

Surviving the Sands of Cyber Entropy, Conflict, Risk and Resiliency

1 August 2023

Phenomenati Consulting

Scott Foote, Managing Director

Steve Foote, Managing Director

© 2023 Phenomenati. All Rights Reserved.



Building on Last Year's Talk...

"Top 10 Challenges (Ty's and Cy's) of Cyber Resiliency"

System-related Challenges

- 1. Cyber Entropy™
- 2. Complexity
- 3. Dependency
- 4. Vulnerability
- 5. Fragility

Acquisition-related Challenges

6. Urgency
 7. Simplicity
 8. Commodity
 9. Efficiency
 10. Fantasy



Survival Strategies

- 1. Develop
- 2. Cultivate
- 3. Promote
- 4. Invest in
- 5. Establish
- 6. Integrate
- 7. Insist on

"Meta" Systems
Domain Awareness
Risk Awareness
Contingencies & Controls
Risk Level Agreements™
Business Operations ← → Security Operations
Governance
Bring Order to Entropy
Acknowledge Conflict
Embrace Risk
Plan for Resilience

1. Develop "Meta" Systems





What is a "Meta" System?

- Comprehensive Knowledge ABOUT the System(s)
 - Technology → Business Processes → Business Objectives
- Knowledge Management (KM) Systems
- Examples



- Digital "Blueprints"
- "Digital Twins"
- Operational Control Systems (e.g., SCADA, ICS)
- Organizational Commitment to Systems Engineering Discipline
 - Designs, Baselines, Asset Management, Change Management, Risk Management



Awareness is Based on Knowledge

Example Knowledge

- Functional Requirements
- Non-Functional Requirements
 - Measures of Performance, Effectiveness, Suitability
 - These ARE the Resiliency Requirements
 - **Design** Documentation
- Original Engineering Tradeoffs
- Dependencies, Criticality, Contingences

2. Cultivate Domain Awareness



Network Awareness

- Asset Discovery
 - Information Assets
 - Service Assets
 - Software Assets
 - "Hardware" Assets
 - Networks
 - Asset Classification
 - Asset Lifecycle Management
- Access Controls (I, A, A, A)
- Attack Surface Management

Awareness Informs Decisions

Mission or Business Awareness

- Business Objectives
- Dependency Discovery
- Eliminate Assumptions
- Single Points of Failure
- Dependency Lifecycle Management
- Business Impact Analysis (BIA)

Threat Awareness

- External Threat Intelligence
- Emerging Obligations
- Disruptive Market Forces
- Internal Threat Intelligence
- Insider Threats
- Supply Chain Threats

- (e.g., Threat Actors)
- (e.g., Privacy Laws)
- (e.g., Generative AI)
- (e.g., Undisciplined Change)
- (e.g., Staff, Executives)
- (e.g., Contractors, Vendors)

3. Promote Risk Awareness



Cyber Risk Landscape Risk Awareness From Abstract to Concrete Scenario Analysis 4 **Risk Identification** MODERATE 15 20 5 5 10 LOW Risk Assessment (Qualitative & Quantitative) 2 Risk Evaluation (above/below tolerance) 16 8 20 4 4 **Risk ID** Likelihood Description Impact 3 Loss of **Confidentiality** of Content provided TO Gen AI IR001 $4 \rightarrow 1$ 3 service(s) 9 Likelihood 15 3 3 6 Poor Integrity of Content received FROM Gen AI service(s) IR002 $3 \rightarrow 2$ $5 \rightarrow 2$ 3 Content received FROM Gen AI service(s) may violate 2 2 4 6 8 10 IR003 2 3 Copyrights Gen AI service(s) selected as an alternative to COMPANY ER001 $4 \rightarrow 3$ $5 \rightarrow 4$ Service(s) 1 2 3 4 5 1 New COMPANY Offering/Service becomes critically IR004 $4 \rightarrow 2$ $4 \rightarrow 3$ dependent on Availability of Gen AI service Threat actors use Gen AI to exploit open source intel for ER002 $4 \rightarrow 3$ 3 3 4 1 2 5 **Reconnaissance** on your staff, business, customers Social Engineering attacks (phishing, smishing, vishing, live, ER003 $3 \rightarrow 2$ $4 \rightarrow 2$ etc.) are becoming much more effective Impact Malware is being rapidly refactored and enhanced (e.g., **Actionable Scenarios** ER004 $5 \rightarrow 4$ 5 3:00 polymorphic improvements) © 2023 Phenomenau. All KIGHLS KESELVEU.

