

Establishing an Intelligence-led Strategy

GSX 2019

Session 4214



Session 4214 Speaker



Toni Chrobot

Risk Confidence Group LLC



Challenges

Add quote

- Fast-paced environment
- Risk landscape is broad
- Stay ahead of risks
- Recognize indicators of threats and hazards
- Communicate with stakeholders and decision makers



RISK CONFIDENCE
GROUP

Session Takeaways:

- Expanded consideration of how physical security, information security, and Information technology resources are inter-dependent.
- Raise awareness and increase visibility to risk and security objectives.
- Consider an approach that brings physical and IT resources together in a collaborative, non-adversarial and productive manner.



Session Takeaways:

“The intelligence-led approach leverages collaboration, drives decision making, and raises awareness *throughout* the organization so I am better positioned to meet my challenges.”



Definitions

- Risk: vulnerabilities and threats that may cause disruption, loss, or damage
- Security: defense against risk that instills different levels of comfort
- Information: knowledge acquired or data obtained
- Intelligence: information, linked and threaded together that makes us smarter



Questions:

- Has my risk and security strategy kept pace with organizational change and the digital information age?
- Are silos creating high-risk gaps?
- Would greater visibility to risks improve my ability to respond and increase my risk confidence?
- How can I dump this on the IT folks?



Dissemination

Requirements

Intelligence In Action

Production

Collection

Analysis



RISK CONFIDENCE
GROUP

Intelligent in Action:

The strategic process of

- asking focused questions
- gathering information
- being able to apply the knowledge gained
- drive strategic collaboration, decision making, and results.



Consider

What are we protecting
against?

- Access
- Coercion | Manipulation
- Fraud | Theft | Harm
- Loss



RISK CONFIDENCE
GROUP

Consider

Physical Security related
concerns

- **Access – Personnel & Facilities**
- **Coercion | Manipulation**
- **Fraud | Theft | Harm**
- **Loss**



RISK CONFIDENCE
GROUP

Consider

IT related concerns

- Access – Phishing & Information systems
- Coercion | Manipulation
- Fraud | Theft | Harm
- Loss of information



RISK CONFIDENCE
GROUP

Requirements

- Who needs access?
- How do we protect against access?
- Are there areas we can't protect = existing vulnerabilities?
- How do we identify coercion or manipulation attempts?
- What is the capability necessary to breach our existing security?
- Where is fraud, theft or harm possible?
- How do we detect and deter fraud?



Consider

Executive Protection

- Access – VIP
- Capability
- Fraud | Theft | Harm
- Loss



RISK CONFIDENCE
GROUP

Consider

Executive Protection

- Where are the risks?
- Person
- Internet
- Location unrest
- Devices
- Other Hazards



RISK CONFIDENCE
GROUP

Insider Threat

Simplifying a complex issue into four complex, relevant areas.

- **Fraud**
- **Espionage**
- **Sabotage**
- **Workplace Violence**



RISK CONFIDENCE
GROUP

Insider Threat

Why it matters.

- Threatens your existence
- Takes on different meanings
- Broad examination of indicators
- Showcases the need for an intelligence-led process



