Infusing Risk Management into Cybersecurity Education

Barbara.Fox@gatech.edu
Georgia Tech Research Institute

Fear

Uncertainty

Doubt

Mid-career Leaders, Decision Makers

- Cybersecurity is an overwhelming sea.
- The more I learn, the less equipped I feel.
- I don't know where to begin.

Opportunity-Driven Student

- Are their efforts more toward improving company cybersecurity posture or promoting their own careers?

Message from software, hardware, and education suppliers:

You are inadequate

You can't protect properly unless you buy more hardware

You need to upgrade to the expensive premier version of our software to truly protect your organization.

You don't have enough expertise, so you need to buy our services.

You need another certification.

You don't have enough skilled personnel.

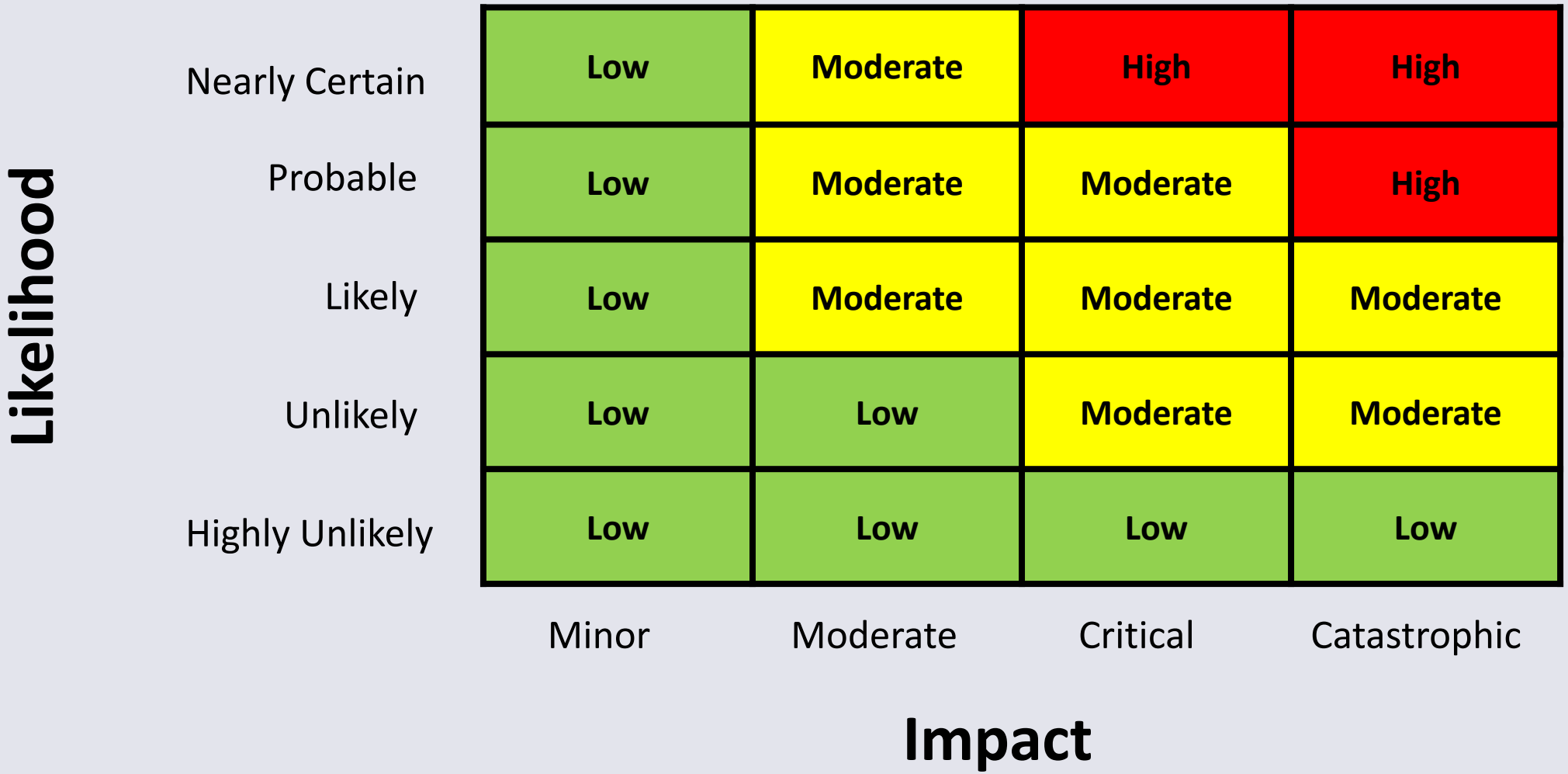
You have the wrong product.