4. Invest in Contingencies & Controls





- Eliminate Vulnerabilities in Critical Dependencies
- Resiliency in Conflict is *not* simply a *Technical* Problem

Address Vulnerabilities in People, Processes, Technologies

Contingency Planning

All Rights Reserved

© 2023 Phenomenati.

- Hope is *not* a Strategy
- − Proactive Investment → Effective Response
- Cross Functional Planning Team(s)
- Identify and Evaluate Options, Alternatives, Redundancies
- Use Cost-Benefit Analyses to Inform Investment Decisions
- Establish the Crisis Decision Making Process & Authorities

Resiliency Is Built on Preparedness

4. Invest in Contingencies & Controls

© 2023 Phenomenati. All Rights Reserved.



Control Types : • Administrative	InT Control Matrix	Preventative	Detective	Corrective
 Physical Technical Control Objective: 	Administrative	Data Classification Data Labeling Data Handling	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)
 Preventative Detective Corrective 	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)

Resiliency derives from **Control** *Effectiveness*



Identify Scenarios through:

- Business Analysis
- Audit Findings

© 2023 Phenomenati. All Rights Reserved.

0:30

Change Management

Ph	énomenati				Risk Level Agreements™	
			Qualitative Assessment			
ID	Threat	Metric	Vulnerability	Metric	Consequence	Metric
R0001	Criminal Theft / Extortion		Weak End-point Protection. Do not adhere to Least Privilege principle. Need to improve Segregation of Duties. Weak lateral movement Detection. Need to improve Data Loss Prevention.		Loss of Confidential information (e.g., Data Breach) leads to: * Customer Loss & Liability (\$) * Reputation Damage * Revenue Loss	
R0002	Supply Chain Attack, Injection of Malicious Software into the Company's offering(s)		Insufficient Application Security Testing (AST) (e.g., scanning of all sw dependencies). Poor protections on DevOps pipeline.		Loss of Integrity in the Company's offering(s) leads to: * Customer Loss & Liability (\$) * Reputation Damage * Revenue Loss	
R0003	Malicious Insider Threat		Need a comprehensive Insider Threat Program (InT), including long-term strategy for full-time staffing, auditing, and continuous improvement. <u>Administrative Controls</u> need improvement: e.g. Insufficient monitoring of engineering and operations staff w/ full privileged access; etc. <u>Technical Controls</u> need improvement: e.g., no UAM/UBA solution; etc. <u>Physical Controls</u> need improvement: e.g., no secure areas in place today; etc.		Loss of Confidential information (e.g., Data Breach) leads to: * Customer Loss & Liability (\$) * Reputation Damage * Revenue Loss	
R0004	Ransomware		Weak End-point Protection. Do not adhere to Least Privilege principle. Need to improve Segregation of Duties. Weak lateral movement Detection. Inadequate Backup/DR Plan.		Loss of information/service Availability leads to: * Customer Loss & Liability (\$) * Reputation Damage * Revenue Loss	

