CARISEC GLOBAL

CYBER SECURITY 2023

Reducing Cyber-Risks through Cyber Resilience

March 07-08

PROUDLY SUPPORTED BY:

BCSI Trustwave® Northpoint cybrilliance Empower Your Business with Cyber Resilience PECB

Strategic Cybersecurity Programs

Presented by Scott Foote,
Managing Director | Phenomenati Consulting

Guidance: Strategic Cybersecurity Programs

Balance Objectives & Obligations of the Business

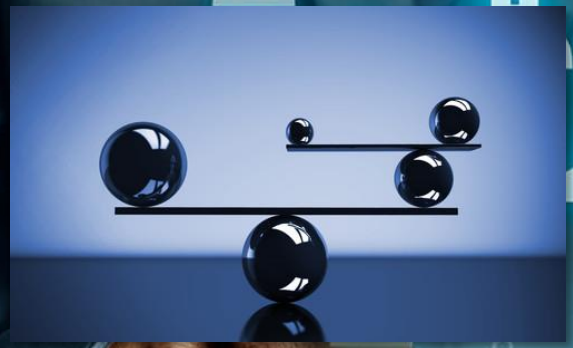
- Objectives = Increase Revenue, Control Costs, Build Value, Expand Business, etc.
- Obligations = Legal, Regulatory, Contractual, Ethical, Stakeholder

Optimize Risk Taking

- New opportunities require some level of Risk Taking
- Inform decisions with the Business Context of potential gains and losses
- Demonstrate Due Diligence and Due Care

Maximize Trust in your Brand

- Trust Through Transparency strengths Reputation
- Investments in Reputation help build Revenue



CARISEC GLOBAL

Integrating Cyber Risk into the overall Risk Management Program

"What does Success Look Like?"

Phenomenati

Risk Level Agreements™ (RLAs)

		Qualitative Assessment						Quantitative Assessment		Risk Levels		Controls				Cost/Benefit Analysis
ID	Risk Type	Threat	Metric	Vulnerability	Metric	Consequences	Metric	SLE	ARO	Qualitative 0 - 25	Quantitative Annualized Loss Expectancy (SLE x ARO = ALE)	Administrative	Physical	Technical	Annualized Cost	
R0001	Legal, Reputational (Cyber)	Criminal Theft / Extortion	5	Need to improve Data Loss Prevention. Do not adhere to Least Privilege principle. Need to improve Segregation of Duties. End-point Protection on cloud assets. Monitoring & Detection on cloud assets not well integrated into Security Ops (Sophos 24x7 SOC service). Need to review the protections on DevOps pipeline.	4	First Party Privacy Breach - Loss of **Client Confidential** material	5	$ 4,000,000	0.25	22.5	$ 1,000,000	$ 100,000	$ -	$ 100,000	$ 200,000	5.00
R0002	Operational, Legal, Reputational (Cyber)	Ransomware	5	Need to improve Data Loss Prevention. Do not adhere to Least Privilege principle. Need to improve Segregation of Duties. End-point Protection on cloud assets. Monitoring & Detection on cloud assets not well integrated into Security Ops (Sophos 24x7 SOC service). Need to review the protections on DevOps pipeline.	4	Loss of **Availability** of the SaaS platform leads to Reputation damaage (loss of Trust, Credibility) and Lost Business (clients, revenue)	5	$ 2,000,000	0.5	22.5	$ 1,000,000	$ 100,000	$ -	$ 300,000	$ 400,000	2.50
R0003	Operational, Legal, Reputational (Cyber)	Compomise of Service, Injection of Malicious Software into the SaaS offering	4	**End-point Protection** on cloud assets. Need to review **protections on DevOps pipeline**. Need to expand/improve **Application Security Testing** (AST) (e.g., scanning of all sw dependencies.	5	Loss of **Integrity** in SaaS Infrastructure leads to loss of either Client or Company Intellectual Property (IP) damages valuation.	5	$ 5,000,000	0.2	22.5	$ 1,000,000	$ 100,000	$ -	$ 100,000	$ 200,000	5.00
R0011	Legal, Reputational (Cyber)	High Expectations of Security & Privacy from Prospects	5	Overall Information Security & Privacy Program has not yet been certified.	4	Lost revenue opportunities. Losses to valuation in financing rounds.	4	$ 1,000,000	4	18	$ 4,000,000	$ 300,000	$ -	$ 500,000	$ 800,000	5.00
R0004	Operational, Legal, Reputational (Cyber)	Insider Threat	3	Administrative Controls need improvement: e.g., background checks for privileged staff w/ "**Need to Know**"; more specific policies on Data Classification, Access Control, Data Handling, Data Retention; addl NDAs; special access training; team experienced with Insider Threat Investigations. Technical Controls need improvement: Need to improve Data Loss Prevention. e.g. No monitoring of Annotators while in system. e.g. No monitoring of engineering and operations staff w/ full privileged access. e.g., No UAM/UBA platform to tune monitor User Behavior effectively. Physical Controls TBD	4	Loss of **Client Confidential** intellectual property, leads to Reputation damage (loss of Trust, Credibility) and Lost Business (clients, revenue)	5	$ 4,000,000	0.5	17.5	$ 2,000,000	$ 100,000	$ -	$ 5,000,000	$ 5,100,000	0.39

