

The Art of Cyber Risk Management

Asaf Weisberg CISM, CISA, CRISC, CEGIT

Amsterdam, 11.4.2019



About the Presenter

- *Asaf Weisberg*, CISM, CRISC, CISA, CGEIT
- Founder & CEO, introSight Ltd.
- Immediate Past President of the ISACA Israel Chapter
- 2019-2020 Director, ISACA Int'l Board of Directors
- Over 25 years of hands-on, managerial and mentoring experience
- Develops Cybersecurity Methodological tools & exercise them in the field





1969

FIRST MANNED MOON LANDING





What I talk about when I talk about Cyber Risks?



ATTACK ORIGINS		ATTACK TYPES		ATTACK TARGETS		LIVE ATTACKS						
#	COUNTRY	#	PORT SERVICE TYPE	#	COUNTRY	TIMESTAMP	ATTACKER	ATTACKER IP	ATTACKER GEO	TARGET GEO	ATTACK TYPE	PORT
215	United States	170	25 smtp	308	United States	11:54:58.746	Gestin De Direccionamiento Uninet	201.122.217.24	Tlaquiltenango...	Dubai, AE	microsoft-ds	445
205	China	110	8080 http-alt	131	United Arab Emirates	11:54:58.616	Microsoft Corporation	157.56.110.245	Redmond, US	De Kalb Junctio...	smtp	25
23	Ukraine	89	23 telnet	36	Spain	11:54:58.273	Microsoft Corporation	207.46.100.254	Redmond, US	De Kalb Junctio...	smtp	25
11	Netherlands	34	3389 ms-wbt-server	22	Italy	11:54:57.836	Microsoft Corporation	157.56.110.249	Redmond, US	De Kalb Junctio...	smtp	25
10	South Korea	30	5900 rfb	15	Singapore	11:54:57.452	Microsoft Corporation	207.46.100.254	Redmond, US	De Kalb Junctio...	smtp	25
8	Spain	15	3306 mysql	6	Saudi Arabia	11:54:57.170	Chinanet Yunnan Province Network	182.243.33.3	Kunming, CN	Lynnwood, US	xsan-filesystem	50864
6	Moldova	13	50864 xsan-filesystem	3	Portugal	11:54:57.000	Chinanet Hubei Province Network	116.211.0.90	Wuhan, CN	Dubai, AE	http-alt	8080
4	Turkey	12	445 microsoft-ds	3	Cyprus	11:54:56.999	Chinanet Hubei Province Network	116.211.0.90	Wuhan, CN	Dubai, AE	http-alt	8080
4	Romania	6	22 ssh	3	Belgium	11:54:56.999	Chinanet Hubei Province Network	116.211.0.90	Wuhan, CN	Dubai, AE	http-alt	8080



HOME

EXPLORE

WHY NORSE?

Why Business Alignment?

Hackers Wipe VEmail Servers, May Shut Down After Catastrophic Data Loss



Technology
Boeing Hit by Cyberattack, Says Jetliner Production Not Affected

By [Julie Johnson](#)
March 29, 2018, 2:03 AM GMT+3 Updated on March 29, 2018, 3:16 AM GMT+3