You are doing an insufficient job unless you have eliminated all risk.

Risk is
the potential of a threat to cause a negative impact.

Risk is measured by the likelihood of the event and the severity of the impact.

What risk are we most concerned about?



Likelihood = Probability

Goal is to manage risk, not eliminate it

Avoid

eliminate the cause

Accept

reward is worth the risk,
but have a contingency plan

Goal is to manage risk, not eliminate it

Avoid

eliminate the cause

Mitigate

reduce probability or impact

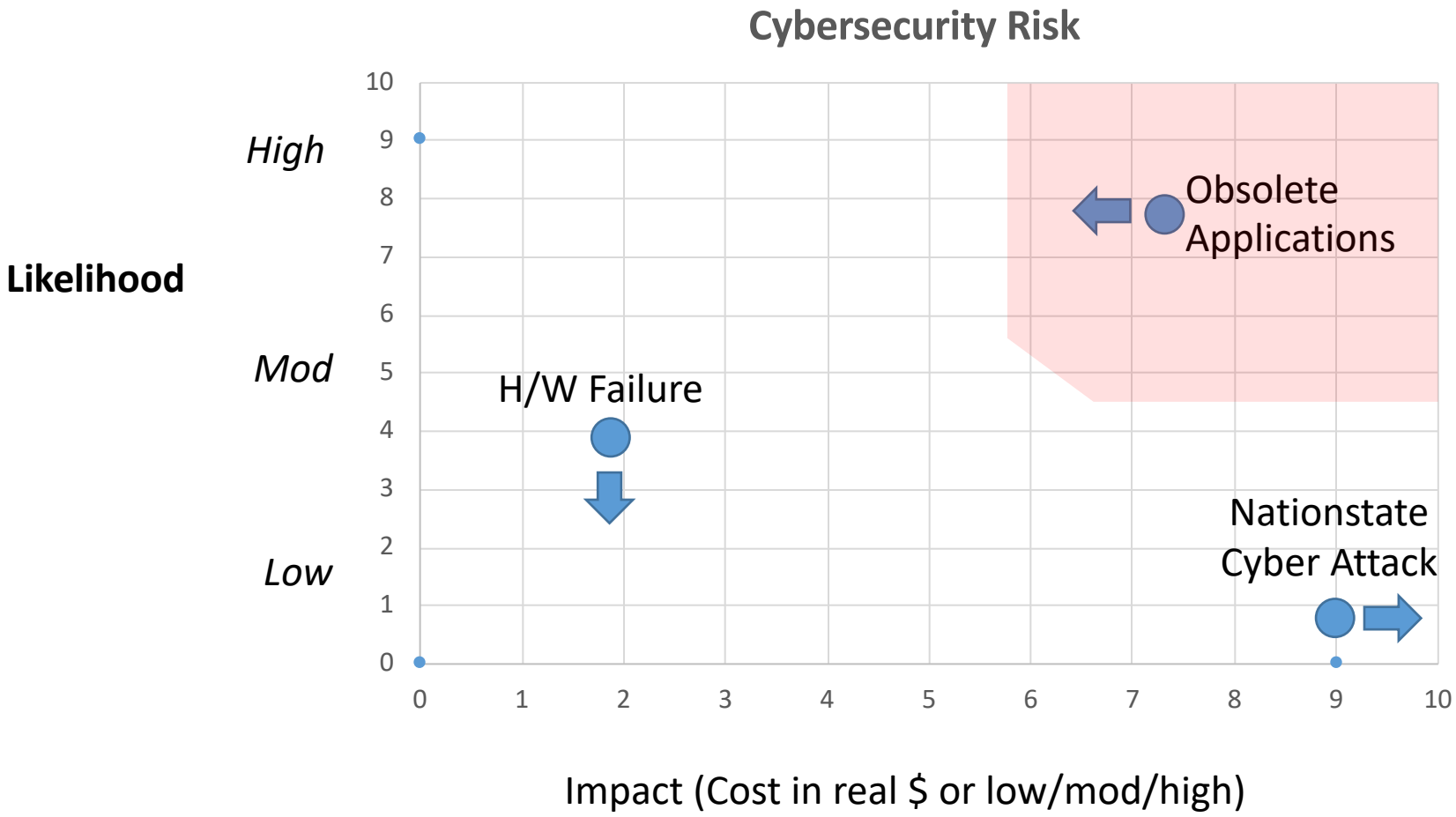
Accept

reward is worth the risk,
but have a contingency plan

Transfer

transfer risk to a third party

Risk Assessment - Qualitative



How do we do this in education?