Risk Level Agreements™ (RLAs)

- Concrete **Risk Scenarios**,
- Assessed **Inherent Risk**,
- **Recommended Controls** to mitigate risk,
- **Risk Treatment Decisions**, and
- Remaining **Residual Risk**,
- the organization's **Risk Tolerance**

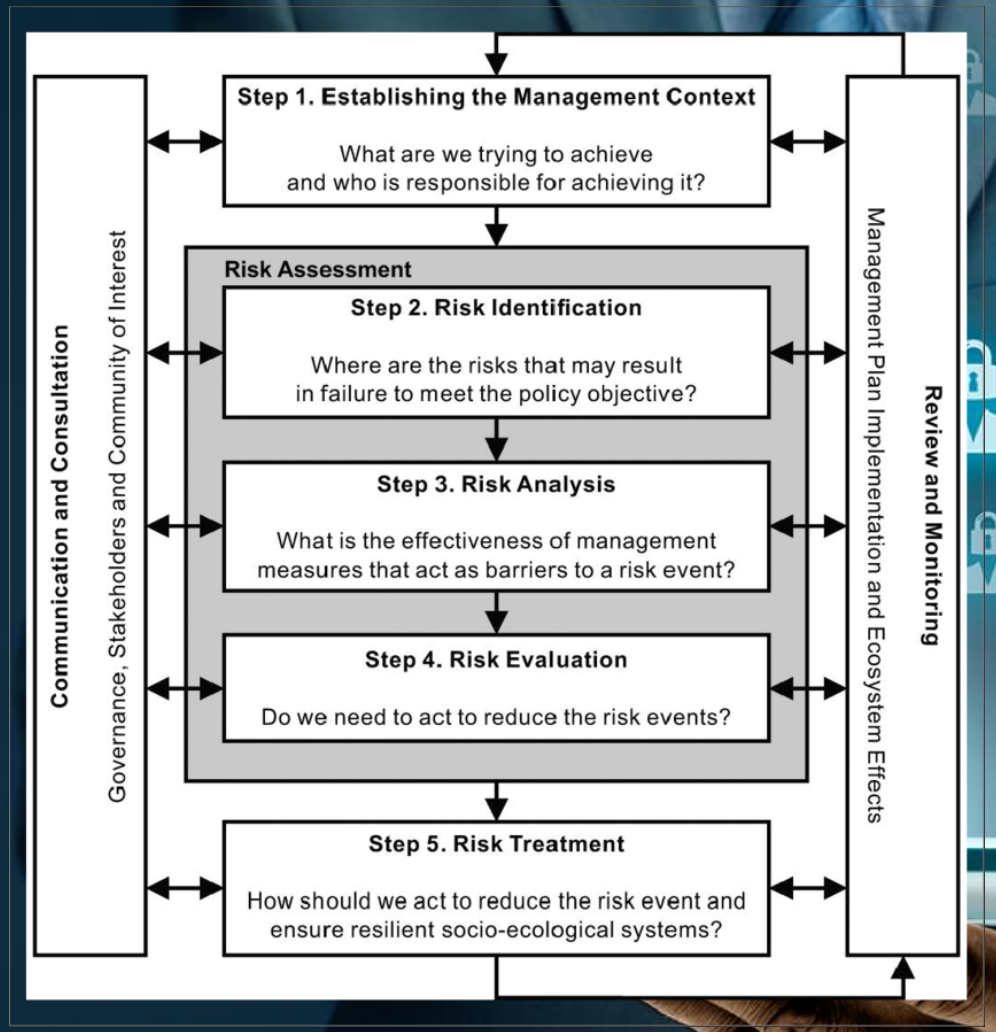
www.risklevelagreements.com

CARISEC GLOBAL

Integrating Cyber Risk into the overall Risk Management Program

Risk Management Program (ref. ISO/IEC 31000)

1. Business ***Context*** (e.g., Objectives & Obligations)
2. Risk ***Identification*** (e.g., Threats, Vulnerabilities, Impact, etc.)
3. Risk ***Assessment*** (e.g., Qualitative and Quantitative)
4. Risk ***Evaluation*** (e.g., Above/Below Risk Tolerance-Appetite)
5. Risk ***Treatment*** (e.g., Reject, Accept, *Mitigate*, Transfer)
6. Monitor & Continuous ***Improvement***
7. ***Communication*** (Critical to *Culture*)



Integrating Cyber Risk into the overall Risk Management Program

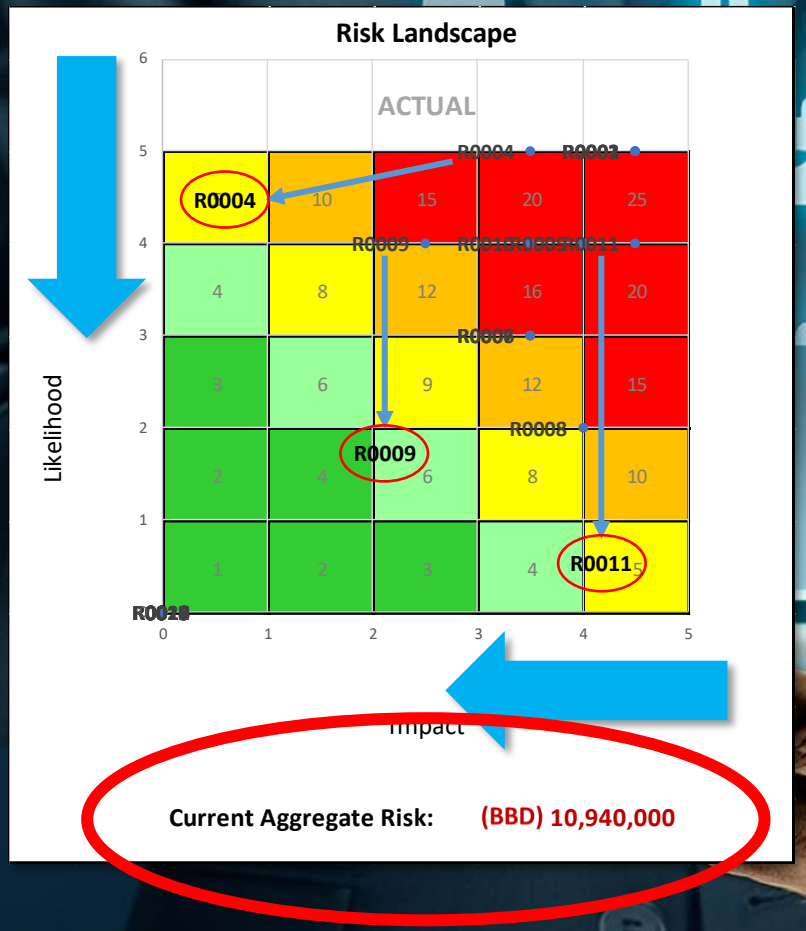
InT Control Matrix	Preventative	Detective	Corrective
Administrative	Policies & Procedures Data Classification Data Labeling Data Handling Data Retention Training Confidentiality Agreements Principle of Least Privilege (Role & Priv Definition)	Background Checks Performance Reviews (HR) Anomaly Reporting ('tips') Comms monitoring (email, chat, Slack, etc.) Social Media monitoring Dark Web monitoring (threat intelligence) Case Investigations	HR <-> Security Integration Termination Procedures Evidence Collection/ Handling Procedures (e.g., chain of custody)
Physical	Secure Areas Physical Access, Guards, Badges Secure "kiosks" Secure Workstations Privacy Screens, non-removable systems Cell Phone Control	"Badging" Activity Floor "Sweeps" CCTV	Badge Deactivation Equipment Recovery & Retention
Technical	Removable Media Control (disable USB, Airdrop, etc.) Browser Lockdown SaaS Access Control changes (Support tool) Data Loss Prevention (DLP) - Active Blocking Secure Data Deletion (beyond retention)	Badge System Integration UAM/UBA SIEM Integration Data Loss Prevention (DLP) - Passive Monitor & Alert	Secure Data Deletion (data class in violation of policy) Evidence Vaulting (chain of custody)