•

•

•

0:30



Risk Level Agreements™ Phenomenati Decompose Risk into: **Threats Vulnerabilities** Vulnerability Consequence ID **Netric** Metric Metric Threat Consequences oss of **Confidential** information (e.g., Data Weak End-point Protection. Do not adhere to Least Privilege principle. Breach) leads to: R0001 Criminal Theft / Extortion Need to improve Segregation of Duties. Customer Loss & Liability (\$) Weak lateral movement Detection. Reputation Damage Need to improve Data Loss Prevention. **Revenue Loss** Loss of Integrity in the Company's offering(s) leads Insufficient Application Security Testing Supply Chain Attack, Injection of Malicious Customer Loss & Liability (\$) R0002 (AST) (e.g., scanning of all sw dependencies). Software into the Company's offering(s) **Reputation Damage** Poor protections on DevOps pipeline. Revenue Loss Need a comprehensive Insider Threat Program (InT), including long-term strategy for full-time staffing, auditing, and continuous improvement. Administrative Controls need improvement: e.g. Insufficient monitoring of engineering and Loss of Confidential information (e.g., Data operations staff w/ full privileged access; Breach) leads to: etc. R0003 Customer Loss & Liability (\$) Malicious Insider Threat Reputation Damage Technical Controls need improvement: Revenue Loss e.g., no UAM/UBA solution; etc. Physical Controls need improvement: e.g., no secure areas in place today; etc. Weak End-point Protection. Loss of information/service Availability leads Do not adhere to Least Privilege principle. to: R0004 Need to improve Segregation of Duties. Customer Loss & Liability (\$) Ransomware Weak lateral movement Detection. **Reputation Damage** © 2023 Phenomenati. All Rights Reserved. adequate Backup/DR Plan. Revenue Loss



www.risklevelagreements.com

Qualify Each Risk:

- Threat
- Vulnerability
- Consequence

Employ a Numeric Scale, for example:

- 1. Negligible
- 2. Minor
- 3. Moderate
- 4. Major
- 5. Significant

P	enomenati				Risk Level Agreements™	
			Qualitative Assessment			
ID	Threat	Metric	Vulnerability	Metric	Consequence	Metric
R0001	Criminal Theft / Extortion	8	WeakEnd-point Protection. Do not adhere to Least Privilege principle Need to improve Segregation of Duties. Weaklateral movement Detection. Need to improve DataLoss Prevention.	9	Loss of Confidential information (e.g., Da Breach) leads to: * Customer Loss & Liability (\$) * Reputation Damage * Revenue Loss	3
R0002	Supply Chain Attack, Injection of Maliciou Software into the Company's offering(s)	6	Insufficient Application Security Testing (AST) (e.g., scanning of all sw dependenci Poor protections on DevOps pipeline.	s). 8	Loss of Integrity in the Company's offering(s) I to: * Customer Loss & Liability (S) * Reputation Damage * Revenue Loss	ads. 10
R0003	Mali cious Insider Threat	8	Need a comprehensive Insider Threat Program (InT), including Long-term strategy for full-time staffing, auditing, and continuous improvement Administrative Controls need improvement: e.g. Trs ufficient monitoring of engineering and operations staff w/ full privileged access; etc. Technical Controls need improvement: e.g., no UAM /UBA solution; etc.	7	Loss of Confidential information (e.g., Da Breach) leads to: * Customer Loss & Liability (\$) * Reputation Damage * Revenue Loss	3





Risk Level Agreements™ Phenomenati Risk Levels Qualitative Assessment Quantitative Assessment Qualitative Quantitative Annual ized Loss ID Vulnerability Consequence SLE ARO 0-100 Threat Metric Metric Metric Expectancy **Quantify** Each Risk: (SLE x ARO = ALE) Weak End-point Protection. Loss of Confidential information (e.g., Data Consequence Do not adhere to Least Privilege principle. Breach) leads to: R0001 Criminal Theft / Extortion Need to improve Segregation of Duties. CustomerLoss & Liability (\$) 4,000,000 0.33 57.6 ŝ. 1,320,000 8 Weak lateral movement Detection. Reputation Damage Need to improve DataLoss Prevention. Revenue Lass **Develop Estimates:** ass of Integrity in the Company's offering(s) leads Single Loss Insufficient Application Security Testing Supply Chain Attack, Injection of Malicious Customer Loss & Liability (S) R0002 (AST) (e.g., scanning of all sw dependencies). 0.2 1,000,000 5.000.000 48 ŝ. 6 Software into the Company's offering(s) Reputation Damage Expectancy (SLE) Poor protections on DevOps pipeline. Revenue Loss Annualized Rate of Need a comprehensive Insider Threat Program InT), including long-term strategy for full-time Occurrence (ARO) staffing, auditing, and continuous improvement. Annualized Loss dministrative Controls need improvement: e.g. 1 rs ufficient monitoring of engineering and Loss of Confidential information (e.g., Data operations staff w/ full privileged access; Breach) leads to: Expectency (ALE) R0003 Mali dous Insider Threat 8 CustomerLoss & Liability (\$) 4,000,000 0.2 44.8 800,000 Reputation Damage Technical Controls need improvement: Revenue Loss e.g., no UAM AUBA solution; vsi cal Controls need improvement: e.g., no secure areas in place today; WeakEnd-point Protection. Loss of information/service Availability leads Do not adhere to Least Privilege principle. R0004 Need to improve Segregation of Duties. CustomerLoss & Liability (\$) 0.25 42 500.000 Ransomware 2,000,000 <u>s</u> Weaklateral movement Detection. Reputation Damage Inadequate Backup/DR Plan. Revenue Lass Loss of **Gient Confidential** material R0005 Insider Threat 8 Non-mali dous employee negligence. 1 40 Ś 500,000 500,000

