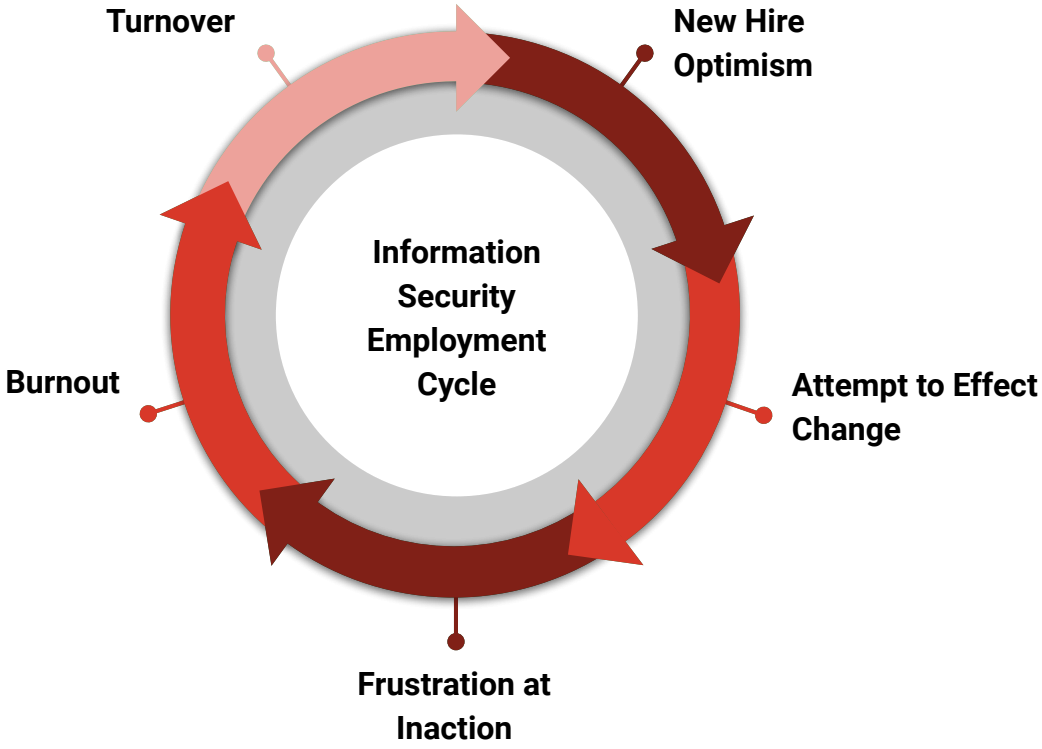
indeed

Learning the Power of the "Not My Responsibility" Mindset

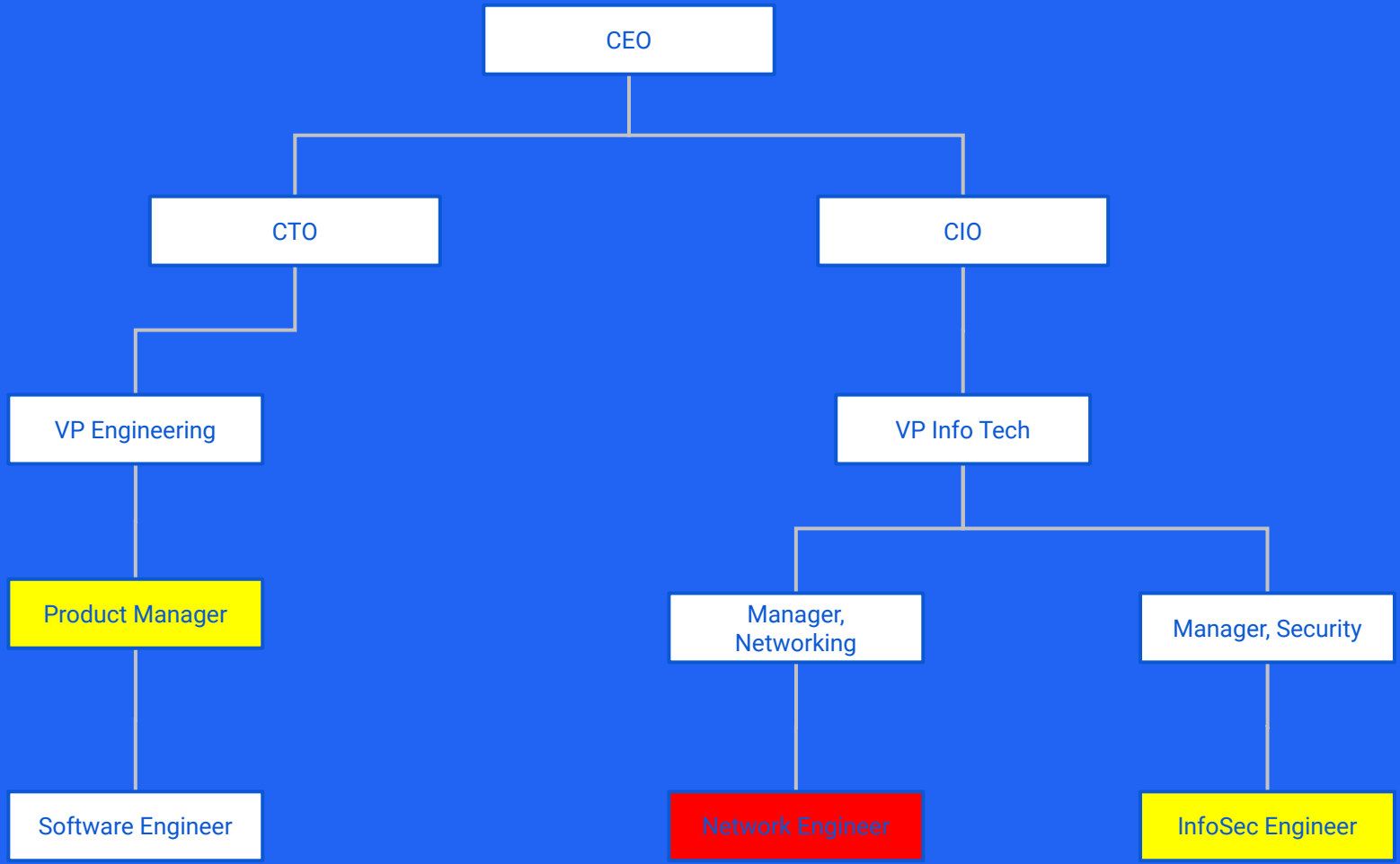
Nick Leghorn

Manager of Information Security Risk Management, Indeed


What
Where
indeed
InfoSec Risk Management
Austin, TX
Find Jobs


Turnover
New Hire Optimism
Information Security Employment Cycle
Burnout
Attempt to Effect Change
Frustration at Inaction

Scenario:
Engineering Manager Wants to Access Production DC From The Road Without a VPN


CEO
CTO
CIO
VP Engineering
VP Info Tech
Product Manager
Manager, Networking
Manager, Security
Software Engineer
Network Engineer
InfoSec Engineer

Understanding Risk

We help people get jobs.

We help the business take healthy risks.


Speed
Security

Why Manage Risk?

- Help the business understand current risk levels
