# Information Security Risk Management (ISRM)

NAVEEN GUPTA (SR. CONSULTANT AND GOVERNANCE, INFORMATION SECURITY, 27 YEARS EXP. GLOBAL MNC)

## Information security

### Different people, different ways to interpret

Vendors: Limited to their products

For Aware Leaders and professionals: Essential and core requirement of their business

For some business leaders: It is job of IT/ Security manager

For some users of technology: It is disruption to their liberty

# What compels us to adapt information security?

#### Internet usage

User can reach anywhere in the world and so as the person with criminal mindset.

It has become world wide web for criminals to interact with reach other, share ideas and work on some common goals.

#### Usage of cloud computing

Risks related to public network usage

At the end of the day, your data is handled by someone else

#### Mobile Devices and embedded devices (IoT) usage

Small screen prone to more human errors and difficult to decide upon the security of app or website being used.

One never knows, if a spy is sitting besides you in the form of IoT device. Sometimes they may listen even when for your they are in switched off mode.

# What compels us to adapt information security?

### Automation and usage of Artificial Intelligence (AI)

More machine dependence, more chances of error and surprises.

- Information Leakage
   Al learns from loads of data and sources and can be a medium of information from different sources which otherwise would be unknown.
- Introduction of new vulnerabilities

  Learning can happen from incorrect data, codes, models etc., which may result in outcomes with previously unknown vulnerabilities
- Incorrect decisions sometimes can be potentially dangerous to our systems or even humans

### Increase of computer literacy and easy connectivity using BT, NFC, Wifi etc

It is a convenience which resulted in easy access and loss of information which otherwise was difficult.

# Information Security Risk Management (ISRM)

## Why is it important?

In order to reduce the likelihood of risks that may jeopardize the confidentiality, integrity or the availability of information system/ asset, thus impacting the overall business objective.

To make a business case for getting the information security budget approved from CFO.

Impact of IS risk can have implications: Operational, Legal, Financial and Reputational.

### Reality check:

This exercise mostly ends up in creating just a paper/ electronic record for compliance purposes

## Important aspects of ISRM strategy

Alignment to business objectives

Factor- in both insider and outsider threats

Accidental and deliberate threats

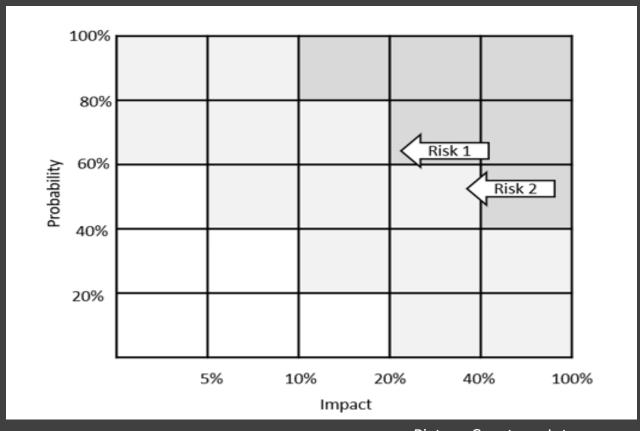
Human, technical, environmental and support system related threats

Threats arising out of implementation of controls

Define your risk appetite

**Define Risk Owners** 

## Prioritization and Mitigation of Risks

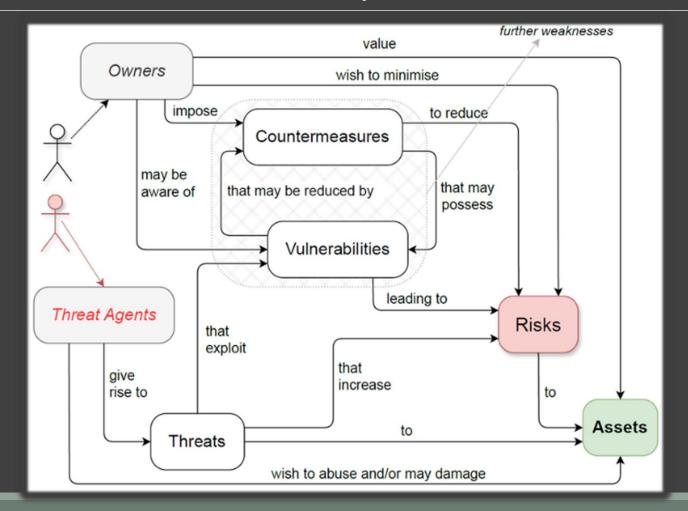


4 Ts in Risk Management

- Treat
- Tolerate
- Transfer
- Terminate

Picture Courtesy: Intaver .com

## Information security maze



Credits: Researchgate.net

# Expiration of IS Risks and outcome of ISRM

Do they really expire?

The answer is NO

Outcome: Set of security controls which may reduce them to the acceptable level

Keep them recorded in Risk Register

Re assess them at periodic interval in light of the environment applicable at time of assessment

Residual Risk

That remains after risk mitigation efforts are in place.

This may increase or decrease over a period of time.

Thus, ISRM is a continuous exercise during life cycle of an asset in an organization or a project.