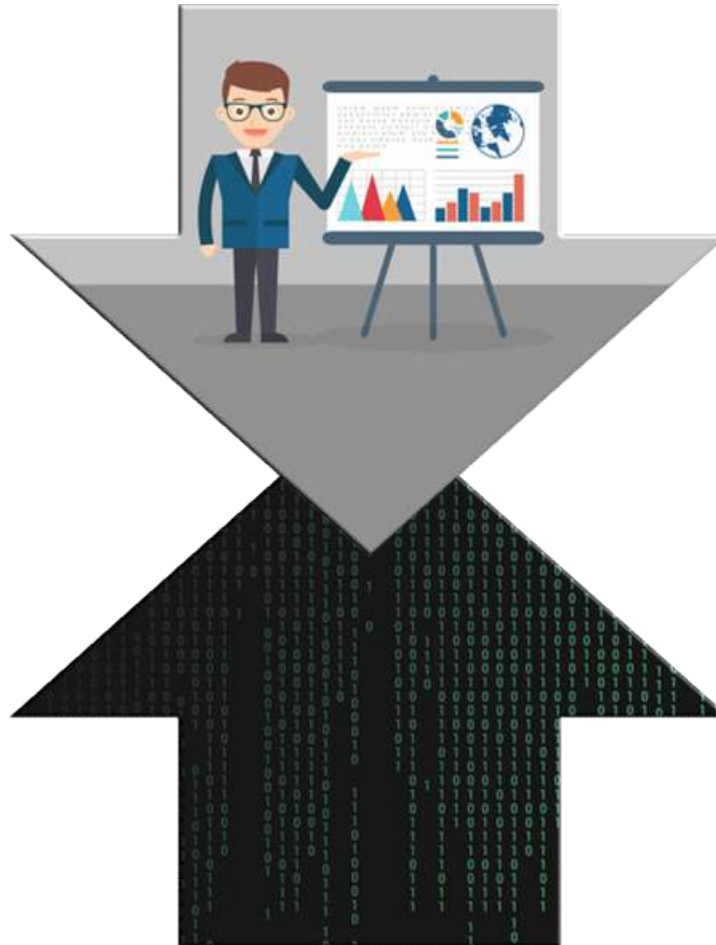
Hackers 'scramble' patient files in Melbourne heart clinic cyber attack
Federal agencies investigating breach, reported to be a ransom demand