- Allow the business to define their “risk tolerance”
- Assist the business in maturing towards a risk based approach even if they aren’t there quite yet

Operational Versus Strategic Risk

Operational Risk Analysis

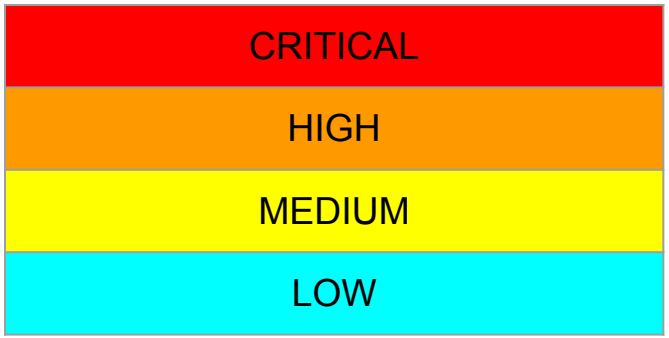
- “Do we care?”
- Transactional, focused on evaluating specific requests as they come.
- Used to define the level of scrutiny required for requests. Goal is to spend the most time on the highest risk issues, let low risk issues self-regulate.
- Requires an understanding of “risk appetite” or “risk tolerance”

Strategic Risk Analysis

- “Should we care?”
- Broader scope, encompases dozens to hundreds of transactions.
- Designed to inform strategy of the company at a high level.
- Informs the level of “risk tolerance”.

How Do We Define Risk?

