RSAConference2022

San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: **PNG-R03**

Due Diligence in the Time of Ransomware

Michael Daniel

President & CEO
Cyber Threat Alliance
@CyAlliancePrez

Megan Stifel

Chief Strategy Officer
Institute for Security and Technology
@MeganStifel

CYBER THREAT ALLIANCE

IST Institute for SECURITY + TECHNOLOGY

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

The Ransomware Task Force

- 60+ experts from industry, government, law enforcement, civil society, and international organizations
- Met from January through April 2021
- Drew on expertise from different sectors to create a comprehensive suite of recommendations
- Issued a report entitled: Combating Ransomware – A Comprehensive Framework for Action

Represented Sectors Included:

- Incident Responders
- Cyber Insurance Providers
- Healthcare Entities
- Cryptocurrency Analysis Firms
- International Law Enforcement
- Financial Regulators
- Platform Providers

TASK FORCE Recommendations FRAMEWORK

The report made 48 recommendations across the four-part framework that:

- ✓ Specified short to medium-term actions.
- ✓ Addressed primarily policy and process.
- ✓ Focused on the US government.

Why did the RTF adopt the Due Diligence concept?

The Ransomware Challenge

Ransomware attacks are inherently stressful events

Many victims make a payment decision without all the facts

Governments are enacting restrictions on ransom payments

Organizations often face criticism for their decision

Employing due diligence techniques mitigates these challenges

What do we mean by “due diligence”?

Taking steps to:

- Assemble the relevant, knowable information
- Analyze that information
- Use the analysis to drive a decision
- Document the analysis and resulting decision

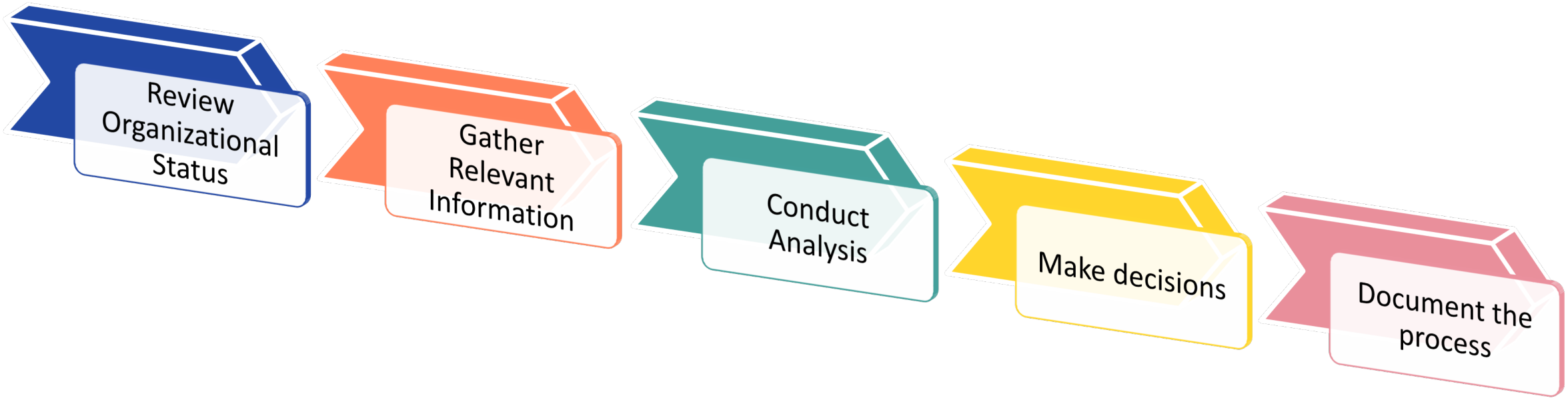
Based on reasonableness, NOT:

- Perfect information
- Exhaustive analysis
- Extraordinary measures
- Unlimited time

