ASSESSING INFORMATION TECHNOLOGY RISKS

ASSESSING INFORMATION TECHNOLOGY RISKS

1. Scope of Information Security Risks
2. How to Identify Risks
3. Analyze Risks
4. Document Risks
5. Develop a Plan
    - Determine Priority of Risks
6. Develop an Incident Response Plan
    - How to Secure
    - How to Recover
    - How to Communicate

STANDARDS FOR INFORMATION SECURITY

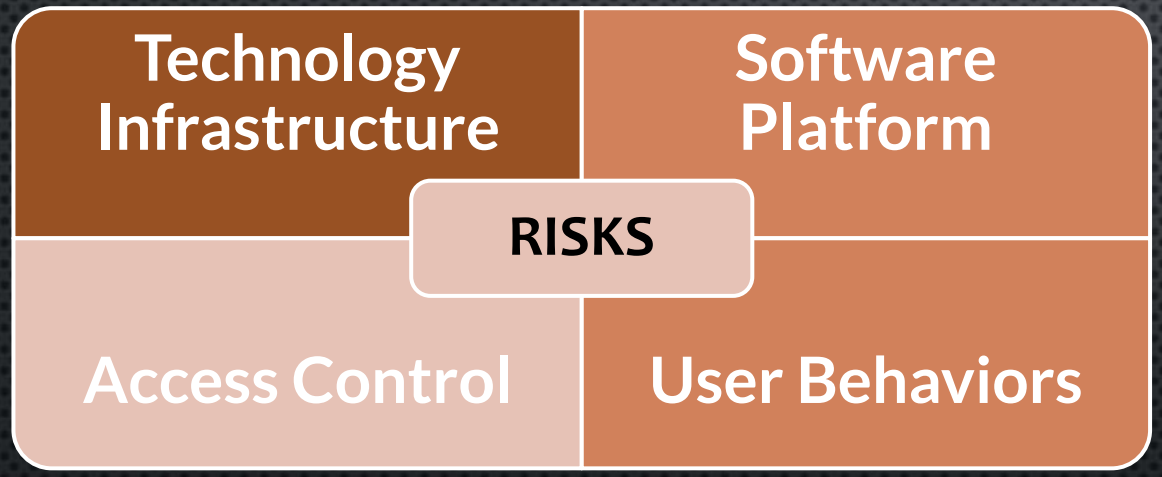
1. **National Institute of Standards and Technology Cybersecurity Framework**
   - Guidelines for government entities on the federal level
2. **International Standardization Organization (ISO 27001)**
   - Internationally accepted standards developed following a management framework
   - ISO 27001/27003 – information security management system (ISMS)
3. **IASME Governance**
   - More for private small and medium-sized enterprises
4. **AICPA – SOC**
   - Standards used by AICPA for collecting and storing personal customer information
5. **Center for Information Security (CIS)**
   - Version 7 – Provides 20 actionable cybersecurity requirements to enhance security.
6. **General Data Protection Regulation (GDPR)**
   - European standards for data protection.

SCOPE OF INFORMATION SECURITY RISKS

GOAL – steal personally identifiable information (PII) to make money without regard to the privacy of the affected individuals or to cause harm.

BOTTOMLINE – expose PIIs and sell them back to the owner/custodian of information or sell them to the dark web.

HOW TO IDENTIFY RISKS



- Penetration Testing
- Software Exploitation
- Ethical Hacking
- User Access Control Audit
- Social Engineering