Describing Risk: Categories



Useful Situations:

- Useful for quick analysis and operational risk management decision making
- Requires less effort to calculate

Potential Issues:

- Imprecise, unhelpful for detailed task prioritization
- Requires management to trust the methodology
- Easy to misinterpret, usually requires a “notional value” associated to make sense

Describing Risk: Annualized Loss Expectancy

Annualized Loss Expectancy	$1 million per year

Useful Situations:

- Excellent for detailed prioritization of tasks
- Easy to understand “return on investment” for mitigations
- Methodology can be supported with documentation

Potential Issues:

- Legal liability in discovery
  - Calculation of potential damages could be used by court to define actual damages
  - Performing the “cold calculation” as in the Ford Pinto case
- Time consuming analysis for every scenario

Describing Risk: Likelihood and Calculated Impact

Likelihood	100 per year
Expected Impact	$1,000 per instance

Useful Situations:

- Good for making the potential damages “personal” for management
- Legal usually more comfortable with this format, statement of supported fact instead of calculation

Potential Issues:

- Legal liability in discovery (minor)
- Requires management to do calculations in their head
- Not useful for granular cost / benefit analysis

Describing Risk: Likelihood and Generic Impact

Likelihood	1:10
Other Companies In This Situation	$10 million

Useful Situations:

- Good for making the potential damages “real” for management
- Legal usually more comfortable with this format, statement of supported fact instead of calculation

Potential Issues:

- Requires management to do calculations in their head
- Damages listed may be significantly different from the expected impact

Describing Risk: Which Is Right?

Style	Operational / Strategic	Stakeholder
Risk Categories	Operational	Operational Risk Management
Annualized Loss Expectancy	Operational	Project Management
Likelihood and Calculated Impact	Strategic	Management / SLT
Likelihood and Generic Impact	Strategic	Management / SLT

Step 1: Analyze The Risk And Determine The Severity

Initial Operational Risk Assessment

	High	Medium	Low
Data Classification (Confidentiality)	Read/Write T1/T0 data	Read/write T2 data + below	Read/write confidential data + below
Perimeter Control (Integrity)	Access to Prod/QA from anywhere	Access up to Dev from below	Access to same sec level EXCEPT Prod/QA
Criticality (Availability)	Required for business critical real-time operation	Required for business critical non real-time operation	Assists business, non-critical

Initial Operational Risk Assessment (Scenario)

	High	Medium	Low
Data Classification (Confidentiality)	Read/Write T1/T0 data	Read/write T2 data + below	Read/write confidential data + below
Perimeter Control (Integrity)	Access to Prod/QA from anywhere	Access up to Dev from below	Access to same sec level EXCEPT Prod/QA
Criticality (Availability)	Required for business critical real-time operation	Required for business critical non real-time operation	Assists business, non-critical

Step 2: Define Priority and Ownership

Risk as Task Prioritization

Risk Level	Level of Scrutiny	Prioritization
HIGH	Manual and individual review with stakeholders and subject matter experts.	Top Priority / Immediate
MEDIUM	Grouped together with similar requests and reviewed with subject matter experts. Generic mitigations suggested.	Placed In Queue
LOW		Logging Only

Risk as Task Prioritization

Risk Level	Level of Scrutiny	Prioritization
HIGH	Manual and individual review with stakeholders and subject matter experts.	Top Priority / Immediate
MEDIUM	Grouped together with similar requests and reviewed with subject matter experts. Generic mitigations suggested.	Placed In Queue
LOW		Logging Only