Recommended Controls reduce:

- Likelihood
- Impact

Residual Risk?

- Aggregate Risk
- Above/Below Risk Tolerance



CARISEC GLOBAL

Board Level Perspective on Cybersecurity Risk: KPIs

Cybersecurity Phenomena		KPIs			
Obligations					
	Laws	new	total	% compliance	
	Industry Regulations	new	total	% compliance	
	Contracts	new	total	% compliance	
Objectives					
	New Opportunities Involving Cybersecurity Criteria	number	percentage	aggregate value	
	Opportunities Won Due to Cybersecurity Criteria	number	percentage	aggregate value	
	Opportunities Lost Due to Cybersecurity Criteria	number	percentage	aggregate value	
Risk Management					
	Quarterly **New Risks** Identified	rate			
	Quarterly **Risk Treatment Decisions**	# Rejected	# Accepted	# Mitigated	# Transferred
	Quarterly **Risk Reduction** = Residual Risk / Inherent Risk	%			
	Current **Aggregate Risk** (BBD)	absolute number			
	Risk Balance = Aggregate Risk / Risk Tolerance	ratio			

Risk Metrics				**Q1**	**Q2**	**Q3**	**Q4**
	Confidentiality	Relative Metric	ONE MINUS the % of Confidential records exposed	95%	100%	100%	100%
		Absolute Metric	Financial Losses due to records exposed	(BBD) 100,000	(BBD) 0	(BBD) 0	(BBD) 0
	Integrity	Relative Metric	ONE MINUS % of Business Transactions that were fraudulent	100%	97%	100%	100%
		Absolute Metric	Financial Losses due to fraud events	(BBD) 0	(BBD) 5,000,000	(BBD) 0	(BBD) 0
	Availability	Relative Metric	ONE MINUS % of Systems (internal and external) that failed their SLA	100%	100%	75%	100%
		Absolute Metric	Financial Losses (e.g., from lost business) due to system outages	(BBD) 0	(BBD) 0	(BBD) 10,000,000	(BBD) 0
	Compliance Factorial™	Relative Metric	A x B x C x D	**61.6%**	**77.2%**	**82.2%**	**93.1%**
			A = % of **Systems** Compliant w/ Security Policies	95.0%	95.0%	98.0%	99.0%
			B = % of **Staff** Compliant w/ Security Policies	90.0%	95.0%	98.0%	99.0%
			C = % of **Vendors** Compliant w/ Security Requirements	80.0%	90.0%	93.0%	95.0%
			D = % of **Compliance w/ Obligations** (contractual, regulatory, legal, etc.)	90.0%	95.0%	92.0%	100.0%

CARISEC GLOBAL

“Cyber-Risk is an overlooked differentiator in cyber"

Q&A

Thank you

PROUDLY SUPPORTED BY:

BCSI Trustwave® Northpoint cybrilliance Empower Your Business with Cyber Resilience PECB