Speaking the Language of Information Security in RIM

Will Fletcher
General Counsel

ZASIO

Legal Disclaimer

Ahoy, me hearty! Avast, ye landlubber! Here be a legal disclaimer writ in the finest pirate tongue. Use these words well, but heed this warning: a pirate's oath be no substitute for a lawyer's writ.

For general information, savvy?

All the treasure ye find here, be it tales, maps, or tall tales of the sea, is for yer entertainment alone. 'Tis not legal or other professional advice, no more than a parrot be a compass. If ye find yerself in Davy Jones's locker over this scuttlebutt, the captain and crew can't be held accountable.

The accuracy of the treasure map

We've done our best to chart a course true and straight, but these waters are treacherous, savvy?. We ain't guaranteeing the plunder be there, nor that the kraken won't rise up and scuttle yer plans. Any decisions ye make be on yer own head, not ours.

Fair winds and following seas

By reading this parchment, ye agree that ye won't bring any mutiny or claims against this crew for what ye find here. Consider yerself warned. Now weigh anchor and hoist the mizzen, but don't say we didn't tell ye!.

What is this presentation about?

- **RIM and Information Security have a lot in common!**

- The lines between records and data management are blurring.

- **Cross-functionality**: You must know a lot more and work collaboratively with others.

- **RIM and IG are key players under the IG tent.**

- **By the End**: You'll know a lot more about Information Security so that you can work more collaboratively with InfoSec to **solve IG problems**.

Let's start with some definitions.

What is **Information Security** (**InfoSec**)?: Managing **risks** to the **confidentiality**, **integrity** and **availability** of **information assets** using **administrative**, **technical,** and **physical controls**.

How is **InfoSec** not **cybersecurity** or **IT security**?

- Cyber and IT are focused on technology and the digital.
- InfoSec is a **business issue.**
- InfoSec covers **all information**, including **records** and **physical records.**

Risks

There will always be risks; risk cannot be eliminated. But it can be managed. InfoSec addresses risks by:

- Acceptance
- Mitigation
- Transfer
- Avoidance

Controls

Administrative: Written policies and procedures, training. Used to manage personal behavior.

Technical: Firewalls, passwords, permissioning, antivirus software.

Physical: Door locks, alarm systems, video surveillance. Manage physical access to information.

The CIA Triad

Confidentiality: Keeping information secret, allowing only authorized disclosure. The opposite of confidentiality is unauthorized disclosure.

Integrity: Accuracy, reliability, correctness. The opposite of integrity is unauthorized alteration.

Availability: Ensuring those authorized to access information have timely, uninterrupted access, when needed. The opposite is unauthorized destruction.

The ACA Triad

Auditing: The logging of events. Recording **unauthorized** or **abnormal** activities.

Compliance: Minimizing exposure to regulators and lawsuits (risk) by working in accordance with a set of laws or standards.

Accountability: Enforcing responsibility for action, particularly violations of organizational policies.

How does RIM line up with InfoSec?:

Generally Accepted Record-Keeping Principles (GARP)®: **ATIP CARD**

Accountability

Transparency

Integrity

Protection

Compliance

Availability

Retention

Disposition

Very well, actually

Accountability = Accountability

Transparency = Auditing

Integrity = Integrity

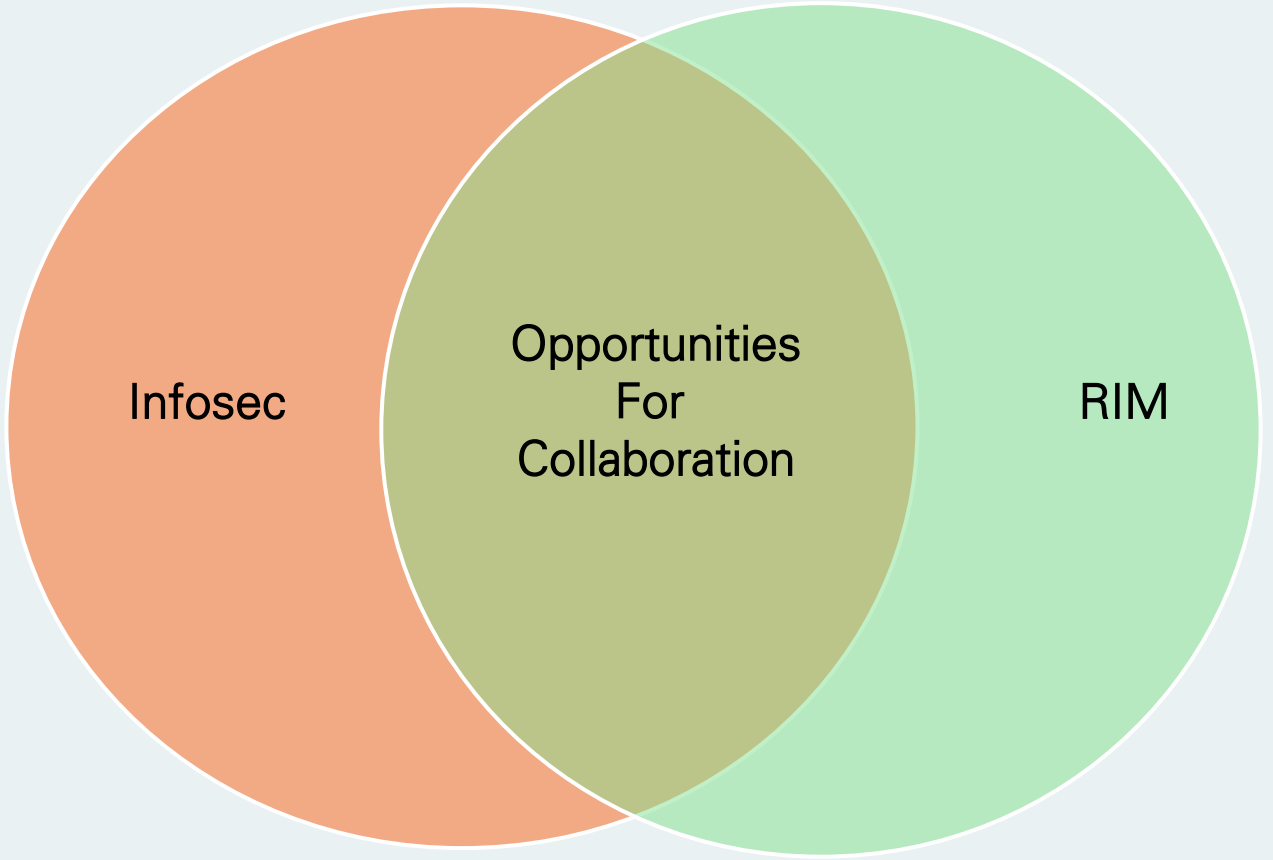
Protection = Confidentiality

Compliance = Compliance

Availability = Availability

Retention

Disposition



Core InfoSec Concerns

Threats: Any harmful activity/event aiming to disrupt your CIA, particularly on computing networks and systems.

Vulnerabilities: Any weakness in your systems and networks that can be exploited by a threat.

Core InfoSec Concerns

Object: Any individual, identifiable item, unit, entity that can be acted upon. Data, a filing cabinet.

Subjects: Anything that performs an action on an object.

Core InfoSec Concerns

Data Classification:

- Confidential
- Restricted
- Public
- Special Category (personal data, sensitive personal data, personal health info, financial data). Under special regulation.

Data classification allows InfoSec to know the value and sensitivity of all information.

Core InfoSec Concerns

Identity: Who is the subject?

Authentication: Now show us proof.

Authorization: What will the subject be able to do with the information asset.

Access Control: Formal process for controlling access to information resources.

Data/System Mapping

InfoSec knows where all the **records**, **Information**, and **data** lives.

InfoSec knows all the storage locations, Databases, processes, and systems.

InfoSec knows all its **objects** and **subjects** and how they interact.

" We can't secure what we don't know we have, and we can't secure what we don't control."

“Incidents”: What InfoSec loses sleep over

Incident: An event that jeopardizes the **CIA** of **information assets**, regardless of cause, whether accidental or malicious.

- a crashed server
- a system malfunction
- breach: exposure of information to an unauthorized third party
    - a stolen file or device
    - an errant email
    - A malicious intrusion resulting in terabytes of data being stolen.

Every “**breach**” is an “**incident**,” but not every incident is a breach.

Left of Boom | Right of Boom

Familiarize yourself with your organization's Incident Response Plan ("IRP")

InfoSec Makes Organizations Resilient

Backup Systems

- Backup versus archives

- Business Continuity and Disaster Recovery
  - Recovery Point Objective (“RPO”)
  - Recovery Time Objective (“RTO”)

InfoSec is achieved through secure system architecture

- Data and process isolation
- Secure perimeters
- Strong authentication and "zero trust"
- Strong passwords and password management
- Robust "firewalls": Constant monitoring, filtering, and blocking
- Strong encryption and key management
- Robust vendor management

Defense of Depth: Many measures layered upon each other, operating independently, so that one control failure does not cause a system failure. The goal of InfoSec is to build a "**trusted system**" where all your controls complement and reinforce each other.

Security Frameworks

- ISO 27001, 27002
- SOC 2
- NIST Cybersecurity Framework, 800-53, 800-171
- HITRUST
- COBIT
- GDPR
- NERC-CIS
- PCI DSS

Other RIM/InfoSec Unifiers

Both RIM and InfoSec involve:

- **Governance**, **Risk**, and **Compliance** (GRC)
- **People**, **processes**, and **technology** (PPT)
- **Lifecycle** programs instead of "one and done"
- Emerging **business/governance** status from "back office"

How to Connect with InfoSec

- Start having “curiosity coffees”
- Ask “what makes your job hard?”
- Schedule a “ride along”
- Participate in “tabletops” together
- Codevelop policies and trainings
- Collaborate on data classification, data and system maps
- Tour a data center!

Thank you

Will.fletcher@zasio.com