Risk Ownership Levels

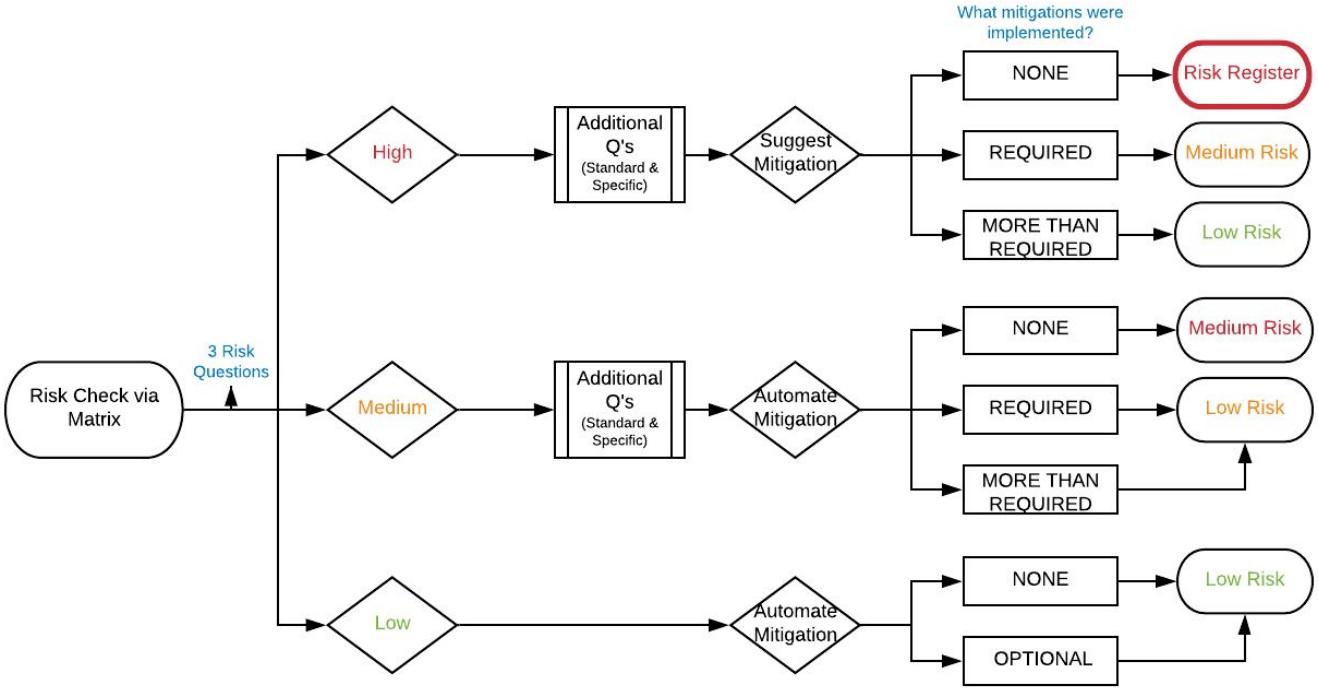
Risk Level	Appropriate Decision Maker
HIGH	Vice President / C-Level (+2 minimum)
MEDIUM	Senior Manager / Director (+1 minimum)
LOW	Manager

Risk Ownership Levels

Risk Level	Appropriate Decision Maker
HIGH	Vice President / C-Level (+2 minimum)
MEDIUM	Senior Manager / Director (+1 minimum)
LOW	Manager

Step 3: Describe Risk to Management and Suggest Mitigations

Operational Risk Management Framework



Operational Risk Assessment (Scenario)

Hello,

The Information Security Team does not provide approval for requests. Instead we present a risk assessment of the requested change, suggest mitigations which would reduce the risk of that request, and identify who within the business can ultimately provide the requested approval.

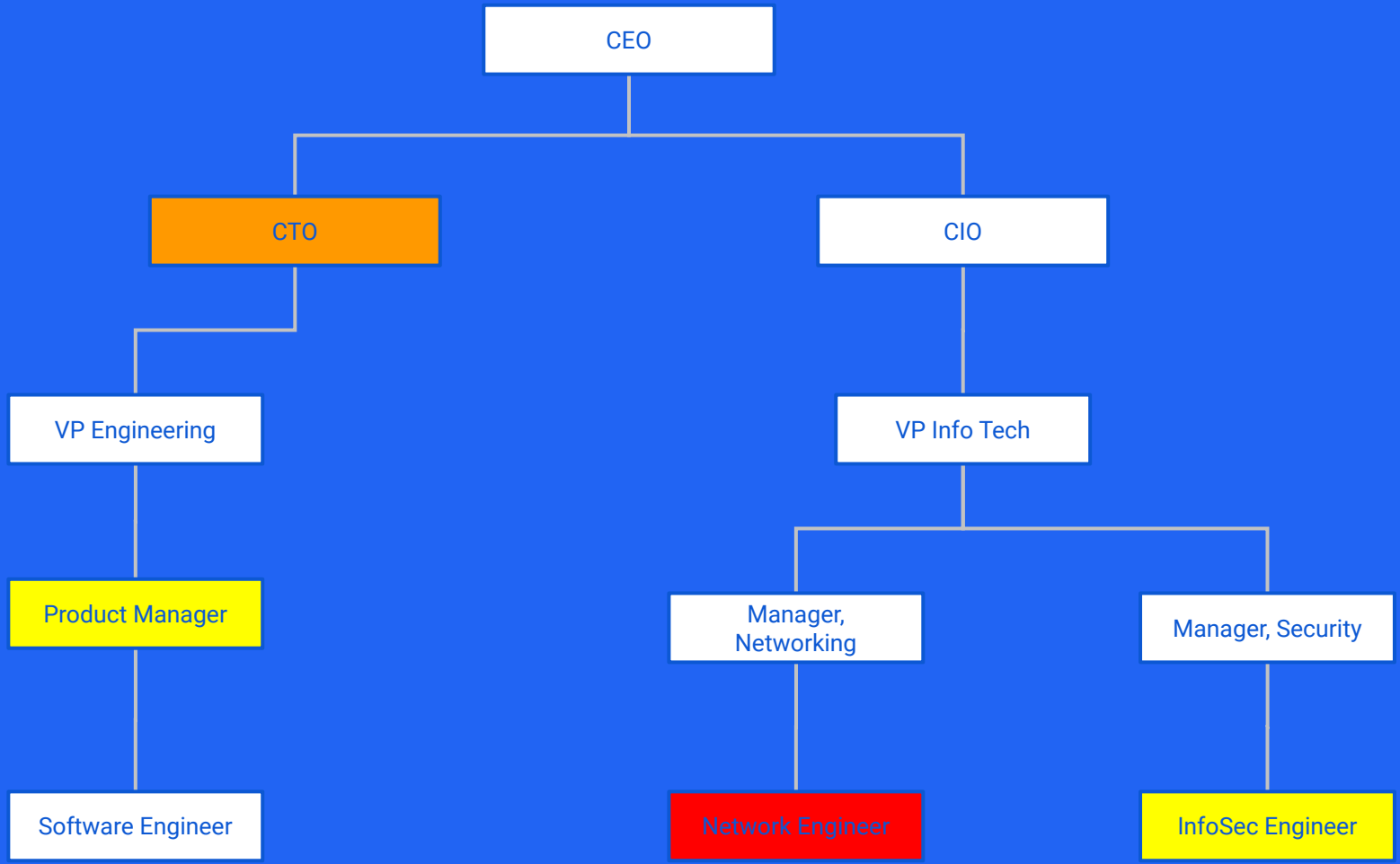
Based on the details of your request, this change has been identified as a **HIGH RISK** to the company.