Community College	• Focus on defensive skills (IT, networking, defend, protect, recover) more than offensive skills (pentesting)
Professional Education	• Leverage non-cyber mid-level professional SMEs, affirming their perspective on what is important and what is most at risk
Undergraduate	• First program – sanitize input, check boundary conditions; Higher quality coding is more valuable than the number of languages; Cybersecurity principles used in all tech projects
Graduate	• Communicate to decision makers in language related to risk, not technology
Community Outreach	• Focus on highest risk actions already in their control – email vigilence, not re-using passwords, changing default passwords on IoT devices
Your Own Organization	• Each department makes at least one suggestion quarterly to improve cybersecurity risk; Monthly awareness vs. once-per-year compliance

Decision Makers

Naive Message

The solution is to spend more money.

Cybersecure Message

You are the Expert.

- Assess your risks with the help of subject matter experts
- Identify low-impact/low-likelihood risks and accept them according to your risk tolerance
- Identify high-impact and high-likelihood risks and determine whether to avoid, mitigate or transfer risks
- Cyber risk is a part of all conversations – include it in a finance class, a human resources class, a leadership class

Software Engineers, Programmers

Naive Message

Learn more languages.

Cybersecure Message

Code securely.

- Validate and sanitize inputs
- Adhere to principle of least privilege
- Modular design
- Testing is built into design and implementation

Information Technology

Naive Message

Focus on the "next big thing."

Cybersecure Message

Build cybersecurity strategies around principles, not tools.

- Use critical thinking skills to analyze, assess, and make decisions.
- Hardware and software purchases should be driven from business needs not market influences.

- Defense-in-depth
- Least privilege
- Trust then verify
- Change management

- Segregate networks
- Separation of duties
- Strong authentication

- Inventory
- Patch management
- Assess vulnerabilities

All Technical Positions

Naive Message

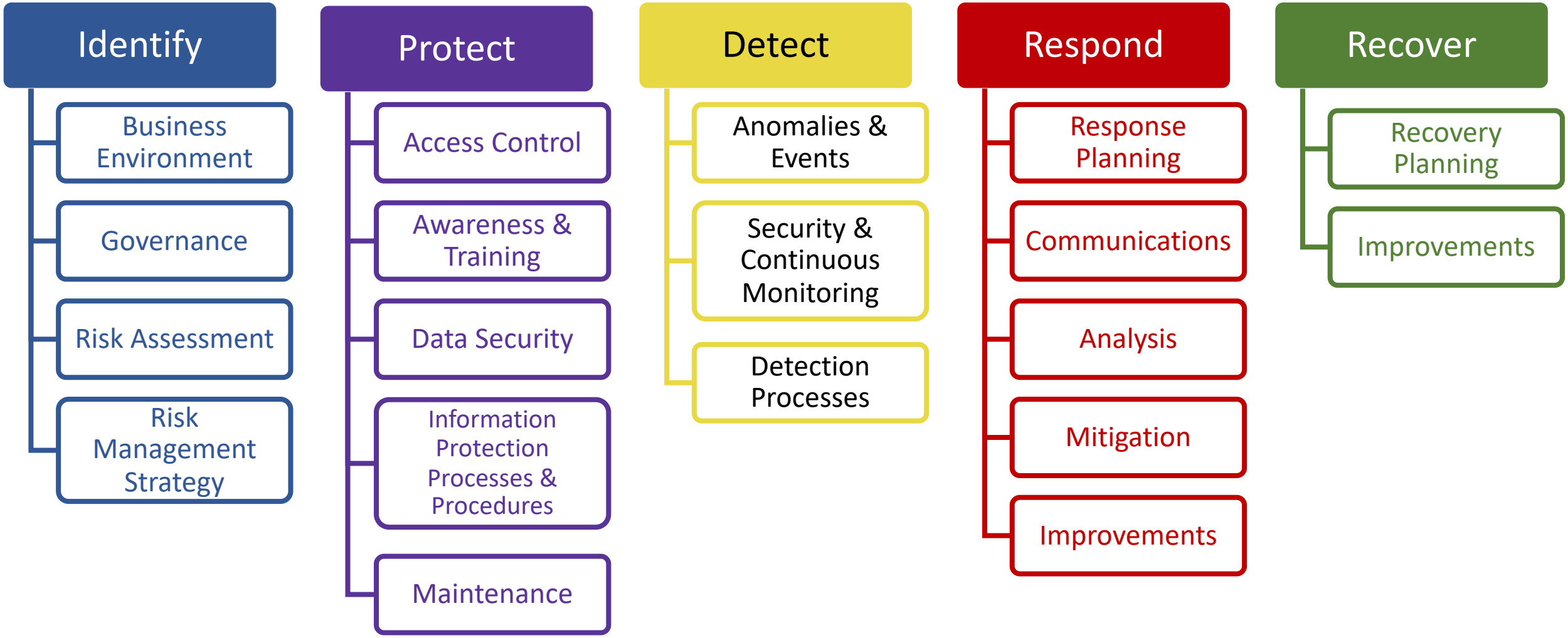
Obfuscate by using insider words like obfuscation.