# Choosing Risk Assessment (RA) Methodology (Objective or Subjective)

### Objective

- Attributes used are discrete. E.g. are Asset/ function type, its value, vulnerability, existing control threat, probability etc.
- Allows one to choose from a list of values for each attribute used in RA.
- Attributes which not straightforward e.g. motivation of threat actor, or surface area of attack etc. We can introduce
  objectivity by adding more sub- parameters to these attributes.
- E.g. ISO27005 methodology published by NIST

#### <u>Subjective</u>

- E.g. Octave
- This helps in scrutinizing every single details about asset.
- Eg. What is asset, why it is used, for what it is used, criticality, its user, its location, its copies, who all access it, from where, its container and so on.
- This doesn't bank on keywords and use actual threat scenarios to assess risks.
- One ends up filling pages and RA for even a single asset.

#### Recommendation: A blend of both

# Thank you.

NAVEEN GUPTA (SR. CONSULTANT AND GOVERNANCE, INFORMATION SECURITY, 27 YEARS EXP. GLOBAL MNC)

Naveen.gupta1977@yahoo.com

91-9811811016

*	Still Newspiech Still is to have being hid ingel on sign and ingen is the verification, overally, or integrity of the shandfull.	Section:	models as south excist in in-thick case.	Market and Control of	SERVICE STATE	Authorities Author	Service Toront	Section people from the control of t	Survivite had dead of long and the state of
	Carlo Carlo Carlo Carlo	152.1015	I colore Profito di sello di Nicolaria (1994) i filiazioni sono di Pro piatro i colore di Min. I Sini di Promisi pia si in spini di progli si sono di saltro i colorizzati simo i sigrifi.  I colore di di Siniazioni si sono di saltro i colorizzati si stato di di Siniazioni si sono di saltro si di saltro i colore di di Siniazioni si sono di si sono di si colore di Siniazioni si si sono di si sono di si sono colore di Siniazioni si si sono di si sono di si sono colore di Siniazioni si si sono di si sono di si sono colore di Siniazioni si si sono di si sono di si sono colore di Siniazioni si si sono di si sono di si sono colore di Siniazioni si si sono di si sono di si sono colore di Siniazioni si				-	Arrest	
	TO THE SERVICE OF THE SERVE OF THE SER	80 (80	A Date of Company No. 1 of paid of these grounds; years of the Management of these desiration and the Company of the paid of the section of the - (that (spaid on years) and and the section of the constitute of the section of th			*	MARKET	ž	The parties with the second of the parties of the p
4	T tigate	100 100	THE SQUART PRINT TO DESCRIPT A STATE SQUART	,	×	-11	-		
4	Common Co	Parties	In the problem of the part of				-	1	
*	With Superior and Printings Service	CON CORN	THE AND TOPING MET'S YEAR THE TOPING AS THE COLUMN THE TOPING AS THE COLUMN THE TOPING AS THE TOPING THE TOPING AS THE TOPING THE TOPING AS THE TOPING THE TOPING AS THE TOPING AS THE TOPING THE TOPING AS THE TOPING AS THE TOPING AS THE TOPING THE TOPING AS THE		1	28	-	Anna	TOTAL  ME DISTRICT AND THE RESTRICTION SQUARTERS AND THE MET DISTRICT AND THE RESTRICTION OF THE PROPERTY AND THE MET DISTRICT AND THE RESTRICTION OF THE PROPERTY AND THE MET DISTRICT AND THE PROPERTY AND THE PROPERTY AND THE MET DISTRICT AND THE PROPERTY AND THE PROPERTY AND THE MET DISTRICT AND THE PROPERTY AND THE PROPERTY AND THE MET DISTRICT  ME
	or Company of the standard execut	FROM	<ul> <li>Displaced makes the appropriate and the end of particular in an all property and the end of the e</li></ul>			**		and a	-

Alle	gm - W	arksheet 19	INFORMATION ASSET	Risk Witekse	шет			
		Information Asset	Configuration of the MDM system					
		Acca of Concern	Proper access gives access to resource assets to inappropriate users					
		(1) Actor We vestil agric sixes?	h the arms of conserve or	torr				
		(2) Means the sould the open do it? What could they do?		By using the administrator rights to give access to impropriate user				
	Threat	(5) Motive that is the unite's reason for shing to		MDM configuration leakage				
information Asset Risk		(4) Outcome What could be all information panel	e reading affect on the	Disclaure				
rmation		(5) Security Requirements the coeffice advantage area's access management to breached		Only the administrature of the MDM system can access and modify those data.				
Info		(6) Probabili What is the Motor could report	ly had he his time americ	∠ High	Mediam	Low		
	Siere		to the argumentation or the agricular and breach of according	(8) Severity  Box acres are fine consequence to the regulation or anot much for legact area?				
					Impact Area	Value	Score	
	The n	ser may steal th	a configuration of the N	Ponductivity	3			
	Run o	malicious code	on the MDM servers		Emercial	2	9	
					Positivities	3	6	
					Relative	Risk Score	21	