To reduce the risk of this requested change we recommend that you enact the following mitigations:

- Implement an IPSEC VPN to establish this connection which conforms to the IAM guidelines and uses 2 factor authentication.
- Ensure all systems connecting over this VPN conform to the system hardening, patch management, and vulnerability management guidelines published by InfoSec.
- Ensure that sensitive data is not transferred over this medium other than for momentary troubleshooting.

If you decide to move forward without all of these mitigations you will need to obtain approval **from the CTO**.

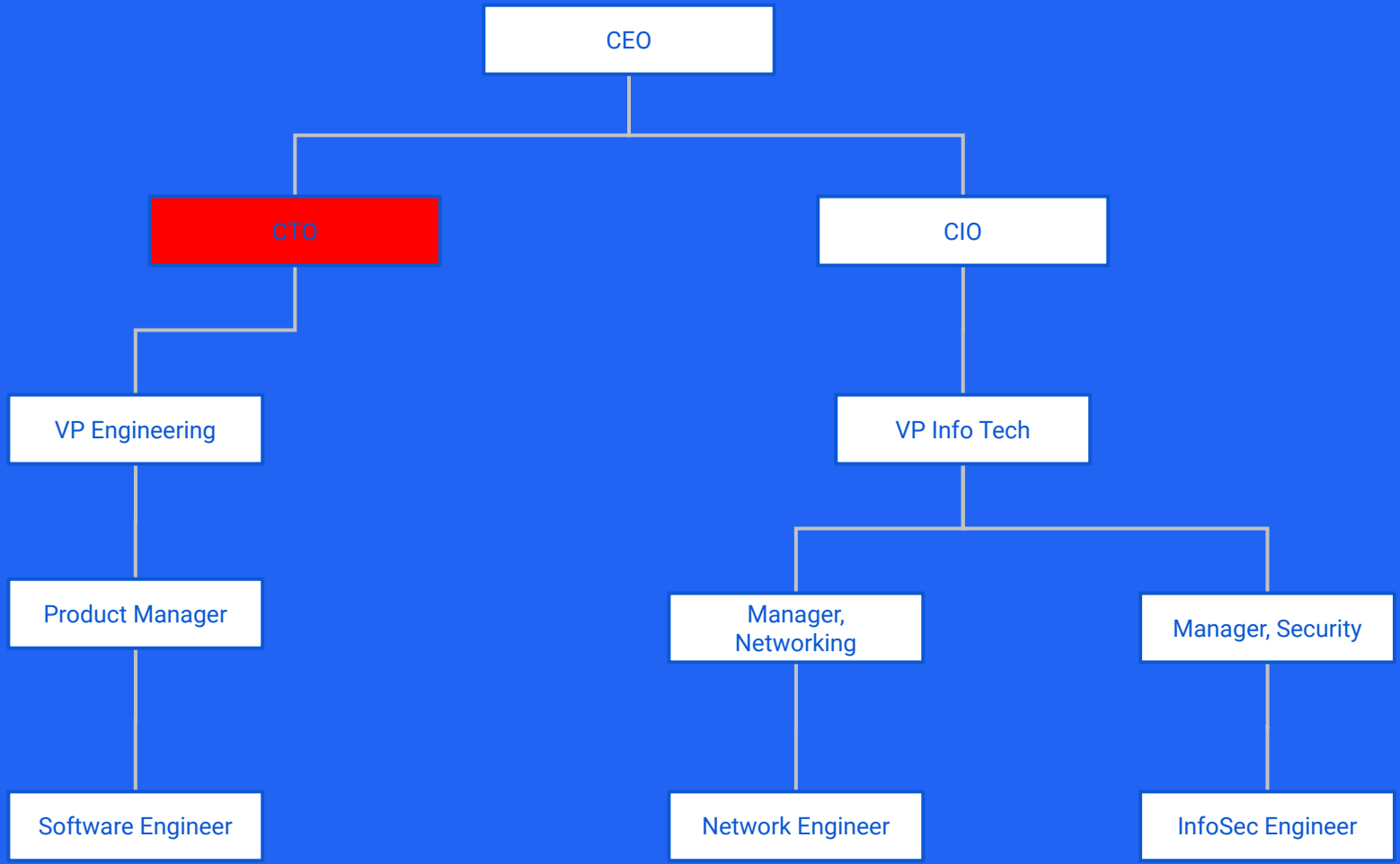
Thank you,
InfoSec Risk Assessment Team


CEO
CTO
CIO
VP Engineering
VP Info Tech
Product Manager
Manager, Networking
Manager, Security
Software Engineer
Network Engineer
InfoSec Engineer

Tailor Discussion of Risk to the Decision Maker

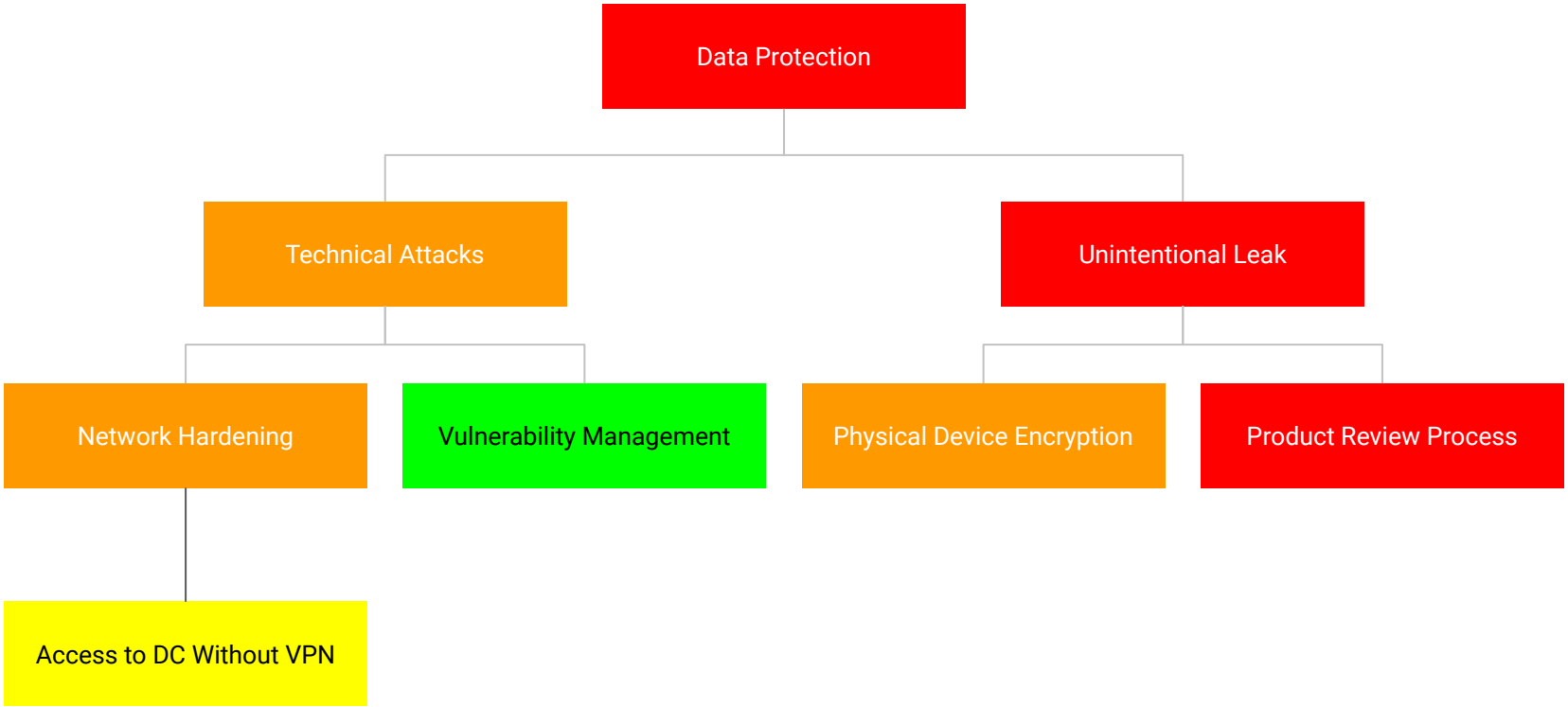
- Decision makers who trust the process and understand InfoSec risk may only need the category of risk.
- Management intuitively understands likelihood and impact, but may prefer either calculated or generic impact.