Bottom-Up or Top-Down?



*Why not Connect
the Two
Approaches?*

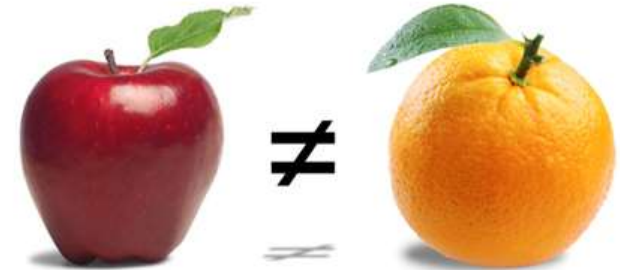




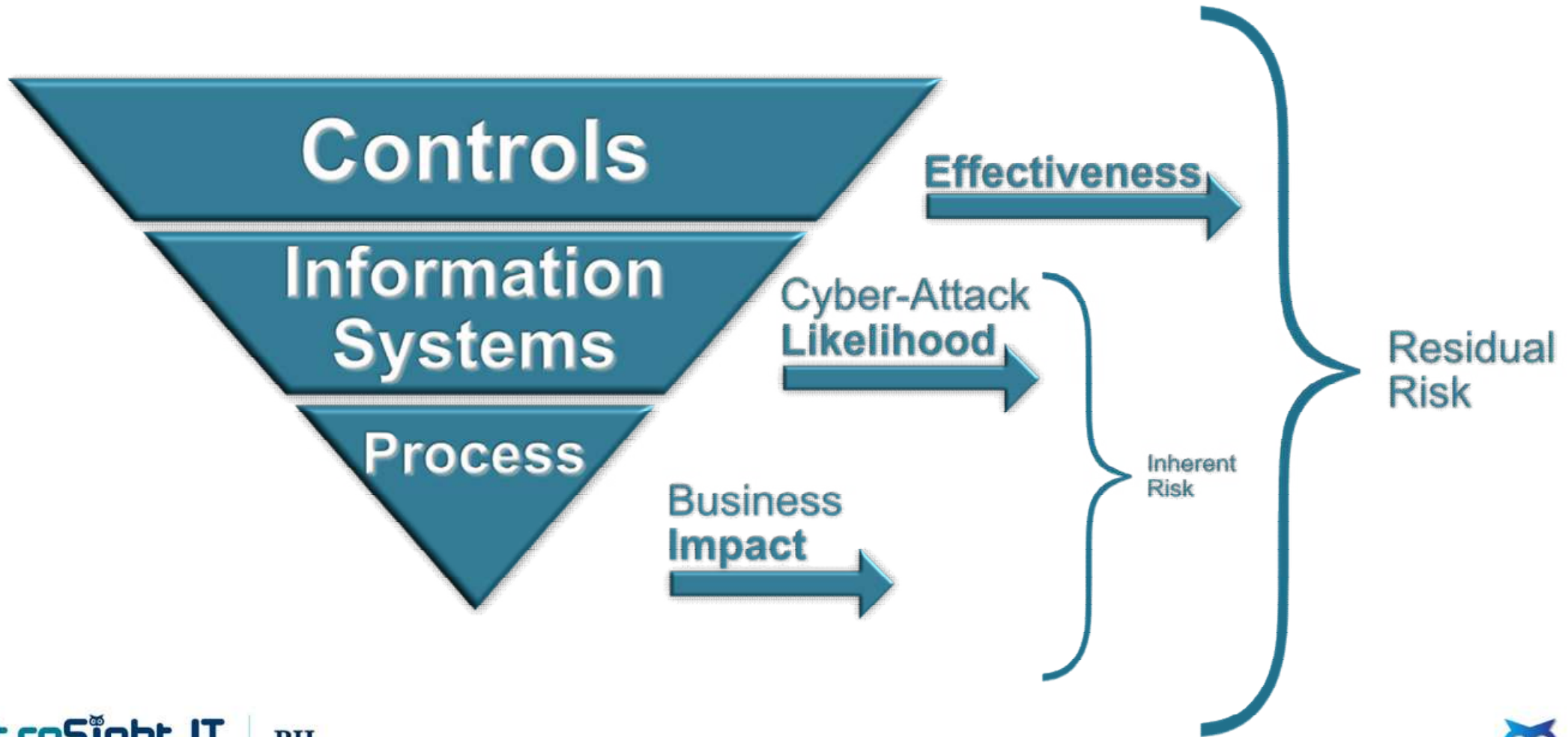
A Business Oriented Cyber Risk Management Model