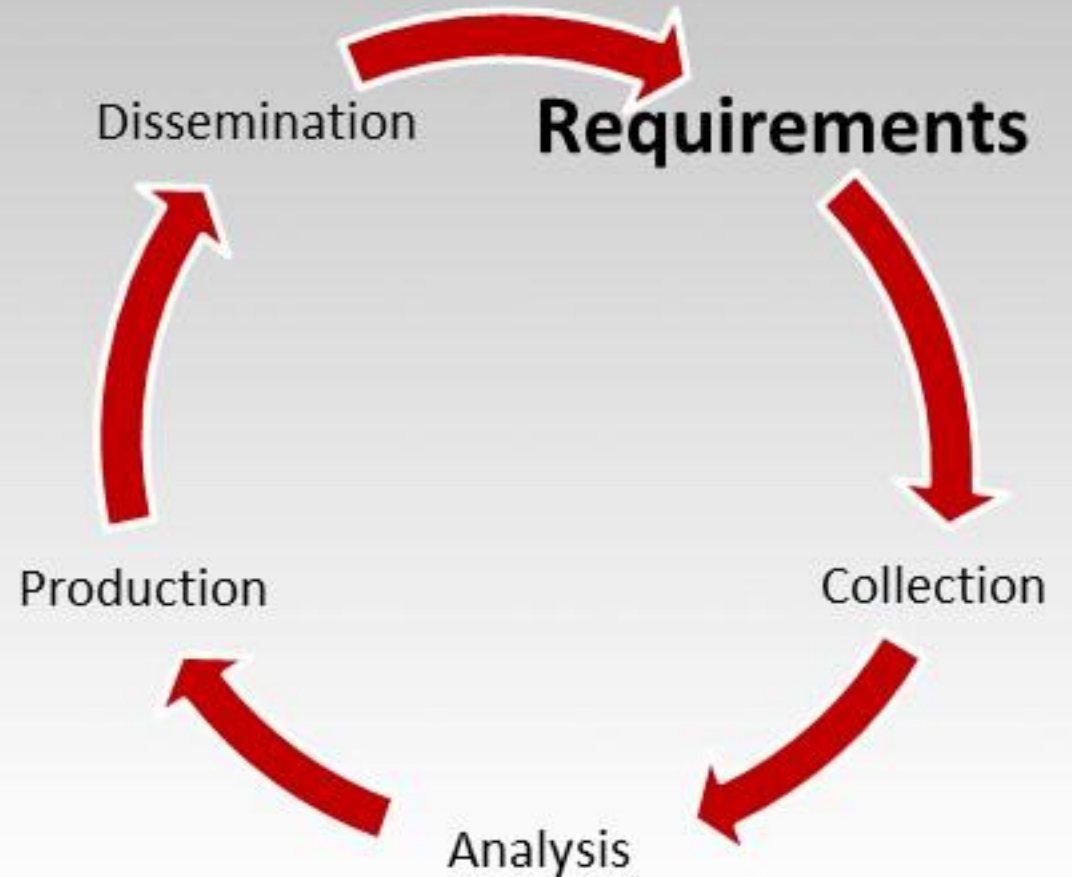
RISK CONFIDENCE
GROUP

Requirements

- What questions are we trying to answer?
- What problems are we trying to solve?
- What are we trying to protect?
- What can an insider do to that poses a threat?

Examples:

- Fraud
- Espionage
- Sabotage
- Workplace Violence



Collection

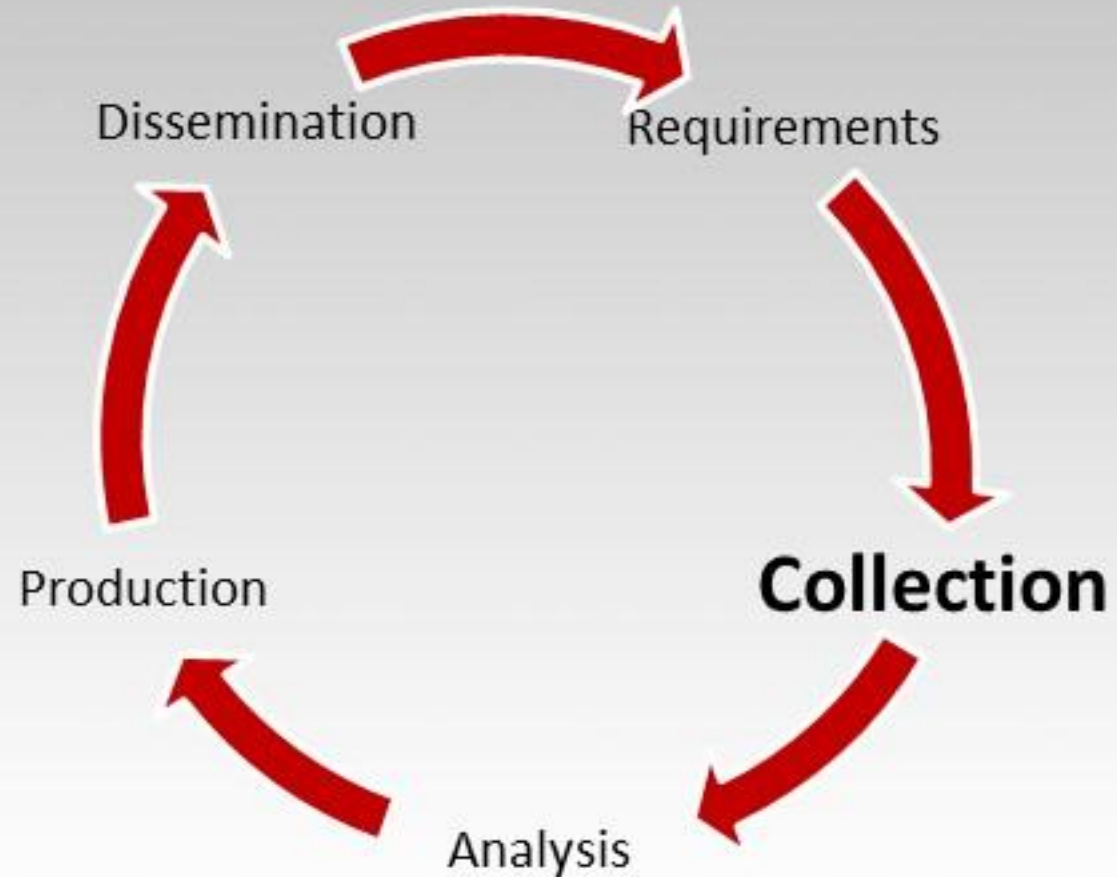
Gather existing data from a variety of sources – often internally and externally.

