNERABILITY?

WHAT IS THE RISK?

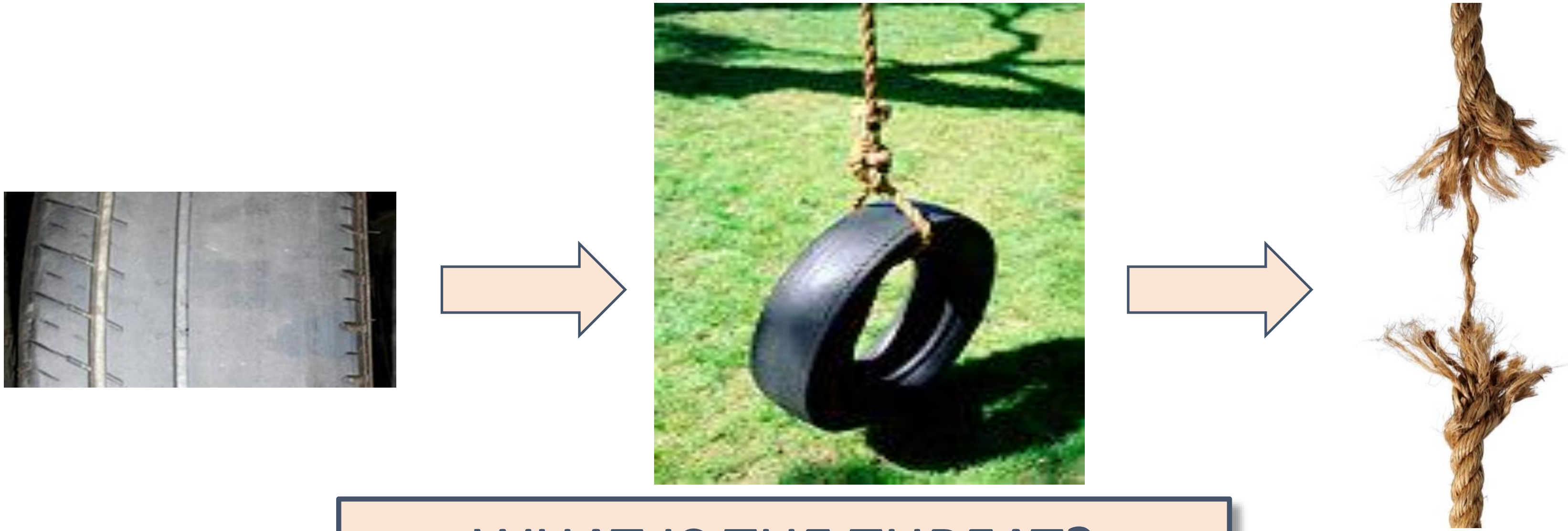
Risk Exercise –
How Much Risk Will You Accept?

WHAT IS THE THREAT?

WHAT IS THE VULNERABILITY?

WHAT IS THE RISK?

Risk Exercise –
How Much Risk Will You Accept?

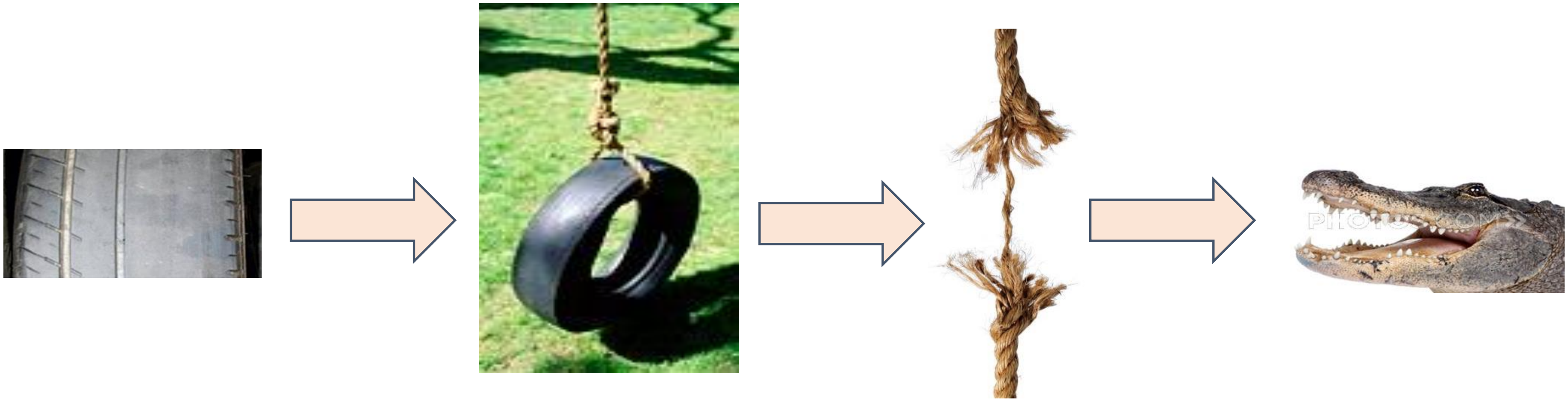


WHAT IS THE THREAT?

WHAT IS THE VULNERABILITY?

WHAT IS THE RISK?

Risk Exercise –
How Much Risk Will You Accept?



WHAT IS THE THREAT?

WHAT IS THE VULNERABILITY?

WHAT IS THE RISK?

Thank You!