The heart of the BCRM is its Mathematical algorithm:

- The algorithm **calculates** the ***Residual Business Risk to processes***, as a function of *Inherent Business Risk & IT controls effectiveness*
- **A Semi-Quantitative** approach, enhanced with ranks and weights, provides granular risk prioritization
- **Prioritization** of the risk reduction plan is based on the calculated *Residual Business Risk*
- **Slicing & Dicing** the calculated data allows analyzing risks from various views



Working with the model

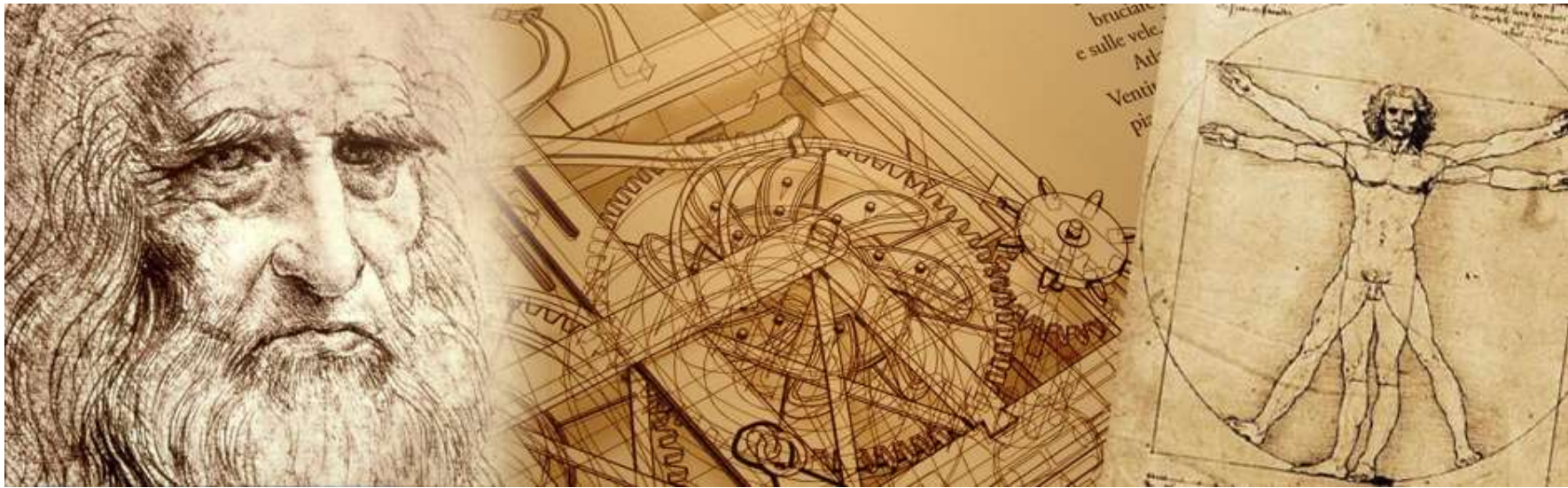


Cyber Risks: "Traditional" Top 10 View

Attack Surface	Process	Residual Risk	
IT Operations	Database management	9.67	H
Information Systems	Long-term savings operations	8.97	H
IT Operations	Storage security management	8.03	H
Web Applications	Customers digital channels management	7.88	M
Info Systems	Health insurance claims	7.79	M
Perimeter	Facility physical security management	7.61	M
Perimeter	Firewall and Perimeter security management	7.54	M
Web Applications	3 rd party digital channels management	7.43	M
Information Systems	Life insurance claims	7.28	M
IT Operations	Mobile device security management	7.26	M

Rank	Range
L	0 - 3.99
M	4 - 11.99
H	12 - 25

The Art of Cyber Risk Management



Efficiently Reduce Cyber Risks According to Business Priorities



Cyber Risks: Process → Systems View

Business Process	Risk		Inherent Risk	Controls Effect'	Residual Risk
Long term savings operations	PII Leakage as a result of a Cyber attack		22.63 H	2.58 L	8.97 H
Due On	System	# of Supported Processes	Inherent Risk	Controls Effect'	Residual Risk
2018	Digital Vaults	2	21.84 H	2.71 L	8.02 H
2018	Messaging	11	16.58 H	1.74 L	7.94 M
2018	SAP	7	16.58 H	2.91 L	6.27 M
2019	Policy sale	2	10.26 H	2.04 L	4.86 M
2019	Digital archive	3	10.26 H	2.73 L	3.73 L
—	Digital forms	1	5.00 M	4.00 M	0.80 L