•Internal

- Security Incidents
- Performance Reports

•External

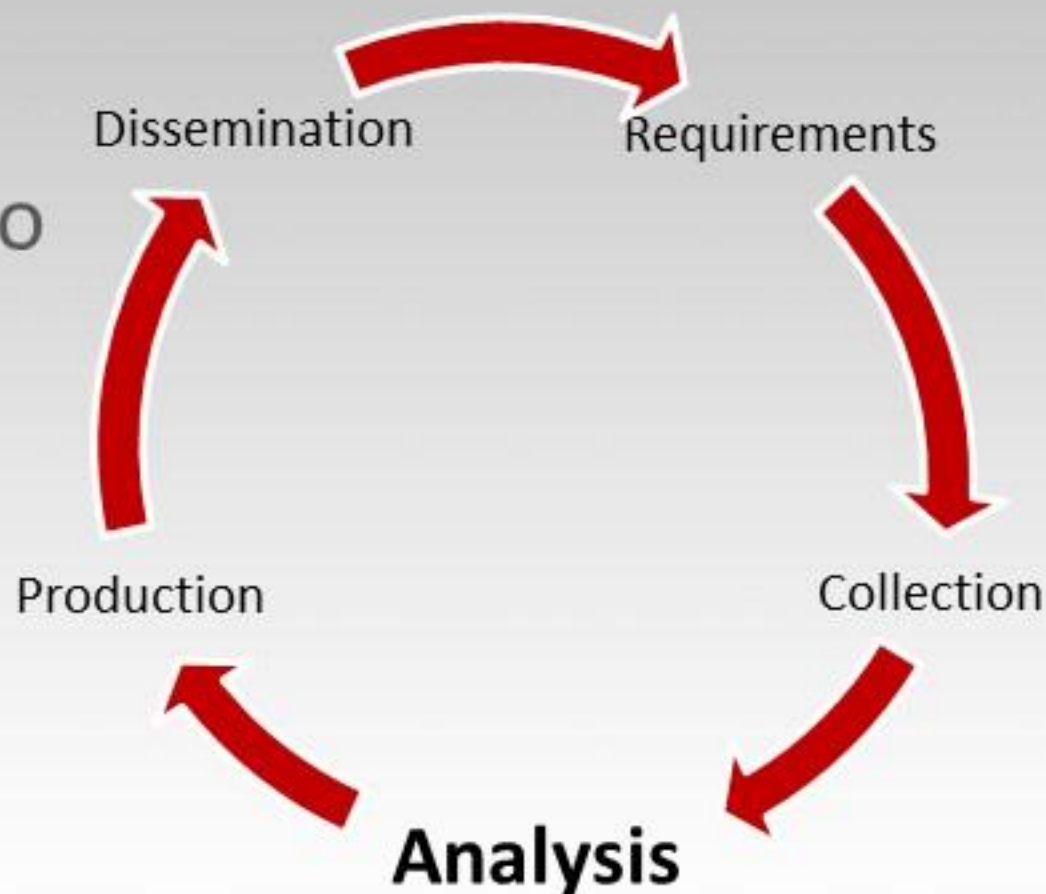
- Public Data
- Social
- Online



Analysis

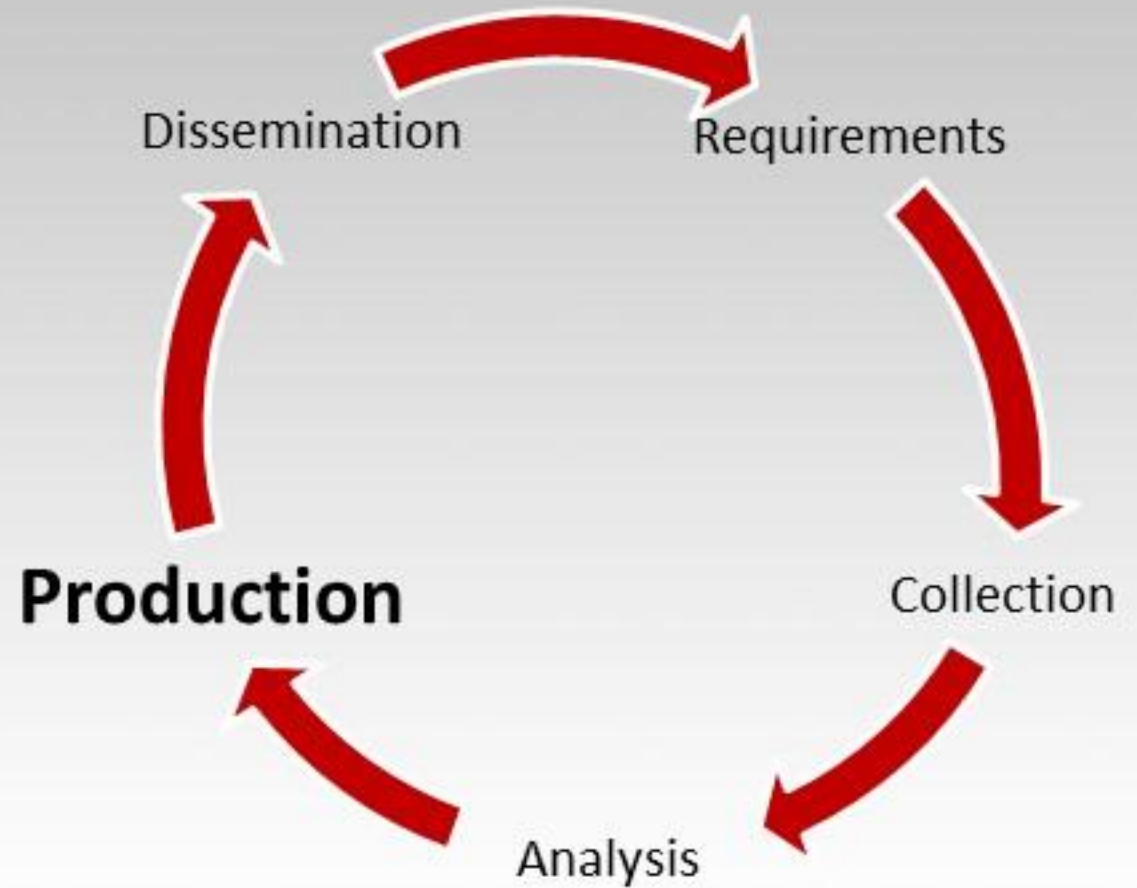
The process of threading the pieces of information together to gain visibility.