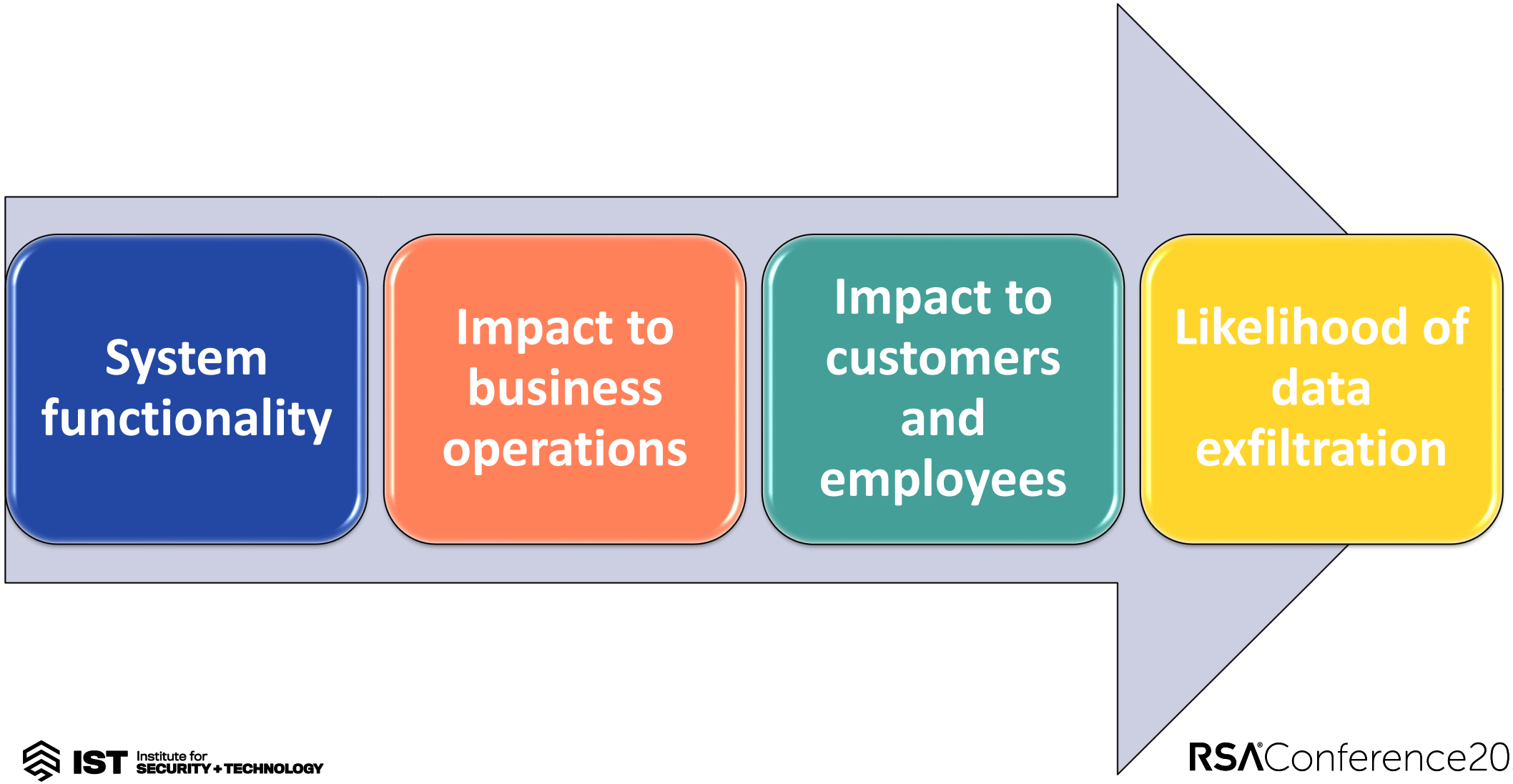
Why conduct a due diligence review?

Imposes discipline during a chaotic, stressful time	✓ Provides needed structure ✓ Ensures availability of relevant, obtainable information
Helps clarify the choice	✓ Eliminates extraneous issues ✓ Highlights benefits and costs of available options
Provides justification for chosen course of action	✓ Can be used with customers, shareholders, investors, the media, regulators, etc. ✓ Demonstrates that actions are based on analysis, not emotion

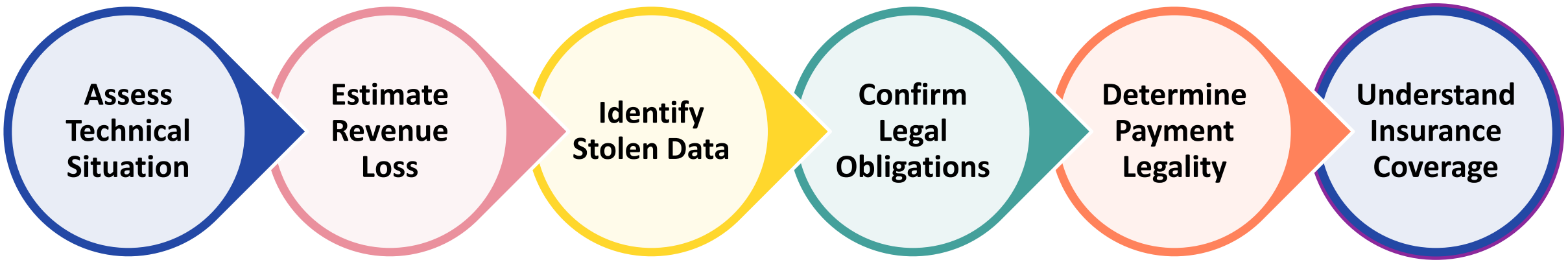
What constitutes due diligence?



Review Organizational Status



Gather Relevant Information



Analyze the Information

This step involves asking a series of questions that bear on the payment question:

- How do the company's values and culture affect the decision?
- How much time would be saved by paying the ransom?
- What costs will be incurred regardless of payment decision?
- What costs or losses will be avoided by paying the ransom?
- What is the reputational effect from either option?
- What is the likelihood of becoming a victim again if payment is made?
- What portion of the costs will insurance cover?

