

# The 30-Second Security Pitch



Rebecca Herold, CIPP, CISSP, CISA,  
CISM, FLMI

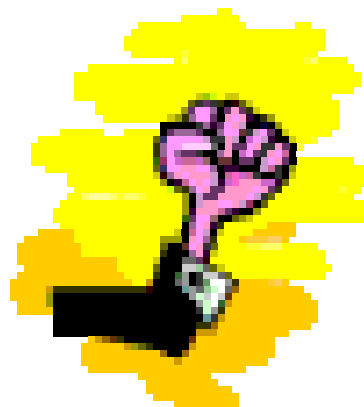
Rebecca Herold, LLC

<http://www.privacyguidance.com>

[RebeccaHerold@rebeccaHerold.com](mailto:RebeccaHerold@rebeccaHerold.com)

# Be Prepared For The Common Executive Questions

## 5 commonly recurring questions



# 1. What Is My Personal Risk?

***“What are the personal risks that business executives face if they fail to implement effective security controls or do not comply with data protection regulations?”***



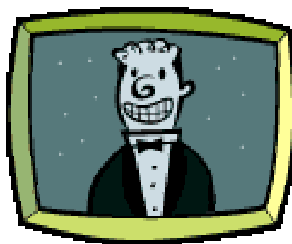
# 1. What Is My Personal Risk?

**One possibility:**

*You, as our organization's business leader, are ultimately responsible for ensuring we have a strong security program in place. If you don't, you personally could get substantial fines and penalties, even including jail time. You also subject our organization to significant fines and penalties, civil suits, diminished brand value, lost customers, and possibly the loss of our business.*

## 2. How Do We Start A Program?

***“What approach should we take to start an effective risk management, security or privacy program?”***



## 2. How Do We Start A Program?

### One possibility:

*Our risk management and information protection program needs to be improved. It will be more effective with the following four components:*

- 1. Your strong and visible support for the program.*
- 2. A good team representing the enterprise, with a strong and experienced leader.*
- 3. A foundation built upon proven information control and technology frameworks.*
- 4. Controls based upon our organization's own unique risks*

## 3. How Is Information Leaked?

*“What are some of the most common ways that information is leaked or compromised?”*



## 3. How Is Information Leaked?

### One possibility:

*We are vulnerable to having PII and sensitive data leaked, resulting in costly information security incidents and privacy breaches, largely due to the following:*

- *Sensitive data included within or attached to email messages.*
- *Mobile computing devices and storage devices that are lost or stolen.*
- *Applications and systems that are built without properly addressing security controls.*
- *Authorized persons making mistakes or purposefully doing malicious things.*
- *Disposing of computers, storage media, and paper without first removing sensitive information.*

*I need your support for the initiatives to address these vulnerabilities.*

## 4. How to Secure Mobile Data?

***“What can we do to secure our mobile data?”***



## 4. How to Secure Mobile Data?

### One possibility:

*PII and other types of sensitive information that pass through networks and are stored on mobile computers and storage devices are highly susceptible to security incidents and privacy breaches. We need to protect this mobile data by:*

- *Having business leaders, such as yourself, strongly support policies and procedures for protecting mobile data.*
- *Encrypting mobile PII.*
- *Providing training and ongoing awareness to personnel for how to safeguard mobile data.*

*I need the support and resources to protect our mobile data.*

## 5. How to Deal With The Insider Threat?

*“What should we do to keep personnel from making mistakes or doing malicious activities?”*

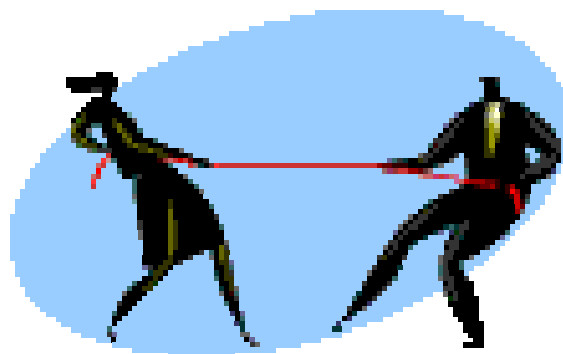
## 5. How to Deal With The Insider Threat?

**One possibility:**

*People will make costly mistakes if they do not receive information security training and ongoing awareness communications. Personnel who want to misuse their authorization to commit fraud, crime, and perform other malicious acts will be able to do so more easily if the workforce is not provided information security education and taught how to recognize the red flags of those around them. If you visibly and actively support our information security and privacy education efforts, we will have personnel who safeguard our business information better, and ultimately improve our business.*

# Unique Issues

**What other issues are you struggling with?**



# Be Prepared!



- 1. Relationship with CxOs**
- 2. Quickly point out business risk area**
- 3. Not the time for details**
- 4. Develop rapport**
- 5. Raise awareness**
- 6. Ask for support!**

# Questions or Comments?



Rebecca Herold, CIPP, CISSP, CISA, CISM, FLMI

Rebecca Herold, LLC

<http://www.privacyguidance.com>

[RebeccaHerold@rebeccaHerold.com](mailto:RebeccaHerold@rebeccaHerold.com)