www.risklevelagreements.com

•

•

•

٠

0:30



Prioritize Risks:

 Sort by Qualitative Risk
 First

Open Discussion:

 Revisit the 1 to N rankings, comparatively

Move On To:

 Sort by Quantitative Risk

Assess Risk Tolerance:

• For EACH Scenario

Pho	enomenati				Risk Level Agreements™								
							_					Level	
			Qualitative Assessment					Quanti tative	Assessment	Qualitat	ive	Que	anti tat
ID	Threat	Metric	Vulnerability	Metric	Consequence	Metric		SLE	ARO	0-10	0	Eq	valized xpecter xARO
R0001	Criminal Theft / Extortion	в	WeakEnd-point Protection. Do not adhere to Least Privilege principle. Need to improve Segregation of Duties. Weaklateral movement Detection. Need to improve DataLoss Prevention.	9	Loss of Confidential information (e.g., Data Breach) Leads to: * Customer Loss & Liability (\$) * Reputation Damage * Revenue Loss	8	\$	4,000,000	0.33	57.6		s	1,3
R0002	Supply Chain Attack, Injection of Malicious Software into the Company's offering(s)	6	Insufficient Application Security Testing (AST) (e.g., scanning of all sw dependencies). Poor protections on DevOps pipeline.	8	Loss of Integrity in the Company's offering(s) leads to: • Customer Loss & Liability (S) • Reputation Damage • Revenue Loss	10	5	s,000,000	0.2	48		ŝ	1,0
R0003	Malicious Insider Threat	8	Need a comprehensive Insider Threat Program (InT), including Long-term strategy for full-time staffing, auditing, and continuous improvement. Administrative Controls need improvement: e.g. Insufficient monitoring of engineering and operations staff w/ full privileged access; etc. Technical Controls need improvement: e.g., no UAM/AUBA solution; etc. <u>Physical Controls</u> need improvement: e.g., no secure areas in place today; etc.	7	Loss of Confidential information (e.g., Data Breach) Leads to: * Customer Loss & Liability (S) * Reputation Damage * Revenue Loss	8	\$	4,000,000	0.2	44.8		s	8
R0004	Ransomware	10	Weak End-point Protection. Do not adhere to Least Privilege principle. Need to improve Segregation of Duties. Weak lateral movement Detection. Inadequate Backup/DR Plan.	6	Loss of information/service Avai lability leads to: * Customer Loss & Liability (\$) * Reputation Damage * Revenue Loss	7	s	2,000,000	0.25	42		s	5
R0005	InsiderThreat	8	Non-mali cious employee negligence.	5	Loss of Gient Confidenti al materi al	10	\$	500,000	1	40		s	5

www.risklevelagreements.com





Estimate Control Costs:

- Consider Total Cost of Ownership
 (TCO)
- Annualize the TCO for each Control/Set