Cybersecure Message

Communicate the risks and the mitigations in terminology that can be understood by the target audience.

- Use case studies to demonstrate the risk
- Talk about the cost of a breach instead of number of records stolen.
- Build a cooperative culture not "us vs. them". It is truly not about compliance but about risk to your job security and your bank account.

NIST Cybersecurity Framework (CSF)



https://www.nist.gov/cyberframework

CIS Top 20 Controls

1	Inventory of Authorized and Unauthorized Devices
2	Inventory of Authorized and Unauthorized Software
3	Secure Configurations for Hardware and Software
4	Continuous Vulnerability Assessment and Remediation
5	Controlled Use of Administrative Privileges
…	

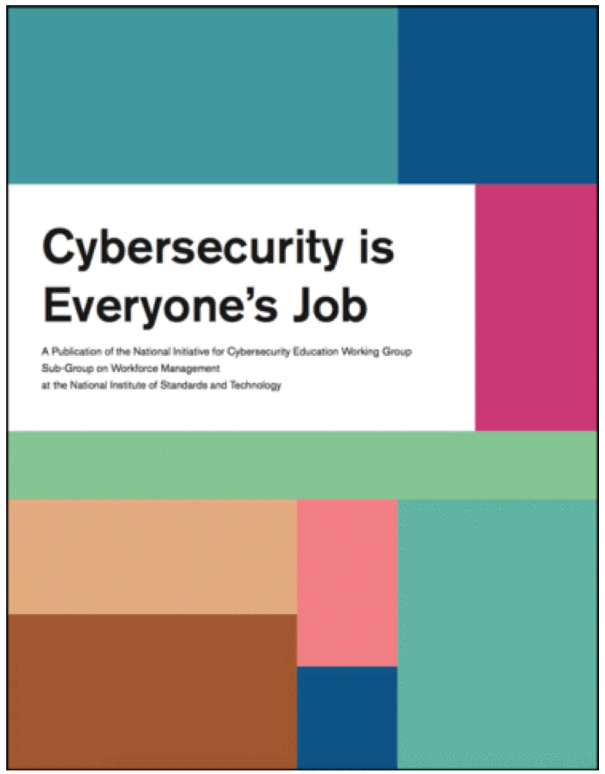
These Top 5 provide an effective defense against approximately 85% of cyber attacks.

CIS - Center for Internet Security

https://learn.cisecurity.org/first-five-controls-download

NIST NICE Guidebook: Cybersecurity is Everyone's Job

- Oriented toward non-cyber professionals



- » Leadership, Planning, and Governance
- » Sales, Marketing, and Communications
- » Facilities, Physical Systems, and Operations
- » Finance and Administration
- » Human Resources
- » Legal and Compliance
- » Information Technology

https://www.nist.gov/sites/default/files/documents/2018/10/15/cybersecurity_is_everyones_job_v1.0.pdf

Cybersecurity Risk Management
All In. All Win.