- Inform & educate
- Make key judgements
- Basis of assessments



Production

A document or brief which concisely conveys the results of analysis.



Disseminator:

Risk Confidence Group LLC

September 12, 2017

SAMPLE YOUR COMPANY WEEKLY REPORT

Questions

We are trying to answer the following questions:

- What are we trying to protect?
- What assets/activity pose a significant risk?
- What are the indicators?
- Who are we at risk?

Influencers

- Mr. X
- Mr. Y
- Dr. Z

Risk Confidence Level

High

Other

Prepared for Client

Intelligence Summary

The most significant threat to the security of the company for this week is the possibility of a data breach. The XXXX activity poses the most significant risk to the sensitive information. A number of our key assets have been compromised, including the XXXX and XXXX. These assets have been compromised via the XXXX and XXXX. The XXXX and XXXX are considered high risk and require immediate attention to prevent a significant risk.

SAMPLE

YOUR COMPANY OR EVENT
INTELLIGENCE REPORT FOR DISSEMINATION

SAMPLE - INTELLIGENCE as of 9/9/19: Possible threat to Mr. Bojangles

Bits of Concern:

- On 6/25/17 a post was identified which indicated a threat to Mr. Bojangles and/or scheduled for 7/4/17
- Threats came from a Twitter account associated with Lisa Lora

Account Information:

- Name: Lisa Lora
- Username: Twitter
- Handle: @linalora
- Location: Lisa L
- Linked to: Facebook
- Joined Twitter: May 2017
- 4,500 list at posts
- 48 Authorized posts
- 121 Likes
- 204 Followers
- Following: 432

Relevant Playoffs:

- @ljajajajajajajaj
- @ljajajajajajajaj
- @ljajajajajajajaj

Key Judgmental Assessment:

- Degree of risk: High
- Access and Means to act: High
- Ability to act: Low

Based on prior incidents involving social media, a threat to Mr. Bojangles or another member of his party is likely.

On 6/25/17 Twitter account @linalora, user of Lisa Lora, provided information of concern for the safety of Mr. Bojangles. Lisa Lora is believed to be a former associate of Lisa Lora who works in the area where Mr. Bojangles lives and in the second floor of a store owned by Lisa Lora. Lisa Lora is believed to be a former associate of Lisa Lora who works in the area where Mr. Bojangles lives and in the second floor of a store owned by Lisa Lora. Lisa Lora is believed to be a former associate of Lisa Lora who works in the area where Mr. Bojangles lives and in the second floor of a store owned by Lisa Lora. Lisa Lora is believed to be a former associate of Lisa Lora who works in the area where Mr. Bojangles lives and in the second floor of a store owned by Lisa Lora.

Based on analysis, Mr. Lorraine is the threat and ability to take physical action against Mr. Bojangles. However, she has no intent to do so. It is highly likely that Mr. Lorraine will attempt to gain access to Mr. Bojangles' temporary location, and she remains a threat to Mr. Bojangles. Based on prior incidents, she will likely begin surveying the location and may attempt to gain access to Mr. Bojangles' location. Mr. Lorraine is a threat and was observed on St. John County online public records relative to her 2015 arrest.