Make Decisions

Analysis should clarify the benefits and costs of the potential choices

Comparing benefits and costs may generate counterintuitive results

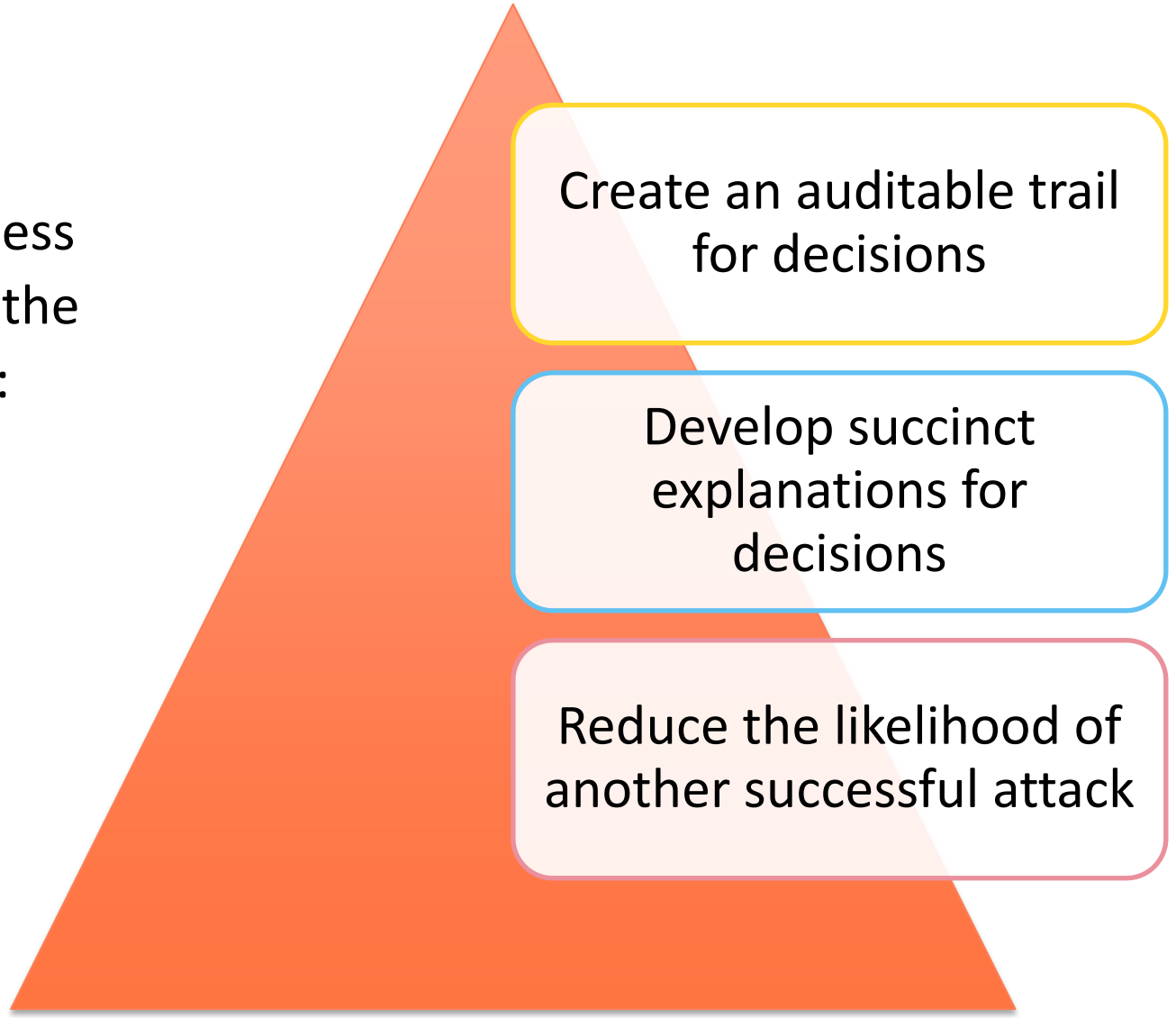
Regardless of the analytic results, the decision to pay or not will remain a judgment call

Beyond the payment decision, the organization will have to decide whether it should:

- ✓ **Report to law enforcement or other government agencies**
- ✓ **Acknowledge the ransomware attack publicly**
- ✓ **Make the payment decision public**

Document Decisions

The final step in the process focuses on documenting the previous four steps to:



Conclusion

Due diligence is not technically complex, but it is organizationally challenging

Does not inform every necessary decision during a ransomware attack

Benefits from following due diligence:

- Assurance that key pieces of information will not be missed
- Clear justification for the pay/not pay decision
- Capability to meet potential government requirements
- Ability to communicate that decision clearly

Committing to such a process before an attack happens is critical

https://securityandtechnology.org/ransomwaretaskforce/report/

Thank you!

Michael Daniel
President & CEO
Cyber Threat Alliance
michaeldaniel@cyberthreatalliance.org

Megan Stifel
Chief Strategy Officer
Institute for Security and Technology
megan@securityandtechnology.org