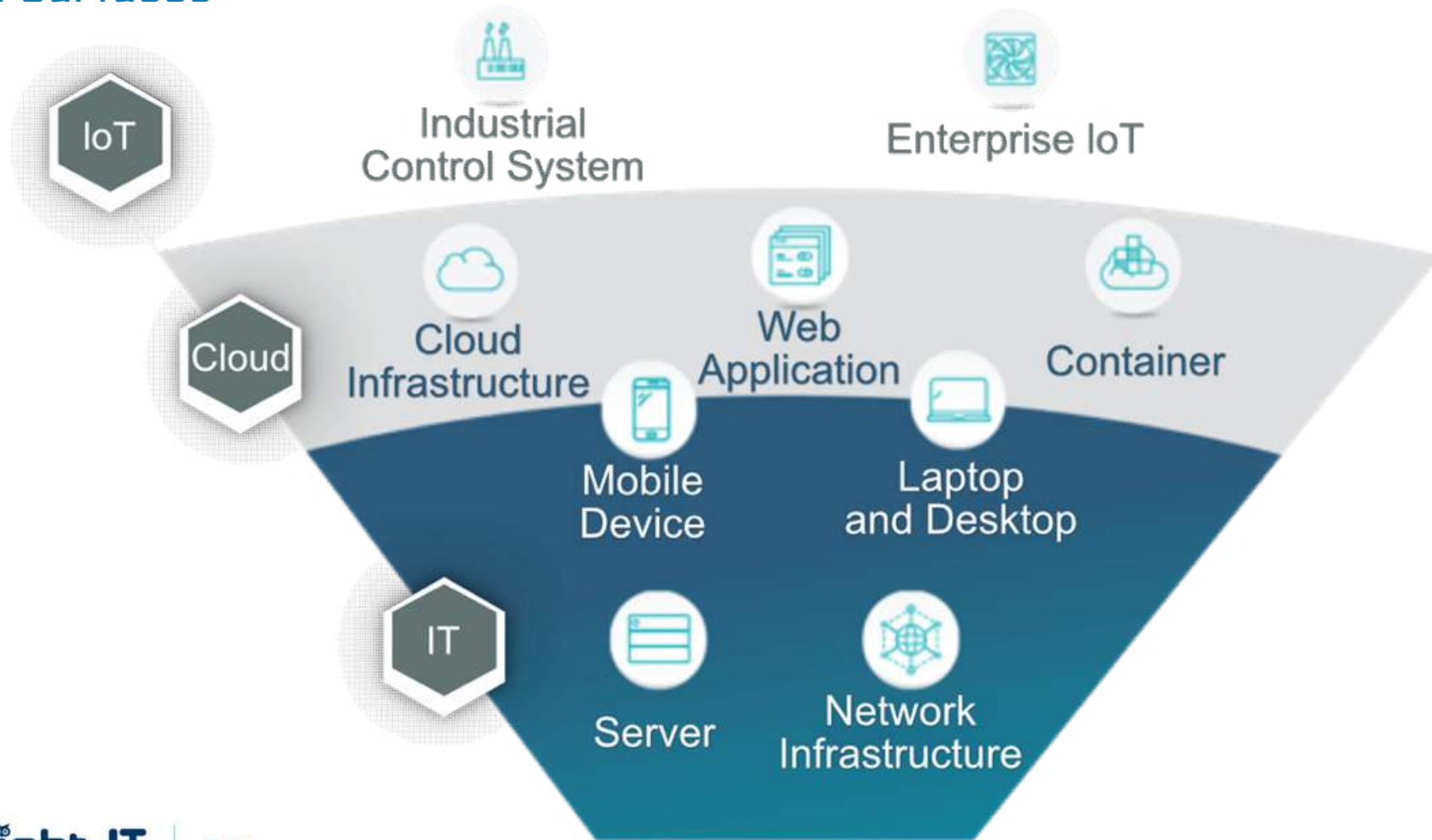




Think like an Attacker

<https://resources.infosecinstitute.com/the-psychological-profile-of-a-hacker-with-emphasis-on-security-awareness/#gref>

Attack Surfaces



Cyber Risks: Attack Surface View

Attack Surface	Process	Residual Risk	
Perimeter	Facility physical security management	7.61	H
Perimeter	Firewall management	7.54	H
Perimeter	Remote access to network	4.02	M
Web Applications	Customers digital channels management	7.88	M
Web Applications	Business partners digital channels MGMT	7.43	M
Web Applications	Suppliers digital channels management	6.89	M
Information Systems	Long-term savings operations	8.97	H
Information Systems	Health insurance claims	7.79	M
Information Systems	Life insurance claims	7.28	M
IT Operations	Database management	9.67	H
IT Operations	Storage security management	8.03	H
IT Operations	Mobile device security management	7.26	M

Attack Surface	Process	Residual Risk	
IT Operations	Database management	9.67	H
Information Systems	Long-term savings operations	8.97	H
IT Operations	Storage security management	8.03	H
Web Applications	Customers digital channels management	7.88	M
Info Systems	Health insurance claims	7.79	M
Perimeter	Facility physical security management	7.61	M
Perimeter	Firewall and Perimeter security management	7.54	M
Web Applications	3 rd party digital channels management	7.43	M
Information Systems	Life insurance claims	7.28	M
IT Operations	Mobile device security management	7.26	M

*"There are only two types of companies:
those that have been hacked,
and those that will be."*



Robert Mueller
FBI Director, 2001-2013

There are two types of
companies: those who
have been hacked, and
those who don't yet know
they have been hacked.



John Chambers
Chief Executive Officer of Cisco

We are going through a Paradigm Shift!