ANALYZE THE RISKS

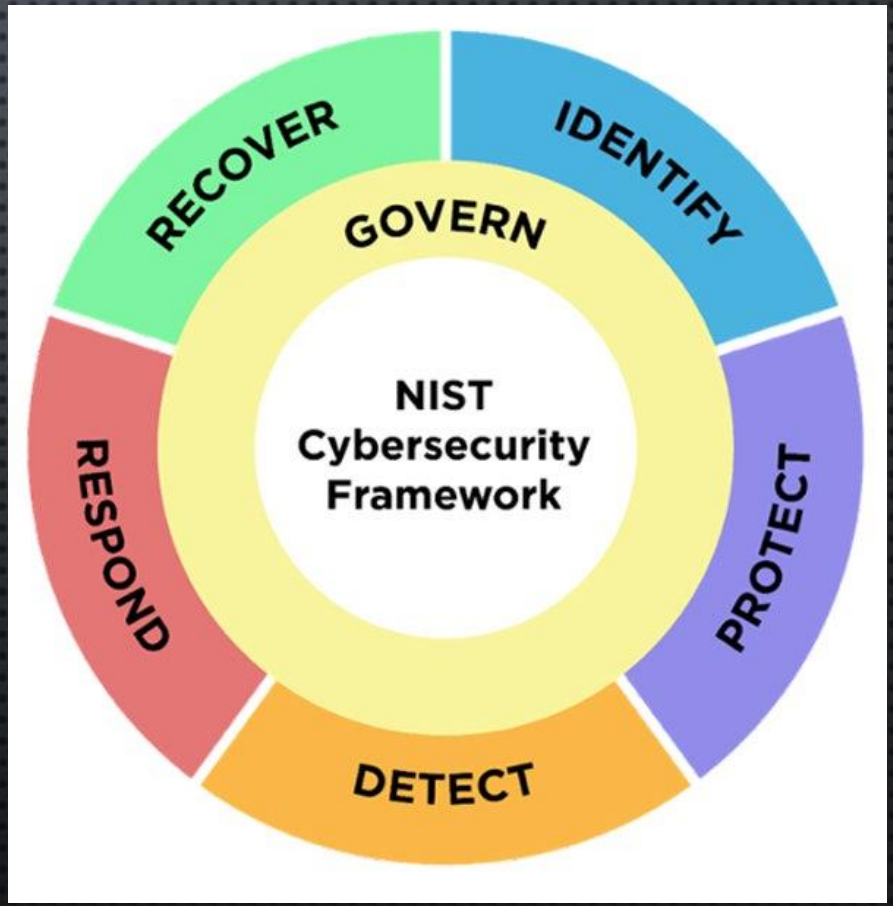
1. Identify Weaknesses and Vulnerabilities
2. Comparing them to Industry Best Practices
   - Authentication
   - Authorization
   - Accounting

1. MFAs
2. Restrict Access to Essential Data Elements Only
3. Review of Access and Authorizations

DOCUMENT THE RISKS

1. Critical to document risks.
2. Develop a Plan.
3. Invest in Information Security.

- Title IV Requirement for Financial Aid Receiving Institutions
- Board Policy and Administrative Procedures



DETERMINE PRIORITY RISKS

1. Laundry list of what to do
2. How do we prioritize?

RISK PRIORITIZATION

- How much money your company will lose if the risk event occurs?
- The chance that this risk event will happen

QUALITATIVE

Risk Likelihood (RL)	Monetary Loss (ML)	Associated RL or ML Value
Almost sure to occur	Very High (>$1M)	Very High
Likely to occur	High ($300K–$1M)	High
An even chance to occur	Medium ($50–300K)	Medium
Not likely to occur	Low ($5–50K)	Low
Almost sure not to occur	Very Low (<$5K)	Very Low

RL and ML Values	Risk Priority
Very High ML and either High or Very High RL	Severe
High RL and High ML, or Very High RL and Medium ML	Significant
Medium RL and Medium RL, or High or Very High RL and Low ML	Moderate
Low RL and Low ML, or Medium RL and Very Low ML	Minor
Very Low RL and Very Low ML, or Low RL and Very Low ML	Minimal

QUANTITATIVE

Risk Likelihood (RL)	Monetary Loss (ML)	Associated RL or ML Value
Almost sure to occur	>$1M	95–100
Likely to occur	$300K–$1M	80–95
Somewhat likely to occur	$50–300K	21–79
Not likely to occur	$5–50K	5–20
Almost sure not to occur	<$5K	0–4

RL x ML	Risk Priority
8,501–10,000	Severe
60,01–8,500	Significant
1,801–6,000	Moderate
301–1,800	Minor
0–300	Minimal

SOURCE: Identify and Prioritize Information Security Risks (netwrix.com)