Step 4: Record Results and Report to Management Chain


CEO
CTO
CIO
VP Engineering
VP Info Tech
Product Manager
Manager, Networking
Manager, Security
Software Engineer
Network Engineer
InfoSec Engineer

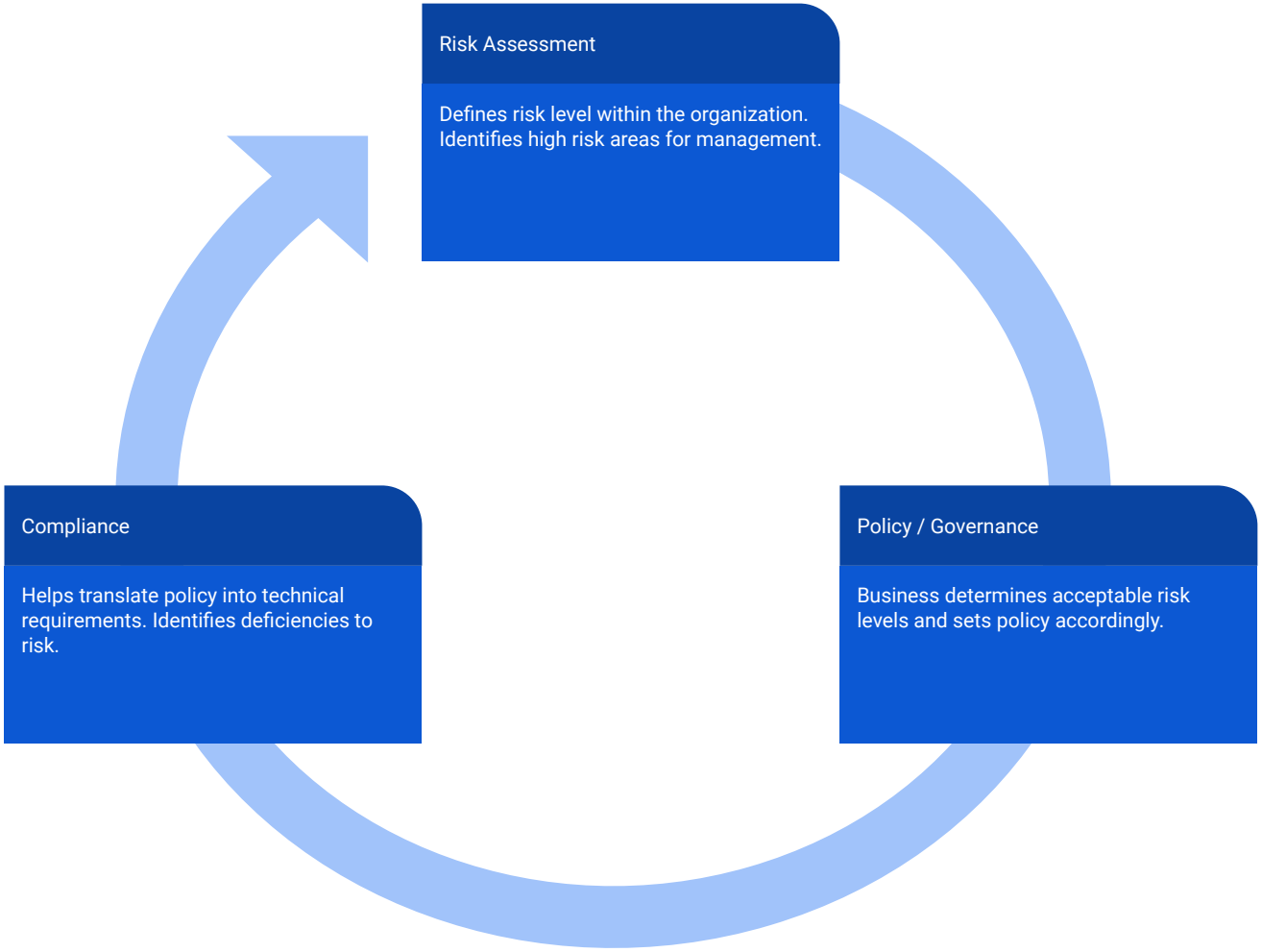
Step 5: Regularly Review Risks and Set Risk Tolerance