NIST Cybersecurity Framework

Prevention

Identify

- Business Environment
- Asset Mapping
- Risk Assessment

Protect

- Access Control
- Awareness
- Data Security

Containment

Detect

- Anomalies & Events
- Security Monitoring
- Detection Processes

Respond

- Response Team
- Mitigation
- Forensics

Recover

- BIA
- DRP
- BCP

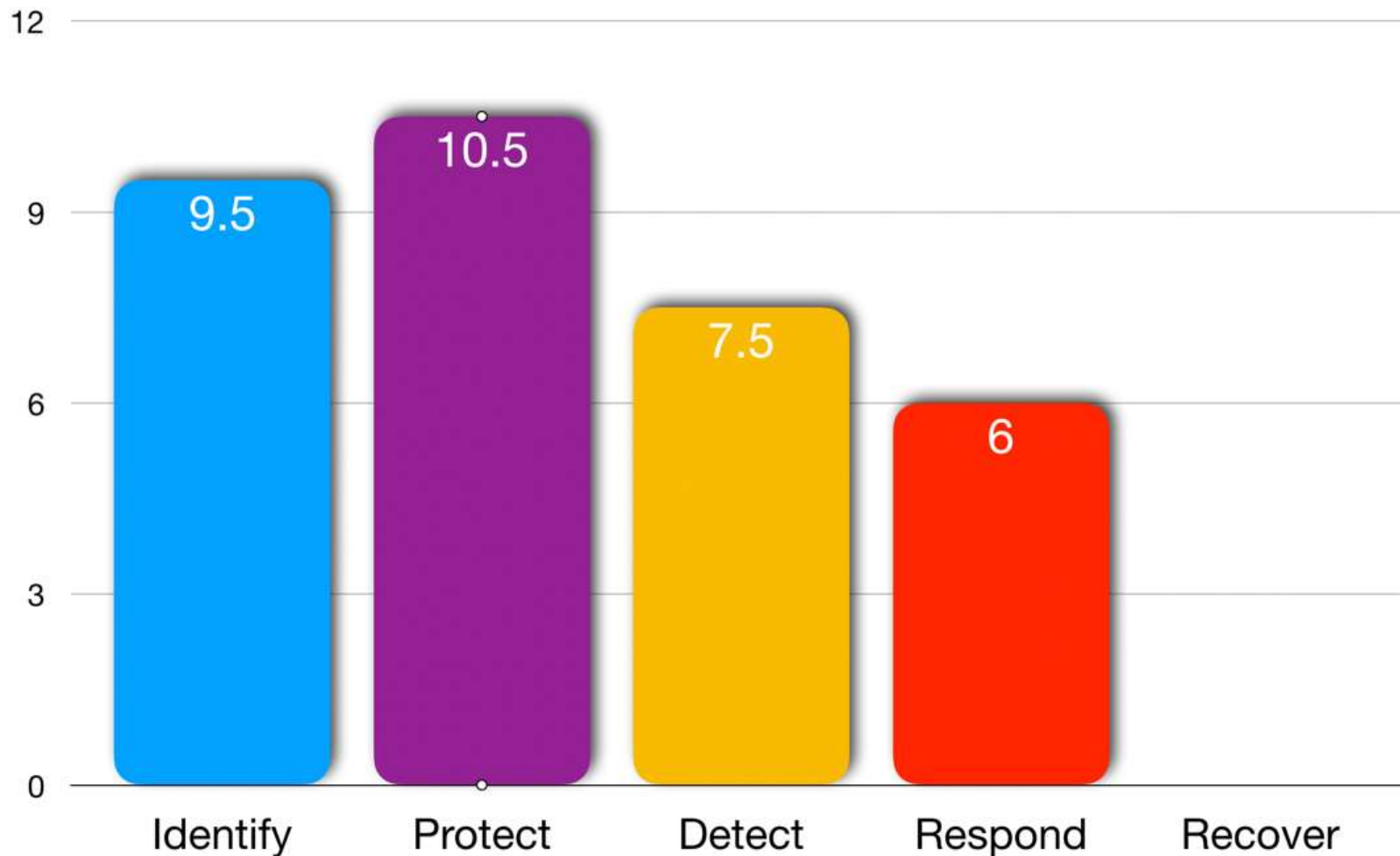


Organizational View: Controls Effect' by NIST Functions

Current state:

Reasonable
"Traditional"
controls

Evolving
"Cyber-Era"
controls



An Adaptive Cyber Risk Management Model

- **Risk management** is a **long term process**, changes are inevitable. The BCRM model allows to:
 - Change risk factors, as new threats emerge
 - Add new controls to mitigate existing risks, as exposure changes
 - Add or remove business processes & information systems
 - Change ranks & weights, according to organization's policy
- **Continuously** update the BCRM with:
 - Risk assessment sprints results
 - Internal audit findings

There is nothing permanent
except change.

Heraclitus



Takeaways



- To establish **Business alignment** - start at the process level
- Adjust resources allocation to support **shifting** from *Prevention* to *Containment*
- **Think like an attacker** - Consider emerging as well as traditional *Attack Surfaces*
- **Prioritize** *Cyber Risk Reduction* activities, according to *Residual Business Risks*
- Adopt **Continuous** Risk Management practices
- **Measure the change** of *Residual Business Risks*, as a result of IT investments

Cyber Risk Management is Art, make sure it is based on facts



Thank You!

asaf.weisberg@introSight.it

<https://www.linkedin.com/in/asafweisberg>