Ph	enomenati				Risk Level Agreements™															
							_				Risk	Levels								
			Qualitative Assessment					Quanti tative	Assessment	Q	ualitative	Quanti				0	Contro	ls .		
ID	Threat	Metric	Vulnerability	Metric	Consequence	Metric		SLE	ARO	(0- 100	Annualiz Expect (SLE x AR	enc	A	ministrativ	Physica		lechnica l	Annualiza Cost	d
R0001	Criminal Theft / Extortion	8	Weak End-point Protection. Do not adhere to Least Privilege principle. Need to improve Segregation of Duties. Weak lateral movement Detection. Need to improve Data Loss Prevention.	9	Loss of Confidential information (e.g., Data Breach) leada to: * Customer Loss & Liability (5) * Reputation Damage * Revenue Loss	8	\$	4,000,000	0.33		57.6	\$ 1	32(00	\$	100,000	s	- \$	650,000	\$ 75	0,000
R0002	Supply Chain Attack, Injection of Malicious Software into the Company's offering(s)	6	Insufficient Application Security Testing (AST) (e.g., scanning of all sw dependencies). Paor protections on DevOps pipeline.	8	Loss of Integrity in the Company's offering(s) hads for: * Customer Loss & Liability (5) * Reputation Damage * Revenue Loss	10	\$	5,000,000	0.2		48	\$ 1	00 00	ţ	100,000	\$	- \$	500,000	\$ 600	0,000
R0003	Malicious Insider Threat	8	Need a comprehensive insider Threat Program (InT), technical program stratagy for Tall-time (InT), technical and continuous interprovement. Address to a sime controls in one of improvement. Address to a sime controls in one of improvement. In a binical Controls i multi privileged access; exc. The binical Controls i multi improvement: e.g., no UMA/IAA solution; exc. Program Controls i multi improvement: e.g., no interne areas in place today; exc.	7	Loss o f Confidential information (e.g., Data Breach) leads to: * "Customer Loss & Liability (5) * Reputation Damage * Revenue Loss	8	5	4,000,000	0.2		44.8	s	801 00	\$	100,000	\$	- s	1,000,000	\$ 1,100	1,000
R0004	Ransomware	10	Weak End-point Protection. Do not adhere to Least Privilege principle. Need to improve Segregation of Duties. Weak lateral movement Detection. Inadequate Backup/DR Plan.	6	Loss of information/service Availability leads to: * Customer Loss & Liability (5) * Reputation Damage * Revenue Loss	7	\$	2,000,000	0.25		42	\$	500 00	\$	100,000	s	- \$	350,000	\$ 450	0,000
R0005	Insi der Threat	8	Non-mali dous employee negligence.	5	Loss of ClientConfidential material	10	\$	500,000	1		40	s	500 00	\$	100,000	\$	- \$	1,000,000	\$ 1,10	1,000
R0006	Fraud - False Executive/Wire Transfer Requests	10	Insufficient authentication of internal communications	Ŋ	Financial loss	6	\$	200,000	0.2		30	s	400	ţ	10,000	\$	- \$	50,000	S GI	0,000
R0007	DDaS, possible extortion	4	Poor DDoS protections in place.	7	Loss of information/service Availability leads to: * Customer Loss & Liability (5) * Reputation Damage * Revenue Loss	9	\$	200,000	0.5		25.2	s	100 00	\$	100,000	\$	- \$	100,000	\$ 200	0,000
R0008	Fraud - False Invoices sent to di ents	8	Insufficient authentication of email services	з	Client frustration. Loss of dient trust	4	\$	100,000	5		9.6	s	500, 0	\$	10,000	\$	- \$	50,000	\$ 60	0,000

www.risklevelagreements.com

© 2023 Phenomenati. All Rights Reserved.