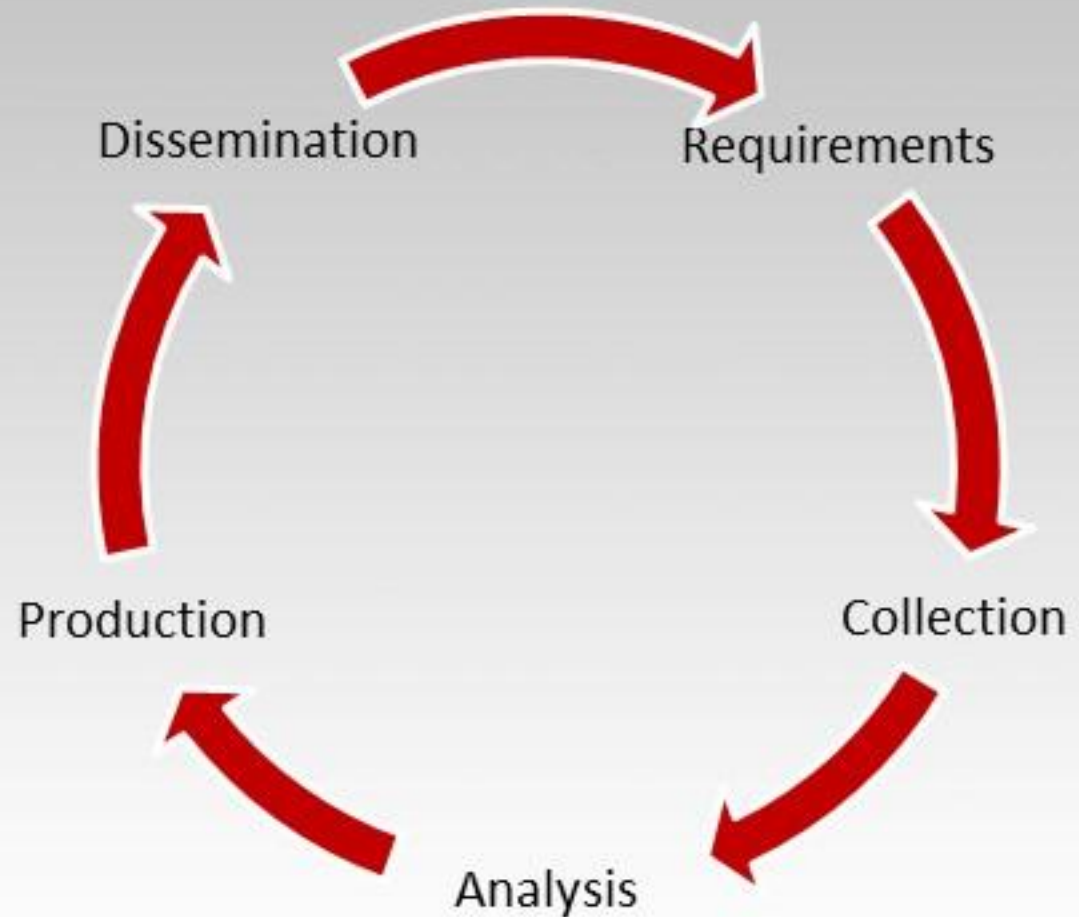
Property of Risk Confidence Group LLC. Copyright 2017



Collaboration

The process brings stakeholders together in a non-adversarial and highly efficient way.

- Increased awareness
- Increased visibility
- Effective risk mitigation



Dissemination

Requirements

**Increased
Visibility**

Production

Collection

Analysis



RISK CONFIDENCE
GROUP

What is your challenge?

- Establishing a strategy?
- Prioritizing risks?
- Increasing visibility?
- Raising awareness?
- Business Continuity?
- Emergency or Crisis?



RISK CONFIDENCE
GROUP

“If we follow an intelligence-led process, we will increase our visibility, leverage collaboration to mitigate operational risk, and enhance overall security.”



Questions & Contacts

Toni Chrabot

Risk Confidence Group LLC

Office: (904) 834-3448

Email: toni.chrabot@riskconfidencegroup.com

URL: <https://www.RiskConfidenceGroup.com>