FINANCIAL IMPLICATIONS

Operational Costs or
Remediation Costs and Legal Bills

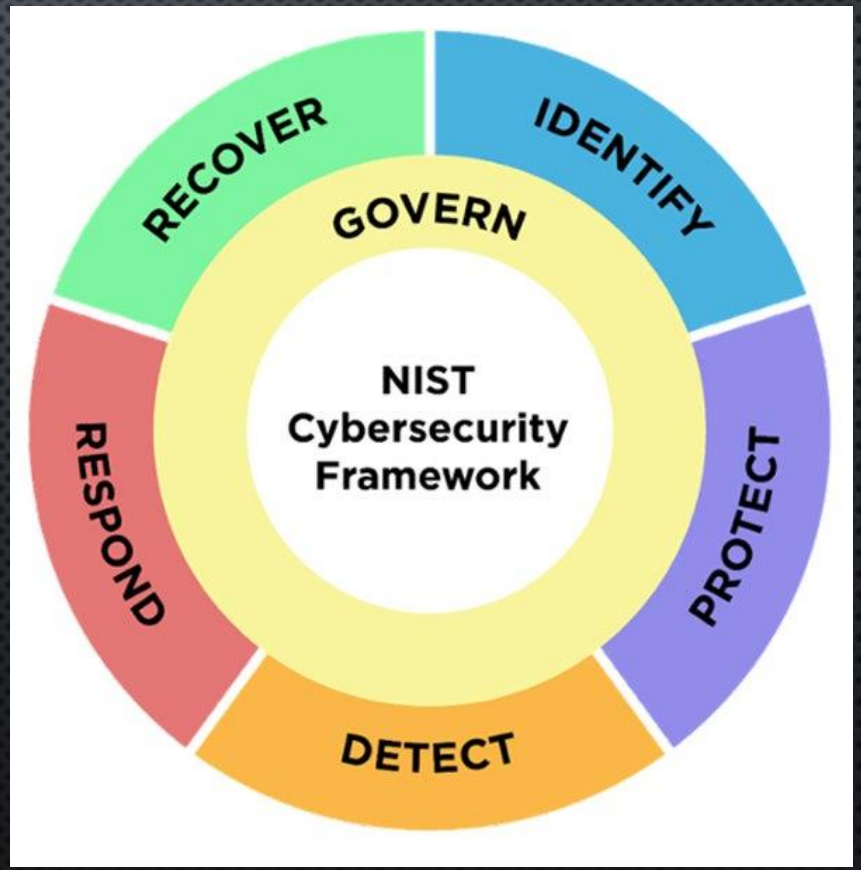
DEVELOP INCIDENT RESPONSE PLAN

The Plan has to answer:

1. How to Secure?
2. How to Recover?
3. How to Communicate?

Essential Elements of the Plan

- Risk Management
- Legal
- Communication



SCENARIO

One week prior to the start of the spring term, the ABC College found out that its systems were infected by a malware that locked all access and there is a demand to pay bitcoin to unlock the systems.

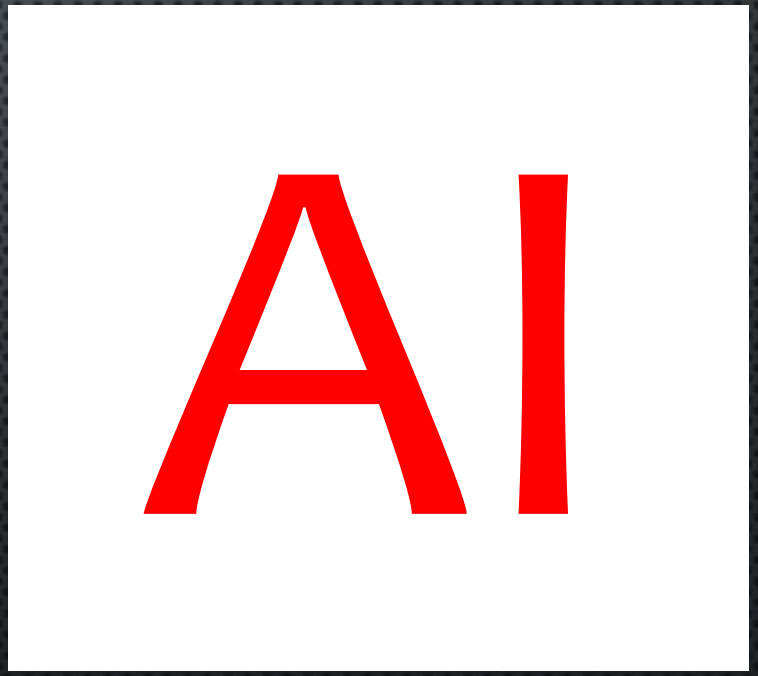
STEPS TO CONSIDER

- INCIDENT COMMAND
- SECURE THE ENVIRONMENT
- CONTACT RISK MANAGER/INSURANCE
- RESTORE THE ENVIRONMENT
- DEVELOP INTERIM SOLUTION
- COMMUNICATE
- DEBRIEF
- UPDATE DISASTER RECOVERY PLAN

Control the Messaging ● Minimize Loss and Protect Reputation ● Assess Next Steps

WHAT'S IN THE HORIZON?

- K-20 Institutions breach = 6.7 million personal records
- $53 Billion cost in downtime between 2018 and September 2023.



Education ransomware attacks cost over $53B in downtime over 5 years | Higher Ed Dive