Analyze Individual Recorded Risks for Groupings



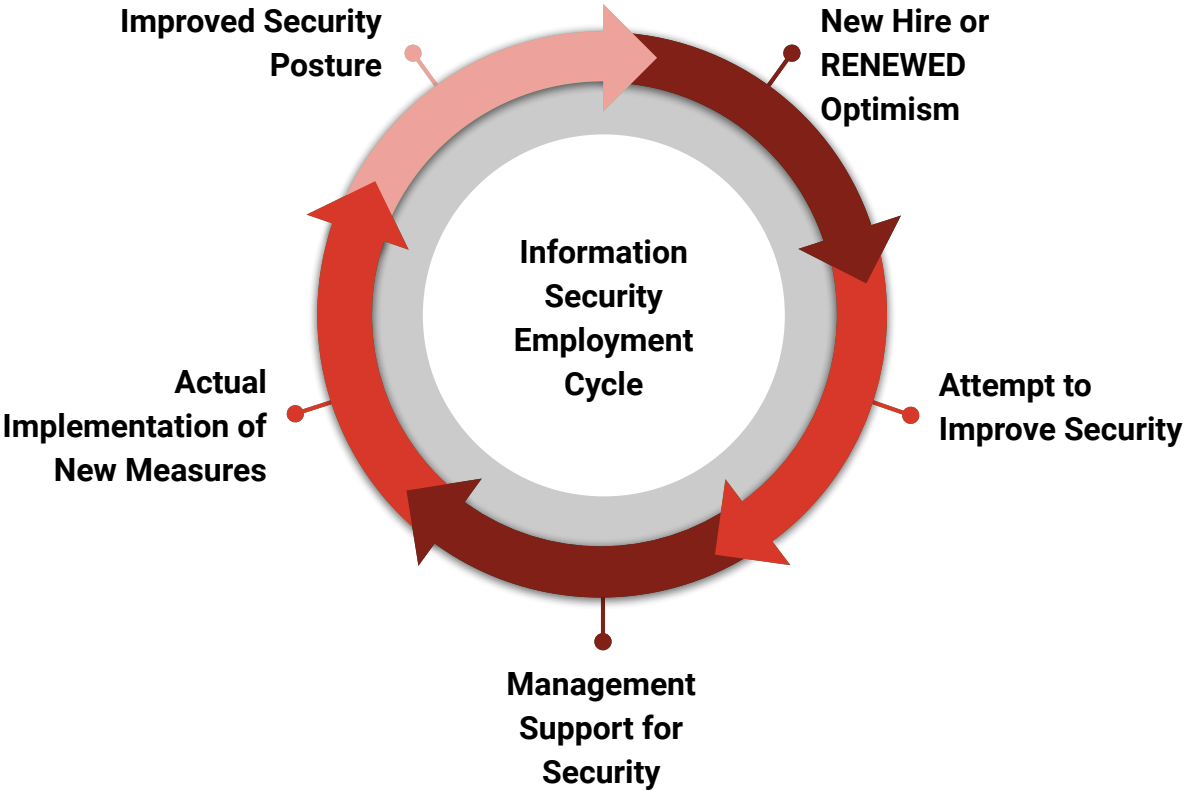
Present Risks to SLT and Define Controls

Risk	Likelihood	Impact
Leak of Sensitive Data	Highly Probable	Company Ending
Regulatory Fines	Improbable	Company Ending
Loss of Reputation	Likely	Severe


Risk Assessment
Defines risk level within the organization. Identifies high risk areas for management.
Policy / Governance
Business determines acceptable risk levels and sets policy accordingly.
Compliance
Helps translate policy into technical requirements. Identifies deficiencies to risk.

Effects of Implementing a Risk Based Security Program

- Improved relationship between security and the business
  - Cooperative instead of adversarial
  - Providing actionable intelligence
- Improved visibility
- Faster response time
  - Pre-defined process for analyzing issues
  - Management sets thresholds


Improved Security Posture
New Hire or RENEWED Optimism
Information Security Employment Cycle
Attempt to Improve Security
Management Support for Security
Actual Implementation of New Measures

Instagram / Twitter

foghorn@NickLeghorn.com

GitHub

Website

Email

We help people get jobs.