0:30



Ph	enomenati				Risk Level Agreements™													ſ	
							_			Ris	sk Lev	rels	_						Cost/Benefit
			Qualitative Assessment					Quanti tative a	Asse ss ment	Qualitative		Quantitative			Con	trols			Analysis
ID	Threat	Metric	Vulnerability	Metric	Consequence	Metric		SLE	ARO	0-100		Expectancy LE x ARO = ALE)	Adm	inistrativ	Physical	Technical	Annualiza Cost		
R0001	Criminal Theft / Extortion	8	Weak End-point Protection. Do not adhrer to Least Privilege principle. Need to improve Segregation of Duties. Weak lateral movement Detection. Need to improve DataLoss Prevention.	9	Loss of Confidential information (e.g., Data Breach) leads to: * Customer Loss & Liability (5) * Reputation Damage * Revenue Loss	8	s	4,000,000	0.33	57.6	s	1,320,000	\$	100,000	\$-	\$ 650,00)\$750	3 , D	1.75
R0002	Supply Chain Attack, Injection of Malicious Software into the Company's offering(s)	6	Insufficient Application Security Testing (AST) (e.g., scanning of all sw dependencies). Poor protections on DevOps pipeline.	8	Loss of Integrity in the Company's offering(s) leads to: • Customer Loss & Liability (5) • Reputation Damage • Revenue Loss	10	\$	5,000,000	0.2	48	ŝ	1,000,000	s	100,000	\$-	\$ 500,00	5 600), D	1Ø
R0003	Malicious Insider Threat	8	Nend a comprehensive trisider Threat Program (nr.), techning longeren stratagy for full-sine staffing, audio ing, and continuous improvement. Admin strata Controls med improvement: e.g. in culficient monitoring of orginanism en operations stuff of full privileged access; etc. Technical Controls med improvement: e.g., no UMM/URA solution; etc. <u>Phonical Controls</u> need improvement: e.g., no tuture areas in place today; etc.	7	Loss o l Confidential information (e.g., Data Breach) leads to: * Customer Loss & Liability (5) * Reputation Damage * Revenue Loss	8	ş	4,000,000	02	44.8	ŝ	800,000	s	100,000	\$-	\$ 1,000,00	0\$1,100), D	0.73
R0004	Ransomware	10	Weak End-point Protection. Do not adhere to Least Privilege principle. Need to improve Segregation of Duties. Weak lateral movement Detection. Inadequate Backup/DR Plan.	6	Loss of information/service Availability leads to: * CustomerLoss & Liability(\$) * Reputation Damage * Revenue Loss	7	\$	2,000,000	0.25	42	s	500, 000	\$	100,000	\$-	\$ 350,00)\$ 450), D	1.11
R0005	InsiderThreat	8	Non-malidous employee negligence.	5	Loss of Client Confidential material	10	\$	500,000	1	40	\$	500,000	s	100,000	\$-	\$ 1,000,00	\$ 1,100), D	0.45
R0006	Fraud - False Executi vo/Wire Transfer Requests	10	Insufficient authentication of internal communications	5	Financial Ioss	6	\$	200,000	0.2	30	s	40,000	s	10,000	s -	\$ 50,00	D \$ 60), D	0.0
R0007	DDoS, possible extortion	4	Paar DDaSprotections in place.	7	Loss of information/service Availability leads to: * Customer Loss & Liability (5) * Reputation Damage * Revenue Loss	9	\$	200,000	0.5	25.2	s	100,000	\$	100,000	\$-	\$ 100,00) \$ 200	a, o	0.50
ROOCS	Fraud - False Invoices sent to di ents	8	Insufficient authentication of email services	з	Client frustration. Loss of dient trust.	4	\$	100,000	5	9.6	s	500, 000	s	10,000	\$-	\$ 50,00	5 60	1 0	8.33

www.risklevelagreements.com

Cost–Benefit Analysis:

- Reduction of Quantifiable Risk
- Cost of Control(s)

B/C Ratio:

0:30

- > 1, good investment
- < 1, weak investment

© 2023 Phenomenati. All Rights Reserved.



Decisions:

- Avoid the Risk
- Accept the Risk
- Mitigate the Risk
- Transfer the Risk

Combining Options:

- Mitigate some Risk,
- & Transfer some Risk

Phe	nomenati				Risk Level Agreements™																					
											Risk I	Levels									куренент					
			Qualitative Assessment					Quanti tative /	Assessment	Qu	alitative	Quanti					Conti	ols			Analysis		DEC	CISIONS		
ID	Threat	Metric	Vulnerability	Metric	Consequence	Metric		SLE	ARO	C	0- 100	Annualiu Expec (SLE x AR	tency	Admi	nistrativ	Phys	ical	Technica	1	Cost Cost		Avoi	id Accept	t Mitigana	Transfer	
0001	Criminal Theft / Extortion	8	Weak End-point Protection. Do not adhere to Least Privilege principle. Need to improve Segregation of Duties. Weak lateral mavement Detection. Need to improve DataLoss Prevention.	9	Loss of Confidential information (e.g., Data Breach) leads to: * Customer Loss & Liability (\$) * Reputation Damage * Revenue Loss	8	\$	4,000,000	0.33		57.6	\$ 1	,320,000	s	100,000	s	-	\$ 650,0	00 \$	750,00	1.75			x	×	
0002	Supply Chain Attack, Injection of Malicious Software into the Company's offering(s)	6	Insufficient Application Security Testing (AST) (e.g., scanning of all sw dependencies). Poor protections on DevOps pipeline.	8	Loss of Integrity in the Company's offerings) hads loc Customer Loss & Liability (S) * Reputation Damage * Revenue Loss	10	\$	5,000,000	0.2		48	\$ 1	,000,000	s	100,000	\$	-	\$ 500,0	00 \$	600,00	1.07			x	x	
0003	Mali dous Insider Threat	8	Neal a comprohension basider Threat Program (br) [Lichading Longaron stratagy for full-time Laffing, availing and constitutions improvement. Administration Controls multi improvement: e.g. In sufficient constitution of orginant mg and pay atoms staff of full privileged access; ex., The hinda Controls multi improvement: e.g., no UMM /UBA solution; ex. Phonard Controls and improvement: e.g., no success areas in place today; ex.	7	Loss of Confidential information (e.g., Data Breach) leads to: * Customer Loss & Liability (5) * Reputation Damage * Revenue Loss	8	\$	4,000,000	0.2		44.8	ŝ	900, 000	s	100,000	\$	-	\$ 1,000,0	00 \$	1,100,00	0.73			x		
0004	Ransomware	10	Weak End-point Protection. Do not adhere to Least Privilege principle. Need to improve Segregation of Duties. Weak lateral movement Detection. Inadequate Backup/DR Plan.	6	Loss of information/service Availability leads to: * Customer Loss & Li ability (S) * Reputation Damage * Revenue Loss	7	5	2,000,000	0.25		42	\$	500, 000	s	100,000	\$	-	\$ 350,0	00 \$	450,00	1.11			x	x	
0005	Insi der Threat	8	Non-mali dous employee negligence.	5	Loss of Gient Confidential material	10	5	500,000	1		40	\$	500, 000	s	100,000	\$	-	\$ 1,000,0	00 \$	1,100,00	0.45			×		
0006	Fraud - False Executi ve/Wire Transfer Requests	10	Insufficient authentication of internal communications	5	Financial loss	6	\$	200,000	0.2		30	s	40,000	s	10,000	Ş	-	5 50,0	00 \$	60,00	0.6			x		
0007	DDoS, possible extortion	4	Poor DDoSprotections in place.	7	Loss of information/service: Availability leads to: * Customer Loss & Li ability (S) * Reputation Damage * Revenue Loss	9	\$	200,000	0.5		25.2	s	100, 000	s	100,000	\$	-	\$ 100,0	00 \$	200,00	0.50		x			
0008	Fraud - False Invoices sent to dients	8	Insufficient authentication of email services	3	Client frustration. Loss of dient trust.	4	\$	100,000	5		9.6	s	500,000	s	10,000	s	-	\$ 50,0	00 \$	60,00	8.33			x		

0:30

www.risklevelagreements.com



Record:

- Decision made
- Date
- Exec Team Members

Track:

- Last Reviewed Date
- Next Review Date

								_														Risk Le	vel Ag	reeme	nts™					
				,	Risk	1									Cost/Benefit Analysis												_			
			Assessment		Qualitative		uantitative					trols		t annual free d	Analysis			SIONS					Authoritie	es					Dates	Next
	SL	E	ARO	1 1	0 - 100		Expectency LE x ARO = ALE)		Administrativ	ve l	Physical	Te	chnical	Annualized Cost		Avoid	Accept	Mitigate	Trans	CEO	Legal	Finance	Sales	Support	Eng	п Т	Date	e Decided	Last Reviewed	Review
s	4,	,000,000	0.33		57.6	\$	1,320,00	o	\$ 100,000	o s	-	s	650,000	\$ 750,000	1.76			x	,	SS	D	MM	cc	RR	NH	СВ	202	22-03-01	2021-09-01	2022-03-01
s	5,	,000,000	0.2		48	s	1,000,00	o	\$ 100,000	o \$	-	ş	500,000	\$ 600,000	1.67			x	,	SS	aı	мм	сс	RR	ΝΗ	СВ	202	22-03-01	2021-09-01	2022-03-01
\$	4,	,000,000	0.2		44.8	Ş	800,00	0	\$ 100,000	o \$	-	ş	1,000,000	\$ 1,100,000	0.73			x		SS	۵	мм	cc	RR	NH	CB	202	22-03-01	2021-09-01	2022-03-01
s	2,	,000,000	0.25		42	\$	500,00	o	\$ 100,000	0\$	-	ş	350,000	\$ 450,000	1.11			x	,	ss	aı	мм	сс	RR	NH	СВ	202	22-03-01	2021-09-01	2022-03-01
\$		500,000	1		40	\$	500,00	0	\$ 100,000	o \$	-	\$	1,000,000	\$ 1,100,000	0.45			x		ss	aı	мм	сс	RR	NH	СВ	202	22-03-01	2021-09-01	2022-03-01
s		200,000	0.2		30	s	40,00	0	\$ 10,000	o \$	-	Ş	50,000	\$ 60,000	0.67			x		SS	DI	ММ	cc	RR	NH	CB	202	22-03-01	2021-09-01	2022-03-01
ş		200,000	0.5		25.2	\$	100,00	0	\$ 100,000	o s	-	s	100,000	\$ 200,000	0.50		x			ss	ar	мм	сс	RR	NH	СВ	202	22-03-01	2021-09-01	2022-03-01
s		100,000	5		9.6	\$	500,00	o	\$ 10,000	o \$	-	Ş	50,000	\$ 60,000	8.33			x		SS	ar	мм	cc	RR	NH	СВ	202	22-03-01	2021-09-01	2022-03-01

www.risklevelagreements.com



6. Integrate Business Operations $\leftarrow \rightarrow$ Security Operations



(*?)

Monitoring and Detection

- Early Warning Systems (e.g., Canaries)
- Normal vs. Suspicious Activity, Behavior
- Indicators of Attack, Behaviors, Compromise

Correction and Recovery

- Network Failover, Recovery & Restoration
- System Failover, Recovery & Restoration
- Service Failover, Recovery & Restoration
- Information Failover, Recovery & Restoration
- User Failover, Recovery & Restoration
- Business Process Failover, Recovery & Restoration

Prevention

- Asset Classification & Labeling
- Disciplined Access Control
- "Need To Know"
- "Least Privilege"
- "Zero Trust" Architecture Patterns
- Data Loss Prevention (DLP)

Deception and Disruption

- Honeypots, Honeynets
- Counter-Intelligence, Investigation
- Disruptive Engagement
- Disinformation (Poison the Exfiltrated Data)

Integration Informs *Decisions*

7. Insist on Governance



Crisis Management

- Incident Response Plan (IRP)
- Disaster Recovery Plan (DRP)
- Business Continuity Plan (BCP)
- Crisis Communications Plan (CCP)
- Practice, Exercise, Test

Risk Management

(discussed earlier)

Threat Modeling

Risk Assessment

Available Mitigations

Risk Informed Decisions

Change Management

Political Threats

Business Impact Assessment

Privacy Impact Assessment

- Economic Threats
- Social Threats
- Technological Threats
- Legal Threats
- Environmental Threats

Vendor Management

- Initial Assessment
- Contractual Commitments
 - Service Level Agreement (SLA) Monitoring
- Regular Audits
- Planned Obsolescence

Governance Prepares for Resiliency

Summary



Survival Strategies

- 1. Develop
- 2. Cultivate
- 3. Promote
- 4. Invest in
- 5. Establish
- 6. Integrate
- 7. Insist on

"Meta" Systems **Domain Awareness Risk Awareness Contingencies & Controls Risk Level Agreements™** Business Operations $\leftarrow \rightarrow$ Security Operations Governance

Bring Order to Entropy

Acknowledge Conflict

Embrace Risk

Plan for Resilience



